A BIZOTTSÁG (EU) 2022/640 HATÁROZATA

(2022. április 7.)

a legfontosabb biztonsági szereplők szerepére és felelősségi körére vonatkozó végrehajtási szabályokról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 249. cikkére,

tekintettel a Bizottságon belüli biztonságról szóló, 2015. március 13-i (EU, Euratom) 2015/443 bizottsági határozatra ([1]),

tekintettel az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2015. március 13-i (EU, Euratom) 2015/444 bizottsági határozatra ([2]),

mivel:

(1) Az (EU, Euratom) 2015/443 és az (EU, Euratom) 2015/444 bizottsági határozat a Bizottság valamennyi szervezeti egységére és létesítményére alkalmazandó.

(2) Szükség esetén az (EU, Euratom) 2015/444 határozatot kiegészítő vagy támogató végrehajtási szabályokat kell elfogadni az említett határozat 60. cikkével összhangban.

(3) Az EU-minősített adatok teljes életciklusa során biztosított védelem érdekében hozott intézkedéseknek arányosnak kell lenniük különösen az adatok biztonsági minősítési szintjével.

(4) A Bizottság kommunikációs és információs rendszereinek védelmét szolgáló biztonsági intézkedéseket az (EU, Euratom) 2017/46 bizottsági határozat ([3]) és különösen annak a Bizottságon belüli informatikai biztonságra vonatkozó alapelvekről szóló 3. cikke és a rendszerfelelősökről szóló 9. cikke határozza meg.

(5) A legfontosabb biztonsági szereplők szerepére és felelősségi körére vonatkozó végrehajtási szabályok célja, hogy iránymutatással szolgáljanak az (EU, Euratom) 2015/443 és az (EU, Euratom) 2015/444 határozatban e szerepekre vonatkozóan meghatározott előfeltételekről és kötelezettségekről.

(6) Az (EU, Euratom) 2015/444 határozat 36. cikkének (7) bekezdése értelmében a Bizottság Biztonsági Hatósága további, biztonsággal kapcsolatos szerepeket is betölt. Az e szerepekhez kapcsolódó feladatokat ez a határozat határozza meg.

(7) A helyi biztonsági tisztviselők és a nyilvántartó hivatalt ellenőrző tisztviselők konkrét felelősségi körökkel rendelkeznek saját szervezeti egységeikben az EU-minősített adatok védelme tekintetében, az (EU, Euratom) 2015/444 határozatnak megfelelően.

(8) A Bizottság 2016. május 4-én határozatot ([4]) fogadott el, amely felhatalmazza a Bizottság biztonsági kérdésekért felelős tagját arra, hogy a Bizottság nevében és felelősségi körében elfogadja az (EU, Euratom) 2015/444 határozat 60. cikkében előírt végrehajtási szabályokat; ezt követően a Bizottság biztonsági ügyekért felelős tagja 2021. április 13-án a Bizottság nevében és felelősségi körében határozatot ([5]) fogadott el e végrehajtási szabályoknak a Humánerőforrásügyi és Biztonsági Főigazgatóság főigazgatójára történő továbbruházásáról,

([1]) HL L 72., 2015.3.17., 41. o.
([2]) HL L 72., 2015.3.17., 53. o.
([3]) A Bizottság (EU, Euratom) 2017/46 határozata (2017. január 10.) az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról (HL L 6., 2017.1.11., 40. o.).
([4]) A Bizottság C(2016) 2797 final határozata (2016. május 4.) a biztonsággal kapcsolatos felhatalmazásról.
([5]) A Bizottság C(2021) 2684 final határozata (2021. április 13.) a biztonsággal kapcsolatos felhatalmazásról szóló C(2016) 2797 bizottsági határozatban biztosított hatáskörök továbbruházásáról.

ELFOGADTA EZT A HATÁROZATOT:

1. FEJEZET

Általános rendelkezések

1. cikk

Tárgy és hatály

(1) Ez a határozat meghatározza a Bizottságon belül az (EU, Euratom) 2015/443 és az (EU, Euratom) 2015/444 határozat értelmében az EU-minősített adatok védelméért felelős legfontosabb biztonsági szereplők szerepét és felelősségi körét.

(2) Ez a határozat a Bizottság valamennyi szervezeti egységére és létesítményére alkalmazandó.

2. FEJEZET

A Humánerőforrásügyi és Biztonsági Főigazgatóság

2. cikk

A Bizottság Biztonsági Hatósága

(1) A Humánerőforrásügyi és Biztonsági Főigazgatóság Biztonsági Igazgatóságának igazgatójának a Bizottság Biztonsági Hatósága tekintendő, az (EU, Euratom) 2015/444 határozat 7. cikkében említettek szerint.

