EURÓPAI UNIÓ

AZ EURÓPAI PARLAMENT **A TANÁCS**

Brüsszel, 2019. március 27.
(OR. en)

2017/0225 (COD) **PE-CONS 86/18**

CYBER 330
TELECOM 491
COPEN 454
COPS 488
COSI 326
CSC 387
CSCI 179
IND 417
JAI 1315
JAIEX 174
POLMIL 231
RELEX 1115
CODEC 2380

JOGALKOTÁSI AKTUSOK ÉS EGYÉB ESZKÖZÖK

Tárgy:	AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS

(EU) 2019/… RENDELETE

(...)

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

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

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

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[1],

tekintettel a Régiók Bizottságának véleményére[2],

rendes jogalkotási eljárás keretében[3],

---

1 HL C 227., 2018.6.28., 86. o.

2 HL C 176., 2018.5.23., 29. o.

3 Az Európai Parlament 2019. március 12-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács ...-i határozata.

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 továbbiakban: az IKT) a mindennapi 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 Unió-szerte elterjedt, mind a polgárok, mind a szervezetek, mind pedig a vállalkozások 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 rendkívül magas számú összekapcsolt digitális eszközt fognak az Unióban használatba venni. Míg egyre növekvő számú berendezés kapcsolódik az internethez, ezen eszközök esetében nincs kellőképpen beépítve a biztonság- és ellenállóképesség, mely elégtelen kiberbiztonsághoz vezet. A tanúsítás korlátozott alkalmazása következtében így sem a magán, sem az intézményi, sem az üzleti felhasználók nem rendelkeznek elegendő információval az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kiberbiztonsági jellemzőiről, ami aláássa a digitális megoldásokba vetett bizalmat. A hálózati és információs rendszerek képesek életünk minden területét segíteni, az Unió gazdasági növekedését pedig ösztönözni. E rendszerek a digitális egységes piac megvalósításának sarokkövét jelentik.

(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 sérülékeny felhasználókat, például a gyerekeket is. Az említett 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 polgárok, a szervezetek és a vállalkozások – a 2003/361/EK bizottsági ajánlásban[1] meghatározott kis- és középvállalkozásoktól (kkv) a kritikus infrastruktúrák üzemeltetőiig terjedően – jobban védve legyenek a kiberfenyegetésekkel szemben.

(4) Azáltal, hogy a releváns információkat elérhetővé teszi a nyilvánosság számára, az 526/2013/EU európai parlamenti és tanácsi rendelettel[2] létrehozott Európai Uniós Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: az ENISA) hozzájárul az uniós kiberbiztonsági ágazat, és elsősorban a kkv-k és az induló innovatív vállalkozások fejlődéséhez. Célszerű, hogy az ENISA szorosabb együttműködésre törekedjen az egyetemekkel és a kutatóintézetekkel annak érdekében, hogy hozzájáruljon az Unión kívülről származó kiberbiztonsági termékektől és szolgáltatásoktól való függőség csökkentéséhez, valamint az Unión belüli ellátási láncok megerősítéséhez.

---

1 A Bizottság ajánlása (2003. május 6.) mikro-, kis- és középvállalkozások fogalmának meghatározására vonatkozóan (HL L 124., 2003.5.20., 36. o.).

2 Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről (HL L 165., 2016.6.18., 41. o.).

(5) 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 és bűnüldöző hatóságok hatásköre és szakpolitikai válaszintézkedései túlnyomórészt nemzeti szintűek. A nagyszabású biztonsági események az egész Unióban megzavarhatják az alapvető szolgáltatások nyújtását. Ezért hatékony és összehangolt uniós szintű reagálásra és válságkezelésre van szükség, melynek alapját célirányos szakpolitikai intézkedéseknek és az európai szolidaritást és kölcsönös segítségnyújtást szolgáló gazdagabb eszköztárnak kell képeznie. Emellett 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 kiberellenálló képességének mindenkori helyzetéről, továbbá szisztematikus legyen a jövőben várható fejlemények, kihívások és fenyegetések előrejelzése uniós és globális szinten egyaránt.

(6) 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. Ezen célkitűzések közéé tartozik, hogy fokozni kell a tagállamok és a vállalkozások képességeit és felkészültségét, valamint javítani kell az együttműködést, az információmegosztást és a koordinációt a tagállamok, valamint az uniós intézmények, szervek és hivatalok között. Továbbá, tekintettel a kiberfenyegetések határok nélküli természetére, szükség van az uniós szintű képességek növelésére, melyek kiegészíthetik a tagállami fellépéseket, különösen a határokon átnyúló, nagyszabású biztonsági események és válságok esetén, figyelembe véve ugyanakkor a nemzeti képességek fenntartásának és továbbfejlesztésének fontosságát, hogy minden szintű kiberfenyegetésre reagálni lehessen.

(7) További erőfeszítésekre van szükség annak érdekében is, hogy növeljük a polgárok, a szervezetek és a vállalkozások a kiberbiztonsági kérdésekre vonatkozó tudatosságát. Emellett, mivel a biztonsági események – különösen a fogyasztók körében – aláássák a digitális szolgáltatókba és magába a digitális egységes piacba vetett bizalmat, a bizalmat tovább kell növelni azáltal, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok biztonsági szintjéről átlátható módon bocsátanak információkat rendelkezésre, kiemelve, hogy még a magas szintű kiberbiztonsági tanúsítás sem garantálhatja, hogy az adott IKT-termék, IKT-szolgáltatás és IKT-folyamat teljesen biztonságos. A bizalom növelését könnyebben el lehet érni az egész Unióra kiterjedő tanúsítással, amely valamennyi nemzeti piacon és minden ágazatban közös kiberbiztonsági követelményeket és értékelési kritériumokat biztosít.

(8) A kiberbiztonság nemcsak technológia függvénye, hanem az emberi magatartás legalább olyan fontos. Éppen ezért határozottan ösztönözni kell a „kiberhigiéniát”, azaz olyan egyszerű rutinintézkedéseket, amelyek rendszeres végrehajtásával és elvégzésével a polgárok, a szervezetek és a vállalkozások minimálisra csökkenthetik a kiberfenyegetések kockázatainak való kitettségüket.

(9) Az uniós kiberbiztonsági struktúrák megerősítése érdekében fontos fenntartani és fejleszteni a tagállamok arra irányuló képességeit, hogy átfogóan tudjanak reagálni a kiberfenyegetésekre, a határokon átnyúló biztonsági eseményeket is beleértve.

(10) Fontos, hogy a vállalkozások és az egyéni fogyasztók pontos információkkal rendelkezzenek arról, hogy az általuk igénybe vett IKT-termékek, IKT-szolgáltatások és IKT-folyamatok biztonságát milyen megbízhatósági szinttel tanúsították. kiberbiztonsági szempontból egyetlen IKT-termék vagy IKT-szolgáltatás sem teljesen biztonságos, ezért az alapvető kiberhigiéniai szabályokat elő kell mozdítani és kiemelten kell kezelni. Tekintettel a dolgok internetével kapcsolatos eszközök növekvő elérhetőségére, számos olyan önkéntes intézkedés létezik, amelyeket a magánszektor tehet az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok biztonságába vetett bizalom erősítése érdekében.

(11) A korszerű IKT-termékek és -rendszerek gyakran foglalnak magukban és alkalmaznak egy vagy több olyan technológiát és alkotóelemet, amelyek harmadik felektől származnak, így például szoftvermodulokat, könyvtárakat vagy felhasználói program interfészeket Ez a harmadik felekre hagyatkozás, amelyre „függőségként” is hivatkoznak, további kiberbiztonsági kockázatokat jelenthet, mivel a harmadik felektől származó alkotóelemekben fellelhető sérülékenységek is befolyásolhatják az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok biztonságosságát. Sok esetben hasznos lehet az ilyen függőségek azonosítása és dokumentálása, mivel az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok végfelhasználói javíthatják kiberbiztonsági kockázatkezelési tevékenységeiket, például azáltal, hogy javítják a felhasználók által alkalmazott, a sérülékenységek kezelésére és orvoslására irányuló eljárásokat.

(12) Az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok tervezésébe és kifejlesztésébe bevont szervezeteket, gyártókat és szolgáltatókat már a tervezés és a kifejlesztés legkorábbi szakaszában ösztönözni kell az említett termékek, folyamatok és szolgáltatások biztonságának védelmére szolgáló intézkedések végrehajtására olyan módon, hogy számoljanak a támadások előfordulásának lehetőségével, azok előre látható hatását pedig a minimálisra csökkentsék (a továbbiakban: a beépített biztonság). A biztonsággal az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes élettartama alatt biztosítani kell, a rosszindulatú felhasználásból eredő károk kockázatának csökkentése érdekében folyamatosan alakítva a tervezési és a fejlesztési eljárásokat.

(13) Célszerű, hogy a vállalkozások, a szervezetek és a magánszektor magasabb fokú biztonságot biztosító módon konfigurálják az általuk tervezett IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat, hogy az első felhasználó a lehető legbiztonságosabb beállításokkal (a továbbiakban: az alapértelmezett biztonság) kaphassa meg az alapértelmezett konfigurációt, ezáltal csökkentve a felhasználókra nehezedő terhet, hogy maguknak kell gondoskodniuk az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelő konfigurálásáról. Fontos, hogy az alapértelmezett biztonság működéséhez ne legyen szükség jelentős mértékű konfigurálásra, vagy speciális műszaki ismeretekre, illetve a felhasználó nem nyilvánvaló magatartására, alkalmazáskor pedig egyszerűen és megbízhatóan kell működnie. Amennyiben – eseti alapon – a kockázat és a felhasználhatóság elemzésének eredményeként azt állapítják meg, hogy az ilyen alapértelmezett beállítás nem valósítható meg, a felhasználókat a legbiztonságosabb beállítás kiválasztására kell ösztönözni.

(14) A 460/2004/EK európai parlamenti és tanácsi rendelet[1] azzal a céllal hozta létre az ENISA-t, hogy hozzájáruljon az Unión belüli magas és hatékony szintű hálózat- és információbiztonság biztosításához, valamint – a polgárok, a fogyasztók, a vállalkozások és a közigazgatási szervek érdekeit szem előtt tartva – a hálózat- és információbiztonsági kultúra kialakításához. Az 1007/2008/EK európai parlamenti és tanácsi rendelet[2] 2012 márciusáig meghosszabbította az ENISA megbízatását. Az 580/2011/EK európai parlamenti és tanácsi rendelet[3] 2013. szeptember 13-ig újfent meghosszabbította az ENISA megbízatását. Az 526/2013/EU európai parlamenti és tanácsi rendeletaz ENISA megbízatását 2020. június 19-ig hosszabbította meg.

---

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

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

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

(15) Az Európai Unió már eddig is fontos lépéseket tett a kiberbiztonság és a digitális technológiákba vetett bizalom növelése érdekében. 2013-ban elfogadásra került az Európai Unió kiberbiztonsági stratégiája, amely irányt szabott az Unió kiberbiztonsági fenyegetésekre és kockázatokra adott politikai válaszlépései kidolgozásának. A polgárok online védelmének javítása érdekében tett erőfeszítései keretében a kiberbiztonság területén az Unió 2016-ban fogadta el az első jogi aktust, az (EU) 2016/1148 európai parlamenti és tanácsi irányelv[1] formájában. Az (EU) 2016/1148 irányelv a 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 ágazatokban, mint például az energetika, a közlekedés, az ivóvízellátás és -elosztás, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, a digitális infrastruktúra, valamint a kulcsfontosságú digitális szolgáltatók (keresőprogramok, felhőalapú számítástechnikai szolgáltatások, online piacterek).

[1] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

Az ENISA kulcsfontosságú szerepet kapott az említett 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. A digitális egységes piacon egyéb jogi eszközök – például az (EU) 2016/679 európai parlamenti és tanácsi rendelet[1], a 2002/58/EK[2] és az (EU) 2018/1972 európai parlamenti és tanácsi irányelv[3] – is hozzájárulnak a kiberbiztonság magas szintjéhez.

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

[2] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31.).

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

(16) Az Európai Unió kiberbiztonsági stratégiájának 2013-as elfogadása és az ENISA megbízatásának legutóbbi felülvizsgálata óta az általános politikai kontextus jelentősen megváltozott, a bizonytalanabbá és kevésbé biztonságossá vált globális környezet következtében is. Ennek fényében, illetve azzal összefüggésben, hogy az ENISA-nak a tanácsadás és a szakértelem terén hivatkozási alapként, illetve az együttműködés és a kapacitásépítés terén közvetítőként, továbbá az új uniós kiberbiztonsági politika keretében betöltött szerepe pozitívan alakult, felül kell vizsgálni az ENISA megbízatását a megváltozott kiberbiztonsági ökoszisztémában betöltött szerepének meghatározása és annak biztosítása érdekében, hogy hatékonyan hozzájáruljon a radikálisan átalakult kiberfenyegetettségi helyzetből fakadó kiberbiztonsági kihívásokra adott uniós reagáláshoz, hiszen ehhez, amint az az ENISA értékeléséből is kiderült, jelenlegi megbízatása nem elegendő.

(17) Az e rendelet által létrehozott ENISA az 526/2013/EU rendelettel korábban létrehozott ENISA jogutódja. Az ENISA-nak az e rendelettel és az egyéb kiberbiztonsági uniós jogi aktusokkal ráruházott feladatokat kell ellátnia, többek között szakértelem rendelkezésre bocsátása és tanácsadás révén, valamint uniós információs és tudásközpontként működve. Elő kell mozdítania a bevált gyakorlatok cseréjét a tagállamok és a magánszektor érdekelt felei között, szakpolitikai javaslatokat kell tennie az Európai Bizottságnak és a tagállamoknak, hivatkozási alapként működve az uniós ágazati szakpolitikai kezdeményezések számára a kiberbiztonsági kérdésekben, és elő kell segítenie egyfelől a tagállamok közötti, másfelől a tagállamok, valamint az uniós intézmények, szervek és hivatalok közötti operatív együttműködést.

(18) A tagállamok állam-, illetve kormányfői szinten ülésező képviselőinek közös megállapodásával hozott 2004/97/EK, Euratom határozat[1] keretében a tagállamok képviselői úgy határoztak, hogy az ENISA székhelye Görögországban lesz, egy, a görög kormány által meghatározandó városban. Az ENISA-t fogadó tagállamnak a lehető legkedvezőbb feltételeket kell biztosítania az ENISA zavartalan és hatékony működéséhez. Az ENISA feladatainak megfelelő és hatékony ellátása, a személyzet felvétele és megtartása, továbbá a hálózatépítési tevékenységek hatékonyságának fokozása érdekében elengedhetetlen, hogy az ENISA székhelye megfelelő helyen legyen, ahol többek között megfelelő közlekedési csatlakozások, valamint az ENISA személyzetének tagjait kísérő házastársaknak és gyermekeknek szükséges létesítmények állnak rendelkezésre. A szükséges szabályokat az ENISA igazgatótanácsának jóváhagyását követően az ENISA és az azt fogadó tagállam közötti megállapodásban kell rögzíteni.

(19) Tekintettel az Unió előtt álló, egyre fokozódó kiberbiztonsági kockázatokra és kihívásokra, növelni kell az ENISA számára elkülönített pénzügyi és emberi erőforrásokat annak érdekében, hogy tükrözze az ENISA megerősített szerepét, feladatait és az uniós digitális ökoszisztémát védő szervezetek ökoszisztémájában betöltött kulcsfontosságú szerepét, lehetővé téve az ENISA számára az e rendelettel ráruházott feladatok hatékony elvégzését.

[1] A tagállamok állam- vagy kormányfői szinten ülésező képviselőinek közös megállapodással hozott 2004/79/EK, Euratom határozata (2003. december 13.) az Európai Unió egyes hivatalai és ügynökségei székhelyéről (HL L 29., 2004.2.3., 15. o.).

(20) Az ENISA-nak 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 ENISA-nak aktívan támogatnia kell a nemzeti erőfeszítéseket és proaktívan hozzá kell járulnia az uniós erőfeszítésekhez, miközben feladatait az uniós intézményekkel, szervekkel és hivatalokkal, valamint a tagállamokkal teljeskörűen együttműködve kell végeznie, elkerülve a párhuzamos munkavégzést és előmozdítva a szinergiát. Ezenkívül a magánszektorral, valamint a többi releváns érdekelt féllel is együtt kell működnie, és a tőlük kapott észrevételeket is figyelembe kell vennie. Feladatainak megállapításával meg kell határozni, hogy az ENISA-nak hogyan kell elérnie célkitűzéseit, de egyben rugalmasságot is biztosítani kell a működéséhez.

(21) Annak érdekében, hogy megfelelő támogatást lehessen nyújtani a tagállamok operatív együttműködéséhez, az ENISA-nak tovább kell erősítenie műszaki és humán képességeit és készségeit. Az ENISA-nak növelnie kell a know-how-ját és kapacitásait. Az ENISA és a tagállamok a nemzeti szakértők ENISA-hoz történő kirendelése, szakértői csoportok létrehozása és személyzeti csere céljából önkéntes alapon programokat alakíthatnának ki.

(22) Az ENISA-nak – a kiberbiztonsági vonatkozású uniós politikák és uniós jog relevanciájának növelése és ezek nemzeti szintű végrehajtása 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 jog kidolgozásához, illetve azok aktualizálásához és felülvizsgálatához kapcsolódik. Az ENISA-nak hivatkozási alapként kell szolgálnia az olyan uniós ágazatspecifikus szakpolitikai és jogalkotási kezdeményezésekkel kapcsolatos tanácsadás és szakértelem terén, amelyek kiberbiztonsági kérdéseket is magukban foglalnak. Az ENISA-nak a tevékenységeiről rendszeresen tájékoztatnia kell az Európai Parlamentet.

(23) A nyílt internet nyilvános alkotóelemei – nevezetesen a főbb protokolljai és infrastruktúrája, amelyek globális közjavak – biztosítják az internet egészének alapvető funkcióit és támogatják annak normál működését. Az ENISA-nak támogatnia kell az internet nyilvános alapelemei, többek között, de nem kizárólag a kulcsfontosságú protokollok (különösen a DNS, a BGP és az IPv6) biztonságos és stabil működését, a domain-név rendszer működését (például az összes legfelső szintű domain működését), valamint a gyökérzóna működését.

(24) Az ENISA alapvető feladata, hogy elősegítse a releváns jogi keretrendszer következetes végrehajtását, különösen az (EU) 2016/1148 irányelv és a kiberbiztonsági vonatkozásokat tartalmazó egyéb releváns jogi eszközök eredményes végrehajtását, ami alapvető fontosságú a kiberellenálló képesség javításához. Tekintettel a kiberbiztonsági fenyegetettségi helyzet gyorsan változó jellegére, egyértelmű, hogy a tagállamokat több szakpolitikai területet is felölelő, átfogóbb megközelítéssel kell támogatni a kiberellenálló képesség kialakítása érdekében.

(25) Az ENISA-nak segítenie kell a tagállamok és az uniós intézmények, szervek és hivatalok arra irányuló erőfeszítéseit, hogy kiépítsék és fokozzák a kiberfenyegetések 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. Az ENISA-nak különösen a nemzeti és uniós számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: a 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 kapacitásaival kapcsolatban végzett tevékenységnek aktívan támogatnia kell a tagállamok a célból hozott intézkedéseit, hogy megfeleljenek az (EU) 2016/1148 irányelvből eredő kötelezettségeiknek, és nem élvezhet elsőbbséget azokkal szemben.

(26) Az ENISA-nak a hálózati és információs rendszerek biztonságára, kiváltképpen a kiberbiztonságra vonatkozó uniós és – kérésre – tagállami szintű stratégiák kidolgozásához és aktualizálásához is támogatást kell nyújtania, valamint elő kell segítenie ezen stratégiák terjesztését, és nyomon kell követnie végrehajtásuk előrehaladását. Az ENISA-nak hozzá kell járulnia a képzésekkel és képzési anyagokkal kapcsolatos igények – többek között a közjogi szervek igényeinek – kielégítéséhez, és a Lakossági Digitális Kompetenciakeretre építve adott esetben kiemelt mértékben gondoskodnia kell az oktatók képzéséről is annak érdekében, hogy segítse a tagállamokat, illetve az uniós intézményeket, szerveket és hivatalokat saját szakképzési kapacitásuk kifejlesztésében.

(27) Az ENISA-nak a kiberbiztonsággal kapcsolatos tudatosságnövelés és oktatás terén támogatnia kell a tagállamokat azáltal, hogy elősegíti a tagállamok közötti szorosabb koordinációt és a bevált gyakorlatok cseréjét. Ez a támogatás többek között magában foglalhatná egy nemzeti oktatási kapcsolattartó pontokból álló hálózat és egy kiberbiztonsági képzési platform kialakítását. A nemzeti oktatási kapcsolattartó pontok hálózata működhetne a nemzeti kapcsolattartó tisztviselők hálózata keretében és kiindulópontot jelenthetne a tagállamokon belüli majdani koordinációhoz.

(28) Az ENISA-nak segítenie kell az (EU) 2016/1148 irányelvvel létrehozott együttműködési csoportot feladatai végrehajtásában, különösen szakértelmével, tanácsadással és a bevált gyakorlatok cseréjének megkönnyítésével, többek között ami az alapvető szolgáltatásokat nyújtó szereplők tagállamok általi azonosítását illeti, valamint a biztonsági kockázatok és biztonsági események terén fennálló, határokon átnyúló függőségek tekintetében.

(29) A köz- és a magánszektor közötti, valamint a magánszektoron belüli együttműködés ösztönzése céljából, különösen a kritikus infrastruktúrák védelmének támogatása érdekében az ENISA-nak 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 nyújt a rendelkezésre álló eszközökkel és eljárásokkal kapcsolatban, továbbá iránymutatást nyújt az információk megosztásával kapcsolatos szabályozási kérdésekben, például előmozdítva az ágazati információmegosztó és -elemző központok létrehozását.

(30) Mivel az IKT-termékekben, az IKT-szolgáltatásokban és az IKT-folyamatokban rejlő sebezhetőségek potenciális negatív hatása egyre nagyobb, a sebezhetőségek észlelésének és orvoslásának fontos szerepe van az átfogó kiberbiztonsági kockázat csökkentésében. Bebizonyosodott, hogy a szervezetek, a sebezhető IKT-termékek gyártói és a sebezhető IKT-szolgáltatások nyújtói, valamint az IKT-folyamatok, továbbá a kiberbiztonsági kutatói közösség és a kormányzatok sebezhetőségeket észlelő tagjai közötti együttműködésnek köszönhetően az IKT-termékekben, az IKT-szolgáltatásokban és az IKT-folyamatokban rejlő sebezhetőségek felfedezésének és orvoslásának aránya egyaránt jelentősen megnőtt. Az összehangolt sebezhetőség-feltárás olyan strukturált együttműködési eljárást takar, amelynek keretében a sebezhetőségeket az információs rendszer tulajdonosának jelentik be, lehetővé téve, hogy a szervezet azelőtt megvizsgálhassa és orvosolhassa a sebezhetőséget, hogy a sebezhetőséggel kapcsolatos részletes információkat harmadik felek vagy a nyilvánosság tudomására hoznák. Az eljárás az említett sebezhetőségek közzétételét illetően az észlelő és a szervezet közötti koordinációt is előírja. Az összehangolt sebezhetőség-feltárásra irányuló eljárások fontos szerepet játszhatnak a kiberbiztonság növelésére tett tagállami erőfeszítések terén.

(31) Az ENISA-nak összesítenie és elemeznie kell a CSIRT-ek és az Európai Parlament, az Európai Tanács, az Európai Unió Tanácsa, az Európai Bizottság, az Európai Unió Bírósága, az Európai Központi Bank, az Európai Számvevőszék, az Európai Külügyi Szolgálat, az Európai Gazdasági és Szociális Bizottság, a Régiók Európai Bizottsága és az Európai Beruházási Bank közötti, az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) szervezetéről és működéséről szóló megállapodás[1] által létrehozott, az uniós intézmények, szervek és hivatalok intézményközi hálózatbiztonsági vészhelyzeteket elhárító csoportja (a továbbiakban: a CERT-EU) által készített és önkéntesen megosztott nemzeti jelentéseket annak érdekében, hogy hozzájáruljon az információcsere közös eljárásainak, nyelvhasználatának és terminológiájának kialakításához. E tekintetben az ENISA-nak a munkájába a magánszektort is be kell vonnia az (EU) 2016/1148 irányelv keretében, amely meghatározza a CSIRT-ek hálózatán belüli, önkéntes alapon történő, operatív szintű technikai információcsere alapjait.

[1] HL C 12., 2018.1.13., 1. o.

(32) Az ENISA-nak nagyszabású, határokon átnyúló biztonsági esemény vagy válsághelyzet esetén hozzá kell járulnia az uniós szintű reagáláshoz. Ezt a feladatot az e rendelet szerinti megbízatásával, valamint az (EU) 2017/1584 bizottsági ajánlás[1] és a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról szóló, 2018. június 26-i tanácsi következtetések nyomán közösen elfogadandó megközelítéssel összhangban kell ellátnia. Az említett feladatba beletartozhat a megfelelő információk összegyűjtése, valamint a CSIRT-ek hálózata és a műszaki közösség, továbbá a válságkezelésért felelős döntéshozók közötti közvetítés is. Az ENISA-nak ezenkívül – egy vagy több tagállam kérésére – támogatnia kell a tagállamok közötti operatív együttműködést a biztonsági események műszaki szempontból való kezelésében, a megfelelő műszaki megoldások tagállamok közötti cseréjének elősegítésével, és információkkal szolgálva a nyilvánosság tájékoztatása céljából. Az ilyen jellegű együttműködés tesztelésére irányuló rendszeres kiberbiztonsági gyakorlatok keretében az ENISA-nak támogatnia kell az operatív együttműködést.

(33) Az operatív együttműködés támogatása során az ENISA-nak igénybe kell vennie a CERT-EU keretében rendelkezésre álló műszaki és operatív szakértelmet. Ezen strukturált együttműködés az ENISA szakértelmére épülhet. Adott esetben a két szervezet között külön megállapodásokat kell kialakítani az együttműködés gyakorlati megvalósításának meghatározása és a párhuzamos tevékenységek elkerülése érdekében.

---

[1] A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (HL L 239., 2017.9.19., 36. o.).

(34) A CSIRT-ek hálózatán belüli operatív együttműködés támogatására irányuló feladatainak ellátása során az ENISA-nak 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 módjaival kapcsolatban, hogy megkönnyítse a jelentős vagy lényeges hatással járó biztonsági események technikai kezelését, illetve hogy gondoskodjon a fenyegetések és biztonsági események elemzéséről. Az ENISA-nak meg kell könnyítenie a jelentős vagy lényeges hatással járó biztonsági események műszaki kezelését mindenekelőtt azáltal, hogy támogatja a műszaki megoldások tagállamok közötti önkéntes megosztását, vagy összefoglaló jellegű technikai információkat állít elő például a tagállamok által önkéntesen megosztott technikai megoldásokról. Az (EU) 2017/1584 ajánlás azt ajánlja a tagállamoknak, hogy jóhiszeműen működjenek együtt, és indokolatlan késedelem nélkül osszák meg egymással és az ENISA-val a nagyszabású biztonsági eseményekkel és válsághelyzetekkel kapcsolatos információkat. Ezek az információk az ENISA segítségére lehetnek az operatív együttműködés támogatásával kapcsolatos feladata ellátása során.