(2) A Bizottság Biztonsági Hatósága az (EU, Euratom) 2015/444 határozatban meghatározott alábbi területeken látja el feladatait, e határozat 3–7. cikkének megfelelően:

a) személyzeti biztonság;

b) fizikai biztonság;

c) az EU-minősített adatok kezelése;

d) az EU-minősített adatokat kezelő kommunikációs és információs rendszerek akkreditációja;

e) ipari biztonság; valamint

f) a minősített adatok cseréje.

(3) A Bizottság Biztonsági Hatósága kötelező képzést biztosít a helyi biztonsági tisztviselők, a helyi biztonsági tisztviselők helyettesei, a nyilvántartó hivatalt ellenőrző tisztviselők és a nyilvántartó hivatalt ellenőrző tisztviselők helyettesei számára, amely bemutatja azok felelősségi körét és feladatait.

3. cikk

Információvédelmi hatóság

Az információvédelmi hatóság az EU-minősített adatok védelmével kapcsolatos alábbi tevékenységekért felel:

a) információvédelmi biztonságpolitikák és biztonsági iránymutatások kidolgozása, valamint ezek hatékonyságának és helytállóságának nyomon követése;

b) a kriptográfiai termékekkel kapcsolatos technikai információk védelme és igazgatása;

c) annak biztosítása, hogy az információvédelmi intézkedések adott esetben megfeleljenek a Bizottság biztonsági és közbeszerzési politikáinak;

d) annak biztosítása, hogy a kriptográfiai termékek kiválasztása a jogosultságot és kiválasztást szabályozó politikáknak megfelelően történjen;

e) konzultáció a rendszerfelelősökkel, a rendszerszolgáltatókkal, a biztonsági szereplőkkel és a felhasználók képviselőivel az információvédelmi biztonságpolitikákról és biztonsági iránymutatásokról.

4. cikk

Biztonsági akkreditációs hatóság

(1) A Bizottság Biztonsági Hatósága felel az (EU) 2015/444 határozat 18. cikkében foglalt követelményeknek megfelelő biztonsági területek és az EU-minősített adatokat kezelő kommunikációs és információs rendszerek akkreditációjáért.

(2) A Bizottság szervezeti egységei konzultálnak a biztonsági akkreditációs hatósággal – adott esetben helyi biztonsági tisztviselőjükkel és helyi információbiztonsági tisztviselőjükkel egyeztetve –, amennyiben egy szervezeti egység az alábbiak valamelyikét tervezi:

a) biztonsági terület kiépítése;

b) kommunikációs és információs rendszer létrehozása az EU-minősített adatok kezelésére;

c) a minősített adatok kezelésére szolgáló bármely egyéb berendezés telepítése, beleértve egy harmadik fél kommunikációs és információs rendszeréhez való kapcsolódást is.

A biztonsági akkreditációs hatóság mind a tervezési, mind a kiépítési vagy fejlesztési szakaszban tanácsot ad e tevékenységekkel kapcsolatban.

(3) Nem kezelhetők EU-minősített adatok biztonsági területen vagy kommunikációs és információs rendszerben mindaddig, amíg a biztonsági akkreditációs hatóság nem adott ki akkreditációt az EU-minősített adatok megfelelő szintjén.

(4) A biztonsági terület akkreditációjához a következő követelményeknek kell eleget tenni:

a) a biztonsági területre vonatkozó tervek jóváhagyása;

b) a külső vállalkozók által elvégzett munkákra vonatkozó szerződések jóváhagyása, figyelembe véve az ipari biztonságra vonatkozó rendelkezéseket, például a vállalkozók és személyzetük biztonsági tanúsítványára vonatkozó követelményeket;

c) az összes szükséges nyilatkozat és megfelelőségi tanúsítvány rendelkezésre állása;

d) a biztonsági terület fizikai vizsgálata annak ellenőrzése céljából, hogy az építőanyagok és építési módok, a belépés-ellenőrzés, a biztonsági berendezések és minden egyéb tétel megfelel-e a Bizottság Biztonsági Hatósága által előírt követelményeknek;

e) az elektromágneses sugárzással szembeni ellenintézkedések validálása minden technikailag biztosított biztonsági terület esetében;

f) a biztonsági üzemeltetési eljárások jóváhagyása a biztonsági területre vonatkozóan.

(5) Az EU-minősített adatokat kezelő kommunikációs és információs rendszerek akkreditációjához a következő követelményeknek kell eleget tenni:

a) a rendszerek akkreditációs stratégiájának kidolgozása;

b) a kommunikációs és információs rendszerek biztonsági tervének validálása kockázatkezelési megközelítés alapján;

c) a kommunikációs és információs rendszerek biztonsági üzemeltetési eljárásának validálása;

d) a biztonsági akkreditációs hatóság által meghatározott minden egyéb szükséges biztonsági dokumentáció validálása;

e) a titkosítási technológiák használatának jóváhagyása;

f) a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat kezelő kommunikációs és információs rendszerek elektromágneses sugárzásnak való kitettségével szembeni ellenintézkedések validálása;

g) a kommunikációs és információs rendszerek vizsgálata annak ellenőrzése céljából, hogy a dokumentált biztonsági intézkedéseket helyesen hajtották-e végre.