(35) Az uniós helyzetismeret támogatását célzó, rendes, műszaki szintű együttműködés részeként az ENISA-nak – a tagállamokkal szoros együttműködésben – rendszeresen el kell készítenie a biztonsági eseményekről és a kiberfenyegetésekről szóló részletes uniós kiberbiztonsági technikai helyzetjelentéseket a nyilvánosan hozzáférhető információk, a saját elemzése és azon jelentések alapján, amelyeket a tagállami CSIRT-ek vagy az (EU) 2016/1148 irányelvvel létrehozott, a hálózati és információs rendszerek biztonságáért felelős egyedüli kapcsolattartó pontok – mindkettő önkéntes alapon –, az Europol Számítástechnikai Bűnözés Elleni Európai Központja (EC3), a CERT-EU és adott esetben az Európai Külügyi Szolgálaton belül az Európai Unió Helyzetelemző Központja (EU INTCEN) megosztottak vele. Az említett jelentést a Tanács és a Bizottság, az Unió külügyi és biztonságpolitikai főképviselője és a CSIRT-ek hálózata rendelkezésére kell bocsátani.

(36) A jelentős vagy lényeges hatással járó biztonsági eseményekre vonatkozóan az érintett tagállamok kérésére elvégzett utólagos műszaki vizsgálatokhoz az ENISA által nyújtott támogatásnak a jövőbeli események megelőzésére kell összpontosítania. Az érintett tagállamoknak meg kell adniuk az ahhoz szükséges információkat és támogatást, hogy az ENISA hatékony támogatást tudjon nyújtani az utólagos műszaki vizsgálathoz.

(37) A tagállamok felkérhetik a biztonsági esemény által érintett vállalkozásokat arra, hogy – a kereskedelmi szempontból érzékeny és a közbiztonsággal kapcsolatos információk védelméhez való joguk sérelme nélkül – a szükséges információk és segítségnyújtás biztosításával működjenek együtt az ENISA-val.

(38) A kiberbiztonság területén jelentkező kihívások jobb megismerése érdekében, valamint a tagállamoknak és az uniós intézményeknek, szerveknek és hivataloknak nyújtandó hosszú távú stratégiai tanácsadás céljából az ENISA-nak elemeznie kell az ismert és az újonnan fellépő kockázatokat. E célból az ENISA-nak a tagállamokkal és adott esetben a statisztikai hivatalokkal és más szervekkel együttműködve össze kell gyűjtenie a nyilvánosan elérhető vagy önkéntesen megosztott releváns információkat, elemzéseket kell készítenie a kialakulóban lévő új technológiákról, valamint tematikus értékeléseket kell végeznie a technológiai innovációknak a hálózat- és információbiztonságra, különösen a kiberbiztonságra gyakorolt várható társadalmi, jogi, gazdasági és szabályozási hatásairól. Az ENISA-nak továbbá a kiberfenyegetések, a sebezhetőségek és a biztonsági események elemzésével támogatnia kell a tagállamokat és az uniós intézményeket, szerveket és hivatalokat az új kiberkockázatok azonosításában és a biztonsági események megelőzésében.

(39) Az ENISA-nak – az Unió ellenálló képességének növelése érdekében – tanácsadással, iránymutatással és a bevált gyakorlatok terjesztésével szakértelem kialakítására kell törekednie azon infrastruktúrák kiberbiztonságának területén, amelyek különösen az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokat támogatják, valamint amelyeket az említett 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 ENISA-nak uniós információs platformot, vagyis egy olyan egyablakos portált kell létrehoznia és fenntartania, ahol a nyilvánosság hozzájuthat az uniós és nemzeti intézményektől, szervektől, hivataloktól és ügynökségektől származó kiberbiztonsági információkhoz. A kiberbiztonsági kockázatokra és a lehetséges ellenintézkedésekre vonatkozó, jobban strukturált formában rendelkezésre álló információkhoz való hozzáférés is segítheti a tagállamokat kapacitásaik megerősítésében, gyakorlataik összehangolásában, valamint ezáltal a kibertámadások elleni általános ellenálló képességük javításában.

(40) Az ENISA-nak hozzá kell járulnia a kiberbiztonsági kockázatokkal kapcsolatos tudatosság növeléséhez – többek között az egész Unióra kiterjedő tudatosságnövelő kampánnyal és az oktatás előmozdításával –, és polgároknak, szervezeteknek és vállalkozásoknak címzett, egyedi felhasználói iránymutatást kell nyújtania a már bevált gyakorlatokkal kapcsolatban. Az ENISA-nak a polgárok, a szervezetek és a vállalkozások szintjén azáltal is hozzá kell járulnia a bevált gyakorlatok és megoldások – többek között a kiberhigiénia és a kiberbiztonsági jártasság – előmozdításához, úgy, hogy összegyűjti és elemzi a jelentős biztonsági eseményekre vonatkozó, nyilvánosan elérhető információkat, valamint jelentéseket és útmutatókat készít és tesz közzé abból a célból, hogy iránymutatást nyújtson a polgárok, a szervezetek és a vállalkozások számára, valamint javítsa felkészültségük és az ellenálló képességük általános szintjét. Az ENISA-nak továbbá kell törekednie arra, hogy a fogyasztók számára fontos információkat nyújtson az alkalmazandó tanúsítási rendszerekről, például iránymutatások és ajánlások kibocsátásával. Emellett a 2018. január 17-i bizottsági közleménnyel létrehozott digitális oktatási cselekvési tervvel összhangban, valamint a tagállamokkal és az uniós intézményekkel, szervekkel és hivatalokkal együttműködve az ENISA-nak rendszeresen kampányokat kell szerveznie a végfelhasználók tájékoztatása és oktatása érdekében, melyek célja a biztonságosabb egyéni online magatartásformák elősegítése, a digitális jártasság előmozdítása, valamint a kibertérben potenciálisan jelenlévő veszélyek tudatosítása – ideértve az adathalászatot, a botneteket, a pénzügyi és banki csalásokat és az adatcsalással kapcsolatos biztonsági eseményeket is magában foglaló online bűnügyi tevékenységeket is –, továbbá az alapvető többfaktoros hitelesítési, hibajavítási, titkosítási, anonimizálási és adatvédelmi tanácsadás előmozdítása.

(41) Az ENISA-nak elő kell mozdítania az uniós szintű beépített biztonságot és a beépített adatvédelmet, és központi szerepet kell játszania az eszközök biztonságosságával és a szolgáltatások biztonságos használatával kapcsolatos végfelhasználói tudatosság minél gyorsabb növelésében. E cél elérése érdekében az ENISA-nak a lehető legjobban ki kell használnia a rendelkezésre álló bevált gyakorlatokat és tapasztalatokat, különösen a felsőoktatási intézményektől és az informatikai biztonsági kutatóktól származó bevált gyakorlatokat és tapasztalatokat.

(42) A kiberbiztonsági ágazatban működő vállalkozások, valamint a kiberbiztonsági megoldások felhasználóinak támogatása érdekében az ENISA-nak 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 tendenciáira vonatkozó információkat.

(43) Az ENISA-nak hozzá kell járulnia az Unió által a nemzetközi szervezetekkel, valamint a releváns nemzetközi együttműködési kereteken belül folytatott együttműködéshez a kiberbiztonság területén. Az ENISA-nak különösen – adott esetben – az olyan szervezekkel folytatott együttműködéshez kell hozzájárulnia, mint az OECD, az EBESZ és a NATO. Ezen együttműködés kiterjedhet egyebek mellett a közös kiberbiztonsági gyakorlatokra és a biztonsági eseményekre való reagálás közös koordinációjára. Ezeket a tevékenységeket az inkluzivitásra, a kölcsönösségre és az uniós döntéshozatal autonómiájára vonatkozó elvek maradéktalan tiszteletben tartása mellett kell végezni, az egyes tagállamok biztonság- és védelempolitikája sajátosságainak sérelme nélkül.

(44) Célkitűzéseinek maradéktalan elérése érdekében az ENISA-nak kapcsolatot kell kialakítania a megfelelő uniós felügyeleti hatóságokkal és más, az Unióban található illetékes hatóságokkal, az uniós intézményekkel, szervekkel és hivatalokkal, többek között a CERT-EU-val, az EC3-mal, az Európai Védelmi Ügynökséggel (EDA), az Európai GNSS Ügynökséggel (GSA), az Európai Elektronikus Hírközlési Szabályozó Hatóságok Testületének Hivatalával (BEREC), a Szabadságon, a Biztonságon és a Jog Érvényesülésén Alapuló Térség Nagyméretű IT-rendszereinek Üzemeltetési Igazgatását Végző Európai Ügynökséggel (eu-LISA), az Európai Központi Bankkal (EKB), az Európai Bankhatósággal (EBH), az Európai Adatvédelmi Testülettel, az Energiaszabályozók Együttműködési Ügynökségével (ACER), az Európai Repülésbiztonsági Ügynökséggel (EASA) és a kiberbiztonságban érintett minden más uniós ügynökséggel. Az ENISA-nak kapcsolatot kell fenntartania az adatvédelemmel foglalkozó hatóságokkal is a know-how és a bevált gyakorlatok cseréje érdekében, valamint tanácsot kell adnia a kiberbiztonság azon vonatkozásaival kapcsolatban, amelyek hatással lehetnek ezek munkájára. A nemzeti és uniós bűnüldöző és adatvédelmi hatóságok képviselőinek lehetőséget kell biztosítani arra, hogy képviseltessék magukat az ENISA tanácsadó csoportjában. Az ENISA-nak a bűnüldöző hatóságokkal folytatott, a munkájukra esetlegesen hatást gyakorló hálózat- és információbiztonsági kérdésekkel kapcsolatos együttműködés során tiszteletben kell tartania a meglévő információs csatornákat és a létező hálózatokat.

(45) Partnerségeket lehet kialakítani azokkal a felsőoktatási intézményekkel, amelyek kutatási kezdeményezésekkel rendelkeznek az érintett területeken, a fogyasztói és egyéb szervezetektől származó hozzájárulások számára pedig megfelelő csatornákat kell biztosítani és azokat figyelembe kell venni.

(46) Az ENISA-nak a CSIRT-ek hálózatának titkársága szerepében támogatnia kell a tagállami CSIRT-ek és a CERT-EU operatív együttműködését, a CSIRT-ek hálózatának az (EU) 2016/1148 irányelvben említett releváns feladatai tekintetében. Az ENISA-nak elő kell mozdítania és támogatnia kell továbbá a megfelelő CSIRT-ek közötti együttműködést a legalább két CSIRT-et is érintő vagy érinthető, az általuk kezelt vagy védett hálózatokat vagy infrastruktúrát érő biztonsági események, támadások és zavarok esetén, figyelembe véve ugyanakkor a CSIRT-ek hálózatának eljárásrendjét.

(47) A kiberbiztonsági eseményekre való reagálással kapcsolatos uniós felkészültség javítása érdekében az ENISA-nak rendszeresen kiberbiztonsági gyakorlatokat kell szerveznie uniós szinten, és kérésükre támogatnia kell a tagállamokat és az uniós intézményeket, szerveket és hivatalokat az ilyen gyakorlatok megszervezésében. Kétévente nagy kiterjedésű átfogó gyakorlatot kell rendezni, amely műszaki, operatív és stratégiai elemeket foglal magában. Emellett az ENISA rendszeresen szervezhet kevésbé átfogó gyakorlatokat ugyanazzal a céllal, azaz a biztonsági eseményekre való reagálással kapcsolatos uniós felkészültség javítása érdekében.

(48) Az ENISA-nak a kiberbiztonsági tanúsítás terén kialakított szakértelmét tovább kell fejlesztenie és fenn kell tartania az erre a területre vonatkozó uniós szakpolitika támogatása érdekében. Az ENISA-nak a meglévő bevált gyakorlatokra kell támaszkodnia, és elő kell mozdítania a kiberbiztonsági tanúsítás Unión belüli elterjesztését, többek között azáltal, hogy hozzájárul az uniós szintű kiberbiztonsági tanúsítási keretrendszer (a továbbiakban: az európai kiberbiztonsági tanúsítási rendszer) létrehozásához és fenntartásához annak érdekében, hogy átláthatóbb legyen az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kiberbiztonsági megbízhatósága, megerősítve ezzel a digitális belső piacba és annak versenyképességébe vetett bizalmat.

(49) A hatékony kiberbiztonsági szakpolitikáknak – a köz- és a magánszektorban egyaránt – kellően kidolgozott kockázatértékelési módszereken kell alapulniuk. A kockázatértékelési módszereket különböző szinteken használják, és eredményes alkalmazásukat illetően nincs közös gyakorlat. A kockázatértékeléssel és az interoperábilis kockázatkezelési megoldásokkal kapcsolatban bevált gyakorlatoknak a köz- és a magánszektorbeli szervezetekben való ösztönzése, illetve kialakítása fokozni fogja az Unió kiberbiztonságát. E célból az ENISA-nak uniós szinten támogatnia kell az uniós érdekelt felek 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.

(50) Az ENISA-nak ösztönöznie kell a tagállamokat, az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok gyártóit vagy nyújtóit általános biztonsági előírásaik szigorítására, hogy minden internetfelhasználó megtehesse a személyes kiberbiztonságához szükséges lépéseket, és hogy erre ösztönözve legyen. Különösen fontos, hogy az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok gyártói vagy nyújtói gondoskodjanak azon IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok szükséges frissítéseiről, amelyek nem felelnek meg a kiberbiztonsági szabványoknak, illetve hogy ezeket visszahívják, visszavonják vagy újrahasznosítsák, az importőröknek és a forgalmazóknak pedig arról kell gondoskodniuk, hogy az általuk az Unióban forgalomba hozott IKT-termékek, IKT-szolgáltatások és IKT-folyamatok megfeleljenek az alkalmazandó követelményeknek, és ne jelentsenek kockázatot az uniós fogyasztók számára.

(51) Az ENISA-nak az illetékes hatóságokkal együttműködve tájékoztatást kell tudni adnia a belső piacon kínált IKT-termékek, IKT-szolgáltatások és IKT-folyamatok kiberbiztonsági szintjéről, és figyelmeztetéseket is ki kell tudni adnia, amelyekben a szolgáltatókat és a gyártókat IKT-termékeik, IKT-szolgáltatásaik és IKT-folyamataik biztonságának – ezen belül kiberbiztonságának – a fokozására szólítja fel.

(52) Az ENISA-nak 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, szervekés hivatalok, valamint adott esetben a tagállamok számára a kiberbiztonság területét érintő kutatási igényekkel és prioritásokkal kapcsolatban. A kutatási igények és prioritások meghatározása érdekében az ENISA-nak konzultálnia kell az érintett felhasználói csoportokkal is. Konkrétabban érdemes együttműködést kiépíteni az Európai Kutatási Tanáccsal, az Európai Innovációs és Technológiai Intézettel, valamint az Európai Unió Biztonságpolitikai Kutatóintézetével.

(53) Az európai kiberbiztonsági tanúsítási rendszerek kidolgozása során az ENISA-nak rendszeresen konzultálnia kell a szabványügyi szervezetekkel, különösen az európai szabványügyi szervezetekkel.

(54) A kiberbiztonsági fenyegetések globális kérdést jelentenek. Szorosabb nemzetközi együttműködésre van szükség a kiberbiztonsági szabványok javítása – és ezen belül a közös viselkedési normák és magatartási kódexek elfogadása, a nemzetközi szabványok használata – és az információmegosztás érdekében, valamint a hálózat- és információbiztonsági kérdésekre adott reagálás tekintetében a gyorsabb nemzetközi együttműködést elősegítő információcsere javítása és egy azokra vonatkozó közös globális megközelítésmód előmozdítása érdekében. Az ENISA-nak e célból támogatnia kell az uniós szerepvállalás fokozását és a harmadik országokkal és a nemzetközi szervezetekkel folytatott együttműködést, adott esetben biztosítva a szükséges szakértelmet és elemzéseket az érintett uniós intézmények, szervek és hivatalok számára.

(55) Az ENISA-nak képesnek kell lennie arra, hogy eleget tegyen a tagállamok és az uniós intézmények, szervek és hivatalok tanácsadásra és segítségnyújtásra vonatkozó eseti megkereséseinek, amennyiben azok az ENISA megbízatásának hatálya alá tartoznak.

(56) Az ENISA irányítását illetően észszerű és ajánlott bizonyos elveket alkalmazni az EU decentralizált ügynökségeivel foglalkozó intézményközi munkacsoport által 2012 júliusában elfogadott együttes nyilatkozatból és közös megközelítésből, melyek célja a decentralizált ügynökségek tevékenységeinek gördülékennyé tétele és teljesítményük javítása. Adott esetben az ENISA munkaprogramjaiban, az ENISA értékeléseiben, valamint az ENISA jelentéstételi és adminisztratív gyakorlatában érvényesíteni kell az együttes nyilatkozatban és a közös megközelítésben adott ajánlásokat is.

(57) Az ENISA tevékenységének általános irányát a tagállamok képviselőiből és a Bizottság képviselőiből álló igazgatótanácsnak kell megállapítania, és biztosítania kell, hogy az ENISA e rendelettel összhangban lássa el feladatait. Az igazgatótanácsot fel kell ruházni mindazokkal a hatáskörökkel, amelyek a költségvetés meghatározásához, a költségvetés végrehajtásának ellenőrzéséhez, a pénzügyi szabályzat elfogadásához, az ENISA átlátható határozathozatali eljárásainak kialakításához, az ENISA egységes programozási dokumentumának elfogadásához, saját eljárási szabályzatának elfogadásához, az ügyvezető igazgató kinevezéséhez, és az ügyvezető igazgató hivatali idejének meghosszabbításához és az ügyvezető igazgató felmentéséhez szükségesek.

(58) Az ENISA megfelelő és hatékony működése érdekében a Bizottságnak és a tagállamoknak biztosítaniuk kell, hogy az igazgatótanács tagjainak kinevezendő személyek megfelelő szakértelemmel és megfelelő tapasztalattal rendelkezzenek. Az igazgatótanács munkájának folytonosságát biztosítandó, a Bizottságnak és a tagállamoknak is törekedniük kell arra, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban.

(59) Az ENISA 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. Az ügyvezető igazgató feladatait teljes mértékben független módon kell, hogy végezze. Az ügyvezető igazgatónak – a Bizottsággal folytatott előzetes konzultációt követően – javaslatot kell tennie az ENISA munkaprogramjára, és meg kell tennie mindazokat a lépéseket, amelyek az ENISA munkaprogramja megfelelő végrehajtásának biztosításához szükségesek. Az ügyvezető igazgatónak el kell készítenie az igazgatótanácshoz benyújtandó éves jelentést, amely kiterjed az ENISA éves munkaprogramjának végrehajtására is, össze kell állítania az ENISA tervezett bevételeire és kiadásaira vonatkozó kimutatástervezetét, 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 eseti munkacsoport létrehozása szükségesnek tekintendő különösen valamely konkrét javaslati európai kiberbiztonsági tanúsítási rendszer (a továbbiakban: javasolt tanúsítási rendszer) kidolgozásával kapcsolatban. Az ügyvezető igazgatónak biztosítania kell, hogy az eseti munkacsoportok tagjainak kiválasztása a lehető legmagasabb szintű szakértelem alapján a nemek közötti egyensúly és a csoport feladatkörének sajátosságaihoz igazodva a tagállami közigazgatási szervek, az uniós intézmények, szervek és hivatalok és a magánszektor – beleértve az ipart, a felhasználókat és a hálózat- és információbiztonság területén működő tudományos szakembereket – közötti megfelelő egyensúly kellő figyelembevételével történjék.

(60) A felügyelőtestületnek hozzá kell járulnia az igazgatótanács hatékony működéséhez. Az igazgatótanács határozataival kapcsolatos előkészítő munkája részeként a felügyelőtestületnek részletesen meg kell vizsgálnia a kapcsolódó információkat, fel kell derítenie a rendelkezésre álló lehetőségeket, valamint tanácsot és megoldásokat kell kínálnia az igazgatótanács vonatkozó határozatainak előkészítéséhez.

(61) A magánszektorral, a fogyasztói szervezetekkel és más érdekeltekkel való rendszeres párbeszéd biztosítása céljából az ENISA-n belül tanácsadó szervként indokolt létrehozni az ENISA tanácsadó csoportot. Az ENISA tanácsadó csoportnak, amelyet az ügyvezető igazgató javaslata alapján az igazgatótanács hoz létre, az érdekeltek számára fontos kérdésekre kell összpontosítania, és fel kell hívnia ezekre az ENISA figyelmét. Az ENISA tanácsadó csoporttal különösen az ENISA éves munkaprogramjának tervezete kapcsán konzultálni kell. Az ENISA tanácsadó csoport összetételének és a csoportra bízott feladatoknak biztosítania kell, hogy az érdekelt felek az ENISA munkájában hatékonyan képviselve legyenek.

(62) Indokolt létrehozni az érdekelt felek kiberbiztonsági tanúsítási csoportját annak érdekében, hogy az a releváns érdekelt felekkel folytatott konzultáció megkönnyítésével segítse az ENISA-t és a Bizottságot. Az érdekelt felek kiberbiztonsági tanúsítási csoportja tagjainak az ágazat képviselőiből kell állnia, akik kiegyensúlyozott arányban képviselik az ágazatot, az IKT-termékeknek és IKT-szolgáltatásoknak mind a kínálati, mind a keresleti oldalát, beleértve különösen a kkv-kat, a digitális szolgáltatókat, az európai és nemzetközi szabványügyi szerveket, a nemzeti akkreditáló testületeket, az adatvédelmi felügyeleti hatóságokat és a 765/2008/EK európai parlamenti és tanácsi rendelet[1] szerinti megfelelőségértékelő szervezeteket, a tudományos életet, valamint a fogyasztói szervezeteket.

[1] Az Európai Parlament és a Tanács 765/2008/EK rendelete (2008. július 9.) a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o.).

(63) Az ENISA-nak szabályokat kell kidolgoznia az összeférhetetlenségek megelőzésére és kezelésére. Az ENISA-nak alkalmaznia kell továbbá a dokumentumokhoz való nyilvános hozzáférésre vonatkozó, a 1049/2001/EK európai parlamenti és tanácsi rendeletben[1] meghatározott uniós rendelkezéseket is. Az ENISA-nak a személyes adatokat az (EU) 2018/1725 európai parlamenti és tanácsi rendeletnek[2] megfelelően kell kezelnie. Be kell tartania továbbá az uniós intézményekre, szervekre és hivatalokra alkalmazandó rendelkezéseket, valamint az információk – különösen a nem minősített érzékeny adatok és az EU-minősített adatok – kezelésére vonatkozó nemzeti jogszabályokat is.

---

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

2 Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

(64) Az ENISA teljes mértékű autonómiájának és függetlenségének biztosítása érdekében, valamint hogy feladatait, többek között a váratlan, sürgős feladatokat is, el tudja látni, az ENISA számára elégséges és önálló költségvetést kell biztosítani, mely bevételeinek elsősorban az Unió hozzájárulásából és az ENISA munkájában részt vevő harmadik országok hozzájárulásából kell származniuk. A megfelelő költségvetés kiemelkedő fontosságú annak biztosításához, hogy az ENISA elegendő kapacitással rendelkezzen bővülő feladatainak ellátásához és célkitűzéseinek teljesítéséhez. Az ENISA személyzete többségének közvetlenül az ENISA megbízatásának operatív végrehajtásával kell foglalkoznia. Lehetőséget kell biztosítani arra, hogy az ENISA-t fogadó tagállam vagy bármely más tagállam az ENISA költségvetéséhez önkéntes alapon hozzájáruljon. Az Unió általános költségvetését terhelő támogatások vonatkozásában továbbra is az uniós költségvetési eljárást kell alkalmazni. Ezenkívül az átláthatóság és az elszámoltathatóság biztosítása érdekében a Számvevőszéknek ellenőriznie kell az ENISA elszámolásait.

(65) A kiberbiztonsági tanúsítás fontos szerepet játszik az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok 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, szolgáltatások és folyamatok 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. Az (EU) 2016/1148 irányelv által szabályozott ágazatok szintén olyan ágazatok, amelyekben a kiberbiztonsági tanúsítás kritikus fontosságú.

(66) 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, IKT-szolgáltatások és IKT-folyamatok egységes piacon való elérhetősége földrajzilag igen széttagolt. Ennek az az oka, hogy a kiberbiztonsági ipar Európában nagyrészt aszerint alakult, hogy az egyes országokban mekkora volt a kereslet a kormányok részéről. Emellett az interoperábilis megoldások (műszaki szabványok), gyakorlatok 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, az uniós és a globális szintű versenyben. Másrészt csökkenti az egyének és a vállalkozások számára hozzáférhető, működőképes és használható kiberbiztonsági technológiák kínálatát. „A digitális egységes piaci stratégia végrehajtásának félidős értékelése – Összekapcsolt digitális egységes piac mindenki számára” című, 2017-es közleményében 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 belső piac jelenlegi széttagoltságára.

(67) Jelenleg az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok esetében csak korlátozott mértékben alkalmazzák a kiberbiztonsági tanúsítást. Amennyiben létezik ilyen, akkor főként tagállami szinten vagy az ipar kezdeményezésére kialakított rendszerek keretében kerül sor erre. Ennek fényében, ha egy nemzeti kiberbiztonsági tanúsító hatóság tanúsítványt bocsát ki, azt a többi tagállam főszabály szerint nem ismeri el. A vállalatoknak így – ha például nemzeti közbeszerzési eljárásokban kívánnak részt venni – előfordulhat, hogy működésük helye szerint több tagállamban is tanúsíttatniuk kell IKT-termékeiket, IKT-szolgáltatásaikat és IKT-folyamataikat, ami növeli a költségeiket. 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, ami akadályozza az Unión belüli kölcsönös elismerési mechanizmusokat.

(68) Történtek már lépések annak érdekében, hogy Európában biztosítva legyen a tanúsítványok kölcsönösen elismerése. Ezek azonban csak részben voltak sikeresek. E tekintetben a legfontosabb példa a vezető tisztviselők információs rendszerek biztonságával foglalkozó csoportján (a továbbiakban: 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. Emiatt az SOG-IS kölcsönös elismerési megállapodás is csak korlátozott hatékonyságú lehet a belső piac szempontjából.

(69) Ezért szükségesnek egy közös megközelítés elfogadása és 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, az IKT-szolgáltatások és az IKT-folyamatok európai kiberbiztonsági tanúsítványainak, valamint uniós megfelelőségi nyilatkozatainak valamennyi tagállamban történő elismerését és használatát. Ennek során kiemelten fontos a meglévő nemzeti és nemzetközi rendszerekre, valamint a kölcsönös elismerési rendszerekre, különösen az SOG-IS-re támaszkodni, valamint lehetővé tenni az ilyen rendszerek keretében már működő rendszerekről az új európai kiberbiztonsági tanúsítási keretrendszer szerinti rendszerekre történő zökkenőmentes átállást. Az európai kiberbiztonsági tanúsítási keretrendszernek kettős célt kell szolgálnia. Egyrészt segítenie kell az európai kiberbiztonsági tanúsítási rendszerek alapján tanúsított IKT-termékek, IKT-szolgáltatások és IKT-folyamatok iránti bizalom növelését. Másrészt segítenie kell elkerülni, hogy egymásnak ellentmondó vagy egymást átfedő nemzeti kiberbiztonsági tanúsítási rendszerek létezzenek, csökkentve ezzel a digitális egységes piacon működő vállalkozások költségeit. Az európai kiberbiztonsági tanúsítási rendszereknek megkülönböztetésmenteseknek kell lenniük, és európai vagy nemzetközi szabványokon kell alapulniuk, kivéve, ha ezek a szabványok nem hatékonyak vagy nem alkalmasak az Unió e tekintetben kitűzött jogos célkitűzéseinek teljesítésére.

(70) Az európai kiberbiztonsági tanúsítási keretrendszert minden tagállamban egységesen kell létrehozni, elkerülendő az egyes tagállamok közötti követelménykülönbségek miatti, visszaélésszerű tanúsításválasztást.

(71) Az európai kiberbiztonsági tanúsítási rendszereknek a nemzetközi és nemzeti szinten már létező elemekre, és szükség esetén fórumok és konzorciumok műszaki előírásaira kell épülniük, levonva a jelenlegi erősségek tanulságait, valamint értékelve és kijavítva a gyengeségeket.