(6) Az akkreditációs követelmények sikeres teljesítését követően a biztonsági akkreditációs hatóság hivatalos engedélyt ad ki az EU-minősített adatoknak a biztonsági területen vagy a kommunikációs és információs rendszerekben való kezelésére, az EU-minősített adatok meghatározott maximális szintjén és legfeljebb 5 évre, a kezelt EU-minősített adatok szintjétől és a kapcsolódó kockázatoktól függően.

(7) A biztonsági szabályok megsértéséről, illetve a biztonsági terület vagy a kommunikációs és információs rendszer kialakításának vagy a kapcsolódó biztonsági intézkedéseknek a jelentős változásáról szóló értesítést követően a biztonsági akkreditációs hatóság felülvizsgálja és szükség esetén visszavonhatja az EU-minősített adatok kezelésére vonatkozó engedélyt mindaddig, amíg az azonosított problémák meg nem oldódnak.

5. cikk

TEMPEST-hatóság

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat kezelő kommunikációs és információs rendszerek védelme érdekében TEMPEST biztonsági intézkedéseket kell, a RESTREINT UE/EU RESTRICTED minősítésű adatok esetében pedig ilyen intézkedéseket lehet végrehajtani.

(2) A TEMPEST-hatóság felelős az EU-minősített adatok nem szándékos elektronikus kiszolgáltatás révén történő illetéktelen tudomásra jutása elleni védelem érdekében hozott intézkedések jóváhagyásáért.

(3) Az EU-minősített adatokat kezelő kommunikációs és információs rendszer felelősének kérésére a TEMPEST-hatóság az adatok minősítési szintjének megfelelő TEMPEST biztonsági intézkedésekre vonatkozó előírásokat ad ki.

(4) A TEMPEST-hatóság a biztonsági területek és az EU-minősített adatoknak a CONFIDENTIAL UE/EU CONFIDENTIAL vagy annál magasabb szintű kezelésére szolgáló kommunikációs és információs rendszerek akkreditációja során műszaki tesztelést végez, és sikeres tesztelés esetén TEMPEST-tanúsítványt állít ki.

(5) A TEMPEST-tanúsítvány legalább a következőket tartalmazza:

a) a tesztelés időpontja;

b) a TEMPEST biztonsági intézkedések leírása a helyszínek terveivel együtt;

c) a tanúsítvány lejáratának dátuma;

d) minden olyan változás, amely a tanúsítványt érvényteleníti;

e) a TEMPEST-hatóság aláírása.

(6) A helyi biztonsági tisztviselő vagy a minősített ülés megszervezéséért felelős szervező – a helyi biztonsági tisztviselővel egyeztetve – felkérheti a TEMPEST-hatóságot az üléstermek tesztelésére, megbizonyosodva arról, hogy azok műszakilag biztonságosak.

6. cikk

Kriptográfiai jóváhagyó hatóság

(1) A kriptográfiai jóváhagyó hatóság felelős a titkosítási technológiák használatának jóváhagyásáért.

(2) A kriptográfiai jóváhagyó hatóság iránymutatást ad ki a titkosítási technológiák használatára és jóváhagyására vonatkozó követelményekről.

(3) A kriptográfiai jóváhagyó hatóság a rendszerfelelős kérésére jóváhagyja a titkosítási megoldások használatát. A jóváhagyásnak legalább a következők kielégítő értékelésén kell alapulnia:

a) a védelmet igénylő információ biztonsági szükségletei;

b) a megoldásba bevont kommunikációs és információs rendszer áttekintése;

c) az eredendő és fennmaradó kockázatok értékelése;

d) a javasolt megoldás leírása;

e) a titkosítási megoldásra vonatkozó biztonsági üzemeltetési eljárások.

(4) A kriptográfiai jóváhagyó hatóságnak nyilvántartást kell vezetnie a jóváhagyott titkosítási megoldásokról.

7. cikk

Kriptográfiai terjesztési hatóság

(1) A kriptográfiai terjesztési hatóság felelős az EU-minősített adatok védelméhez használt kriptográfiai anyagoknak (elsősorban titkosítási berendezéseknek, kriptográfiai kulcsoknak, tanúsítványoknak és kapcsolódó hitelesítőknek) a következők részére történő terjesztéséért:

a) Bizottságon belüli felhasználók vagy szervezeti egységek a külső felek által kezelt kommunikációs és információs rendszerek esetében;

b) Bizottságon kívüli felhasználók vagy szervezetek a Bizottság által kezelt kommunikációs és információs rendszerek esetében.