(72) Rugalmas kiberbiztonsági megoldásokra van szükség ahhoz, hogy az ipar megbirkózhasson a kiberfenyegetésekkel, és ezért minden tanúsítási rendszert úgy kell tervezni, hogy elkerülje a gyors elavulás kockázatát.

(73) A Bizottságot fel kell hatalmazni arra, hogy európai kiberbiztonsági tanúsítási rendszereket fogadjon el az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok 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 ipar vagy más magánszervezetek által működtetett tanúsítási rendszereknek nem kell e rendelet hatálya alá tartozniuk. Az ilyen rendszereket működtető szervezetek azonban javasolhatják a Bizottságnak annak mérlegelését, hogy az említett rendszerek alapul vehetők-e európai kiberbiztonsági tanúsítási rendszerként való jóváhagyás céljából.

(74) E rendelet rendelkezései nem sértik az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására vonatkozó egyedi szabályokat megállapító uniós jogot. Különösen az (EU) 2016/679 rendelet állapít meg tanúsítási mechanizmusok és adatvédelmi bélyegzők, illetve jelölések létrehozására vonatkozó rendelkezéseket az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveleteknek az említett rendeletnek való megfelelése bizonyításának céljából előírásait. Az ilyen tanúsítási mechanizmusoknak és adatvédelmi bélyegzőknek, illetve jelöléseknek lehetővé kell tennie az érintettek számára, hogy gyorsan értékelni tudják a releváns IKT-termékek, IKT-szolgáltatások és IKT-folyamatok adatvédelmi szintjét. Ez a rendelet nem sérti az adatkezelési műveleteknek az (EU) 2016/679 rendelet szerinti tanúsítását, még akkor sem, ha az ilyen műveletek IKT-termékekbe, IKT-szolgáltatásokba és IKT-folyamatokba vannak beágyazva.

(75) Az európai kiberbiztonsági tanúsítási rendszerek célja annak biztosítása, hogy az ilyen rendszerek keretében tanúsított IKT-termékek, IKT-szolgáltatások és IKT-folyamatok megfeleljenek az a célból meghatározott követelményeknek, hogy védjék a termékek, szolgáltatások és folyamatok által tárolt, továbbított vagy kezelt adatok, illetve az említett termékek, szolgáltatások és folyamatok által biztosított vagy elérhetővé tett kapcsolódó funkciók vagy szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és titkosságát azok teljes életciklusa alatt. Lehetetlen e rendeletben az összes IKT-termék, IKT-szolgáltatás és IKT-folyamat vonatkozásában részletesen meghatározni a kiberbiztonsági követelményeket. Az említett termékekhez, szolgáltatásokhoz és folyamatokhoz kapcsolódó IKT-termékek, IKT-szolgáltatások és IKT-folyamatok, valamint kiberbiztonsági igények olyan különbözők, hogy nagyon nehéz minden körülmények között 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 célkitűzéseknek kell kiegészíteni. Azt, hogy ezeket a célkitűzéseket egyes IKT-termékek, IKT-szolgáltatások és IKT-folyamatok esetében hogyan kell elérni, részleteiben a Bizottság által elfogadott egyedi tanúsítási rendszer szintjén kell meghatározni, például szabványokra vagy műszaki előírásokra való hivatkozás révén, ha nem áll rendelkezésre megfelelő szabvány.

(76) Az európai kiberbiztonsági tanúsítási rendszerek keretében alkalmazandó műszaki előírásoknak tiszteletben kell tartaniuk az 1025/2012/EU európai parlamenti és tanácsi rendelet[1] II. mellékletében megállapított elveket. Kellően indokolt esetekben azonban, amikor az említett műszaki előírások olyan európai kiberbiztonsági tanúsítási rendszer keretében alkalmazandók, amely „magas” megbízhatósági szintre vonatkozik, szükségessé válhat az említett elvektől való kis mértékű eltérés. Az ilyen eltérés indokait nyilvánossá kell tenni.

[1] Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről (HL L 316., 2012.11.14., 12. o.).

(77) A megfelelőségértékelés olyan eljárás, amelynek során értékelik, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat megfelel-e az előírt követelményeknek. Ezt az eljárást egy független harmadik fél folytatja le, aki nem lehet az értékelendő IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója vagy nyújtója. Az európai kiberbiztonsági tanúsítvány kiállítására az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat sikeres értékelését követően kerülhet sor. Az európai kiberbiztonsági tanúsítvány igazolásnak tekintendő arra nézve, hogy az értékelést megfelelően elvégezték. A megbízhatósági szinttől függően az európai kiberbiztonsági tanúsítási rendszerben elő kell írni, hogy az európai kiberbiztonsági tanúsítványt magánjogi vagy közjogi szerv állítja-e ki. A megfelelőségértékelés és a tanúsítás önmagában nem garantálja, hogy a tanúsított IKT-termékek, IKT-szolgáltatások és IKT-folyamatok kiberbiztonsági szempontból biztonságosak. Inkább olyan eljárásokról és műszaki módszertanokról van szó, amelynek célja annak tanúsítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok bevizsgáltak, és azok megfelelnek bizonyos máshol, – például műszaki szabványokban– meghatározott kiberbiztonsági követelményeknek.

(78) Az európai kiberbiztonsági tanúsítvány felhasználójának az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok használatához kapcsolódó kockázatok elemzése alapján kell megválasztania a megfelelő tanúsítást és az ahhoz kapcsolódó biztonsági követelményeket. A megbízhatósági szintnek tehát arányban kell állnia az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat rendeltetés szerinti használatához kapcsolódó kockázat szintjével.

(79) Az európai kiberbiztonsági tanúsítási rendszerek keretében lehetővé lehetne tenni, hogy a megfelelőségértékelésre az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártójának vagy nyújtójának kizárólagos felelőssége mellett kerüljön sor (a továbbiakban: megfelelőségi önértékelés). Ilyen esetekben elegendőnek kell lennie, hogy az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok a gyártója vagy nyújtója maga végzi el az összes annak biztosítására szolgáló vizsgálatot, hogy az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok megfelelnek az európai kiberbiztonsági tanúsítási rendszer követelményeinek. A megfelelőségi önértékelés az olyan, kevésbé összetett IKT-termékek, IKT-szolgáltatások és IKT-folyamatok esetében tekinthető megfelelőnek, amelyek alacsony kockázatot jelentenek a közérdekre nézve, például az egyszerű tervezési vagy gyártási mechanizmusok. Ezenkívül megfelelőségi önértékelés kizárólag az „alap” megbízhatósági szintnek megfelelő IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok esetében engedhető meg.

(80) Az európai kiberbiztonsági tanúsítási rendszerek keretében lehetővé lehetne tenni az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok megfelelőségi önértékelését és tanúsítását. Ebben az esetben a rendszernek világos, közérthető módszerekkel kell szolgálnia a célból, hogy a fogyasztók vagy más felhasználók különbséget tudjanak tenni az olyan IKT-termékek, IKT-szolgáltatások és IKT-folyamatok között, amelyek tekintetében az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártója vagy nyújtója felelős az értékeléséért, és azon IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok között, amelyeket harmadik fél tanúsított.

(81) Az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok azon gyártójának vagy nyújtójának, aki vagy amely megfelelőségi önértékelést végez, lehetővé kell tenni, hogy a megfelelőségértékelési eljárás részeként uniós megfelelőségi nyilatkozatot állítson ki, és azt aláírja. Az uniós megfelelőségi nyilatkozat egy olyan dokumentum, amely megállapítja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat megfelel az európai kiberbiztonsági tanúsítási rendszer követelményeinek. Az uniós megfelelőségi nyilatkozat kiállításával és aláírásával az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat gyártója vagy nyújtója felelősséget vállal azért, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelel az európai kiberbiztonsági tanúsítási rendszer jogi követelményeinek. Az uniós megfelelőségi nyilatkozat másolati példányát meg kell küldeni a nemzeti kiberbiztonsági tanúsító hatóságnak és az ENISA-nak.

(82) Az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok gyártójának vagy nyújtójának a releváns európai kiberbiztonsági tanúsítási rendszerben meghatározott ideig az illetékes nemzeti kiberbiztonsági tanúsító hatóság rendelkezésére kell bocsátania az uniós megfelelőségi nyilatkozatot, valamint az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok európai kiberbiztonsági tanúsítási rendszernek való megfelelésével kapcsolatos műszaki dokumentációt és minden egyéb releváns információt. A műszaki dokumentációnak tartalmaznia kell a rendszer keretében alkalmazandó követelményeket, és – a megfelelőségi önértékelés szempontjából releváns mértékben – le kell fednie az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat tervezését, gyártását és működését. A műszaki dokumentációt úgy kell összeállítani, hogy lehetővé tegye annak értékelését, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelel-e a rendszer keretében alkalmazandó követelményeknek.

(83) Az európai kiberbiztonsági tanúsítási keretrendszer irányítása figyelembe veszi a tagállamok, valamint az érdekelt felek megfelelő bevonását, továbbá meghatározza, hogy milyen szerepet tölt be a Bizottság az európai kiberbiztonsági tanúsítási rendszerek tervezésében, az azokra vonatkozó javaslattételben, a kérelmezésükben, az előkészítésükben, az elfogadásukban és a felülvizsgálatukban.

(84) A Bizottságnak az európai kiberbiztonsági tanúsítási csoport és az érdekelt felek kiberbiztonsági tanúsítási csoportja segítségével, nyílt és széleskörű konzultációt követően az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó uniós gördülő munkaprogramot kell kidolgoznia, és azt jogilag nem kötelező erejű eszköz formájában közzé kell tennie. Az uniós gördülő munkaprogramnak olyan stratégiai dokumentumnak kell lennie, amely lehetővé teszi különösen az ipar, a nemzeti hatóságok és a szabványügyi szervezetek számára, hogy előre felkészüljenek a jövőbeli európai kiberbiztonsági tanúsítási rendszerekre. Az uniós gördülő munkaprogramnak magában kell foglalnia egy többéves áttekintést azokról a javasolt tanúsítási rendszerekről, amelyek kidolgozására a Bizottság adott indokok alapján felkérést szándékozik intézni az ENISA-hoz. A Bizottságnak IKT-szabványosítási gördülőterve és az európai szabványügyi szervekhez beérkező szabványosítási kérelmek előkészítése során figyelembe kell vennie az uniós gördülő munkaprogramot. Tekintettel az új technológiák gyors bevezetésére és igénybevételére, valamint a korábban ismeretlen kiberbiztonsági kockázatokra és jogalkotási vagy piaci fejleményekre, helyénvaló, hogy a Bizottság vagy az európai kiberbiztonsági tanúsítási csoport felkérhesse az ENISA-t olyan javasolt tanúsítási rendszerek kidolgozására, amelyek nem képezték az uniós gördülő munkaprogram részét. Ilyen esetben a Bizottságnak és az európai kiberbiztonsági tanúsítási csoportnak értékelnie kell az ilyen felkérés szükségességét, figyelembe véve e rendelet átfogó céljait és célkitűzéseit, valamint az ENISA erőforrás-tervezése és -használata folytonosságának biztosítását.

Az ENISA-nak az említett felkérést követően indokolatlan késlekedés nélkül ki kell dolgoznia a javasolt tanúsítási rendszert a konkrét IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozóan. A Bizottságnak értékelnie kell e felkérésének a konkrét piacra gyakorolt pozitív és negatív hatásait, különösen a kkv-k, az innováció, az említett piacra való belépés előtt álló akadályok és a végfelhasználók költségei tekintetében. A Bizottságot fel kell hatalmazni arra, hogy végrehajtási jogi aktusok útján – az ENISA által kidolgozott javasolt tanúsítási rendszer alapján – elfogadja az európai kiberbiztonsági tanúsítási rendszert. Figyelemmel e rendeletben megállapított általános célra és biztonsági célkitűzésekre, a Bizottság által elfogadott európai kiberbiztonsági tanúsítási rendszereknek bizonyos elemeket minimálisan meg kell határozniuk az adott rendszer tárgya, hatálya és működése vonatkozásában. Ezen elemeknek többek között ki kell terjedniük a kiberbiztonsági tanúsítás hatályára és tárgyára, ideértve a hatálya alá tartozó IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok kategóriáit, a kiberbiztonsági követelmények részletes leírására, például szabványokra vagy műszaki előírásokra való hivatkozások révén, az egyedi értékelési kritériumokra és értékelési módszerekre, továbbá a szándékolt megbízhatósági szintre („alap”, „jelentős” vagy „magas”), valamint adott esetben az értékelési szintekre. Az ENISA visszautasíthatja az európai kiberbiztonsági tanúsítási csoporttól érkező felkérést. Ezt a döntést az igazgatótanácsnak kell meghoznia, és azt kellően indokolni kell.

(85) Az ENISA-nak honlapot kell fenntartania, amelyen tájékoztatást kell nyújtania az európai kiberbiztonsági tanúsítási rendszerekről és azoknak publicitást kell biztosítania, a honlapon szerepelniük kell többek között a javasolt európai tanúsítási rendszerek kidolgozására irányuló felkéréseknek, valamint a kidolgozási szakaszban az ENISA által folytatott konzultációk során kapott visszajelzéseknek is. A honlapon az e rendelet alapján kiadott európai kiberbiztonsági tanúsítványokra és uniós megfelelőségi nyilatkozatokra – ideértve az európai kiberbiztonsági tanúsítványok és uniós megfelelőségi nyilatkozatok visszavonását és azok lejáratát is – vonatkozó információkat kell elérhetővé tenni. A honlapon fel kell tüntetni azokat a nemzeti kiberbiztonsági tanúsítási rendszereket is, amelyeket egy európai kiberbiztonsági tanúsítási rendszer váltott fel.

(86) Az európai tanúsítási rendszerek megbízhatósági szintje jelenti az az iránti bizalom alapját, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat teljesíti egy adott európai kiberbiztonsági tanúsítási rendszer biztonsági követelményeit. Az európai tanúsítási keretrendszer következetességének biztosítása érdekében az európai kiberbiztonsági tanúsítási rendszernek meg kell határoznia az adott rendszer keretében kiadott európai kiberbiztonsági tanúsítványok és uniós megfelelőségi nyilatkozatok megbízhatósági szintjeit. Az egyes európai kiberbiztonsági tanúsítványok az „alap”, „jelentős” vagy „magas” megbízhatósági szintek egyikére hivatkozhatnak, míg az uniós megfelelőségi nyilatkozat csak az „alap” megbízhatósági szintre. A megbízhatósági szintek megfelelnének az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat értékelése szigorúságának és mélységének, és azokat a rájuk vonatkozó műszaki előírások, szabványok és eljárások – melyek célja a biztonsági események hatásainak mérséklése, illetve azok megelőzése –, többek között a műszaki ellenőrzések, határoznák meg. Az egyes megbízhatósági szinteket a tanúsítást alkalmazó különböző ágazati területek között következetesen kell alkalmazni.

(87) Az európai kiberbiztonsági tanúsítási rendszerekben az alkalmazott értékelési módszertan szigorúságától és mélységétől függően több értékelési szint is meghatározható. Az értékelési szinteknek meg kell felelniük a megbízhatósági szintek egyikének, és azokhoz a megbízhatósági komponensek egy megfelelő kombinációját kell társítani. Minden megbízhatósági szint esetében az IKT-terméknek, az IKT-szolgáltatásnak vagy az IKT-folyamatnak a tanúsítási rendszer szerint meghatározott számos biztonságos funkcióval kell rendelkeznie, ilyen lehet például az alapértelmezésben biztonságos konfiguráció, az aláírt kód, a biztonságos frissítés, a sebezhetőségek kihasználhatóságának mérséklése, vagy a veremmemória/halommemória teljes körű védelme. Ezeket a funkciókat biztonságorientált fejlesztési megközelítésmódot és az ahhoz társított eszközöket alkalmazva kell kifejleszteni, illetve fenntartani annak biztosítása érdekében, hogy a szoftver és a hardver szintjén hatékony mechanizmusok kerüljenek beépítésre, megbízható módon.

(88) Az „alap” megbízhatósági szint esetében az értékelésnek legalább a következő megbízhatósági elemekre kell kiterjednie: az értékelés legalább az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat műszaki dokumentációjának a megfelelőségértékelő szervezet általi áttekintését foglalja magában. Amennyiben a tanúsítás IKT-folyamatokra is kiterjed, az IKT-termék vagy IKT-szolgáltatás tervezésére, fejlesztésére és karbantartására szolgáló folyamatot is műszaki felülvizsgálatnak kell alávetni. Amikor egy európai kiberbiztonsági tanúsítási rendszer megfelelőségi önértékelést ír elő, elegendőnek kell tekinteni, ha az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat gyártója vagy nyújtója elvégezte az IKT-terméknek, az IKT-szolgáltatásnak vagy az IKT-folyamatnak a tanúsítási rendszer követelményeinek való megfelelésére vonatkozó önértékelést.

(89) A „jelentős” megbízhatósági szint esetében az értékelésnek – az „alap” megbízhatósági szint követelményein felül – legalább annak ellenőrzésére kell kiterjednie, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat biztonsági funkciói megfelelnek-e a műszaki dokumentációnak.

(90) A „magas” megbízhatósági szint esetében az értékelésnek – a „jelentős” megbízhatósági szint követelményein felül – legalább olyan hatékonysági tesztet kell tartalmaznia, amely felméri, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat biztonsági funkciói ellenállóak-e a jelentős szakértelemmel és erőforrásokkal rendelkező személyek által végrehajtott kifinomult kibertámadásokkal szemben.

(91) Az európai kiberbiztonsági tanúsítás és az uniós megfelelőségi nyilatkozat igénybevételének továbbra is önkéntes alapon kell történnie, kivéve ha az uniós jog vagy az uniós joggal összhangban elfogadott tagállami jog ettől eltérően rendelkezik. Összehangolt uniós jog hiányában a tagállamok az (EU) 2015/1535 európai parlamenti és tanácsi irányelvvel[1] összhangban elfogadhatnak valamely európai kiberbiztonsági tanúsítási rendszer keretében kötelező tanúsítást előíró nemzeti műszaki szabályokat. A tagállamok a közbeszerzésekkel és a 2014/24/EU európai parlamenti és tanácsi irányelvvel[2] összefüggésben is igénybe vehetik az európai kiberbiztonsági tanúsítást.

---

[1] Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (HL L 241., 2015.9.17.).

[2] Az Európai Parlament és a Tanács 2014/24/EU irányelve (2014. február 26.) a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

(92) Az Unió kiberbiztonsági szintjének növelése érdekében a jövőben szükségessé válhat, hogy egyes területeken konkrét kiberbiztonsági követelményeket állapítsanak meg, és azok tanúsítását kötelezővé tegyék bizonyos IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok esetében. A Bizottságnak rendszeresen nyomon kell követnie, hogy az elfogadott európai kiberbiztonsági tanúsítási rendszerek milyen hatást gyakorolnak a biztonságos IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok belső piacon való elérhetőségére, valamint rendszeresen értékelnie kell, hogy az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok Unión belüli gyártói vagy nyújtói milyen mértékben alkalmazzák a tanúsítási rendszereket. Az európai kiberbiztonsági tanúsítási rendszerek hatékonyságát, és azt, hogy valamely konkrét rendszert kötelezővé kell-e tenni, a kiberbiztonsági vonatkozású uniós jogszabályok – különösen az (EU) 2016/1148 irányelv – fényében kell értékelni, az alapvető szolgáltatásokat nyújtó szereplők által használt hálózati és információs rendszerek biztonságosságát figyelembe véve.

(93) Az európai kiberbiztonsági tanúsítványoknak és az uniós megfelelési nyilatkozatoknak segítenie kell a végfelhasználókat, hogy tájékozott döntéseket tudjanak hozni. A tanúsított IKT-termékekhez, IKT-szolgáltatásokhoz vagy IKT-folyamatokhoz, valamint az olyan IKT-termékekhez, IKT-szolgáltatásokhoz vagy IKT-folyamatokhoz amelyek vonatkozásában uniós megfelelési nyilatkozatot állítottak ki olyan strukturált információkat kell mellékelni, amely a várható végfelhasználóktól műszaki szintjéhez igazodik. Minden ilyen információnak rendelkezésre kell állnia online, valamint adott esetben fizikai formában. A végfelhasználó számára hozzáférést kell biztosítani a tanúsítási rendszer hivatkozási számára, a megbízhatósági szintre, az IKT-termékekhez, IKT-szolgáltatásokhoz vagy IKT-folyamatokhoz kapcsolódó kiberbiztonsági kockázatok leírására és a kibocsátó hatóságra vagy szervezetre vonatkozó információhoz, vagy lehetővé kell tenni számára az európai kiberbiztonsági tanúsítvány egy másolati példányának megszerzését. Ezenkívül a végfelhasználót tájékoztatni kell az IKT-termékek, IKT-szolgáltatások vagy IKT- folyamatok gyártója vagy a szolgáltatója kiberbiztonságra vonatkozó támogatási politikájáról, vagyis arról, hogy a végfelhasználó mennyi ideig számíthat arra, hogy kiberbiztonsági frissítéseket vagy javítóprogramokat kap. Adott esetben iránymutatással kell szolgálni arra vonatkozóan, hogy a végfelhasználó milyen lépéseket vagy beállításokat végezhet el az IKT-termék vagy az IKT-szolgáltatás kiberbiztonságának fenntartása vagy javítása érdekében, valamint tájékoztatni kell az egyedüli kapcsolattartó pont elérhetőségéről, amelynél kibertámadás esetén bejelentést tehet és támogatást kaphat (az automatikus bejelentésen túlmenően). Ezeknek az információknak elérhetőnek kell lenniük egy, az európai kiberbiztonsági tanúsítási rendszerekről információkat nyújtó honlapon, és azokat rendszeresen frissíteni kell.

(94) E rendelet céljainak elérése és a belső piac széttagoltságának elkerülése érdekében az európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termékekre, IKT-szolgáltatásokra vagy IKT-folyamatokra vonatkozó nemzeti kiberbiztonsági tanúsítási rendszerek és eljárások a Bizottság által végrehajtási jogi aktusokban meghatározott időponttól kezdve joghatásukat vesztik. Emellett a tagállamok nem vezethetnek be olyan IKT-termékekre, IKT-szolgáltatásokra vagy IKT-folyamatokra vonatkozó új nemzeti kiberbiztonsági tanúsítási rendszereket, amelyek már valamely létező európai kiberbiztonsági tanúsítási rendszer hatálya alá tartoznak. A tagállamokat ugyanakkor semmi nem akadályozhatja abban, hogy nemzetbiztonsági célokra nemzeti kiberbiztonsági tanúsítási rendszereket vezessenek be vagy tartsanak fenn. A tagállamoknak minden esetben tájékoztatniuk kell a Bizottságot és az európai kiberbiztonsági tanúsítási csoportot, ha szándékukban áll egy új nemzeti kiberbiztonsági tanúsítási rendszer bevezetése. A Bizottságnak és az európai kiberbiztonsági tanúsítási csoportnak értékelnie kell, az új nemzeti kiberbiztonsági tanúsítási rendszernek a belső piac megfelelő működésére gyakorolt hatását, valamint hogy fennáll-e stratégiai érdek annak indítványozására, hogy ahelyett egy európai kiberbiztonsági tanúsítási rendszert alkalmazzanak.

(95) Az európai kiberbiztonsági tanúsítási rendszerek hozzá kívánnak járulni az Unióban alkalmazott kiberbiztonsági gyakorlatok összehangolásához. Hozzá kell járulniuk az Unión belüli kiberbiztonsági szint növeléséhez. Az európai kiberbiztonsági tanúsítási rendszerek tervezése során figyelembe kell venni és lehetővé kell tenni új innovációk kidolgozását a kiberbiztonság terén.

(96) Az európai kiberbiztonsági tanúsítási rendszereknek figyelembe kell venniük az aktuális szoftver- és hardverfejlesztési módszereket, és különösen a gyakori szoftver- és firmware-frissítéseknek az egyes európai kiberbiztonsági tanúsítványokra gyakorolt hatását. Az európai kiberbiztonsági tanúsítási rendszerekben meg kell határozni, hogy milyen körülmények esetén kell egy frissítés miatt újratanúsítani egy IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot, illetve leszűkíteni egy adott európai kiberbiztonsági tanúsítvány hatályát, figyelembe véve a frissítés bármely lehetséges negatív hatását az adott tanúsítvány biztonsági követelményeinek teljesítésére.

(97) Amint egy európai kiberbiztonsági tanúsítási rendszer elfogadásra kerül, az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok gyártói vagy nyújtói számára lehetővé kell tenni, hogy egy általuk választott megfelelőségértékelő szervezethez az Unió területén belül bárhol benyújthassák IKT-termékeik vagy IKT-szolgáltatásaik tanúsítására irányuló kérelmüket. A megfelelőségértékelő szervezeteket egy akkreditáló testületnek kell akkreditálnia, amennyiben azok megfelelnek az e rendeletben meghatározott bizonyos különös követelményeknek. Az akkreditáció legfeljebb öt évre szólhat, és azonos feltételek mellett megújítható, feltéve, hogy a megfelelőségértékelő szervezet még mindig teljesíti a követelményeket. A nemzeti 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 megsérti ezt a rendeletet.

(98) Ha a nemzeti jogszabályokban olyan nemzeti szabványokra történik hivatkozás, amelyek egy európai kiberbiztonsági tanúsítási rendszer hatálybalépése okán joghatásukat vesztették, az zavaró lehet. A tagállamoknak ezért tükrözniük kell nemzeti jogszabályaikban az európai kiberbiztonsági tanúsítási rendszerek elfogadását.

(99) Az Unióban alkalmazott szabványok egyenértékűségének elérése, a kölcsönös elismerés előmozdítása, valamint az európai kiberbiztonsági tanúsítványok és az uniós megfelelőségi nyilatkozatok általános elfogadottságának elősegítése érdekében kölcsönös felülvizsgálati rendszert kell kialakítani a nemzeti kiberbiztonsági tanúsító hatóságok között. A kölcsönös felülvizsgálatnak olyan eljárásokra kell kiterjednie, amelyek az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok európai kiberbiztonsági tanúsítványoknak való megfelelésének felügyeletére, az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok megfelelőségi önértékelést végző gyártói vagy nyújtói kötelezettségeinek nyomon követésére, a megfelelőségértékelő szervezetek nyomon követésére és arra irányulnak, hogy a „magas” megbízhatósági szintre szóló tanúsítványokat kiállító szervezetek személyzetének szakértelme megfelelő-e. A Bizottságnak – végrehajtási jogi aktusok útján – legalább öt évre szóló kölcsönös felülvizsgálati tervet kell létrehoznia, valamint meg kell határoznia a kölcsönös felülvizsgálati rendszer működésére vonatkozó kritériumokat és módszereket.

(100) Egyes európai kiberbiztonsági tanúsítási rendszerek – az európai kiberbiztonsági tanúsítási keretrendszeren belül az összes nemzeti kiberbiztonsági tanúsító hatóságra kiterjedően létrehozandó általános kölcsönös felülvizsgálati rendszer sérelme nélkül – magukban foglalhatnak olyan kölcsönös értékelési mechanizmust, amely az adott rendszerek keretében IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra „magas” megbízhatósági szintű európai kiberbiztonsági tanúsítványokat kiállító szervezetek között alkalmazandó. Az európai kiberbiztonsági tanúsítási csoportnak támogatnia kell az ilyen kölcsönös értékelési mechanizmusok végrehajtását. Az ilyen kölcsönös értékelés során különösen azt kell értékelni, hogy az érintett szervezetek harmonizált módon végzik-e feladataikat, és az kiterjedhet a jogorvoslati mechanizmusokra is. A kölcsönös értékelés eredményét nyilvánosan hozzáférhetővé kell tenni. Az érintett szervezetek megfelelő intézkedéseket hozhatnak annak érdekében, hogy kiigazítsák gyakorlataikat és szakismereteiket.