(2) A kriptográfiai terjesztési hatóság az (EU) 2015/443 határozat 17. cikkének (3) bekezdésével összhangban más szervezeti egységekre ruházhatja át a kriptográfiai anyagok harmadik felek részére történő terjesztését.

(3) A kriptográfiai terjesztési hatóság biztosítja, hogy minden kriptográfiai anyagot olyan biztonságos csatornákon keresztül küldjenek el, amelyek védelmet nyújtanak és bizonyítékot szolgáltatnak a manipulálás ellen, az ezen anyagok által védett EU-minősített adatok minősítési szintjére vonatkozó biztonsági szabályokkal összhangban.

(4) A kriptográfiai terjesztési hatóság iránymutatást nyújt a helyi biztonsági tisztviselőnek és adott esetben a kriptográfiai anyagok előállításában, terjesztésében vagy felhasználásában részt vevő bizottsági szervezeti egységek helyi informatikai biztonsági tisztviselőinek.

(5) A kriptográfiai terjesztési hatóság biztosítja, hogy a terjesztési folyamathoz megfelelő biztonsági üzemeltetési eljárások álljanak rendelkezésre.

3. FEJEZET

A Bizottság szervezeti egységei

8. cikk

Osztályvezetők

(1) Minden osztályvezető kinevezi a következőket:

a) szervezeti egységenként vagy kabinetenként egy-egy helyi biztonsági tisztviselő és adott esetben egy vagy több helyettes;

b) az EU-minősített adatokat nyilvántartó hivatalt működtető szervezeti egységenként egy-egy, nyilvántartó hivatalt ellenőrző tisztviselő és adott esetben egy vagy több helyettes;

c) egy-egy rendszerfelelős minden egyes, EU-minősített adatokat kezelő kommunikációs és információs rendszerhez.

(2) A helyi biztonsági tisztviselőknek, a helyi biztonsági tisztviselők helyetteseinek, a nyilvántartó hivatalt ellenőrző tisztviselőknek és a nyilvántartó hivatalt ellenőrző tisztviselők helyetteseinek a kinevezése előtt az osztályvezető a Humánerőforrásügyi és Biztonsági Főigazgatóság Biztonsági Igazgatósága igazgatójának jóváhagyását kéri.

(3) Az osztályvezető a helyi biztonsági tisztviselővel konzultálva azonosítja azokat az álláshelyeket, amelyek esetében az EU-minősített adatokhoz való hozzáféréshez tanúsítványra van szükség. Az ilyen álláshelyekre pályázókat a felvételi eljárás során tájékoztatni kell a tanúsítványra vonatkozó követelményről.

(4) Az EU-minősített adatok birtokában lévő szervezeti egységek vezetői felelősek azért, hogy szükség esetén a vészhelyzeti megsemmisítési és kiürítési terveket aktiválják. A terveknek alternatívát kell tartalmazniuk az olyan helyzetekre, amikor az osztályvezető nem elérhető.

9. cikk

Az EU-minősített adatokat kezelő kommunikációs és információs rendszerek rendszerfelelősei

(1) A rendszerfelelős az EU-minősített adatokat kezelő kommunikációs és információs rendszer megvalósítására irányuló projekt során a lehető leghamarabb felveszi a kapcsolatot a biztonsági akkreditációs hatósággal a vonatkozó biztonsági szabványok és követelmények meghatározása, valamint a biztonsági akkreditáció folyamatának megkezdése érdekében.

(2) A rendszerfelelős biztosítja, hogy a biztonsági intézkedések megfeleljenek a biztonsági akkreditációs hatóság követelményeinek, és hogy a kommunikációs és információs rendszer az akkreditációja előtt ne kezeljen EU-minősített adatokat.

(3) A rendszerfelelős a titkosítási technológiák használatának jóváhagyása céljából felveszi a kapcsolatot a kriptográfiai jóváhagyó hatósággal. A rendszerfelelősök előzetes jóváhagyás nélkül nem működtethetnek titkosítási technológiákat az előállítási rendszerekben.

(4) A rendszerfelelős a kommunikációs és információs rendszerek biztonságával kapcsolatos kérdésekben konzultál a szervezeti egység helyi információbiztonsági tisztviselőjével.

(5) A rendszerfelelős legalább évente felülvizsgálja az adott rendszerre alkalmazott biztonsági intézkedéseket, beleértve annak biztonsági tervét is.

(6) Amennyiben a kommunikációs és információs rendszerben olyan biztonsági esemény következik be, amely arra utal, hogy a kommunikációs és információs rendszer már nem képes megfelelően védeni az EU-minősített adatokat, a rendszerfelelős tájékoztatja a helyi biztonsági tisztviselőt, és haladéktalanul felveszi a kapcsolatot a biztonsági akkreditációs hatósággal, hogy tanácsot kérjen a további lépésekhez. Ilyen esetben az akkreditáció felfüggeszthető, és a rendszer üzemen kívül helyezhető mindaddig, amíg meg nem történik a megfelelő korrekciós intézkedés.