(101) A tagállamoknak ki kell jelölniük egy vagy több nemzeti kiberbiztonsági tanúsító hatóságot, az e rendeletből eredő követelményeknek való megfelelés felügyelete érdekében. Nemzeti kiberbiztonsági tanúsító hatóság lehet már létező vagy újonnan létrehozott hatóság is. A tagállamok számára lehetővé kell tenni továbbá, hogy egy másik tagállammal való megállapodás alapján az adott másik tagállam területén egy vagy több nemzeti kiberbiztonsági tanúsító hatóságot jelöljenek ki.

(102) A nemzeti kiberbiztonsági hatóságnak különösen, hogy nyomon kell követnie és be kell tartatnia az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok illetékességi területükön letelepedett gyártóinak vagy nyújtóinak az uniós megfelelőségi nyilatkozathoz kapcsolódó kötelezettségeit, segítenie kell – szakértelmével és megfelelő információkkal – a nemzeti akkreditáló szervezeteket a megfelelőségértékelő szervezetek tevékenységeinek nyomon követésében és felügyeletében, engedélyeznie kell a megfelelőségértékelő szervezeteknek, hogy ellássák feladataikat, amennyiben ezek a szervezetek teljesítik a valamely európai kiberbiztonsági tanúsítási rendszerben meghatározott kiegészítő követelményeket, továbbá figyelemmel kell kísérnie a kiberbiztonsági tanúsítás területén bekövetkező releváns fejleményeket. A nemzeti kiberbiztonsági tanúsító hatóságoknak kezelniük kell az általuk kiadott európai kiberbiztonsági tanúsítványok, illetve a megfelelőségértékelő szervezetek által kiadott európai kiberbiztonsági tanúsítványok kapcsán természetes vagy jogi személyek által benyújtott panaszokat, amennyiben az említett tanúsítványok „magas” megbízhatósági szintre vonatkoznak, megfelelő mértékben ki kell vizsgálniuk a panasz tárgyát, és észszerű időn belül tájékoztatniuk kell a panaszost a vizsgálat előrehaladásáról és eredményéről. Ezen túlmenően a nemzeti kiberbiztonsági tanúsító hatóságoknak együtt kell működniük a többi nemzeti kiberbiztonsági tanúsító hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, hogy bizonyos IKT-termékek, IKT-szolgáltatások és IKT-folyamatok lehetséges, hogy nem felelnek meg e rendelet vagy egyes európai kiberbiztonsági tanúsítási rendszerek követelményeinek. A Bizottságnak elő kell segítenie ezt az információcserét egy általános elektronikus információs támogató rendszer rendelkezésre bocsátásával, mint amilyen például a piacfelügyeleti információs és kommunikációs rendszer (ICSMS) és az Európai Uniós Gyors Tájékoztatási Rendszer (RAPEX), amelyeket a piacfelügyeleti hatóságok a 765/2008/EK rendeletnek megfelelően már használnak.

(103) 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. Az európai kiberbiztonsági tanúsítási csoport fő feladata, hogy tanácsot adjon és segítséget nyújtson a Bizottságnak az európai kiberbiztonsági tanúsítási keretrendszer következetes végrehajtásának és alkalmazásának biztosítására irányuló munkája során, segítse az ENISA-t és szorosan együttműködjön vele a javasolt kiberbiztonsági tanúsítási rendszerek kidolgozásában, kellően indokolt esetekben felkérje az ENISA-t javasolt kiberbiztonsági tanúsítási rendszer kidolgozására, valamint az ENISA-nak címzett véleményeket fogadjon el a javasolt tanúsítási rendszerekről és a Bizottságnak címzett véleményeket fogadjon el a létező európai kiberbiztonsági tanúsítási rendszerek fenntartásával és felülvizsgálatával kapcsolatban. Az európai kiberbiztonsági tanúsítási csoportnak elő kell segítenie a bevált gyakorlatok és a szakismeretek cseréjét a megfelelőségértékelő szervezetek engedélyezéséért és az európai kiberbiztonsági tanúsítványok kiadásáért felelős különféle nemzeti kiberbiztonsági tanúsító hatóságok között.

(104) A jövőbeli európai kiberbiztonsági tanúsítási rendszerek ismertebbé és elfogadottabbá tétele érdekében az Bizottság általános vagy ágazatspecifikus kiberbiztonsági iránymutatásokat adhat ki, például a helyes kiberbiztonsági gyakorlatokról vagy a felelős kiberbiztonsági magatartásról, kiemelve a tanúsított IKT-termékek, IKT-szolgáltatások és IKT-folyamatok használatának kedvező hatását.

(105) A kereskedelem további megkönnyítése érdekében, továbbá az IKT-ellátási láncok globális dimenziójának tudatában az Unió az Európai Unió működéséről szóló szerződés (EUMSZ) 218. cikkével összhangban kölcsönös elismerési megállapodásokat köthet az európai kiberbiztonsági tanúsítványokra vonatkozóan. A Bizottság az ENISA és az európai kiberbiztonsági tanúsítási csoport tanácsának figyelembevételével ajánlást tehet ilyen irányú tárgyalások megkezdésére. Minden egyes európai kiberbiztonsági tanúsítási rendszeren belül egyedi feltételeket kell meghatározni a harmadik országokkal kötendő említett kölcsönös elismerési megállapodásokra vonatkozóan.

(106) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek[1] megfelelően kell gyakorolni.

(107) Vizsgálóbizottsági eljárást kell alkalmazni az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok európai kiberbiztonsági tanúsítási rendszereire, az ENISA általi vizsgálat lefolytatásának szabályaira, a nemzeti kiberbiztonsági tanúsító hatóságok kölcsönös felülvizsgálatára vonatkozó tervre, valamint az akkreditált megfelelőségértékelő szervezeteknek a nemzeti kiberbiztonsági tanúsító hatóságok általi Bizottságnak történő bejelentése körülményeire, formátumára és eljárására vonatkozó végrehajtási jogi aktusok elfogadására.

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

(108) Az ENISA működését rendszeres és független értékelésnek kell alávetni. Az értékelés során figyelembe kell az ENISA célkitűzéseit, munkamódszereit, és feladatai – különösen az uniós szintű operatív együttműködéssel kapcsolatos feladatai – relevanciáját. Ezen értékelésnek ki kell terjednie az európai kiberbiztonsági tanúsítási keretrendszer hatásának, eredményességének és hatékonyságának értékelésére is. Felülvizsgálat esetén a Bizottságnak értékelnie kell, hogy miként lehetne megerősíteni az ENISA azon szerepét, hogy hivatkozási alapként szolgál a tanácsadás és a szakértelem terén, és értékelnie kell azt a lehetőséget is, hogy az ENISA szerepet kapjon a harmadik országbeli olyan IKT-termékek, IKT-szolgáltatások és IKT-folyamatok értékelésének támogatásában, amelyek nem felelnek meg az uniós szabályoknak, amennyiben ezen termékek, szolgáltatások és folyamatok belépnek az Unióba.

(109) Mivel e rendelet céljait a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban e célok jobban megvalósíthatók, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés (EUSZ) 5. cikkében foglalt szubszidiaritási elvnek megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl a e célok eléréséhez szükséges mértéket.

(110) Az 526/2013/EU rendeletet hatályon kívül kell helyezni,

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 kiberellenálló képesség és a kiberbiztonságba vetett bizalom magas szintjének elérése érdekében ez a rendelet megállapítja:

a) az ENISA (a továbbiakban: az Európai Uniós Kiberbiztonsági Ügynökség) célkitűzéseit, feladatait és szervezeti vonatkozásait; valamint

b) az európai kiberbiztonsági tanúsítási rendszerek létrehozásának keretrendszerét az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok megfelelő kiberbiztonsági szintjének az Unióban történő biztosítása céljából, valamint abból a célból, hogy megakadályozza a belső piac széttagoltságát az Unión belüli kiberbiztonsági tanúsítási rendszerek tekintetében.

Az első albekezdés b) pontjában említett keretrendszer az egyéb uniós jogi aktusokban az önkéntes vagy kötelező tanúsításra vonatkozóan előírt különös rendelkezések sérelme nélkül alkalmazandó.

(2) Ez a rendelet nem érinti a közbiztonsággal, a honvédelemmel és a nemzetbiztonsággal kapcsolatos tevékenységekkel, valamint az állam büntetőjog területén folytatott tevékenységeivel kapcsolatos tagállami hatásköröket.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „kiberbiztonság”: azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek;

2. „hálózati és információs rendszer”: az (EU) 2016/1148 irányelv 4. cikkének 1. pontjában meghatározott hálózati és információs rendszer;

3. „a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia”: az (EU) 2016/1148 irányelv 4. cikkének 3. pontjában meghatározott hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia;

4. „alapvető szolgáltatásokat nyújtó szereplő”: az (EU) 2016/1148 irányelv 4. cikkének 4. pontjában meghatározott alapvető szolgáltatásokat nyújtó szereplő;

5. „digitális szolgáltató”: az (EU) 2016/1148 irányelv 4. cikkének 6. pontjában meghatározott digitális szolgáltató;

6. „biztonsági esemény”: az (EU) 2016/1148 irányelv 4. cikkének 7. pontjában meghatározott biztonsági esemény;

7. „biztonsági esemény kezelése”: az (EU) 2016/1148 irányelv 4. cikkének 8. pontjában meghatározott biztonsági esemény kezelése;

8. „kiberfenyegetés”: bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat;

9. „európai kiberbiztonsági tanúsítási rendszer”: adott IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok tanúsítására vagy megfelelőségértékelésére alkalmazandó szabályok, műszaki követelmények, szabványok és eljárások uniós szinten meghatározott átfogó rendszere;

10. „nemzeti kiberbiztonsági tanúsítási rendszer”: az adott tanúsítási rendszer hatálya alá tartozó IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására vagy megfelelőségértékelésére alkalmazandó, valamely nemzeti hatóság által kidolgozott és elfogadott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere;

11. „európai kiberbiztonsági tanúsítvány”: az illetékes szerv által kibocsátott dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy megfelel-e valamely európai kiberbiztonsági tanúsítási rendszer konkrét biztonsági követelményeknek;

12. „IKT-termék ”: valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja;

13. „IKT-szolgáltatás”: olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll;

14. „IKT-folyamat”: valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége;

15. „akkreditáció”: a 765/2008/EK rendelet 2. cikkének 10. pontjában meghatározott akkreditálás;

16. „nemzeti akkreditáló testület”: a 765/2008/EK rendelet 2. cikkének 11. pontjában meghatározott nemzeti akkreditáló testület;

17. „megfelelőségértékelés”: a 765/2008/EK rendelet 2. cikkének 12. pontjában meghatározott megfelelőségértékelés;

18. „megfelelőségértékelő szervezet”: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezet;

19. „szabvány”: az 1025/2012/EU rendelet 2. cikkének 1. pontjában meghatározott szabvány,

20. „műszaki előírás”: olyan dokumentum, amely megadja, hogy valamely IKT-terméknek, IKT-szolgáltatásnak vagy IKT-folyamatnak milyen műszaki követelményeket kell teljesítenie vagy arra milyen megfelelőségértékelési eljárások vonatkoznak;

21. „megbízhatósági szint”: az az iránti bizalom alapja, hogy valamely IKT-termék, IKT-szolgáltatás vagy IKT-folyamat teljesíti egy adott európai kiberbiztonsági tanúsítási rendszer biztonsági követelményeit, megmutatja, hogy valamely IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot milyen szinten értékeltek, de a megbízhatósági szint nem méri az érintett IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok biztonságát.

22. „megfelelőségi önértékelés”: az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok gyártói vagy szolgáltatói által végzett olyan tevékenység, amely értékeli, hogy az adott IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok teljesítik-e egy adott európai kiberbiztonsági tanúsítási rendszer biztonsági követelményeit.

II. CÍM
ENISA (AZ EURÓPAI UNIÓS KIBERBIZTONSÁGI ÜGYNÖKSÉG)

I. fejezet
Megbízatás és célkitűzések

3. cikk

Megbízatás

(1) Az ENISA-nak el kell végeznie az e rendelet által ráruházott feladatokat, az egységesen magas szintű kiberbiztonság elérése céljából az egész Unióban, többek között annak révén, hogy aktív támogatást nyújt a tagállamoknak, valamint az uniós intézményeknek, szerveknek és hivataloknak a kiberbiztonság javításához. Az ENISA-nak az uniós intézmények, szervek és hivatalok, valamint egyéb uniós érdekelt felek számára a kiberbiztonsággal kapcsolatos tanácsadás és szakértelem referenciapontjaként kell szolgálnia.

Az ENISA-nak az e rendelet által ráruházott feladatok ellátásával hozzá kell járulnia a belső piac széttagoltságának csökkentéséhez.

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

(3) Feladatainak ellátása során az ENISA-nak függetlenül kell eljárnia, és egyúttal el kell kerülnie a tagállamok tevékenységeivel való párhuzamosságokat, figyelembe véve a tagállamokban meglévő szakértelmet.

(4) Az ENISA-nak ki kell építenie saját, az e rendelet által ráruházott feladatok ellátásához szükséges erőforrásait, ideértve a műszaki és a humán képességeket és készségeket is.

4. cikk

Célkitűzések

(1) Az ENISA-nak kiberbiztonsági szakértői központként kell működnie függetlensége, az általa biztosított tanácsadás, segítségnyújtás és információk tudományos és műszaki minősége, működési eljárásainak átláthatósága, működési módszerei, valamint a feladatai ellátásában tanúsított gondosság révén.

(2) Az ENISA-nak segítséget kell nyújtania az uniós intézmények, szervek és hivatalok, valamint a tagállamok számára a kiberbiztonsággal kapcsolatos uniós szakpolitikák, többek között a kiberbiztonsággal kapcsolatos ágazati szakpolitikák kidolgozásában és végrehajtásában.

(3) Az ENISA-nak támogatnia kell az Unión belüli kapacitásépítést és felkészültséget azáltal, hogy segítséget nyújt az uniós intézmények, szervek és hivatalok, valamint a tagállamok, illetve a köz- és a magánszféra érdekelt felei számára hálózati és információs rendszereik védelmének fokozása, a kiberellenálló képesség és a kiberbiztonsági eseményekre való reagálási kapacitások fejlesztése és javítása, valamint a kiberbiztonsági készségek és kompetenciák fejlesztése érdekében.

(4) Az ENISA-nak a kiberbiztonsággal kapcsolatos kérdésekben elő kell mozdítania az uniós szintű együttműködést – beleértve az információmegosztást – és koordinációt a tagállamok, az uniós intézmények, szervek és hivatalok, valamint a köz- és a magánszféra releváns érdekelt felei között.

(5) Az ENISA-nak hozzá kell járulnia az uniós szintű kiberbiztonsági képességek növeléséhez annak érdekében, hogy támogassa a kiberfenyegetések megelőzése és az azokra való reagálás terén tett tagállami intézkedéseket, különösen a határokon átnyúló biztonsági események esetében.

(6) Az ENISA-nak elő kell mozdítania az európai kiberbiztonsági tanúsítás használatát a belső piac széttagoltságának elkerülése érdekében. Az ENISA-nak hozzá kell járulnia egy európai kiberbiztonsági tanúsítási keretrendszernek az e rendelet III. címével összhangban történő létrehozásához és fenntartásához, annak érdekében, hogy a kiberbiztonság tekintetében átláthatóbbá váljon, hogy mennyire megbízhatóak az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok, megerősítve ezzel a digitális belső piacba és annak versenyképességébe vetett bizalmat.

(7) Az ENISA-nak elő kell segítenie azt, hogy a polgárok, a szervezetek és a vállalkozások a kiberbiztonsághoz kapcsolódó kérdések – ideértve a kiberhigiéniát és a kiberbiztonsági jártasságot is – tekintetében nagy fokú kiberbiztonsági tudatossággal rendelkezzenek.

II. fejezet
Feladatok

5. cikk

Az uniós szakpolitika és jogszabályok kidolgozása és végrehajtása

Az ENISA-nak az alábbiakkal kell hozzájárulnia az uniós szakpolitika és jogszabályok kidolgozásához és végrehajtásához:

1. segítségnyújtás és tanácsadás a kiberbiztonság területére vonatkozó uniós szakpolitika és jogszabályok, valamint a kiberbiztonsági kérdéseket magukban foglaló ágazatspecifikus szakpolitikai és jogalkotási kezdeményezések kidolgozásához és felülvizsgálatához, különösen független vélemény és elemzések nyújtása, valamint előkészítő munka révén;

2. segítségnyújtás a tagállamok számára a kiberbiztonsággal kapcsolatos uniós szakpolitika és jogszabályok következetes végrehajtásához, különösen 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. segítségnyújtás a tagállamok, valamint az uniós intézmények, szervek és hivatalok számára olyan kiberbiztonsági szakpolitikák kidolgozásához és előmozdításához, amelyek a nyílt internet nyilvános alkotóelemei általános elérhetőségének vagy integritásának fenntartásához kapcsolódnak;

4. szakértelemmel és segítségnyújtással való hozzájárulás az (EU) 2016/1148 irányelv 11. cikke szerinti együttműködési csoport munkájához;

5. az alábbiak támogatása:

   a) az elektronikus azonosítás és a bizalmi szolgáltatások területére vonatkozó uniós szakpolitika kidolgozása és végrehajtása, különösen tanácsadással és műszaki iránymutatásokkal, valamint a bevált gyakorlatok illetékes hatóságok közötti cseréjének elősegítésével;

   b) az elektronikus hírközlés magasabb biztonsági szintjének előmozdítása, többek között tanácsadással és szakértelemmel, valamint a bevált gyakorlatok illetékes hatóságok közötti cseréjének elősegítésével;

   c) az adatvédelemhez és a magánélet tiszteletben tartásához kapcsolódó uniós szakpolitikák és jogszabályok egyes kiberbiztonsági vonatkozásainak végrehajtása a tagállamok tekintetében, többek között – kérésre – az Európai Adatvédelmi Testület részére történő tanácsadással;

6. az uniós szakpolitikai tevékenységek rendszeres felülvizsgálatához nyújtott támogatás a vonatkozó jogi keretrendszer végrehajtásának állásáról szóló éves jelentés előkészítésével, a következők tekintetében:

   a) az egyedüli kapcsolattartó pontok által az (EU) 2016/1148 irányelv 10. cikkének (3) bekezdése alapján az együttműködési csoportnak nyújtott, a tagállami biztonságiesemény-bejelentésekre vonatkozó információ;

b) a felügyeleti szervek által a 910/2014/EU európai parlamenti és tanácsi rendelet[1] 19. cikkének (3) bekezdése alapján az ENISA-nak nyújtott, a bizalmi szolgáltatóktól beérkezett, a biztonság megsértésére és az adatok sértetlenségének megszűnésére vonatkozó bejelentések összefoglalója;

c) az illetékes hatóságok által az (EU) 2018/1972 irányelv 40. cikke alapján az ENISA-nak benyújtott, a nyilvános elektronikus hírközlő hálózatokat üzemeltető vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók által tett biztonságiesemény-bejelentések.

6. cikk

Kapacitásépítés

(1) Az ENISA-nak támogatnia kell:

a) a tagállamokat a kiberfenyegetések és a biztonsági események megelőzésének, észlelésének és elemzésének, valamint az ezekre való reagálási képességnek a javítására irányuló erőfeszítéseikben, ismereteket és szaktudást biztosítva számukra;

b) a tagállamokat és az uniós intézményeket, szerveket és hivatalokat, hogy önkéntes módon sebezhetőségfeltárási politikákat dolgozzanak ki és hajtsanak végre;

[1] Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

c) az uniós intézményeket, szerveket és hivatalokat a kiberfenyegetések és a biztonsági események megelőzésének, észlelésének és elemzésének, valamint az ezekre való reagálási képességnek a javítására irányuló erőfeszítéseikben, különösen a CERT-EU megfelelő támogatása révén;

d) kérés esetén a tagállamokat a nemzeti CSIRT-ek továbbfejlesztésében az (EU) 2016/1148 irányelv 9. cikkének (5) bekezdése alapján;

e) kérés esetén a tagállamokat a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia kidolgozásában az (EU) 2016/1148 irányelv 7. cikkének (2) bekezdése alapján, valamint az említett stratégiák terjesztésének előmozdításában és azok Unióban történő végrehajtása figyelemmel kísérésében a bevált gyakorlatok előmozdítása érdekében;

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

g) a nemzeti és az uniós CSIRT-eket képességeik fejlesztésében, többek között a párbeszéd és az információcsere előmozdítása révén, annak biztosítása érdekében, hogy a technika legutóbbi állására tekintettel minden CSIRT rendelkezzen közös minimumképességekkel, és a bevált gyakorlatok szerint működjön;

h) a tagállamokat a 7. cikk (5) bekezdésében említett, uniós szintű rendszeres és legalább kétévenkénti kiberbiztonsági gyakorlatok megszervezésével, valamint a gyakorlatok értékelésén és a levont tanulságokon alapuló szakpolitikai ajánlások kidolgozásával;

i) a releváns állami szerveket a kiberbiztonsággal kapcsolatos képzések kínálásával, adott esetben az érdekelt felekkel együttműködve;

j) az együttműködési csoportot, a bevált gyakorlatok megosztásában, különösen az alapvető szolgáltatásokat nyújtó szereplők tagállamok általi azonosítása tekintetében – beleértve a határokon átnyúló függőségeket, a biztonsági kockázatokra és biztonsági eseményekre vonatkozóan is – az (EU) 2016/1148 irányelv 11. cikke (3) bekezdése l) pontja alapján.

(2) Az ENISA-nak támogatnia kell az ágazatokon belüli és az azok közötti információmegosztást, különösen az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokban, azáltal, hogy rendelkezésre bocsátja a rendelkezésre álló eszközökkel és eljárásokkal, valamint az információk megosztásával kapcsolatos szabályozási kérdések kezelésének mikéntjével kapcsolatban bevált gyakorlatokat és iránymutatást nyújt azokra vonatkozóan.

7. cikk

Uniós szintű operatív együttműködés

(1) Az ENISA-nak támogatnia kell a tagállamok, az uniós intézmények, szervek és hivatalok közötti, valamint az érdekeltek közötti operatív együttműködést.

(2) Az ENISA-nak operatív szinten kell együttműködnie és szinergiákat kell kialakítania az uniós intézményekkel, szervekkel és hivatalokkal, 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 know-how és a bevált gyakorlatok megosztása;

b) kiberbiztonsággal kapcsolatos releváns kérdésekkel kapcsolatos tanácsadás nyújtása és iránymutatások kiadása;

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 ENISA-nak kell biztosítania a CSIRT-ek hálózatának titkárságát, és ebben a minőségében aktívan támogatnia kell a hálózat tagjai közötti információmegosztást és együttműködést.

(4) Az ENISA-nak támogatnia kell a tagállamokat a CSIRT-ek hálózatán belüli operatív együttműködésben a következők révén:

a) a biztonsági események megelőzésére, észlelésére és az azokra való reagálásra irányuló képességeik javításának mikéntjével kapcsolatos tanácsadás, valamint – egy vagy több tagállam kérésére – egy adott kiberfenyegetéssel kapcsolatos tanácsadás;

b) segítségnyújtás egy vagy több tagállam kérésére a jelentős vagy lényeges hatással járó biztonsági események értékelésében szakértelem biztosítása, valamint ezen biztonsági események műszaki kezelésének megkönnyítése révén, többek között különösen a releváns információk és a műszaki megoldások tagállamok közötti önkéntes megosztásának támogatása révén;

c) a sebezhetőségek és a biztonsági események elemzése a nyilvánosan elérhető információk, vagy a tagállamok által önkéntes alapon e célból szolgáltatott információk alapján; és

d) egy vagy több tagállam kérésére támogatás az (EU) 2016/1148 irányelv értelmében vett jelentős vagy lényeges hatású biztonsági események utólagos műszaki vizsgálatához.

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

(5) Az ENISA-nak rendszeresen kiberbiztonsági gyakorlatokat kell szerveznie uniós szinten, és kérésre támogatást kell biztosítania a tagállamoknak, valamint az uniós intézményeknek, szerveknek és hivataloknak kiberbiztonsági gyakorlatok szervezéséhez. Az ilyen kiberbiztonsági uniós szintű gyakorlatok műszaki, operatív vagy stratégiai elemeket tartalmazhatnak. Az ENISA-nak kétévente szerveznie kell egy nagyszabású átfogó gyakorlatot.

Az ENISA-nak továbbá adott esetben hozzá kell járulnia és segítséget kell nyújtania az ágazati kiberbiztonsági gyakorlatok megszervezéséhez a releváns szervezetekkel együtt, amelyek részt vesznek az uniós szintű kiberbiztonsági gyakorlatokban is.

(6) Az ENISA-nak a tagállamokkal szoros együttműködésben rendszeres és részletes uniós kiberbiztonsági műszaki helyzetjelentést kell készítenie a biztonsági eseményekről és a kiberfenyegetésekről nyilvánosan hozzáférhető információk, saját elemzése, valamint többek között a tagállamok CSIRT-jei, az (EU) 2016/1148 irányelvvel létrehozott egyedüli kapcsolattartó pontok (mindkettő esetében önkéntes alapon), az EC3 és a CERT-EU által rendelkezésre bocsátott jelentések alapján.

(7) Az ENISA-nak 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) a nyilvánosan hozzáférhető vagy az önkéntes alapon megosztott, nemzeti forrásokból származó jelentések összesítése és elemzése a közös helyzetismeret kialakításához való hozzájárulás céljából;

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

c) kérésre a biztonsági események vagy válságok műszaki kezelésének elősegítése, többek között különösen a műszaki megoldások tagállamok közötti önkéntes megosztásának támogatása révén;

d) az uniós intézmények, szervek és hivatalok, valamint kérésükre a tagállamok támogatása az említett biztonsági eseményekkel vagy válságokkal kapcsolatos nyilvános kommunikációban;

e) az említett biztonsági eseményekre vagy válságokra való reagálást célzó együttműködési tervek tesztelése uniós szinten, és kérésükre a tagállamok támogatása ezen tervek nemzeti szintű tesztelésében.

8. cikk

Piac, kiberbiztonsági tanúsítás, valamint szabványosítás

(1) Az ENISA-nak támogatnia kell és elő kell mozdítania az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok e rendelet III. címében meghatározott kiberbiztonsági tanúsítására vonatkozó uniós szakpolitika kidolgozását és végrehajtását, az alábbiak révén:

a) a kapcsolódó területeken folytatott szabványosítás fejleményeinek folyamatos nyomon követése és az európai kiberbiztonsági tanúsítási rendszerek fejlesztéséhez használandó megfelelő műszaki előírásokra vonatkozó ajánlások az 54. cikk (1) bekezdésének c) pontja alapján az olyan esetekre, amikor nem állnak rendelkezésre szabványok;

b) javaslati európai kiberbiztonsági tanúsítási rendszerek (a továbbiakban: javasolt tanúsítási rendszerek) kidolgozása IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozóan a 49. cikkel összhangban;

c) az elfogadott európai kiberbiztonsági tanúsítási rendszerek értékelése a 49. cikk (8) bekezdésével összhangban;

d) részvétel az 59. cikk (4) bekezdése szerinti kölcsönös felülvizsgálatban;

e) a Bizottság támogatása az európai kiberbiztonsági tanúsítási csoport titkárságának a 62. cikk (5) bekezdése alapján történő biztosításában.

(2) Az érdekelt felek kiberbiztonsági tanúsítási csoportjának titkárságát a 22. cikk (4) bekezdése alapján az ENISA biztosítja.

(3) Az ENISA-nak az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kiberbiztonsági követelményeire vonatkozó iránymutatásokat kell összeállítania és közzétennie, valamint bevált gyakorlatokat kialakítania, formális, strukturált és átlátható módon együttműködve a nemzeti kiberbiztonsági tanúsító hatóságokkal és az ágazattal.