(7) A rendszerfelelős mindenkor teljes mértékben támogatja a biztonsági akkreditációs hatóságot a kommunikációs és információs rendszer akkreditációjával kapcsolatos feladatai során.

10. cikk

Információvédelmi üzemeltetési hatóság

Az információvédelmi üzemeltetési hatóság minden egyes kommunikációs és információs rendszer tekintetében felelős a következőkért:

a) biztonsági dokumentáció elkészítése a biztonsági politikákkal és iránymutatásokkal összhangban, különös tekintettel a biztonsági tervre, a rendszerrel kapcsolatos biztonsági üzemeltetési eljárásokra és a kommunikációs és információs rendszer akkreditációs folyamatán belüli kriptográfiai dokumentációra;

b) részvétel a rendszerspecifikus technikai biztonsági intézkedések, eszközök és szoftverek kiválasztásában és tesztelésében, a végrehajtásuk felügyelete és annak biztosítása, hogy azokat a vonatkozó biztonsági dokumentációnak megfelelően, biztonságosan telepítsék, konfigurálják és tartsák karban;

c) részvétel a TEMPEST biztonsági intézkedések és eszközök kiválasztásában, amennyiben azt a biztonsági terv előírja, és a TEMPEST-hatósággal együttműködve gondoskodás azok biztonságos telepítéséről és karbantartásáról;

d) a rendszer működésével kapcsolatos biztonsági üzemeltetési eljárások végrehajtásának és alkalmazásának nyomon követése;

e) kriptográfiai termékek igazgatása és kezelése a kriptográfiai terjesztési hatósággal együttműködésben a kriptográfiai anyagok és ellenőrzött tételek megfelelő őrzésének biztosítása érdekében, és adott esetben kriptográfiai változók generálása;

f) a biztonsági elemzések felülvizsgálatának és tesztelésének elvégzése a biztonsági akkreditációs hatóság által előírtaknak megfelelően, különösen a vonatkozó kockázati jelentések elkészítése céljából;

g) kommunikációs és információs rendszerekre vonatkozó specifikus információvédelmi képzések biztosítása;

h) kommunikációs és információs rendszerekre vonatkozó specifikus biztonsági intézkedések végrehajtása és működtetése.

4. FEJEZET

Helyi biztonsági tisztviselő

11. cikk

A helyi biztonsági tisztviselő kinevezése

(1) A helyi biztonsági tisztviselő és helyettesei tisztviselőként vagy ideiglenes alkalmazottként látják el feladataikat.

(2) Valamennyi helyi biztonsági tisztviselőnek és helyettes helyi biztonsági tisztviselőnek a SECRET UE/EU SECRET szintig és szükség esetén a TRES SECRET UE/EU TOP SECRET szintig érvényes biztonsági tanúsítvánnyal kell rendelkeznie az EU-minősített adatokhoz való hozzáféréshez. A helyi biztonsági tisztviselőnek vagy helyettesének a kinevezése előtt meg kell szereznie a biztonsági tanúsítványt.

(3) A Bizottság képviseletei felkérhetik a Bizottság Biztonsági Hatóságát, hogy biztosítson kivételt az (1) és (2) bekezdésben meghatározott követelmények alól.

12. cikk

A biztonsági területekre vonatkozó biztonsági üzemeltetési eljárások

(1) Az érintett bizottsági szervezeti egység helyi biztonsági tisztviselője biztonsági üzemeltetési eljárásokat dolgoz ki a felelősségi körébe tartozó minden egyes biztonsági területre vonatkozóan.

(2) A helyi biztonsági tisztviselő biztosítja, hogy a biztonsági üzemeltetési eljárások tartalmazzák a következő követelményeket:

a) munkaidőben kizárólag a személyzet érvényes biztonsági tanúsítvánnyal rendelkező és bizonyítottan CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű dokumentumokhoz való hozzáférésre jogosult tagjai számára engedélyezhető a biztonsági területre való, kíséret nélküli belépés;

b) munkaidőn kívül a biztonsági területre kíséret nélkül kizárólag az adott szervezeti egység helyi biztonsági tisztviselője, a biztonsági terület nyilvántartó hivatalt ellenőrző tisztviselője (tisztviselői), ezek helyettesei, valamint a Humánerőforrásügyi és Biztonsági Főigazgatóság Biztonsági Igazgatóságának felhatalmazott tagjai léphetnek be;

c) az olyan adatrögzítő és kommunikációs eszközök, mint például a mobiltelefonok, számítógépek, kamerák vagy más intelligens eszközök nem vihetők be a biztonsági területekre a Bizottság Biztonsági Hatóságának előzetes engedélye nélkül; a fentiektől való bármely eltéréshez a Bizottság Biztonsági Hatóságának előzetes engedélye szükséges; a helyi biztonsági tisztviselő kapcsolattartó pontként jár el;