(4) Az ENISA-nak hozzá kell járulnia az értékelési és tanúsítási folyamattal kapcsolatos kapacitásépítéshez iránymutatások kidolgozásával és kibocsátásával, valamint kérésükre a tagállamoknak nyújtott támogatással.

(5) Az ENISA-nak elő kell segítenie a kockázatkezelésre és az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok biztonságára vonatkozó európai és nemzetközi szabványok kidolgozását.

(6) Az ENISA-nak a tagállamokkal és az ágazattal együttműködésben tanácsot kell adnia és iránymutatásokat kell készítenie az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó biztonsági követelményekkel kapcsolatos műszaki területekre, valamint a már létező szabványokra – a tagállamok nemzeti szabványait is beleértve – vonatkozóan, az (EU) 2016/1148 irányelv 19. cikkének (2) bekezdése alapján.

(7) Az ENISA-nak a kiberbiztonsági piac keresleti és kínálati oldalára jellemző fő tendenciákat rendszeresen elemeznie, és ezen elemzéseket terjesztenie kell, az Unió kiberbiztonsági piacának megerősítése céljából.

9. cikk

Ismeretek és tájékoztatás

Az ENISA-nak:

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

b) el kell végeznie a kiberbiztonsági fenyegetések és események hosszú távú stratégiai elemzését a kialakulóban lévő tendenciák azonosítása és a kiberbiztonsági események megelőzésének elősegítése érdekében;

c) a tagállami hatóságok szakértőivel és a releváns érdekelt felekkel együttműködve tanácsot kell adnia, iránymutatásokat kell készítenie és 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 szolgáltatások nyújtói által használt infrastruktúrák biztonságával kapcsolatban;

d) össze kell gyűjtenie, rendszereznie kell és a nyilvánosság számára elérhetővé kell tennie egy külön erre a célra szolgáló portálon az uniós intézmények, szervek és hivatalok által, valamint az önkéntes alapon a tagállamok és a magán- és közszférabeli érdekeltek által a kiberbiztonsággal kapcsolatban rendelkezésre bocsátott információkat;

e) össze kell gyűjtenie és elemeznie kell a jelentős biztonsági eseményekkel kapcsolatos nyilvánosan hozzáférhető információkat, valamint jelentéseket kell készítenie annak érdekében, hogy Unió-szerte iránymutatást nyújtson a polgárok, a szervezetek és a vállalkozások számára.

10. cikk

Tudatosítás és oktatás

Az ENISA-nak:

a) növelnie kell a közvélemény kiberbiztonsági kockázatokkal kapcsolatos tudatosságát, és a bevált gyakorlatokról az egyedi felhasználóknak szánt iránymutatást kell nyújtania a polgárok, a szervezetek és a vállalkozások számára, többek között a kiberhigiéniát és a kiberbiztonsági jártasságot illetően;

b) rendszeres tájékoztató kampányokat kell szerveznie a tagállamokkal, az uniós intézményekkel, szervekkel és hivatalokkal, valamint az ágazati szereplőkkel együttműködve, hogy az Unión belül fokozódjon a kiberbiztonság és annak láthatósága, valamint ösztönöznie kell a széleskörű nyilvános vitát;

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

d) támogatnia kell a tagállamok közötti szorosabb koordinációt és a bevált gyakorlatok intenzívebb cseréjét a kiberbiztonsággal kapcsolatos tudatosság és a kiberbiztonsággal kapcsolatos oktatás területén.

11. cikk

Kutatás és innováció

A kutatás és az innováció tekintetében az ENISA-nak:

a) tanácsokkal kell ellátnia az uniós intézményeket, szerveket és hivatalokat, valamint a tagállamokat a tekintetben, hogy a kiberbiztonság területén milyen kutatási szükségleteknek és prioritásoknak kell eleget tenni, hogy eredményesen lehessen reagálni a jelenlegi és jövőbeli kockázatokra és kiberfenyegetésekre, beleértve az új és kialakulóban lévő információs és kommunikációs technológiákat érintőket is, és, hogy eredményesen lehessen alkalmazni a kockázatmegelőző technológiákat;

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

c) hozzá kell járulnia a kiberbiztonság területén az uniós szintű stratégiai kutatáshoz és innovációhoz.

12. cikk

Nemzetközi együttműködés

Az ENISA-nak a kiberbiztonsággal kapcsolatos kérdésekre vonatkozó nemzetközi együttműködés elősegítése érdekében hozzá kell járulnia a harmadik országokkal és nemzetközi szervezetekkel, valamint a vonatkozó nemzetközi együttműködési kereteken belül folytatandó együttműködésre irányuló uniós erőfeszítésekhez azáltal, hogy:

a) adott esetben megfigyelőként részt vesz a nemzetközi gyakorlatok szervezésében, valamint az ilyen gyakorlatok eredményeiről elemzést és jelentést készít az igazgatótanácsnak;

b) a Bizottság kérésére elősegíti a bevált módszerek cseréjét;

c) a Bizottság kérésre szakértelemmel támogatja a Bizottságot;

d) a 62. cikkel létrehozott európai kiberbiztonsági tanúsítási csoporttal együttműködve tanácsadást és támogatást nyújt a Bizottságnak a kiberbiztonsági tanúsítványok harmadik országokkal való kölcsönös elismerésére vonatkozó megállapodásokhoz kapcsolódó kérdésekben.

II. fejezet
Az ENISA felépítése

13. cikk

Az ENISA struktúrája

Az ENISA igazgatási és irányítási struktúrája a következőkből áll:

a) az igazgatótanács;

b) a felügyelőtestület;

c) az ügyvezető igazgató;

d) az ENISA tanácsadó csoportja;

e) a nemzeti kapcsolattartó tisztviselők hálózata.

1. SZAKASZ

IGAZGATÓTANÁCS

14. cikk

Az igazgatótanács összetétele

(1) Az igazgatótanács tagállamonként egy, a tagállam által kijelölt tagból és a Bizottság által kijelölt két tagból áll. Valamennyi tag szavazati joggal rendelkezik.

(2) Az igazgatótanács minden egyes tagja rendelkezik egy póttaggal. A póttag a tagot képviseli annak távollétében.

(3) Az igazgatótanács tagjait és azok póttagjait a kiberbiztonság terén meglévő tudásuk alapján kell kinevezni, a megfelelő vezetői, igazgatási és költségvetési készségeik figyelembevételével. Az igazgatótanács munkájának folytonosságát biztosítandó, a Bizottság és a tagállamok törekednek arra, hogy képviselőik ne cserélődjenek túl gyakran az igazgatótanácsban. A Bizottság és a tagállamok törekednek arra, hogy a nők és férfiak kiegyensúlyozott arányban legyenek képviselve az igazgatótanácsban.

(4) Az igazgatótanács tagjainak és azok póttagjainak hivatali ideje négy év. Ez a hivatali idő megújítható.

15. cikk

Az igazgatótanács feladatköre

(1) Az igazgatótanács:

a) meghatározza az ENISA működésének általános irányát, és biztosítja, hogy az ENISA az e rendeletben megállapított szabályoknak és elveknek megfelelően végezze tevékenységét; biztosítja továbbá, hogy az ENISA munkája összhangban legyen a tagállamok által és az Unió szintjén folytatott tevékenységekkel;

b) elfogadja az ENISA 24. cikkben említett egységes programozási dokumentumának tervezetét, mielőtt a dokumentumot benyújtanák a Bizottsághoz véleményezésre;

c) a Bizottság véleményének figyelembevételével elfogadja az ENISA egységes programozási dokumentumát;

d) felügyeli az egységes programozási dokumentumban szereplő többéves és éves programozás végrehajtását;

e) elfogadja az ENISA éves költségvetését, és a III. fejezettel összhangban ellátja az ENISA költségvetéséhez kapcsolódó egyéb feladatokat;

f) értékeli és elfogadja az ENISA tevékenységéről szóló összevont éves jelentést, amely tartalmazza az elszámolást és azt, hogy az ENISA hogyan teljesítette teljesítménymutatóit, a következő év július 1-jéig megküldi az éves jelentést és annak értékelését az Európai Parlament, a Tanács, a Bizottság és a Számvevőszék részére, valamint közzéteszi az éves jelentést;

g) elfogadja az ENISA-ra alkalmazandó pénzügyi szabályzatot a 32. cikkel összhangban;

h) olyan csalás elleni stratégiát fogad el, amely – figyelemmel a végrehajtandó intézkedések költség-haszon elemzésére – arányos a csalási kockázatokkal;

i) az igazgatótanács tagjai tekintetében az összeférhetetlenségek megelőzésére és kezelésére vonatkozó szabályokat fogad el;

j) biztosítja az Európai Csalás Elleni Hivatal (OLAF) vizsgálataiból és a különböző belső vagy külső ellenőrzési jelentésekből és értékelésekből következő megállapítások és ajánlások megfelelő nyomon követését;

k) elfogadja eljárási szabályzatát, ideértve a meghatározott feladatoknak a 19. cikk (7) bekezdése alapján történő átruházására vonatkozó ideiglenes határozatok szabályait;

l) a (2) bekezdéssel összhangban az ENISA személyzete vonatkozásában gyakorolja a 259/68/EGK, Euratom, ESZAK tanácsi rendelettel[1] megállapított, az Európai Unió tisztviselőinek személyzeti szabályzatában (a továbbiakban: személyzeti szabályzat) és az Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben (a továbbiakban: az egyéb alkalmazottakra vonatkozó alkalmazási feltételek) a kinevezésre jogosult hatóságra és a munkaszerződések megkötésére jogosult hatóságra ruházott hatásköröket (a továbbiakban: a kinevezésre jogosult hatóságot megillető hatáskörök);

m) a személyzeti szabályzat 110. cikkével összhangban végrehajtási szabályokat fogad el a személyzeti szabályzat és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek érvényre juttatása céljából;

n) a 36. cikkel összhangban kinevezi az ügyvezető igazgatót, és adott esetben meghosszabbítja hivatali idejét, vagy felmenti hivatalából;

o) számvitelért felelős tisztviselőt nevez ki, aki lehet a Bizottság számvitelért felelős tisztviselője is, és aki feladatai ellátása során teljes mértékben függetlenül jár el;

p) meghozza az ENISA belső struktúráinak kialakításával és szükség szerint az említett belső struktúrák módosításával kapcsolatos összes döntést, az ENISA tevékenységével kapcsolatos szükségletek és a hatékony és eredményes költségvetési gazdálkodás figyelembevételével;

[1] HL L 56., 1968.3.4., 1. o.

q) a 7. cikk tekintetében munkamegállapodások létrehozását engedélyezi;

r) a 42. cikkel összhangban munkamegállapodások létrehozását és megkötését engedélyezi.

(2) Az igazgatótanács a személyzeti szabályzat 110. cikkével összhangban, a személyzeti szabályzat 2. cikkének (1) bekezdése és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek 6. cikke alapján határozat elfogadása útján a kinevezésre jogosult hatóságot megillető vonatkozó hatásköröket az ügyvezető igazgatóra ruházza, és megállapítja azon feltételeket, amelyek mellett a hatáskör-átruházás felfüggeszthető. Az ügyvezető igazgató jogosult e hatáskörök további átruházására.

(3) Amennyiben kivételes körülmények szükségessé teszik, az igazgatótanács határozatban ideiglenesen felfüggesztheti a kinevezésre jogosult hatóságot megillető, az ügyvezető igazgatóra ruházott hatásköröket, illetve az ügyvezető igazgató által továbbruházott hatásköröket, és azokat maga gyakorolja vagy e hatásköröket valamelyik tagjára vagy a személyzetnek az ügyvezető igazgatótól eltérő tagjára ruházza.

16. cikk

Az igazgatótanács elnöke

Az igazgatótanácsnak tagjai közül tagjai szavazatainak kétharmados többségével elnököt és elnökhelyettest választ. Az elnök és az elnökhelyettesek hivatali ideje négy év, hivatali idejük egy alkalommal megújítható. Ha igazgatótanácsi tagságuk hivatali idejük alatt bármikor megszűnik, ugyanezen a napon elnöki vagy elnökhelyettesi megbízatásuk is automatikusan megszűnik. Ha az elnök nem tudja ellátni feladatait, az elnökhelyettes az elnököt hivatalból helyettesíti.

17. cikk

Az igazgatótanács ülései

(1) Az igazgatótanács üléseit az elnök hívja össze.

(2) Az igazgatótanácsnak évente legalább két rendes ülést kell tart. Ezen túlmenően az igazgatótanács az elnök kérésére, a Bizottság kérésére vagy tagjai legalább egyharmadának kérésére rendkívüli ülést tart.

(3) Az ügyvezető igazgatónak részt kell vennie az igazgatótanács ülésein, de szavazati joggal nem rendelkezik.

(4) Az ENISA tanácsadó csoportjának tagjai az elnök meghívására szavazati jog nélkül részt vehetnek az igazgatótanács ülésein.

(5) Az igazgatótanács tagjai és azok póttagjai – az igazgatótanács eljárási szabályzatával összhangban – az üléseken tanácsadók és szakértők segítségét is igénybe vehetik.

(6) Az ENISA az igazgatótanács számára a titkárságot biztosít.

18. cikk

Az igazgatótanács szavazási szabályai

(1) Az igazgatótanács határozatait tagjai többségének szavazatával fogadja el.

(2) Az egységes programozási dokumentum, az éves költségvetés, az ügyvezető igazgató kinevezése, hivatali idejének meghosszabbítása vagy hivatalból való felmentése elfogadásához az igazgatótanács tagjai szavazatának kétharmados többsége szükséges.

(3) Minden tag egy szavazattal rendelkezik. Valamely tag távolléte esetén az őt helyettesítő póttag jogosult a tagot megillető szavazati jog gyakorlására.

(4) Az igazgatótanács elnöke részt vesz a szavazásban.

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

(6) Az igazgatótanács eljárási szabályzata részletesebben rendelkezik a szavazás szabályairól, így különösen arról, hogy egy tag milyen feltételek mellett járhat el egy másik tag nevében.

2. SZAKASZ

FELÜGYELŐTESTÜLET

19. cikk

A felügyelőtestület

(1) Az igazgatótanács munkáját a felügyelőtestület segíti.

(2) A felügyelőtestület:

a) előkészíti az igazgatótanács által elfogadandó határozatokat;

b) az igazgatótanáccsal együtt biztosítja az OLAF vizsgálataiból, valamint a különböző belső vagy külső ellenőrzési jelentésekből és értékelésekből származó megállapítások és ajánlások megfelelő nyomon követését;

c) az ügyvezető igazgató 20. cikkben meghatározott feladatainak sérelme nélkül segítséget nyújt és tanácsot ad az ügyvezető igazgató számára az igazgatótanács igazgatási és költségvetési ügyekben hozott határozatainak a 20. cikk szerinti végrehajtásához.

(3) A felügyelőtestület öt tagból áll. A felügyelőtestület tagjait az igazgatótanács tagjai közül nevezik ki. Az egyik tag az igazgatótanács elnöke, aki betöltheti a felügyelőtestület elnöki tisztségét is, egy másik tag pedig a Bizottság egyik képviselője. A felügyelőtestület tagjainak kinevezésénél törekedni kell a nemek közötti egyensúly biztosítására a felügyelőtestületben. Az ügyvezető igazgatónak részt kell vennie a felügyelőtestület ülésein, de szavazati joggal nem rendelkezik.

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

(5) A felügyelőtestület legalább háromhavonta egyszer ülésezik. A felügyelőtestület elnöke a tagok kérésére további üléseket hív össze.

(6) A felügyelőtestület eljárási szabályzatát az igazgatótanács állapítja meg.

(7) Amennyiben sürgősség miatt szükséges, a felügyelőtestület az igazgatótanács nevében meghozhat bizonyos ideiglenes határozatokat, különösen az igazgatási irányítást érintő kérdésekben, ideértve a kinevezésre jogosult hatóság hatáskörei átruházásának felfüggesztését és a költségvetési kérdéseket is. Az ilyen ideiglenes határozatokról az igazgatótanácsot indokolatlan késedelem nélkül értesíteni kell. Azigazgatótanácsnak a határozat meghozatalától számított legfeljebb három hónapon belül döntenie kell, hogy jóváhagyja vagy elutasítja az ideiglenes határozatot. A felügyelőtestület az igazgatótanács nevében nem hozhat olyan határozatot, amely jóváhagyásához az igazgatótanács tagjainak kétharmados többsége szükséges.

3. SZAKASZ

ÜGYVEZETŐ IGAZGATÓ

20. cikk

Az ügyvezető igazgató feladatai

(1) Az ENISA-t 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, feladatai teljesítéséről beszámol az Európai Parlamentnek. A Tanács is felkérheti az ügyvezető igazgatót, hogy számoljon be feladatai teljesítéséről.

(3) Az ügyvezető igazgató feladatai a következők:

a) az ENISA napi ügyvitele;

b) az igazgatótanács által elfogadott határozatok végrehajtása;

c) az egységes programozási dokumentum tervezetének elkészítése és annak benyújtása az igazgatótanácshoz jóváhagyás céljából a Bizottsághoz való benyújtást megelőzően;

d) az egységes programozási dokumentum végrehajtása, majd beszámolás arról az igazgatótanácsnak;

e) összevont éves jelentés készítése az ENISA tevékenységéről, az ENISA éves munkaprogramjának 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 OLAF vizsgálataiból származó megállapítások nyomán, továbbá kétévente jelentéstétel az elért haladásról a Bizottságnak, valamint rendszeresen az igazgatótanácsnak;

h) 32. cikkben említett, az ENISA-ra alkalmazandó pénzügyi szabályzat tervezetének elkészítése;

i) az ENISA tervezett bevételekre és kiadásokra vonatkozó kimutatás tervezetének elkészítése és költségvetésének végrehajtása;

j) az Unió pénzügyi érdekeinek védelme a csalás, a korrupció és egyéb jogellenes tevékenységek elleni megelőző intézkedések alkalmazásával, hatékony ellenőrzésekkel, illetve szabálytalanságok észlelése esetén a jogalap nélkül kifizetett összegek visszafizettetésével, valamint adott esetben hatékony, arányos és visszatartó erejű közigazgatási és pénzügyi szankciók kiszabásával;

k) az ENISA csalás elleni stratégiájának elkészítése és annak benyújtása az igazgatótanácshoz jóváhagyás céljából;

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

m) az uniós szakpolitika következetes alakításának és végrehajtásának biztosítása érdekében rendszeres vélemény- és információcsere az uniós intézményekkel, szervekkel és hivatalokkal azok kiberbiztonsági tevékenységeire vonatkozóan;

n) az e rendeletben az ügyvezető igazgatóra ruházott további feladatok ellátása.

(4) Szükség esetén és az ENISA célkitűzései és feladatai keretében az ügyvezető igazgató eseti munkacsoportokat hozhat létre, amelyek szakértőkből, többek között az illetékes tagállami hatóságok szakértőiből állnak. Az ügyvezető igazgató erről az igazgatótanácsot előzetesen tájékoztatja. Különösen a munkacsoportok összetételével, a munkacsoportban részt vevő szakértőknek az ügyvezető igazgató általi kinevezésével, valamint a munkacsoportok működésével kapcsolatos eljárásokat az ENISA belső működési szabályzatában kell meghatározni.

(5) Az ügyvezető igazgató szükség esetén az ENISA feladatainak hatékony és eredményes ellátása céljából, megfelelő költség-haszon-elemzés alapján dönthet egy vagy több helyi iroda 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 ENISA 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. A helyi irodák mindegyikében a szükséges minimumra kell korlátozni a személyzet összesített létszámát, és az nem haladhatja meg az ENISA-nak a székhelye szerinti tagállamban található személyzete teljes létszámának 40 %-át. Az egyes helyi irodák személyzetének létszáma nem haladhatja meg az ENISA-nak a székhelye szerinti tagállamban található személyzete teljes létszámának 10 %-át.

A helyi irodát létrehozó határozatban úgy kell megállapítani a helyi iroda által ellátandó tevékenységek körét, hogy ne legyenek szükségtelen költségek és indokolatlan átfedések az ENISA igazgatási feladatai közötti.

4. SZAKASZ

AZ ENISA TANÁCSADÓ CSOPORTJA, AZ ÉRDEKELT FELEK KIBERBIZTONSÁGI TANÚSÍTÁSI CSOPORTJA ÉS A NEMZETI KAPCSOLATTARTÓ TISZTVISELŐK HÁLÓZATA

21. cikk

Az ENISA tanácsadó csoportja

(1) Az igazgatótanács az ügyvezető igazgató javaslatára átlátható módon létrehozza az ENISA tanácsadó csoportját, amely a releváns érdekelt feleket – például az IKT-ágazatot, a nyilvános elektronikus hírközlő hálózatok és nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, a kkv-kat, az alapvető szolgáltatásokat nyújtó szereplőket, a fogyasztói csoportokat és a kiberbiztonság területén tevékenykedő tudományos szakembereket – képviselő elismert szakértőkből, valamint az (EU) 2018/1972 irányelvvel összhangban bejelentett illetékes hatóságok, az európai szabványügyi szervek, továbbá a bűnüldöző hatóságok és az adatvédelmi felügyeleti hatóságok képviselőiből áll. Az igazgatótanácsnak törekednie kell a nemek közötti, a földrajzi, valamint az érdekelt felek különböző csoportjai közötti megfelelő egyensúly biztosítására.

(2) Az ENISA tanácsadó csoportjának különösen az összetételével, az ügyvezető igazgató (1) bekezdésben említett javaslatával, tagjainak számával és kinevezésével, valamint az ENISA tanácsadó csoportjának működésével kapcsolatos eljárásokat az ENISA belső működési szabályzatában kell meghatározni, és azokat nyilvánosságra kell hozni.

(3) Az ENISA tanácsadó csoportjában az elnöki teendőket az ügyvezető igazgató vagy az általa eseti alapon kinevezett személy látja el.

(4) Az ENISA tanácsadó csoportja tagjainak hivatali ideje két és fél év. Az ENISA tanácsadó csoportjának nem lehetnek olyan tagjai, akik az igazgatótanácsnak is tagjai. Az ENISA tanácsadó csoportjának ülésein jelen lehetnek, és munkájában részt vehetnek a Bizottságtól és a tagállamokból érkező szakértők. Az ENISA tanácsadó csoportjának üléseire és a munkájában való részvételre az ügyvezető igazgató által relevánsnak ítélt egyéb szervek olyan képviselői is meghívhatók, akik nem tagjai az ENISA tanácsadó csoportjának.

(5) Az ENISA tanácsadó csoportja – e rendelet III. címe rendelkezéseinek alkalmazása kivételével – tanácsadással segíti az ENISA-t feladatainak ellátásában. Az ENISA tanácsadó csoport különösen az ENISA munkaprogramjára vonatkozó javaslat elkészítéséhez és a releváns érdekelt felekkel a munkaprogramot érintő kérdésekről folytatandó párbeszéd biztosításához ad tanácsot az ügyvezető igazgatónak.

(6) Az ENISA tanácsadó csoportja rendszeresen tájékoztatja tevékenységeiről az igazgatótanácsot.

22. cikk

Az érdekelt felek kiberbiztonsági tanúsítási csoportja

(1) Létrejön az érdekel felek kiberbiztonsági tanúsítási csoportja.

(2) Az érdekelt felek kiberbiztonsági tanúsítási csoportja a releváns érdekelt feleket képviselő elismert szakértőkből kiválasztott tagokból áll. Az érdekelt felek kiberbiztonsági tanúsítási csoportjának tagjait a Bizottság választja ki az ENISA javaslata alapján, átlátható és nyílt pályázati eljárás során, biztosítva az érdekelt felek különböző csoportjai közötti egyensúlyt, valamint megfelelő nemek közötti és a földrajzi egyensúlyt.

(3) Az érdekelt felek kiberbiztonsági tanúsítási csoportja:

a) tanácsot ad a Bizottságnak az európai kiberbiztonsági tanúsítási kerettel kapcsolatos stratégiai kérdéseket illetően;

b) kérésre tanácsot ad az ENISA számára az ENISA piaccal, kiberbiztonsági tanúsítással és szabványosítással kapcsolatos feladataihoz kapcsolódó általános és stratégiai kérdésekben;

c) segítséget nyújt a Bizottság számára a 47. cikkben említett uniós gördülő munkaprogram előkészítéséhez;

d) véleményt ad az uniós gördülő munkaprogramról a 47. cikk (4) bekezdése alapján; valamint

e) a 47. és a 48. cikkben foglaltak szerint sürgős esetekben tanácsot ad a Bizottság és az európai kiberbiztonsági tanúsítási csoport számára olyan további tanúsítási rendszerek szükségességével kapcsolatban, amelyek nem szerepelnek az uniós gördülő munkaprogramban.

(4) Az érdekelt felek kiberbiztonsági tanúsítási csoportja társelnöki tisztét a Bizottság és az ENISA képviselői töltik be, a titkárságát pedig az ENISA biztosítja.

23. cikk

A nemzeti kapcsolattartó tisztviselők hálózata

(1) Az igazgatótanács – az ügyvezető igazgató javaslata alapján – létrehozza a nemzeti kapcsolattartó tisztviselők hálózatát, amely valamennyi tagállamok képviselőiből (a továbbiakban: nemzeti kapcsolattartó tisztviselők) áll. Minden tagállam egy képviselőt jelöl ki a nemzeti kapcsolattartó tisztviselők hálózatába. A nemzeti kapcsolattartó tisztviselők hálózatának üléseire többféle szakértői formációban kerülhet sor.

(2) A nemzeti kapcsolattartó tisztviselők hálózatának különösen az ENISA és a tagállamok közötti információcserét kell megkönnyítenie, valamint támogatnia kell az ENISA-t abban, hogy Unió-szerte eljuttassa a tevékenységeivel, a megállapításaival és az ajánlásaival kapcsolatos információkat a releváns érdekelt felekhez.

(3) A nemzeti kapcsolattartó tisztviselőknek nemzeti szinten központi kapcsolattartó pontként kell működniük, hogy az ENISA éves munkaprogramjának végrehajtásával összefüggésben megkönnyítsék az ENISA és a nemzeti szakértők közötti együttműködést.

(4) Míg a nemzeti kapcsolattartó tisztviselőknek szorosan együtt kell működniük az igazgatótanács országukat képviselői tagjával, a nemzeti kapcsolattartó tisztviselők hálózatának el kell kerülnie a párhuzamos munkavégzést mind az igazgatótanáccsal, mind a többi uniós fórummal.

(5) A nemzeti kapcsolattartó tisztviselők hálózatának feladatait és eljárásait az ENISA belső működési szabályzatában kell meghatározni, és azokat nyilvánosságra kell hozni.

5. SZAKASZ

MŰKÖDÉS

24. cikk

Egységes programozási dokumentum

(1) Az ENISA a többéves és éves munkaprogramját tartalmazó egységes programozási dokumentummal összhangban működik, amelynek az ENISA valamennyi tervezett tevékenységét magában kell foglalnia.

(2) Az ügyvezető igazgató – az 1271/2013/EU felhatalmazáson alapuló bizottsági rendelet[1] 32. cikkével összhangban és a Bizottság által meghatározott iránymutatások figyelembevételével – minden évben elkészíti a többéves és éves programozást tartalmazó egységes programozási dokumentum tervezetét, amely a megfelelő pénzügyi- és humán erőforrásokra is kiterjed.

(3) Az igazgatótanács minden évben november 30-ig elfogadja az (1) bekezdésben említett egységes programozási dokumentumot, és a rákövetkező évben legkésőbb január 31-ig továbbítja azt az Európai Parlamentnek, a Tanácsnak és a Bizottságnak, valamint továbbítja az említett dokumentum később aktualizált változatait is.

(4) Az egységes programozási dokumentum az Unió általános költségvetésének végleges elfogadását követően válik véglegessé, és szükség esetén annak megfelelően ki kell igazítani.

(5) Az éves munkaprogram tartalmazza a részletes célkitűzéseket és az elvárt eredményeket, beleértve a kapcsolódó teljesítménymutatókat. Emellett – a tevékenységalapú költségvetés-tervezés és irányítás elveivel összhangban – ismerteti a finanszírozandó fellépéseket, és megjelöli az egyes fellépésekhez rendelt pénzügyi- és humán erőforrásokat. Az éves munkaprogram összhangban áll a (7) bekezdésben említett többéves munkaprogrammal. Az éves munkaprogram egyértelműen jelezi, hogy az előző pénzügyi évhez képest az ENISA mely feladata új, változott vagy szűnt meg.

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

(6) Amikor az ENISA új feladatot kap, az igazgatótanács módosítja az elfogadott éves munkaprogramot. Az éves munkaprogram minden lényeges módosítását ugyanazzal az eljárással kell elfogadni, mint az eredeti éves munkaprogramot. Az igazgatótanács az éves munkaprogram nem lényeges módosítására vonatkozó hatáskörét az ügyvezető igazgatóra ruházhatja.

(7) A többéves munkaprogramnak 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 amikor az a 67. cikkben említett értékelés kimenetelének figyelembevétele céljából szükséges – aktualizálni kell.

25. cikk

Érdekeltségi nyilatkozat

(1) Az igazgatótanács tagjai, az ügyvezető igazgató és a tagállamok által ideiglenesen kirendelt tisztviselők mindegyike kötelezettségvállalási nyilatkozat tesz, továbbá nyilatkozik 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 minden egyes ülés kezdetén pontosan és teljeskörűen nyilatkozni az egyes napirendi pontokkal kapcsolatos bármely olyan érdekéről, amelyről feltehető, hogy függetlenségét befolyásolhatja, az ilyen napirendi pontok megvitatásában való részvételtől és az azokról való szavazástól pedig köteles tartózkodni.

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

26. cikk

Átláthatóság

(1) Az ENISA tevékenységét nagyfokú átláthatóság mellett, a 28. cikkel összhangban végzi.

(2) Az ENISA biztosítja, hogy a nyilvánosság és minden érdekelt fél – különösen munkájának eredményeiről – megfelelő, tárgyilagos, megbízható és könnyen hozzáférhető információt kapjon. Az ENISA továbbá köteles a nyilvánosság elé tárni a 25. cikkel összhangban tett érdekeltségi nyilatkozatokat.

(3) Az igazgatótanács az ügyvezető igazgató javaslatára eljárva engedélyezheti, hogy érdekelt felek az ENISA egyes tevékenységeinek folyamatában megfigyelőként részt vegyenek.

(4) Az ENISA-nak belső működési szabályzatában meg kell állapítania az (1) és a (2) bekezdésben említett átláthatósági szabályok végrehajtására vonatkozó gyakorlati rendelkezéseket.

27. cikk

Titoktartás

(1) A 28. cikk sérelme nélkül, az ENISA nem adhatja tovább harmadik felek részére az általa kezelt vagy hozzá beérkezett olyan információkat, amelyek tekintetében indokolással ellátott kérelmet nyújtottak be a bizalmas kezelés iránt.

(2) Az igazgatótanács tagjai, az ügyvezető igazgató, az ENISA tanácsadó csoportjának tagjai, az eseti munkacsoportok munkájában részt vevő külső szakértők és az ENISA személyzetének tagjai – beleértve a tagállamok által ideiglenesen kirendelt tisztviselőket is – feladataik megszűnte után is az EUMSZ 339. cikke szerinti titoktartási kötelezettségek hatálya alá tartoznak.

(3) Az ENISA belső működési szabályzatában megállapítja az (1) és a (2) bekezdésben említett titoktartási szabályok végrehajtására vonatkozó gyakorlati rendelkezéseket.

(4) Amennyiben az ENISA feladatainak ellátásához szükséges, az igazgatótanácsnak lehetővé kell tennie az ENISA számára, hogy minősített adatokat kezeljen. Ebben az esetben az ENISA-nak a Bizottság szolgálataival egyetértésben biztonsági szabályokat kell elfogadnia az (EU, Euratom) 2015/443[1] és az (EU, Euratom) 2015/444 bizottsági határozatban[2] megállapított biztonsági elvek alkalmazásáról. Ezeknek a biztonsági szabályoknak a minősített adatok cseréjére, kezelésére és tárolására vonatkozó rendelkezéseket is kell tartalmaznia.

---

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

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

28. cikk

Dokumentumokhoz való hozzáférés

(1) Az ENISA birtokában lévő dokumentumokra az 1049/2001/EK rendelet alkalmazandó.

(2) Az igazgatótanács ... [hat hónappal e rendelet hatálybalépésének időpontját követően]-ig elfogadja az 1049/2001/EK rendelet végrehajtására vonatkozó rendelkezéseket.

(3) Az ENISA 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 Bíróság előtt kereset indítható.

III. fejezet

Az ENISA költségvetésének megállapítása és szerkezete

29. cikk

Az ENISA költségvetésének megállapítása

(1) Az ügyvezető igazgató minden évben elkészíti az ENISA következő pénzügyi évre vonatkozó, bevételeket és kiadásokat tartalmazó előzetes előirányzat-tervezetét, a létszámtervet is beleértve, és megküldi azt az igazgatótanácsnak. A bevételeknek és a kiadásoknak egyensúlyban kell lenniük.

(2) Az igazgatótanács az előzetes előirányzat-tervezet alapján minden évben elkészíti az ENISA következő pénzügyi évre szóló tervezett bevételi és kiadási előirányzat-tervezetét.

(3) Az igazgatótanács minden év január 31-ig megküldi az egységes programozási dokumentum részét képező előirányzat-tervezetet a Bizottságnak és azoknak a harmadik országoknak, amelyekkel az Unió a 42. cikk (2) bekezdésében említett megállapodást kötött.

(4) Az előirányzat-tervezet alapján a Bizottság a létszámtervhez általa szükségesnek tartott becsült összegeket, valamint az általános költségvetést terhelő hozzájárulás összegét bevezeti az Unió általános költségvetésének tervezetébe, amely előirányzat-tervezetet az EUMSZ 314. cikkének megfelelően a az Európai Parlament elé a Tanács elé terjeszt.

(5) Az ENISA részére az Uniótól nyújtandó hozzájárulásra vonatkozó előirányzatokat az Európai Parlament és a Tanács engedélyezi.

(6) Az ENISA létszámtervét az Európai Parlament és a Tanács fogadja el.

(7) Az ENISA költségvetését az igazgatótanács az egységes programozási dokumentummal együtt fogadja el. Az ENISA költségvetése az Unió általános költségvetésének végleges elfogadását követően válik véglegessé. Az igazgatótanács az ENISA költségvetését és egységes programozási dokumentumát szükség esetén az Unió általános költségvetéséhez igazítja.

30. cikk

Az ENISA költségvetésének szerkezete

(1) Az ENISA bevételei az egyéb források sérelme nélkül a következőkből származnak:

a) az Unió általános költségvetésből kapott hozzájárulás;

b) a meghatározott kiadási tételekhez rendelt bevételek az ENISA 32. cikkben említett pénzügyi szabályzatával összhangban;

c) uniós finanszírozás hozzájárulási megállapodások vagy eseti vissza nem térítendő támogatások formájában, a 32. cikkben említett pénzügyi szabályzattal, valamint az Unió szakpolitikáit támogató megfelelő intézkedések rendelkezéseivel összhangban;

d) hozzájárulások azon harmadik országoktól, amelyek a 42. cikkben említettek szerint részt vesznek az ENISA munkájában;

e) a tagállamok által pénzben vagy természetben nyújtott önkéntes hozzájárulások.

Az első albekezdés e) pontja alapján önkéntes hozzájárulást nyújtó tagállamok nem tarthatnak igényt semmilyen különös jogra vagy ellenszolgáltatásra e hozzájárulásért cserébe.

(2) Az ENISA kiadásait a személyzeti, az igazgatási, a műszaki támogatási, az infrastrukturális és a működési kiadások, valamint a harmadik felekkel kötött szerződésekből eredő kiadások alkotják.

31. cikk

Az ENISA költségvetésének végrehajtása

(1) Az ENISA költségvetésének végrehajtásáért az ügyvezető igazgató felel.

(2) A Bizottság belső ellenőre ugyanazokkal a hatáskörökkel rendelkezik az ENISA felett, mint a Bizottság szervezeti egységei felett.

(3) Az ENISA számvitelért felelős tisztviselője a pénzügyi évre (a továbbiakban: n. év) vonatkozó előzetes beszámolót a következő pénzügyi év (a továbbiakban: n+1. év) március 1-jéig megküldi a Bizottság számvitelért felelős tisztviselőjének és a Számvevőszéknek.

(4) A Számvevőszék által az ENISA n. évre vonatkozó előzetes beszámolójára vonatkozóan az (EU, Euratom) 2018/1046 rendelet[1] 246. cikke szerint tett észrevételek kézhezvételét követően az ENISA számvitelért felelős tisztviselője saját felelőssége mellett elkészíti az az ENISA adott évre vonatkozó végleges beszámolóját, amelyet az ügyvezető igazgató véleményezésre benyújt az igazgatótanácsnak.

(5) Az igazgatótanács véleményezi az ENISA végleges beszámolóját.

---

[1] Az Európai Parlament és a Tanács (EU, Euratom) 2018/1046 rendelete (2018. július 18.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról, az 1296/2013/EU, az 1301/2013/EU, az 1303/2013/EU, az 1304/2013/EU, az 1309/2013/EU, az 1316/2013/EU, a 223/2014/EU és a 283/2014/EU rendelet és az 541/2014/EU határozat módosításáról, valamint a 966/2012/EU, Euratom rendelet hatályon kívül helyezéséről (HL L 193., 2018.7.30., 1. o.).

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

(7) Az ENISA számvitelért felelős tisztviselője az n+1. év július 1-jéig – az igazgatótanács véleményével együtt – megküldi az ENISA végleges beszámolóját az Európai Parlamentnek, a Tanácsnak, a Bizottság számvitelért felelős tisztviselőjének és a Számvevőszéknek.

(8) Az ENISA végleges beszámolójának továbbításával egyidejűleg az ENISA számvitelért felelős tisztviselője az e végleges beszámolóra vonatkozó teljességi nyilatkozatot is benyújt a Számvevőszéknek, egy másolati példányt pedig a Bizottság számvitelért felelős tisztviselőjének.

(9) Az ügyvezető igazgató az n+1. év november 15-ig közzéteszi az ENISA végleges beszámolóját az *Európai Unió Hivatalos Lapjában.*

(10) Az ügyvezető igazgató az n+1. év szeptember 30-áig választ küld a Számvevőszék észrevételeire, és e válaszról másolatot küld az igazgatótanácsnak és a Bizottságnak.

(11) Az ügyvezető igazgató az Európai Parlament kérésére az (EU, Euratom) 2018/1046 rendelet 261. cikke (3) bekezdésével összhangban benyújt az Európai Parlamentnek minden, a mentesítési eljárás adott pénzügyi évre történő szabályszerű alkalmazásához szükséges információt.

(12) Az Európai Parlament a Tanács ajánlása alapján az n+2. év május 15-e előtt mentesíti az ügyvezető igazgatót az n. évi költségvetés végrehajtására vonatkozó felelőssége alól.

32. cikk

Pénzügyi szabályok

Az ENISA-ra alkalmazandó pénzügyi szabályokat a Bizottsággal folytatott konzultációt követően az igazgatótanács fogadja el. Ezek a szabályok nem térhetnek el az 1271/2013/EU felhatalmazáson alapuló rendelettől, kivéve, ha az eltérés az ENISA működéséhez kifejezetten szükséges, és ahhoz a Bizottság előzetesen hozzájárult.

33. cikk

Csalás elleni küzdelem

(1) A csalás, korrupció és más jogellenes tevékenységek elleni, a 883/2013/EU, Euratom európai parlamenti és tanácsi rendelet[1] szerinti küzdelem elősegítése céljából az ENISA ... [hat hónappal e rendelet hatálybalépésének időpontját követően]-ig csatlakozik az Európai Parlament, az Európai Unió Tanácsa és az Európai Közösségek Bizottsága közötti, az Európai Csalás Elleni Hivatal (OLAF) belső vizsgálatairól szóló, 1999. május 25-i intézményközi megállapodáshoz[2]. Az ENISA az említett megállapodás mellékletében szereplő mintát alkalmazva elfogadja az ENISA személyzetére alkalmazandó megfelelő rendelkezéseket.

(2) A Számvevőszék jogosult dokumentumok és helyszíni ellenőrzések alapján ellenőrzést végezni valamennyi, vissza nem térítendő támogatásban részesülő kedvezményezettnél, vállalkozónál és alvállalkozónál, akik az ENISA-tól uniós forrásból részesültek.

---

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

[2] HL L 136., 1999.5.31., 15. o.

(3) Az OLAF – a 883/2013/EU, Euratom rendeletben, valamint a 2185/96/Euratom, EK tanácsi rendeletben[1] meghatározott rendelkezésekkel és eljárásokkal összhangban vizsgálatokat – többek között helyszíni ellenőrzéseket és vizsgálatokat – végezhet annak megállapítása céljából, hogy az ENISA által finanszírozott, vissza nem térítendő támogatással vagy valamely szerződéssel összefüggésben történt-e csalás, korrupció vagy bármilyen más jogellenes tevékenység, amely sérti az Unió pénzügyi érdekeit..

(4) Az (1), a (2) és a (3) bekezdés sérelme nélkül az ENISA harmadik országokkal és nemzetközi szervezetekkel kötött együttműködési megállapodásainak, továbbá az általa kötött szerződéseknek, támogatási megállapodásoknak és támogatási határozatoknak tartalmazniuk kell olyan rendelkezéseket, amelyek kifejezetten felhatalmazzák a Számvevőszéket és az OLAF-ot arra, hogy saját hatáskörüknek megfelelően lefolytassák az ilyen ellenőrzéseket és vizsgálatokat.

IV. fejezet
Személyzet

34. cikk
Általános rendelkezések

Az ENISA személyzetére a személyzeti szabályzatot és az egyéb alkalmazottakra vonatkozó alkalmazási feltételeket, valamint a személyzeti szabályzat és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek végrehajtása céljából az uniós intézmények közötti megállapodással elfogadott szabályokat kell alkalmazni.

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

35. cikk

Kiváltságok és mentességek

Az ENISA-re és személyzetére alkalmazni kell az EUSZ-hez és az EUMSZ-hez csatolt, az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyvet.

36. cikk

Az ügyvezető igazgató

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

(2) Az ügyvezető igazgatót nyílt és átlátható kiválasztási eljárás keretében az igazgatótanács nevezi ki a Bizottság által javasolt jelöltek listájáról.

(3) Az ügyvezető igazgató szerződésének megkötése céljából az ENISA-t az igazgatótanács elnöke képviseli.

(4) A kinevezés előtt az igazgatótanács által kiválasztott jelölt meghívást kap arra, hogy nyilatkozatot tegyen az Európai Parlament illetékes bizottsága előtt, és válaszoljon a parlamenti képviselők kérdéseire.

(5) Az ügyvezető igazgató hivatali ideje öt év. Ezen időszak letelte előtt a Bizottság felmérést végez az ügyvezető igazgató teljesítményéről, valamint az ENISA jövőbeli feladatairól és kihívásairól.

(6) Az igazgatótanács az ügyvezető kinevezésével, hivatali idejének meghosszabbításával vagy felmentésével kapcsolatos határozatait a 18. cikk (2) bekezdésével összhangban hozza meg.

(7) Az igazgatótanács az (5) bekezdésben említett értékelést figyelembe véve, a Bizottság javaslata alapján eljárva az ügyvezető igazgató hivatali idejét egy alkalommal, legfeljebb öt évvel meghosszabbíthatja.

(8) Az igazgatótanács tájékoztatja az Európai Parlamentet arról, hogy meg kívánja hosszabbítani az ügyvezető igazgató hivatali idejét. Az ezen meghosszabbítás előtti három hónapon belül az ügyvezető igazgató – amennyiben meghívást kap – nyilatkozatot tesz az Európai Parlament illetékes bizottsága előtt, és válaszol a képviselők kérdéseire.

(9) Az az ügyvezető igazgató, akinek a hivatali ideje meghosszabbításra került, nem vehet részt az ugyanezen tisztség betöltésére irányuló újabb kiválasztási eljárásokban.

(10) Az ügyvezető igazgató kizárólag az igazgatótanácsnak a Bizottság javaslata alapján meghozott határozatával hívható vissza hivatalából.

37. cikk

Kirendelt nemzeti szakértők és egyéb személyzet

(1) Az ENISA igénybe vehet kirendelt nemzeti szakértőket és egyéb, nem az ENISA alkalmazásában álló személyzetet. Rájuk a személyzeti szabályzat és az egyéb alkalmazottakra vonatkozó alkalmazási feltételek nem alkalmazandók.

(2) Az igazgatótanács határozatot fogad el a nemzeti szakértők ENISA-hoz való kirendelésére vonatkozó szabályok megállapításáról.

V. fejezet

Az ENISA-ra vonatkozó általános rendelkezések

38. cikk

Az ENISA jogállása

(1) Az ENISA az Unió szerve, és jogi személyiséggel rendelkezik.

(2) Az ENISA-t minden egyes tagállamban a nemzeti jog szerint a jogi személyeket megillető legteljesebb jogképességgel rendelkezik. Az ENISA különösen ingó és ingatlan vagyont szerezhet és azzal rendelkezhet, továbbá perképességgel rendelkezik.

(3) Az ENISA-t az ügyvezető igazgató képviseli.

39. cikk

Az ENISA felelőssége

(1) Az ENISA szerződéses felelősségét az adott szerződésre alkalmazandó jog szabályozza.

(2) Az Európai Unió Bírósága rendelkezik joghatósággal arra, hogy az ENISA által kötött szerződésekben foglalt választottbírósági kikötés alapján ítéletet hozzon.

(3) Szerződésen kívüli felelősség esetén az ENISA – a tagállamok jogrendszereinek közös általános elveivel összhangban – megtéríti az általa vagy alkalmazottai által feladataik teljesítése során okozott károkat.

(4) A (3) bekezdésben említett károk megtérítésével kapcsolatosan az Európai Unió Bírósága rendelkezik joghatósággal.

(5) Az ENISA alkalmazottainak az ENISA-val szemben fennálló személyes felelősségét az ENISA személyzetére e tekintetben alkalmazandó feltételek szabályozzák.

40. cikk

Nyelvhasználati szabályok

(1) Az ENISA-ra az 1. tanácsi rendelet[1] alkalmazandó. A tagállamok és a tagállamok által kijelölt egyéb szervek az Unió intézményeinek általuk választott bármely hivatalos nyelvén fordulhatnak az ENISA-hoz, és jogosultak ugyanezen a nyelven választ kapni.

(2) Az ENISA működéséhez szükséges fordítási szolgáltatásokat az Európai Unió Szerveinek Fordítóközpontja biztosítja.

41. cikk

A személyes adatok védelme

(1) A személyes adatok ENISA általi kezelésére az (EU) 2018/1725 rendeletet kell alkalmazni.

(2) Az igazgatótanács elfogadja az (EU) 2018/1725 rendelet 45. cikkének (3) bekezdésében említett végrehajtási szabályokat. Az igazgatótanács további, az (EU) 2018/1725 rendelet ENISA általi alkalmazásához szükséges intézkedéseket fogadhat el.

[1] A Tanács 1. rendelete az Európai Gazdasági Közösség által használt nyelvek meghatározásáról (HL 17., 1958.10.6., 385. o.).

42. cikk

Együttműködés harmadik országokkal és nemzetközi szervezetekkel

(1) Az e rendeletben meghatározott célkitűzések eléréséhez szükséges mértékben az ENISA együttműködhet harmadik országok illetékes hatóságaival és nemzetközi szervezetekkel. Ebből a célból az ENISA a Bizottság előzetes jóváhagyásával munkamegállapodásokat köthet harmadik országok hatóságaival és a nemzetközi szervezetekkel. Ezek a megállapodások az Unióval és tagállamaival szemben nem keletkeztethetnek jogi kötelezettséget.

(2) Az ENISA nyitott azon harmadik országok részvételére, amelyek ebből a célból megállapodást kötöttek az Unióval. Ezen megállapodások vonatkozó rendelkezései alapján munkamegállapodásokat kell kötni, meghatározva különösen az érintett harmadik országoknak az ENISA munkájában való részvétele jellegét, terjedelmét és módját, valamint az ENISA kezdeményezéseiben való részvételre, a pénzügyi hozzájárulásra és a személyzetre vonatkozó rendelkezéseket. A személyzeti kérdéseket illetően ezeknek a szabályoknak minden esetben meg kell felelniük a személyzeti szabályzatnak és az egyéb alkalmazottakra vonatkozó alkalmazási feltételeknek.

(3) Az igazgatótanács az ENISA hatáskörébe tartozó kérdések vonatkozásában stratégiát fogad el a harmadik országokkal és nemzetközi szervezetekkel fenntartott kapcsolatokra vonatkozóan. A Bizottság az ügyvezető igazgatóval kötött megfelelő munkamegállapodások útján biztosítja, hogy az ENISA a megbízatásával összhangban és a meglévő intézményi kereteken belül működjön.

43. cikk

Biztonsági szabályok a nem minősített érzékeny adatok és a minősített adatok védelmére

A Bizottsággal folytatott konzultációt követően az ENISA a Bizottságnak az (EU, Euratom) 2015/443 és az (EU, Euratom) 2015/444 határozatban meghatározott, a nem minősített érzékeny adatok és az EU-minősített adatok védelmére vonatkozó biztonsági elveit alkalmazó biztonsági szabályokat fogad el. Az ENISA biztonsági szabályai az ilyen adatok cseréjére, kezelésére és tárolására vonatkozó rendelkezéseket foglalnak magukban.

44. cikk

Székhely-megállapodás és működési feltételek

(1) Az ENISA fogadó tagállamon belüli elhelyezéséhez szükséges rendelkezéseket, a fogadó tagállam által rendelkezésre bocsátandó létesítményekre vonatkozó rendelkezéseket, továbbá az ügyvezető igazgatóra, az igazgatótanács tagjaira, valamint az ENISA személyzetre és családtagjaikra a fogadó tagállamban alkalmazandó különös szabályokat az ENISA és a fogadó tagállam által – az igazgatótanács jóváhagyásának megszerzése után – megkötött székhely-megállapodásban kell rögzíteni.

(2) Az ENISA fogadó tagállama biztosítja a lehető legjobb feltételeket az ENISA megfelelő működéséhez, figyelembe véve a székhely megközelíthetőségét, a személyzet gyermekeinek biztosított megfelelő oktatási lehetőségeket, valamint a személyzet gyermekeinek és házastársainak esetében a munkaerőpiachoz, a társadalombiztosításhoz és az egészségügyi ellátáshoz való megfelelő hozzáférést is.

45. cikk

Igazgatási ellenőrzés

Az ENISA működésével kapcsolatban az európai ombudsman az EUMSZ 228. cikkével összhangban felügyeletet gyakorol.

III. CÍM
KIBERBIZTONSÁGI TANÚSÍTÁSI KERETRENDSZER

46. cikk

Az európai kiberbiztonsági tanúsítási keretrendszer

(1) Létrejön az európai kiberbiztonsági tanúsítási keretrendszer, annak érdekében, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok digitális egységes piacának létrehozása céljából a kiberbiztonság szintjének az Unión belüli javítása és az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó, uniós szinten összehangolt megközelítés lehetővé tétele útján javuljanak a belső piac működésének feltételei.

(2) Az európai kiberbiztonsági tanúsítási keretrendszer meghatároz egy mechanizmust az európai kiberbiztonsági tanúsítási rendszerek létrehozására, valamint annak tanúsítására, hogy az e rendszerekkel összhangban értékelt IKT-termékek, IKT-szolgáltatások és IKT-folyamatok megfelelnek adott biztonsági követelményeknek, az e termékek, szolgáltatások és folyamatok által tárolt vagy továbbított vagy kezelt adatok, vagy az általuk ellátott funkciók vagy kínált szolgáltatások rendelkezésre állásának, hitelességének, sértetlenségének vagy titkosságának azok teljes életciklusa alatti védelme céljából.

47. cikk

Az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó uniós gördülő munkaprogram

(1) A Bizottság közzéteszi az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó uniós gördülő munkaprogramot (a továbbiakban: az uniós gördülő munkaprogram), amelyben meghatározza a jövőbeli európai kiberbiztonsági tanúsítási rendszerek stratégiai prioritásait.

(2) Az uniós gördülő munkaprogramnak magában kell foglalnia különösen azon IKT-termékek, IKT-szolgáltatások és IKT-folyamatok vagy ezek kategóriáinak jegyzékét, amelyek alkalmasak arra, hogy valamely európai kiberbiztonsági tanúsítási rendszer hatálya alá vonják őket.

(3) Bármely konkrét IKT-terméknek, IKT-szolgáltatásnak és IKT-folyamatnak vagy ezek kategóriáinak az uniós gördülő munkaprogramban való szerepeltetését igazolni kell a következő indokok közül egy vagy több alapján:

a) olyan nemzeti kiberbiztonsági tanúsítási rendszerek rendelkezésre állása és kidolgozása, amelyek hatálya IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok egy konkrét kategóriájára kiterjed, különösen a széttagoltság veszélyére tekintettel;

b) vonatkozó uniós vagy tagállami jog vagy szakpolitikák;

c) piaci kereslet;

d) változások a kiberfenyegetettségi helyzetben;

e) az európai kiberbiztonsági tanúsítási csoport általi valamely konkrét rendszer javaslati szintű kidolgozására irányuló kérelem.

(4) A Bizottság kellően figyelembe veszi az európai kiberbiztonsági tanúsítási csoport és az érdekelt felek kiberbiztonsági tanúsítási csoportja által az uniós gördülő munkaprogram tervezetéről kiadott véleményeket.

(5) Az első uniós gördülő munkaprogramot ... [tizenkét hónappal e rendelet hatálybalépésének időpontját követően]-ig kell közzétenni. Az uniós gördülő munkaprogramot háromévente legalább egyszer, illetve szükség esetén gyakrabban aktualizálni kell.

48. cikk

Európai kiberbiztonsági tanúsítási rendszer létrehozása iránti kérelem

(1) A Bizottság felkérheti az ENISA-t, hogy a munkaprogram alapján dolgozzon ki egy javasolt rendszert vagy az uniós gördülő munkaprogram alapján vizsgáljon felül egy létező európai kiberbiztonsági tanúsítási rendszert.

(2) Kellően indokolt esetben a Bizottság vagy az európai kiberbiztonsági tanúsítási csoport kérheti az ENISA-t, hogy dolgozzon ki egy olyan javaslati rendszert, vagy vizsgáljon felül olyan létező európai kiberbiztonsági tanúsítási rendszert, amely nem szerepel az uniós gördülő munkaprogramban. Az uniós gördülő munkaprogramot ennek megfelelően aktualizálni kell.

49. cikk

Valamely európai kiberbiztonsági tanúsítási rendszer kidolgozása, elfogadása és felülvizsgálata

(1) Az ENISA-nak a Bizottság 48. cikk szerinti kérése alapján ki kell dolgoznia egy olyan javaslati rendszert, amely megfelel az 51., az 52. és az 54. cikkben meghatározott követelményeknek.

(2) Az ENISA az európai kiberbiztonsági tanúsítási csoport 48. cikk (2) bekezdése szerinti kérése alapján kidolgozhat egy olyan javaslati rendszert, amely megfelel az 51., az 52. és az 54. cikkben meghatározott követelményeknek. E kérés visszautasítása esetén az ENISA köteles azt megindokolni. E kérés visszautasításáról az igazgatótanács dönthet.

(3) A javaslati rendszer kidolgozása során az ENISA valamennyi érdekelt féllel – hivatalos, nyílt, átlátható és inkluzív konzultációs folyamat útján – köteles konzultálni.

(4) Minden egyes javaslati rendszer tekintetében az ENISA-nak a 20. cikk (4) bekezdésével összhangban ad hoc munkacsoportot hoz létre, az ENISA számára konkrét tanácsadás nyújtása és szakértelem biztosítása céljából.