d) a belső vagy külső személyzethez tartozó minden személyt, aki engedélyt kér a biztonsági területre való belépésre, de nem felel meg a fenti a) pontban meghatározott kritériumoknak, mindenkor egy megfelelően felhatalmazott alkalmazottnak kell kísérnie és felügyelnie; a biztonsági területre való minden ilyen belépést rögzíteni kell a biztonsági terület bejáratánál vezetett naplóban;

e) a helyi biztonsági tisztviselő biztosítja, hogy a biztonsági területet nyomon követő behatolásészlelő rendszerek mindenkor aktívak legyenek és megfelelően működjenek, valamint kezeli az összes kapcsolódó jelszót, kulcsot, PIN-kódot vagy más hozzáférési és hitelesítési mechanizmust;

f) a biztonsági területen előforduló riasztásokat jelenteni kell a Humánerőforrásügyi és Biztonsági Főigazgatóság Biztonsági Igazgatóságának, amely haladéktalanul értesíti a helyi biztonsági tisztviselőt;

g) annak a szervezeti egységnek a helyi biztonsági tisztviselője, ahol a biztonsági terület található, a riasztást vagy biztonsági eseményt követő valamennyi beavatkozásról nyilvántartást vezet;

h) eljárásokat kell bevezetni a biztonsági területen belüli riasztások vagy egyéb vészhelyzetek esetére, beleértve a személyzet evakuálását és szükség esetén a Bizottság Biztonsági Hatóságának felügyelete alatt álló vészhelyzeti csoport és a külső vészhelyzeti szolgálatok gyors reagálásának biztosítását;

i) a helyi biztonsági tisztviselőnek haladéktalanul jelentenie kell a Bizottság Biztonsági Hatósága felé a biztonság bármely olyan megsértését, amely egy biztonsági területen belül vagy azzal kapcsolatban következik be, a megfelelő válaszlépések meghatározása érdekében;

j) a biztonsági területen belül található irodákat, helyiségeket és széfeket zárva kell tartani, amikor ott nem tartózkodik senki;

k) a személyzetnek tartózkodnia kell attól, hogy a biztonságos terület folyosóin vagy más közös területein a minősített adatokról beszéljenek, ha a közelben engedéllyel nem rendelkező személyek találhatók.

13. cikk

Biztonsági kulcsok és kombinációk

(1) A helyi biztonsági tisztviselő általános felelősséggel tartozik a biztonsági területeken használt vagy az oda való belépést biztosító kulcsok és kombinációk megfelelő kezeléséért és tárolásáért. A kulcsokat és kombinációkat biztonsági tárolóeszközben kell tárolni, és azokat legalább olyan szintű védelemben kell részesíteni, mint azokat az adatokat, amelyekhez hozzáférést biztosítanak.

(2) A helyi biztonsági tisztviselő nyilvántartást vezet a biztonsági tárolóeszközökről és páncélszobákról, továbbá naprakész listát tart fenn a személyzet azon tagjairól, akik azokhoz kíséret nélkül hozzáférhetnek.

(3) A helyi biztonsági tisztviselő nyilvántartást vezet a biztonsági tárolóeszközök és páncélszobák kulcsairól, valamint a személyzet azon tagjairól, akikre azokat rábízták. Minden egyes kiadott kulcsról átvételi elismervényt kell megőrizni, amely tartalmazza a kulcs azonosító számát, az átvevő nevét, az átvétel dátumát és időpontját.

(4) Kulcsok és kombinációk kizárólag olyan személyeknek adhatók ki, akik számára szükséges azok ismerete, és akik megfelelő engedéllyel rendelkeznek az EU-minősített adatokhoz való hozzáférésre. Amennyiben ezek a feltételek már nem teljesülnek, a helyi biztonsági tisztviselő az érintett kulcsokat visszavonja.

(5) A helyi biztonsági tisztviselő felelős a tartalékkulcsok és valamennyi kombináció írásos jegyzékének őrzéséért. Ez utóbbiakat külön lepecsételt, nem átlátszó, aláírással és keltezéssel ellátott borítékokban kell elhelyezni, amelyeket át kell adni a kulcsokért felelős személyeknek. Ezeket a borítékokat a legmagasabb minősítési szintű anyagok esetében alkalmazandó biztonsági tárolóeszközben, azaz megfelelő tárolóeszközben vagy páncélszobában kell tárolni.

(6) Ha a kombináció megváltoztatása vagy a kulcs rotációja során a helyi biztonsági tisztviselő arra utaló jeleket észlel, hogy a borítékot manipulálták vagy megsértették, ezt biztonsági eseményként kezeli, és erről haladéktalanul tájékoztatja a Bizottság Biztonsági Hatóságát.

(7) A biztonsági tárolóeszközök kombinációinak megváltoztatását a biztonsági területeken belül, a helyi biztonsági tisztviselő felügyelete mellett kell elvégezni. A kombinációkat legalább 12 havonta, illetve minden olyan alkalommal újra be kell állítani, amikor:

a) új tárolóeszköz érkezik vagy új zárat szerelnek fel (az alapértelmezett kombinációkat azonnal meg kell változtatni);

b) fennáll a gyanúja vagy bebizonyosodott, hogy EU-minősített adatok illetéktelen személyek tudomására jutottak;

c) a kombináció birtokában lévő valamely személynek már nincs szüksége hozzáférésre.

(8) A helyi biztonsági tisztviselő nyilvántartást vezet a (7) bekezdésben említett kombinációváltoztatások időpontjairól.

14. cikk

Az EU-minősített adatok védelmét szolgáló vészkiürítési és megsemmisítési tervek

(1) A helyi biztonsági tisztviselő segíti az osztályvezetőt az EU-minősített adatok védelmét szolgáló vészkiürítési és megsemmisítési tervek kidolgozásában, a Biztonsági Igazgatóság (DG HR.DS) iránymutatása alapján.

(2) A helyi biztonsági tisztviselő biztosítja, hogy az (1) bekezdésben említett tervek végrehajtásához szükséges berendezések azonnal rendelkezésre álljanak és üzemképes állapotban maradjanak.

(3) A helyi biztonsági tisztviselő az (1) bekezdésben említett tervekben megnevezett tisztviselőkkel együtt legalább 12 havonta felülvizsgálja a tervek felkészültségi állapotát, és megteszi a szükséges intézkedéseket azok naprakésszé tétele érdekében.

15. cikk

Biztonsági tanúsítványok

(1) A helyi biztonsági tisztviselő nyilvántartást vezet a szervezeti egységen belül a Bizottság biztonsági tanúsítványához kötött valamennyi álláshelyről és az ezen álláshelyeket betöltő személyekről. A biztonsági tanúsítványra vonatkozó követelményt a felvételi eljárás során fel kell tüntetni az álláshirdetésben, és ezt az interjú során is jelezni kell a pályázó felé.

(2) A helyi biztonsági tisztviselő felügyeli az EU-minősített adatokhoz való hozzáférés céljából benyújtott biztonsági tanúsítvány iránti kérelmeket. A helyi biztonsági tisztviselő kapcsolattartó pontként működik a szervezeti egységen belül, és a biztonsági tanúsítványok tekintetében kapcsolatot tart a Bizottság Biztonsági Hatóságával.

(3) A helyi biztonsági tisztviselő kezdeményezi a biztonsági tanúsítvány iránti eljárás megindítására irányuló kérelmet a személyzet érintett tagja tekintetében, és biztosítja, hogy az érintett haladéktalanul visszaküldje a nemzeti biztonsági tanúsítványra vonatkozó kérdőívet a Bizottság Biztonsági Hatóságának.

(4) A helyi biztonsági tisztviselő biztosítja, hogy a szervezeti egység biztonsági ellenőrzésen átesett tagjai a biztonsági tanúsítványuk megszerzése céljából vegyenek részt az EU-minősített adatokról szóló kötelező tájékoztatón.

(5) A helyi biztonsági tisztviselő rendszeres kapcsolatot tart a szervezeti egység humánerőforrás-szolgálatával és tájékoztatást kér a biztonsági tanúsítványhoz kötött álláshelyeket érintő változásokról, és minden ilyen változásról haladéktalanul tájékoztatja a Bizottság Biztonsági Hatóságát.

(6) A helyi biztonsági tisztviselő tájékoztatja a Bizottság Biztonsági Hatóságát arról, ha olyan új munkatárs érkezik, aki már rendelkezik biztonsági tanúsítvánnyal, és így az olyan álláshelyet kapjon, amelyet csak biztonsági tanúsítvánnyal rendelkező alkalmazott tölthet be.

(7) A helyi biztonsági tisztviselő gondoskodik arról, hogy a szervezeti egység személyzetének tagjai az előírt határidőn belül befejezzék a biztonsági tanúsítványuk megújítására irányuló eljárást. Amennyiben a személyzet valamely tagja megtagadja az eljárás lefolytatását, az érintettet olyan munkakörbe kell áthelyezni, amelyhez nincs szükség biztonsági tanúsítvánnyal rendelkező alkalmazottra.

16. cikk

EU-minősített adatokat nyilvántartó hivatal

(1) Amennyiben egy szervezeti egység EU-minősített adatokat nyilvántartó hivatalt működtet, a helyi biztonsági tisztviselő felügyeli a nyilvántartó hivatalt ellenőrző tisztviselőknek az EU-minősített adatok kezelésével és az EU-minősített adatok védelmére vonatkozó biztonsági szabályoknak való megfeleléssel kapcsolatos tevékenységeit.