(5) Az ENISA szorosan együttműködik az európai kiberbiztonsági tanúsítási csoporttal. Az európai kiberbiztonsági tanúsítási csoportnak segítséget és szakértői tanácsadást kell biztosítania az ENISA számára a javaslati rendszer kidolgozása kapcsán, és véleményt kell elfogadnia a javasolt rendszerről.

(6) Az ENISA-nak a (3), a (4) és az (5) bekezdéssel összhangban kidolgozott javaslati rendszer Bizottságnak történő továbbítása előtt a lehető legkörültekintőbben figyelembe kell vennie az európai kiberbiztonsági tanúsítási csoport véleményét. Az európai kiberbiztonsági tanúsítási csoport véleménye az ENISA-ra nézve nem kötelező érvényű, és ezen vélemény hiánya nem akadályozza az ENISA-t a javasolt rendszer Bizottságnak történő továbbításában.

(7) A Bizottság az ENISA által kidolgozott javasolt rendszer alapján végrehajtási jogi aktusokat fogadhat el, amelyekben az IKT-termékekre, az IKT-szolgáltatásokra és az IKT-folyamatokra vonatkozó, az 51., az 52. és az 54. cikkben meghatározott követelményeknek megfelelő európai kiberbiztonsági tanúsítási rendszerekről rendelkezik. Ezeket a végrehajtási jogi aktusokat a 66. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(8) Az ENISA-nak legalább ötévente értékelnie kell minden egyes elfogadott európai kiberbiztonsági tanúsítási rendszert, az érdekelt felektől kapott visszajelzések figyelembevételével. Ha szükséges, a Bizottság vagy az európai kiberbiztonsági tanúsítási csoport felkérheti az ENISA-t, hogy a 48. és e cikkel összhangban indítsa el a módosított javaslati rendszer kidolgozására irányuló folyamatot.

50. cikk

Az európai kiberbiztonsági tanúsítási rendszerek honlapja

(1) Az európai kiberbiztonsági tanúsítási rendszerekről, az európai kiberbiztonsági tanúsítványokról és az uniós megfelelőségi nyilatkozatokról – ideértve a már nem érvényes európai kiberbiztonsági tanúsítási rendszerekre, a visszavont és lejárt európai kiberbiztonsági tanúsítványokra és az uniós megfelelőségi nyilatkozatokra, valamint az 55. cikkel összhangban rendelkezésre bocsátott kiberbiztonsági információkra mutató linkeket tartalmazó adattárakra vonatkozó információkat – tájékoztatás és az azokkal kapcsolatos publicitás biztosítása céljából az ENISA egy külön e célra szolgáló honlapot tart fenn.

(2) Az (1) bekezdésben említett honlapon adott esetben fel kell tüntetni azokat a nemzeti kiberbiztonsági tanúsítási rendszereket is, amelyeket egy európai kiberbiztonsági tanúsítási rendszer váltott fel.

51. 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, az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt;

b) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan megsemmisítéssel, elvesztéssel vagy megváltoztatással, vagy a hozzáférhetetlenséggel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt;

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

d) az ismert függőségek és sebezhetőségek azonosítása és dokumentálása;

e) annak rögzítése, hogy ki, mikor és mely adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt;

f) annak ellenőrizhetővé tétele, hogy ki, mikor és mely adatokat, szolgáltatásokat vagy funkciókat vette igénybe, használt vagy egyéb módon kezelt;

g) annak ellenőrzése, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok nem tartalmaznak ismert sebezhetőségeket;

h) fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, a szolgáltatások és a funkciók rendelkezésre állásának, valamint az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek a mihamarabbi helyreállítása;

i) az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok alapértelmezetten és tervezetten biztonságosak;

j) az IKT--termékek, az IKT-szolgáltatások és az IKT-folyamatok szoftvere és hardvere naprakész, esetükben nem állnak fenn közismert sebezhetőségek, és rendelkezésre állnak a biztonságos frissítésükre szolgáló mechanizmusok.

52. cikk

Az európai kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjei

(1) Az európai kiberbiztonsági tanúsítási rendszerek az IKT-termékekre, az IKT-szolgáltatásokra és az IKT-folyamatokra az „alap”, a „jelentős” és a „magas” megbízhatósági szintek közül egy vagy több szintet határozhatnak meg. A megbízhatósági szintnek a biztonsági események valószínűsége és hatása szempontjából arányban kell állnia az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat rendeltetés szerinti használatához kapcsolódó kockázat szintjével.

(2) Az európai kiberbiztonsági tanúsítványoknak és az uniós megfelelőségi nyilatkozatoknak hivatkozniuk kell az azon európai kiberbiztonsági tanúsítási rendszerben meghatározott bármely megbízhatósági szintre, amely alapján az európai kiberbiztonsági tanúsítványt vagy az uniós megfelelőségi nyilatkozatot kibocsátották.

(3) A releváns európai kiberbiztonsági tanúsítási rendszernek meg kell határoznia a minden egyes megbízhatósági szintnek megfelelő biztonsági követelményeket, ideértve a megfelelő biztonsági funkciókat és az IKT-termékre, az IKT-szolgáltatásra vagy az IKT-folyamatra alkalmazandó értékelés megfelelő szigorúságát és mélységét.

(4) A tanúsítványnak vagy az uniós megfelelőségi nyilatkozatnak hivatkoznia kell a rájuk vonatkozó műszaki előírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre, melyek célja a kiberbiztonsági események kockázatának csökkentése, illetve azok megelőzése.

(5) Az „alap” megbízhatósági szintet feltüntető európai kiberbiztonsági tanúsítvány vagy uniós megfelelőségi nyilatkozat arra vonatkozóan szolgál biztosítékkal, hogy azok az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok, amelyekre vonatkozóan az említett tanúsítványt vagy az említett uniós megfelelőségi nyilatkozatot kibocsátották, teljesítik a vonatkozó biztonsági követelményeket – többek között a biztonsági funkciókat – és olyan szintű értékelésen estek át, amely a biztonsági eseményekkel és támadásokkal kapcsolatos alapvető, ismert kockázatok minimalizálására törekszik. Az elvégzendő értékelési tevékenységeknek magukban kell foglalniuk legalább a műszaki dokumentáció áttekintését. Ha az ilyen áttekintés nem megfelelő, egyenlő hatású helyettesítő értékelési tevékenységeket kell végezni.

(6) A „jelentős” megbízhatósági szintet feltüntető európai kiberbiztonsági tanúsítvány arra vonatkozóan szolgál biztosítékkal, hogy azok az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok, amelyekre vonatkozóan az említett tanúsítványt kibocsátották, teljesítik a vonatkozó biztonsági követelményeket – többek között a biztonsági funkciókat – és olyan szintű értékelésen estek át, amely az ismert kiberbiztonsági kockázatok, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások minimalizálására törekszik. Az elvégzendő értékelési tevékenységeknek legalább az alábbiakat kell magukban foglalniuk: a közismert sebezhetőségek hiánya megállapításának felülvizsgálata és az annak megállapítására szolgáló tesztelés, hogy az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok megfelelően működtetik-e a szükséges biztonsági funkciókat. Ha ezen értékelési tevékenységek egyike sem megfelelő, egyenlő hatású helyettesítő értékelési tevékenységeket kell végezni.

(7) A „magas” megbízhatósági szintet feltüntető európai kiberbiztonsági tanúsítvány arra vonatkozóan szolgál biztosítékkal, hogy azon IKT-termékek, IKT-szolgáltatások és IKT-folyamatok, amelyekre vonatkozóan az említett tanúsítványt kibocsátották, teljesítik a vonatkozó biztonsági követelményeket – többek között a biztonsági funkciókat – és olyan szintű értékelésen estek át, amely a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által, a tudomány legutolsó állása szerinti technológiával végrehajtott kibertámadások minimalizálására törekszik. Az elvégzendő értékelési tevékenységeknek legalább az alábbiakat kell magukban foglalniuk: a közismert sebezhetőségek hiánya megállapításának felülvizsgálata; az annak megállapítására szolgáló tesztelés, hogy az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok megfelelően, a legfejlettebb technika szerint működtetik-e a szükséges biztonsági funkciókat; valamint behatolásvizsgálatok révén annak értékelése, hogy azok mennyire ellenállóak a jól képzett elkövetők által végrehajtott támadásokkal szemben. Ha ezen értékelési tevékenységek egyike sem megfelelő, egyenlő hatású helyettesítő értékelési tevékenységeket kell végezni.

(8) Az alkalmazott értékelési módszer szigorúságától és mélységétől függően egy európai kiberbiztonsági tanúsítási rendszerben több értékelési szint is meghatározható. Az értékelési szintek mindegyikének meg kell felelnie a megbízhatósági szintek egyikének, és azokat a megbízhatósági komponensek megfelelő kombinációjának megadásával kell meghatározni.

53. cikk

Megfelelőségi önértékelés

(1) Egy európai kiberbiztonsági tanúsítási rendszer lehetővé teheti, hogy az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártójának vagy nyújtójának kizárólagos felelőssége mellett megfelelőségi önértékelésre kerüljön sor. Megfelelőségi önértékelés csak az „alap” megbízhatósági szintnek megfelelő, alacsony kockázatot jelentő IKT-termékek, IKT-szolgáltatások és IKT-folyamatok vagy európai kiberbiztonsági tanúsítási rendszerek esetében engedhető meg.

(2) Az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártója vagy nyújtója uniós megfelelőségi nyilatkozatot állíthat ki arról, hogy megtörtént annak bizonyítása, hogy a tanúsítási rendszer követelményei teljesülnek. E nyilatkozat kiállításával az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártója vagy nyújtója felelősséget vállal azért, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelel az adott tanúsítási rendszer által előírt követelményeknek.

(3) Az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártójának vagy nyújtójának az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben meghatározott ideig az 58. cikk (1) bekezdésében említett nemzeti kiberbiztonsági tanúsító hatóság rendelkezésére kell bocsátania az uniós megfelelőségi nyilatkozatot, a műszaki dokumentációt és az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok tanúsítási rendszernek való megfelelésével kapcsolatos összes egyéb releváns információt. Az uniós megfelelőségi nyilatkozat másolati példányát meg kell küldeni a nemzeti kiberbiztonsági tanúsító hatóságnak és az ENISA-nak.

(4) Egy uniós megfelelőségi nyilatkozat kiállítása az uniós vagy a tagállami jog eltérő rendelkezése hiányában önkéntes.

(5) Az uniós megfelelőségi nyilatkozatot minden tagállamban el kell ismerni.

54. cikk

Az európai kiberbiztonsági tanúsítási rendszerek elemei

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

a) a tanúsítási rendszer tárgya és hatálya, ideértve a hatálya alá tartozó IKT-termékek, IKT-szolgáltatások és IKT-folyamatok típusát vagy kategóriáit;

b) a tanúsítási rendszer céljának és annak az egyértelmű meghatározása, hogy a kiválasztott szabványok, értékelési módszerek és megbízhatósági szintek hogyan felelnek meg a rendszer célfelhasználói igényeinek;

c) hivatkozás az értékelésben alkalmazott nemzetközi, európai vagy nemzeti szabványokra, vagy ha nem állnak rendelkezésre ilyen szabványok, vagy azok nem megfelelőek, az 1025/2012/EU rendelet II. mellékletében meghatározott követelményeket teljesítő műszaki előírásokra, vagy ha ilyen előírások nem állnak rendelkezésre, az európai kiberbiztonsági tanúsítási rendszerben meghatározott műszaki előírásra vagy egyéb kiberbiztonsági követelményekre;

d) adott esetben egy vagy több megbízhatósági szint;

e) annak megjelölése, hogy a megfelelőségi önértékelés megengedett-e az adott rendszerben;

f) adott esetben a megfelelőségértékelő szervezetekre alkalmazandó konkrét vagy kiegészítő követelmények, a kiberbiztonsági követelmények értékelésére való szakmai felkészültség biztosítása érdekében;

g) az alkalmazandó konkrét értékelési kritériumok és módszerek, ideértve az értékelés típusait is, az 51. cikkben említett biztonságiá célkitűzések elérésének bizonyítása érdekében;

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

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

j) az IKT-termékeknek, az IKT-szolgáltatásoknak és az IKT-folyamatoknak az európai kiberbiztonsági tanúsítványok vagy az uniós megfelelőségi nyilatkozatok követelményeinek való megfelelése nyomon követésének szabályai, ideértve a meghatározott kiberbiztonsági követelményeknek való folyamatos megfelelés bizonyítására szolgáló mechanizmusokat is;

k) adott esetben az európai kiberbiztonsági tanúsítvány kibocsátására, fenntartására, meghosszabbítására és megújítására, valamint a hatályának bővítésére vagy szűkítésére vonatkozó feltételek;

l) az annak következményeire vonatkozó szabályok, ha a tanúsított vagy uniós megfelelőségi nyilatkozat hatálya alá tartozó IKT-termékek, IKT-szolgáltatások és IKT-folyamatok nem felelnek meg a tanúsítási rendszer követelményeinek;

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

n) adott esetben a megfelelőségértékelő szervezetek nyilvántartásainak megőrzésére vonatkozó szabályok;

o) az azonos típusú vagy kategóriájú IKT- termékekre, IKT-szolgáltatásokra és IKT-folyamatokra kiterjedő nemzeti vagy nemzetközi kiberbiztonsági tanúsítási rendszerek, biztonsági követelmények, értékelési kritériumok és módszerek, valamint megbízhatósági szintek azonosítása;

p) a kiadandó európai kiberbiztonsági tanúsítvány és uniós megfelelőségi nyilatkozat tartalma és formátuma;

q) az uniós megfelelőségi nyilatkozatnak, a műszaki dokumentációnak, valamint minden egyéb releváns információnak az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártója vagy nyújtója általi rendelkezésre bocsátásának időtartama;

r) a rendszer alapján kibocsátott európai kiberbiztonsági tanúsítványok maximális érvényességi ideje;

s) a rendszer alapján kibocsátott, módosított vagy visszavont európai kiberbiztonsági tanúsítványokra vonatkozó közzétételi politika;

t) a tanúsítási rendszerek harmadik országokkal való kölcsönös elismerésének feltételei;

u) adott esetben az 56. cikk (6) bekezdése alapján a rendszer által a „magas” megbízhatósági szintű európai kiberbiztonsági tanúsítványokat kiállító hatóságokra és szervekre létrehozott szakértői értékelési mechanizmusra vonatkozó szabályok. Ez a mechanizmus nem érinti az 59. cikkben előírt kölcsönös felülvizsgálatot;

v) a kiegészítő kiberbiztonsági információ 55. cikkel összhangban történő megadása és frissítése során az IKT-termékek, IKT-szolgáltatások vagy IKT-eljárások gyártói vagy szolgáltatói által alkalmazandó formátumok és követendő eljárások.

(2) Az európai kiberbiztonsági tanúsítási rendszer meghatározott követelményeinek összhangban kell állniuk az alkalmazandó jogi követelményekkel, különösen az összehangolt uniós jogból eredő követelményekkel.

(3) Amennyiben egy adott uniós jogi aktus úgy rendelkezik, egy európai kiberbiztonsági tanúsítási rendszer keretében kiadott tanúsítás vagy uniós megfelelőségi nyilatkozat felhasználható az adott jogi aktus követelményeinek való megfelelés vélelmének igazolására.

(4) Összehangolt uniós jog hiányában, a tagállami jog úgy is rendelkezhet, hogy egy európai kiberbiztonsági tanúsítási rendszer a jogi követelményeknek való megfelelés vélelmezésére is használható.

55. cikk

Kiegészítő kiberbiztonsági információ a tanúsított IKT-termékekkel, IKT-szolgáltatásokkal és IKT-folyamatokkal kapcsolatban

(1) A tanúsított IKT-termékek, IKT-szolgáltatások, vagy IKT-folyamatok gyártói vagy nyújtói, vagy az olyan IKT-termékek, IKT-szolgáltatások, vagy IKT-folyamatok gyártói vagy nyújtói, amelyek tekintetében uniós megfelelőségi nyilatkozatot állítottak ki a következő kiegészítő információkat kötelesek nyilvánosan elérhetővé tenni:

a) a végfelhasználóknak az IKT-termékek vagy IKT-szolgáltatások biztonságos konfigurálásában, beszerelésében, telepítésében, üzemeltetésében és karbantartásában segítséget nyújtó iránymutatások és ajánlások;

b) a végfelhasználók számára nyújtott biztonsági támogatás időtartama, különös tekintettel a kiberbiztonsághoz kapcsolódó frissítések rendelkezésre állására;

c) a gyártó vagy a szolgáltatást nyújtó kapcsolattartási adatai, valamint a végfelhasználóktól vagy biztonsági kutatóktól érkező, sebezhetőséggel kapcsolatos információk fogadásának elfogadott módszerei;

d) az IKT-termékhez, IKT-szolgáltatáshoz vagy IKT-folyamathoz kapcsolódó, nyilvánosságra hozott sebezhetőségeket tartalmazó online adatbankokra és a releváns kiberbiztonsági tanácsadókra mutató hivatkozások.

(2) Az (1) bekezdésben említett információkat elektronikus formában kell rendelkezésre bocsátani, és legalább a vonatkozó európai kiberbiztonsági tanúsítvány vagy uniós megfelelőségi nyilatkozat lejáratáig biztosítani kell az elérhetőségüket, illetve szükség szerint naprakésszé kell tenni őket.

56. cikk

Kiberbiztonsági tanúsítás

(1) A 49. cikk alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek keretében tanúsított IKT-termékekről, IKT-szolgáltatásokról és IKT-folyamatokról vélelmezni kell, hogy megfelelnek az e rendszerek által támasztott követelményeknek.

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

(3) A Bizottság az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok Unión belüli megfelelő szintű kiberbiztonságának biztosítása és a belső piac működésének javítása érdekében rendszeresen értékeli az elfogadott európai kiberbiztonsági tanúsítási rendszerek hatékonyságát és alkalmazását, valamint azt, hogy valamely konkrét európai kiberbiztonsági rendszert a vonatkozó uniós jog útján kötelezővé kell-e tenni. Az első ilyen értékelést legkésőbb 2023. december 31-ig el kell végezni, az ezt követő értékeléseket pedig legalább kétévenként. A Bizottság az említett értékelés eredményeitől függően azonosítja a valamely létező tanúsítási rendszer hatálya alá tartozó azon IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat, amelyeket kötelező tanúsítási rendszer hatálya alá kell vonni.

A Bizottság elsősorban az (EU) 2016/1148 irányelv II. mellékletében felsorolt ágazatokra összpontosít, amelyek értékelését legkésőbb két évvel az első európai kiberbiztonsági tanúsítási rendszer elfogadását követően végzi el.

Az értékelés elkészítése során a Bizottság:

a) figyelembe veszi az intézkedéseknek az ilyen IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok gyártóira vagy nyújtóira és a felhasználókra gyakorolt hatásait ezen intézkedések költségei, valamint a megcélzott IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok várható magasabb biztonsági szintjéből eredő társadalmi vagy gazdasági előnyök tekintetében;

b) figyelembe veszi a vonatkozó tagállami és harmadik országbeli jog létezését és alkalmazását;

c) nyílt, átlátható és inkluzív konzultációt folytat valamennyi releváns érdekelt féllel és tagállammal;

d) figyelembe veszi a végrehajtási határidőket, az átmeneti intézkedéseket és időszakokat, tekintettel különösen az intézkedésnek az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok gyártóira vagy szolgáltatóira – többek között a kkv-kra – gyakorolt lehetséges hatására;

e) olyan javaslatot terjeszt elő, amely alapján az önkéntes tanúsítási rendszerről a kötelező tanúsítási rendszerre való átállás a lehető leggyorsabb és leghatékonyabb módon hajtható végre.

(4) Az e cikk szerinti, „alap” vagy „jelentős” megbízhatósági szintre hivatkozó európai kiberbiztonsági tanúsítványt a 60. cikkben említett megfelelőségértékelő szervezetek a 49. cikk alapján a Bizottság által elfogadott európai kiberbiztonsági tanúsítási rendszerben foglalt kritériumok alapján adják ki.

(5) A (4) bekezdéstől eltérve, kellően indokolt esetben egy európai kiberbiztonsági tanúsítási rendszer előírhatja, hogy e rendszer keretében csak közjogi szerv adhat ki európai kiberbiztonsági tanúsítványt, amennyiben az ilyen eltérést kellően megindokolják. E szervnek a következők valamelyikének kell lennie:

a) az 58. cikk (1) bekezdésében említett nemzeti kiberbiztonsági tanúsító hatóság;

b) a 60. cikk (1) bekezdése szerinti megfelelőségértékelő szervezetként akkreditált közjogi szerv.

(6) Ha a 49. cikk szerint elfogadott európai kiberbiztonsági tanúsítási rendszer „magas” megbízhatósági szintet ír elő, az adott rendszer keretében az európai kiberbiztonsági tanúsítványt csak nemzeti kiberbiztonsági tanúsító hatóság állíthatja ki, vagy megfelelőségértékelő szervezet abban az esetben, ha:

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

b) az említett európai kiberbiztonsági tanúsítványok kiállításának feladatát a nemzeti kiberbiztonsági tanúsító hatóság általános jelleggel átruházta az adott megfelelőségértékelő szervezetre.

(7) Az IKT-termékeiket, IKT-szolgáltatásaikat vagy IKT-folyamataikat tanúsítási mechanizmusnak alávető természetes vagy jogi személyek kötelesek az 58. cikkben említett nemzeti kiberbiztonsági tanúsító hatóság– amennyiben az európai kiberbiztonsági tanúsítványt e hatóság állította ki –, vagy a 60. cikkben említett megfelelőségértékelő szervezet rendelkezésére bocsátani a tanúsítási lefolytatásához szükséges összes információt.

(8) Az európai kiberbiztonsági tanúsítvány jogosultjának tájékoztatnia kell a (7) bekezdésben említett hatóságot vagy szervezetet minden olyan, a tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságát érintő, utólag észlelt sebezhetőségről vagy rendellenességről, amely hatással lehet az említett termék, szolgáltatás vagy folyamat tanúsítással összefüggő követelményeknek való megfelelésére. Ez a hatóság vagy szervezet az említett információt köteles indokolatlan késedelem nélkül továbbítani az érintett nemzeti kiberbiztonsági tanúsító hatóságnak.

(9) Az európai kiberbiztonsági tanúsítványokat az európai kiberbiztonsági tanúsítási rendszerben meghatározott időtartamra kell kiállítani, és megújíthatók, feltéve hogy a vonatkozó követelmények továbbra is teljesülnek.

(10) Az e cikk alapján kiadott európai kiberbiztonsági tanúsítványokat valamennyi tagállamban el kell ismerni.

57. cikk

Nemzeti kiberbiztonsági tanúsítási rendszerek és tanúsítványok

(1) E cikk (3) bekezdésének sérelme nélkül a nemzeti kiberbiztonsági tanúsítási rendszerek és az IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozó olyan kapcsolódó eljárások, amelyek egy európai kiberbiztonsági tanúsítási rendszer hatálya alá tartoznak, a 49. cikk (7) bekezdése alapján elfogadott végrehajtási jogi aktusban meghatározott időponttól nem bírnak joghatással. A nemzeti kiberbiztonsági tanúsítási rendszerek és az IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozó olyan kapcsolódó eljárások, amelyek nem tartoznak egy európai kiberbiztonsági tanúsítási rendszer hatálya alá, továbbra is fennmaradnak.

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

(3) A nemzeti kiberbiztonsági tanúsítási rendszerek alapján kiadott, és valamely európai kiberbiztonsági tanúsítási rendszer hatálya alá tartozó meglévő tanúsítványok lejáratuk időpontjáig érvényesek maradnak.

(4) A belső piac széttagoltságának elkerülése érdekében a tagállamok tájékoztatják a Bizottságot és az európai kiberbiztonsági tanúsítási csoportot az új nemzeti kiberbiztonsági tanúsítási rendszerek kidolgozására irányuló szándékukról.

58. cikk

Nemzeti kiberbiztonsági tanúsító hatóságok

(1) Minden tagállam a saját területén kijelöl egy vagy több nemzeti kiberbiztonsági tanúsító hatóságot, vagy egy másik tagállammal történő megállapodás alapján, egy vagy több ezen másik tagállamban letelepedett nemzeti kiberbiztonsági tanúsító hatóságot a kijelölő tagállam felügyeleti feladatainak ellátásáért felelős hatóságként.

(2) Minden tagállam tájékoztatja a Bizottságot arról, hogy mely hatóságokat jelölt ki nemzeti kiberbiztonsági tanúsító hatóságként. Amennyiben egy tagállam több hatóságot jelöl ki, arról is tájékoztatja a Bizottságot, hogy az egyes hatóságokat milyen feladatokkal bízta meg.

(3) Az 56. cikk (5) bekezdése a) pontjának, valamint az 56. cikk (6) bekezdésének sérelme nélkül, az egyes nemzeti kiberbiztonsági tanúsító hatóságoknak – a szervezetét, a finanszírozási határozatokat, a jogi felépítését és a döntéshozatalát illetően – függetlennek kell lenniük az általa felügyelt szervezetektől.

(4) A tagállamok gondoskodnak arról, hogy a nemzeti kiberbiztonsági tanúsító hatóságok azon tevékenységei, amelyek az európai kiberbiztonsági tanúsítványoknak az 56. cikk (5) bekezdésének a) pontjában, valamint az 56. cikk (6) bekezdésében említett kiállításával kapcsolatosak, szigorúan el legyenek választva az e cikkben megállapított felügyeleti tevékenységeiktől, és e tevékenységek ellátása egymástól függetlenül történjen.

(5) A tagállamok biztosítják, hogy a nemzeti kiberbiztonsági tanúsító hatóságok rendelkezzenek a hatáskörük gyakorlásához, valamint a feladataik hatékony és eredményes elvégzéséhez szükséges megfelelő forrásokkal.

(6) E rendelet hatékony végrehajtása érdekében célszerű, hogy ezek a nemzeti kiberbiztonsági tanúsító hatóságok – aktív, hatékony, eredményes és biztonságos módon – részt vegyenek az európai kiberbiztonsági tanúsítási csoportban.

(7) A nemzeti kiberbiztonsági tanúsító hatóságok:

a) más illetékes piacfelügyeleti hatóságokkal együttműködve felügyelik és betartatják az IKT-termékeknek, az IKT-szolgáltatásoknak és az IKT-folyamatoknak az illetékességi területükön kiadott európai kiberbiztonsági tanúsítványok követelményeinek való megfelelése nyomon követésére vonatkozó, az 54. cikk (1) bekezdésének j) pontja alapján az európai kiberbiztonsági tanúsítási rendszerekbe foglalt szabályokat;

b) betartatják az IKT-termékeknek, az IKT-szolgáltatásoknak vagy az IKT-folyamatoknak az illetékességi területükön letelepedett és megfelelőségi önértékelést végző gyártóira vagy nyújtóira vonatkozó kötelezettségeket és nyomon követik az azoknak való megfelelést, így különösen betartatják az 53. cikk (2) és (3) bekezdésében, valamint az alkalmazandó európai kiberbiztonsági tanúsítási rendszerben megállapított, az említett gyártókra és szolgáltatókra vonatkozó kötelezettségeket és nyomon követik az azoknak való megfelelést;

c) a 60. cikk (3) bekezdésének sérelme nélkül, e rendelet alkalmazása céljából aktívan segítik és támogatják a nemzeti akkreditáló szerveket a megfelelőségértékelő szervezetek tevékenységeinek nyomon követésében és felügyeletében;

d) nyomon követik és felügyelik az 56. cikk (5) bekezdésében említett közjogi szervek tevékenységeit;

e) adott esetben a 60. cikk (3) bekezdésével összhangban engedélyezik a megfelelőségértékelő szervezeteket, valamint – amennyiben a megfelelőségértékelő szervezetek megszegik e rendelet követelményeit – korlátozzák, felfüggesztik vagy visszavonják az érvényes engedélyeket;

f) kezelik a természetes vagy jogi személyeknek a nemzeti kiberbiztonsági tanúsító hatóságok által kiadott európai kiberbiztonsági tanúsítványokkal vagy az 56. cikk (6) bekezdésével összhangban a megfelelőségértékelő szervezetek által kiadott európai kiberbiztonsági tanúsítványokkal, vagy az 53. cikk alapján kiadott uniós megfelelőségi nyilatkozatokkal kapcsolatban benyújtott panaszait, valamint megfelelő mértékben kivizsgálják az ilyen panasz tárgyát, továbbá észszerű időn belül tájékoztatják a panaszost a vizsgálat előrehaladásáról és eredményéről;

g) évente összefoglaló jelentésben beszámolnak az ENISA-nak és az európai kiberbiztonsági tanúsítási csoportnak az e bekezdés b), c) és d) pontja és a (8) bekezdés alapján végzett tevékenységekről;

h) együttműködnek a többi nemzeti kiberbiztonsági tanúsító hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos IKT-termékek, IKT-szolgáltatások és IKT-folyamatok nem felelnek meg e rendelet vagy egyes európai kiberbiztonsági tanúsítási rendszerek követelményeinek; és

i) figyelemmel kísérik a kiberbiztonsági tanúsítás terén zajló releváns fejleményeket.

(8) 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) az e címnek való megfelelésük ellenőrzése céljából ellenőrzések formájában vizsgálatokat végezhet a megfelelőségértékelő szervezeteknél, az európai kiberbiztonsági tanúsítványok jogosultjainál és az uniós megfelelőségi nyilatkozatok kibocsátóinál;

c) a nemzeti joggal összhangban meghozhatja a megfelelő intézkedéseket annak biztosítása érdekében, hogy a megfelelőségértékelő szervezetek, az európai kiberbiztonsági tanúsítványok jogosultjai és az uniós megfelelőségi nyilatkozatok kibocsátói megfeleljenek e rendeletnek, illetve az adott európai kiberbiztonsági tanúsítási rendszernek;

d) beléphetnek bármely megfelelőségértékelő szervezet vagy az európai kiberbiztonsági tanúsítványok bármely jogosultjának helyiségeibe az uniós vagy a tagállami eljárásjoggal összhangban folytatott vizsgálatok elvégzése céljából;

e) a nemzeti joggal összhangban visszavonhatja a nemzeti kiberbiztonsági tanúsító hatóságok által kiadott európai kiberbiztonsági tanúsítványokat vagy az 56. cikk (6) bekezdésével összhangban a megfelelőségértékelő szervezetek által kiadott európai kiberbiztonsági tanúsítványokat, amennyiben az említett tanúsítványok nem felelnek meg e rendeletnek vagy az adott európai kiberbiztonsági tanúsítási rendszernek;

f) a 65. cikknek megfelelően a nemzeti joggal összhangban szankciókat rendelhet el, valamint előírhatja az e rendeletben meghatározott kötelezettségek megszegésének azonnali megszüntetését.

(9) A nemzeti kiberbiztonsági tanúsító hatóságoknak együtt kell működniük egymással és a Bizottsággal, különösen az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kiberbiztonságára vonatkozó kiberbiztonsági tanúsítással és műszaki kérdésekkel kapcsolatos információk, tapasztalatok és bevált gyakorlatok cseréje révén.

59. cikk

Kölcsönös felülvizsgálat

(1) Az európai kiberbiztonsági tanúsítványok és az uniós megfelelőségi nyilatkozatok tekintetében alkalmazott szabványok az Unióban való egyenértékűségének elérése céljából a nemzeti kiberbiztonsági tanúsító hatóságokat kölcsönös felülvizsgálatnak kell alávetni.

(2) A kölcsönös felülvizsgálatot hatékony és átlátható értékelési feltételek és eljárások alapján kell végezni, különösen a szervezeti és humán erőforrások, valamint az eljárási követelmények, a titoktartás és a panaszok tekintetében.

(3) A kölcsönös felülvizsgálat a következőket értékeli:

a) adott esetben, hogy a nemzeti kiberbiztonsági tanúsító hatóságok azon tevékenységei, amelyek az európai kiberbiztonsági tanúsítványoknak az 56. cikk (5) bekezdésének a) pontjában és az 56. cikk (6) bekezdésében említett kiadásával kapcsolatosak, szigorúan el vannak-e választva az 58. cikkben megállapított felügyeleti tevékenységeiktől, és hogy az említett tevékenységek ellátása egymástól függetlenül történik-e;

b) az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok európai kiberbiztonsági tanúsítványoknak való megfelelésének nyomon követésére szolgáló szabályoknak az 58. cikk (7) bekezdésének a) pontja alapján történő felügyeletére és betartatására szolgáló eljárásokat;

c) az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok gyártóira vagy nyújtóira vonatkozó kötelezettségeknek az 58. cikk (7) bekezdésének b) pontja alapján történő nyomon követésére és betartatására szolgáló eljárásokat;

d) a megfelelőségértékelő szervezetek tevékenységeinek nyomon követésére, engedélyezésére és felügyeletére szolgáló eljárásokat;

e) adott esetben azt, hogy az 56. cikk (6) bekezdése alapján „magas” megbízhatósági szintre szóló tanúsítványokat kiállító hatóságok vagy szervezetek személyzetének szakértelme megfelelő-e.

(4) A kölcsönös felülvizsgálatot más tagállamokból legalább két nemzeti kiberbiztonsági tanúsító hatóságnak és a Bizottságnak kell elvégeznie legalább ötévente egyszer. Az ENISA részt vehet a kölcsönös felülvizsgálatban.

(5) A Bizottság végrehajtási jogi aktusokat fogadhat el a kölcsönös felülvizsgálatok legalább ötéves időszakot lefedő tervének megállapítására, a kölcsönös felülvizsgálatot végző csoport összetételére, a kölcsönös felülvizsgálatnál alkalmazandó módszertanra, valamint a kölcsönös felülvizsgálatok menetrendjére, gyakoriságára és az azokhoz kapcsolódó egyéb feladatokra vonatkozó kritériumok meghatározására vonatkozóan. A Bizottság az említett végrehajtási jogi aktusok elfogadásakor megfelelően figyelembe veszi az európai kiberbiztonsági tanúsítási csoport észrevételeit. Ezeket a végrehajtási jogi aktusokat a 66. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(6) Az európai kiberbiztonsági tanúsítási csoportnak meg kell vizsgálnia a kölcsönös felülvizsgálatok eredményét, amelyről olyan összefoglalót kell készítenie, amely nyilvánosan hozzáférhetővé tehető, továbbá szükség esetén iránymutatásokat vagy ajánlásokat kell kibocsátani az érintett szervezetek által megteendő fellépésekről vagy meghozandó intézkedésekről.

60. cikk

Megfelelőségértékelő szervezetek

(1) A megfelelőségértékelő szervezeteket a 765/2008/EK rendelet alapján kijelölt nemzeti akkreditáló testületek akkreditálják. Ez az akkreditáció csak akkor adható meg, ha megfelelőségértékelő szervezet megfelel az e rendelet mellékletében meghatározott követelményeknek.

(2) Ha egy európai kiberbiztonsági tanúsítványt egy nemzeti kiberbiztonsági tanúsító hatóság állít ki az 56. cikk (5) cikkének a) pontja, illetve az 56. cikkének (6) bekezdése alapján, a nemzeti kiberbiztonsági tanúsító hatóság tanúsító szervének e cikk (1) bekezdése szerint megfelelőségértékelő szervezetként akkreditált szervnek kell lennie.

(3) Amennyiben az európai kiberbiztonsági tanúsítási rendszerek az 54. cikk (1) bekezdésének f) pontja alapján konkrét vagy kiegészítő követelményeket állapítanak meg, a nemzeti kiberbiztonsági tanúsító hatóság kizárólag azoknak a megfelelőségértékelő szervezeteknek engedélyezi az ilyen rendszerek keretében végzendő feladatok ellátását, amelyek megfelelnek az említett követelményeknek.

(4) Az (1) bekezdésben említett akkreditáció a megfelelőségértékelő szervezetek számára legfeljebb öt évre adható meg, és azonos feltételek mellett megújítható, feltéve, hogy az adott megfelelőségértékelő szervezet még mindig teljesíti az e cikkben meghatározott követelményeket. A nemzeti akkreditáló testületeknek észszerű időkereten belül minden megfelelő intézkedést meg kell tenniük a megfelelőségértékelő szervezet (1) bekezdés alapján megadott akkreditációjának a korlátozása, felfüggesztése vagy visszavonása érdekében, amennyiben az akkreditáció feltételei nem, vagy már nem teljesülnek, vagy ha a megfelelőségértékelő szervezet megsérti ezt a rendeletet.

61. cikk

Bejelentés

(1) A nemzeti kiberbiztonsági tanúsító hatóságoknak minden egyes európai kiberbiztonsági tanúsítási rendszer vonatkozásában be kell jelenteniük a Bizottságnak azokat a megfelelőségértékelő szervezeteket amelyeket akkreditáltak, és – adott esetben – a 60. cikk (3) bekezdése alapján az 52. cikkben említett, meghatározott megbízhatósági szintű európai kiberbiztonsági tanúsítványok kiadására feljogosítottak. A nemzeti kiberbiztonsági tanúsító hatóságoknak az említettekben a későbbiekben bekövetkezett bármilyen változást indokolatlan késedelem nélkül be kell jelenteniük a Bizottságnak.

(2) Egy évvel az adott európai kiberbiztonsági tanúsítási rendszer hatálybalépését követően a Bizottság az *Európai Unió Hivatalos Lapjában* közzéteszi az adott rendszer keretében bejelentett megfelelőségértékelő szervezetek jegyzékét.

(3) Amennyiben a (2) bekezdésben említett határidő lejárta után érkezik a Bizottsághoz bejelentés, a Bizottság a bejelentett megfelelőségértékelő szervezetek jegyzékének módosításait az említett bejelentés kézhezvételétől számított két hónapon belül közzéteszi az *Európai Unió Hivatalos Lapjában.*

(4) Valamely nemzeti kiberbiztonsági tanúsító hatóság kérelmet nyújthat be a Bizottsághoz az adott hatóság által bejelentett megfelelőségértékelő szervezetnek a bejelentett megfelelőségértékelő szervezetek (2) bekezdésben említett jegyzékéből való törlése iránt. A Bizottság a nemzeti kiberbiztonsági tanúsító hatóság kérelmének kézhezvételétől számított egy hónapon belül közzéteszi az említett jegyzék megfelelő módosításait az *Európai Unió Hivatalos Lapjában*.

(5) A Bizottság végrehajtási jogi aktusokat fogadhat el, hogy meghatározza az e cikk (1) bekezdésében említett bejelentésekre vonatkozó körülményeket, formátumokat és eljárásokat. E végrehajtási jogi aktusokat a 66. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

62. cikk

Európai kiberbiztonsági tanúsítási csoport

(1) Létrejön az európai kiberbiztonsági tanúsítási csoport.

(2) Az európai kiberbiztonsági tanúsítási csoport a nemzeti kiberbiztonsági tanúsító hatóságok képviselőiből vagy más illetékes nemzeti hatóságok képviselőiből áll. Az európai kiberbiztonsági tanúsítási csoport valamely tagja legfeljebb két tagállamot képviselhet.

(3) Az érdekelt felek és az érintett harmadik felek meghívást kaphatnak az európai kiberbiztonsági tanúsítási csoport ülésein való részvételre, és részt vehetnek annak munkájában.

(4) Az európai kiberbiztonsági tanúsítási csoport feladatai a következők:

a) tanácsot ad és segítséget nyújt a Bizottságnak az e cím rendelkezéseinek következetes végrehajtására és alkalmazására irányuló munkájával kapcsolatban, különös tekintettel az uniós gördülő munkaprogramra, a kiberbiztonsági tanúsítási szakpolitikával kapcsolatos kérdésekre, a szakpolitikai megközelítések összehangolására, valamint az európai kiberbiztonsági tanúsítási rendszerek kidolgozására;

b) segítséget nyújt és tanácsot ad az ENISA-nak, valamint együttműködik az ENISA-val a javasolt tanúsítási rendszerek e rendelet 49. cikke szerinti kidolgozásával kapcsolatban;

c) a 49. cikk alapján véleményt fogad el az ENISA által kidolgozott javasolt tanúsítási rendszerekről;

d) felkéri az ENISA-t, hogy a 48. cikk (2) bekezdése alapján javasolt tanúsítási rendszert dolgozzon ki;

e) a Bizottságnak címzett véleményeket fogad el a létező európai kiberbiztonsági tanúsítási rendszerek fenntartásával és felülvizsgálatával kapcsolatban;

f) tanulmányozza a kiberbiztonsági tanúsítás terén zajló releváns fejleményeket, és megosztja a kiberbiztonsági tanúsítási rendszerekkel kapcsolatos információkat és bevált gyakorlatokat;

g) kapacitásépítés és információcsere útján előmozdítja a nemzeti kiberbiztonsági tanúsító hatóságok közötti, e cím rendelkezései szerinti együttműködést, különösen a kiberbiztonsági tanúsítással kapcsolatos kérdésekre vonatkozó hatékony információcserére szolgáló módszerek kialakítása révén;

h) támogatást biztosít az 54. cikke (1) bekezdésének u) pontja szerinti, valamely európai kiberbiztonsági tanúsítási rendszer szabályaival összhangban álló szakértői értékelési mechanizmus végrehajtásához;

i) előmozdítja az európai kiberbiztonsági tanúsítási rendszerek összhangba hozását a nemzetközileg elismert szabványokkal, többek között a létező európai kiberbiztonsági tanúsítási rendszerek felülvizsgálata, és adott esetben az ENISA számára ajánlások megfogalmazása által, hogy az vegye fel a kapcsolatot a megfelelő nemzetközi szabványügyi szervezetekkel a rendelkezésre álló nemzetközileg elismert szabványok hiányosságainak kezelése céljából.

(5) Az európai kiberbiztonsági tanúsítási csoport elnöki tisztét az ENISA segítségével a Bizottság tölti be, és a 8. cikk (1) bekezdése e) pontjával összhangban az európai kiberbiztonsági tanúsítási csoport titkárságát a Bizottság biztosítja.

63. cikk

A panasztétel joga

(1) A természetes és a jogi személyeknek joguk van panaszt benyújtani az európai kiberbiztonsági tanúsítvány kibocsátójánál vagy ha a panasz valamely megfelelőségértékelő szervezet által az 56. cikk (6) bekezdésével összhangban eljárva kiadott európai kiberbiztonsági tanúsítványra vonatkozik a releváns nemzeti kiberbiztonsági tanúsító hatóságnál.

(2) Az a hatóság vagy szervezet, amelyhez a panaszt benyújtották, köteles tájékoztatni a panaszost az eljárás előrehaladásáról és a meghozott határozatról, valamint a 64. cikkben említett hatékony bírósági jogorvoslathoz való jogról.

64. cikk

A hatékony bírósági jogorvoslathoz való jog

(1) Bármely közigazgatási vagy egyéb nem bírósági jogorvoslat sérelme nélkül minden természetes és jogi személynek joga van a hatékony bírósági jogorvoslathoz az alábbiak tekintetében:

a) a 63. cikk (1) bekezdésében említett hatóságok vagy szervezetek által hozott határozatok, ideértve adott esetben a természetes és jogi személyeket feljogosító európai kiberbiztonsági tanúsítványok nem megfelelő kiadásával, kiadásának elmaradásával vagy elismerésével kapcsolatban hozott határozatokat;

b) a 63. cikk (1) bekezdésében említett hatóságokhoz vagy szervezetekhez benyújtott panasz ügyében történő eljárás elmulasztása.

(2) Az e cikk szerinti bírósági eljárást azon tagállam bírósága előtt kell megindítani, amelyben az a hatóság vagy szervezet, amely ellen a bírósági jogorvoslattal élni kívánnak található.

65. cikk

Szankciók

A tagállamok megállapítják az e cím és az európai kiberbiztonsági tanúsítási rendszerek megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük. A tagállamok haladéktalanul tájékoztatják a Bizottságot az említett szabályokról és tájékoztatják a Bizottságot az e szabályokat érintő minden későbbi módosításról.

IV. CÍM
ZÁRÓ RENDELKEZÉSEK

66. cikk

Bizottsági eljárás

(1) A Bizottságot egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikke (4) bekezdésének b) pontját kell alkalmazni.

67. cikk

Értékelés és felülvizsgálat

(1) A Bizottság … [öt évvel e rendelet hatálybalépését követően]-ig, majd azt követően ötévente értékeli az ENISA és munkamódszerei hatását, eredményességét és hatékonyságát, hogy szükséges-e módosítani az ENISA megbízatását, hogy egy ilyen módosítás milyen pénzügyi vonzatokkal járna. Az értékelésben figyelembe kell venni minden olyan visszajelzést, amelyet az ENISA a tevékenységével kapcsolatban kapott. Amennyiben a Bizottság megítélése szerint az ENISA működése kitűzött céljai, megbízatása és feladatai tekintetében a továbbiakban nem indokolt, javasolhatja e rendeletnek az ENISA-ra vonatkozó rendelkezései tekintetében történő módosítását.

(2) Az értékelésben fel kell mérni a III. címben foglalt rendelkezések hatását, eredményességét és hatékonyságát az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok Unión belüli megfelelő szintű kiberbiztonságának biztosítására és a belső piac működésének javítására vonatkozó célkitűzések tekintetében is.

(3) Az értékelésben fel kell mérni, hogy szükség van-e alapvető kiberbiztonsági követelményekre a belső piachoz való hozzáférés tekintetében olyan IKT-termékek, IKT-szolgáltatások és IKT-folyamatok uniós piacra való belépésének megelőzése érdekében, amelyek nem felelnek meg az alapszintű kiberbiztonsági követelményeknek.

(4) A Bizottság az értékelésről szóló jelentést ... [öt évvel e rendelet hatálybalépését követően]-ig, majd azt követően ötévente következtetéseivel együtt megküldi az Európai Parlamentnek, a Tanácsnak, és az igazgatótanácsnak. A jelentés megállapításait közzé kell tenni.

68. cikk

Hatályon kívül helyezés és jogutódlás

(1) Az 526/2013/EU rendelet … [e rendelet hatálybalépésének időpontja]-ával/ével hatályát veszti.

(2) Az 526/2013/EU rendeletre és az említett rendelettel létrehozott ENISA-ra való hivatkozásokat erre a rendeletre, illetve az e rendelettel létrehozott ENISA-ra való hivatkozásnak kell tekinteni.

(3) Az az e rendelettel létrehozott ENISA mindennemű tulajdonviszony, megállapodás, jogi kötelezettség, munkaszerződés, pénzügyi kötelezettségvállalás és felelősség vonatkozásában az 526/2013/EU rendelettel létrehozott ENISA jogutódja. Az igazgatóság és a végrehajtó testület által az 526/2013/EU rendelettel összhangban hozott valamennyi határozat érvényben marad, feltéve, hogy azok megfelelnek e rendeletnek.

(4) Az ENISA … [e rendelet hatálybalépésének időpontja]-tól/től határozatlan időtartamra jön létre.

(5) Az 526/2013/EU rendelet 24. cikkének (4) bekezdése alapján kinevezett ügyvezető igazgató hivatali idejének fennmaradó részében hivatalban marad és ellátja az e rendelet 20. cikkében említett ügyvezetői igazgatói feladatokat. Szerződésének egyéb feltételei nem változnak.

(6) Az igazgatóságnak az 526/2013/EU rendelet 6. cikke alapján kinevezett tagjai és azok helyettesei hivatali idejük fennmaradó részében hivatalban maradnak és ellátják az e rendelet 15. cikkében említett igazgatósági feladatokat.

69. cikk

Hatálybalépés

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

(2) Az 58., a 60., a 61., a 63., a 64. és a 65. cikket … [24 hónappal e rendelet hatálybalépésének időpontját követően]-tól/-től kell alkalmazni.

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

Kelt,

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

MELLÉKLET

A MEGFELELŐSÉGÉRTÉKELŐ SZERVEZETEK ÁLTAL TELJESÍTENDŐ KÖVETELMÉNYEK

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

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

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

3. Megfelelőségértékelő szervezetnek tekinthető olyan szervezet is, amely az általa értékelt IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok tervezésében, gyártásában, nyújtásában, összeszerelésében, használatában vagy karbantartásában részt vevő vállalkozásokat képviselő vállalkozói szövetséghez vagy szakmai egyesüléshez tartozik, feltéve, hogy bizonyítottan független és esetében bizonyítottan nem áll fenn összeférhetetlenség.

4. A megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyek nem lehetnek tervezői, gyártói, nyújtói, üzembe helyezői, vásárlói, tulajdonosai, felhasználói vagy karbantartói az értékelt IKT-terméknek, IKT-szolgáltatásnak vagy IKT-folyamatnak, valamint nem lehetnek az említett felek meghatalmazott képviselői sem. Ez a tilalom nem zárja ki a megfelelőségértékelő szervezet működéséhez szükséges, értékelt IKT-termékek használatát, sem az ilyen IKT-termékek személyes célra történő használatát.

5. A megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyek nem vehetnek részt közvetlenül az értékelt IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok tervezésében, gyártásában és kivitelezésében, értékesítésében, üzembe helyezésében, használatában és karbantartásában, valamint nem képviselhetnek az ilyen tevékenységekben részt vevő feleket. A megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési feladatok elvégzéséért felelős személyek nem vehetnek részt olyan tevékenységben sem, amely megfelelőségértékelési tevékenységük tekintetében veszélyeztetné döntéshozói függetlenségüket vagy feddhetetlenségüket. Ezt a tilalmat különösen a tanácsadói szolgáltatásokra is alkalmazni kell.

6. Amennyiben egy megfelelőségértékelő szervezet állami szerv vagy intézmény tulajdonában van vagy ilyen működteti, biztosítani és dokumentálni kell a függetlenséget és az összeférhetetlenség hiányát a nemzeti kiberbiztonsági tanúsító hatóság és a megfelelőségértékelő szervezet között.

7. A megfelelőségértékelő szervezeteknek biztosítaniuk kell, hogy leányvállalataik és alvállalkozóik tevékenysége ne befolyásolja megfelelőségértékelési tevékenységeik bizalmasságát, objektivitását és pártatlanságát.

8. A megfelelőségértékelő szervezeteknek és személyzetüknek a legmagasabb szintű szakmai feddhetetlenséggel és az adott szakterületen elvárható műszaki felkészültséggel kell megfelelőségértékelési tevékenységüket végezniük, és függetlennek kell lenniük minden olyan – többek között pénzügyi jellegű – nyomásgyakorlástól és ösztönzéstől, amely befolyásolhatná ítélőképességüket vagy megfelelőségértékelési tevékenységük eredményeit, különösen az említett tevékenységek eredményeiben érdekelt személyek vagy azok csoportja tekintetében.

9. A megfelelőségértékelő szervezetnek képesnek kell lennie az e rendelet alapján ráruházott valamennyi megfelelőségértékelési feladat elvégzésére, függetlenül attól, hogy ezeket a feladatokat a megfelelőségértékelő szervezet maga, vagy az ő nevében és az ő felelőssége mellett valaki más végzi el. Alvállalkozók megbízását vagy külső személyzettel történő konzultációt megfelelően dokumentálni kell, ezekben közvetítő nem vonható be, valamint írásos megállapodást kell készíteni, amely többek között kiterjed a bizalmas ügykezelésre és az összeférhetetlenségre. Az elvégzett feladatokért teljes mértékben az adott megfelelőségértékelő szervezet felelős.

10. A megfelelőségértékelő szervezetnek minden megfelelőségértékelési eljárás és az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok minden típusa, kategóriája és alkategóriája tekintetében mindenkor rendelkeznie kell a szükséges:

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

b) azon eljárások leírásával, amelyekkel összhangban a megfelelőségértékelést végzik, hogy biztosítva legyen ezen eljárások átláthatósága és megismételhetőségük lehetősége. Rendelkeznie kell megfelelő politikákkal és eljárásokkal, amelyek különbséget tesznek a 61. cikk alapján bejelentett szervezetként végzett feladatai és az egyéb tevékenységei között;

c) olyan, tevékenységeinek elvégzésére szolgáló eljárásokkal, amelyek kellően figyelembe veszik az adott vállalkozás méretét, az ágazatot, amelyben a vállalkozás a tevékenységét folytatja, a vállalkozás szerkezetét, az érintett IKT-termék, IKT-szolgáltatás vagy IKT-folyamat műszaki összetettségének fokát, valamint azt, hogy tömeg- vagy sorozatgyártásról van-e szó.

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

12. A megfelelőségértékelési tevékenységek elvégzéséért felelős személyeknek rendelkezniük kell a következőkkel:

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

b) az általuk végzett megfelelőségértékelések követelményeinek kielégítő ismerete és megfelelő hatáskör az említett értékelések elvégzésére;

c) az alkalmazandó követelmények és vizsgálati előírások megfelelő ismerete és megértése;

d) a megfelelőségértékelések elvégzését igazoló tanúsítványok, nyilvántartások és jelentések elkészítésének képessége.

13. Biztosítani kell a megfelelőségértékelő szervezetek, azok felső vezetése és a megfelelőségértékelési tevékenységek elvégzéséért felelős személyek, valamint az alvállalkozók pártatlanságát.

14. A megfelelőségértékelő szervezet felső vezetése és megfelelőségértékelési tevékenységek elvégzéséért felelős személyzet javadalmazása nem függhet az elvégzett megfelelőségértékelések számától és ezen értékelések eredményétől.

15. A megfelelőségértékelő szervezeteknek felelősségbiztosítással kell rendelkezniük, kivéve, ha a felelősség nemzeti jogával összhangban a tagállamot terheli, vagy ha a tagállam közvetlenül felel a megfelelőségértékelésért.

16. A megfelelőségértékelő szervezet és személyzete, valamint bizottságai, leányvállalatai, alvállalkozói, továbbá egy megfelelőségértékelő szervezet bármely kapcsolódó szervezete vagy külső szervezeteinek személyzete minden olyan információ tekintetében, amely e rendelet vagy az e rendeletből fakadó joghatások érvényesülését biztosító nemzeti jog rendelkezései alapján ellátott megfelelőségértékelési feladatainak végrehajtása során jutott birtokába, köteles megőrizni a bizalmasságot, és betartani a szakmai titoktartás követelményeit, kivéve ha a közzétételt az említett személyekre alkalmazandó uniós vagy tagállami jog írja elő, és kivéve azon tagállamok illetékes hatóságainak viszonylatában, ahol a tevékenységét gyakorolja. A szellemitulajdon-jogok védelmét biztosítani kell. A pont követelményei tekintetében.

17. A 16. pont kivételével, e melléklet követelményei nem zárják ki a műszaki információk és a szabályozási iránymutatás megosztását a megfelelőségértékelő szervezet és a tanúsítást kérelmező vagy kérelmezni tervező személy között.

18. A megfelelőségértékelő szervezeteknek következetes, tisztességes és észszerű feltételek szerint kell működniük, a díjak tekintetében figyelembe véve a kkv-k érdekeit.

19. A megfelelőségértékelő szervezeteknek teljesíteniük kell az IKT-termékek, az IKT-szolgáltatások vagy az IKT- folyamatok tanúsítását végző megfelelőségértékelő szervezetek akkreditálása tekintetében a 765/2008/EK rendelettel összehangolt vonatkozó szabvány követelményeit.

20. A megfelelőségértékelő szervezeteknek biztosítaniuk kell, hogy a megfelelőségértékelések céljára használt vizsgálati laboratóriumok megfeleljenek a vizsgálatokat végző laboratóriumok akkreditálása tekintetében a 765/2008/EK rendelettel összehangolt vonatkozó szabvány követelményeinek.