(2) A helyi biztonsági tisztviselő legalább 12 havonta, illetve a nyilvántartó hivatalt ellenőrző tisztviselő vagy annak helyettese változását követően elvégzi a következő ellenőrzéseket:

a) az EU-minősített adatokat nyilvántartó hivatal dokumentumai mintájának ellenőrzése a státuszuk és a minősített dokumentumok nyilvántartásának pontossága megerősítése céljából;

b) az EU-minősített adatok átvételi és továbbítási elismervényei mintájának ellenőrzése, amely az ilyen adatoknak az EU-minősített adatokat nyilvántartó hivatalhoz vagy onnan való terjesztéséhez szolgál;

c) a megsemmisítési igazolások mintájának ellenőrzése.

(3) A helyi biztonsági tisztviselő legalább havonta szúrópróbaszerűen ellenőrzi a minősített dokumentumok nyilvántartását és a közelmúltban átvett minősített dokumentumokat annak biztosítása érdekében, hogy a dokumentumokat helyesen vegyék nyilvántartásba.

(4) Minden ellenőrzést rögzíteni kell a minősített dokumentumok nyilvántartásának naplójában.

17. cikk

Egyéb biztonsági feladatok

A helyi biztonsági tisztviselő egyéb biztonsági feladatait biztonsági közleményben kell meghatározni, amely különösen a személyek, a helyiségek és egyéb eszközök, valamint az információk fizikai biztonságára terjed ki.

5. FEJEZET

A nyilvántartó hivatalt ellenőrző tisztviselő

18. cikk

A nyilvántartó hivatalt ellenőrző tisztviselő kinevezése

(1) A nyilvántartó hivatalt ellenőrző tisztviselő és helyettesei tisztviselőként vagy ideiglenes alkalmazottként látják el feladataikat.

(2) Valamennyi nyilvántartó hivatalt ellenőrző tisztviselőnek és azok helyetteseinek a SECRET UE/EU SECRET szintig és szükség esetén a TRES SECRET UE/EU TOP SECRET szintig érvényes biztonsági tanúsítvánnyal kell rendelkeznie az EU-minősített adatokhoz való hozzáféréshez. A nyilvántartó hivatalt ellenőrző tisztviselőnek vagy helyettesének a kinevezése előtt meg kell szereznie a biztonsági tanúsítványt.

(3) A Bizottság képviseletei felkérhetik a Bizottság Biztonsági Hatóságát, hogy biztosítson kivételt az (1) és (2) bekezdésben meghatározott követelmények alól.

19. cikk

Felelősségi kör

(1) A nyilvántartó hivatalt ellenőrző tisztviselők biztonsági célból nyilvántartásba veszik a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősítésű adatokat, amikor azok

a) megérkeznek a Bizottság szervezeti egységébe vagy elhagyják azt; vagy

b) megérkeznek a kommunikációs és információs rendszerbe vagy elhagyják azt.

(2) A nyilvántartó hivatalt ellenőrző tisztviselők a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítésű adatok teljes életciklusa során nyilvántartásba veszik az azokat érintő összes eseményt. A nyilvántartó hivatalt ellenőrző tisztviselők biztosítják továbbá, hogy minden olyan RESTREINT UE/EU RESTRICTED vagy azzal egyenértékű minősítésű adatról nyilvántartást vezessenek, amelyet harmadik országokkal és nemzetközi szervezetekkel cserélnek ki. Ezt Főtitkárság által kezelt, az EU-minősített adatokat nyilvántartó hivatallal koordinálva kell elvégezni.

(3) A nyilvántartó hivatalt ellenőrző tisztviselő a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű dokumentumokat rögzíti a minősített dokumentumok nyilvántartásában, és biztosítja azok biztonságos tárolását az EU-minősített adatokat nyilvántartó hivatalnál.

(4) A nyilvántartó hivatalt ellenőrző tisztviselő segíti a Bizottság személyzetét a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatok létrehozásában és küldésében.

(5) Amennyiben a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű dokumentumok érkeznek más szervezeti egységektől vagy külső felektől, a nyilvántartó hivatalt ellenőrző tisztviselő biztosítja, hogy a kézbesítési elismervényt megfelelően visszajuttassák a küldő félnek.

(6) Mielőtt lehetővé tenné a személyzet valamely tagja számára az EU-minősített adatokat nyilvántartó hivatal által tárolt minősített dokumentumokhoz való hozzáférést, a nyilvántartó hivatalt ellenőrző tisztviselő a helyi biztonsági tisztviselővel együtt ellenőrzi, hogy az adott személy rendelkezik-e a Bizottság Biztonsági Hatósága által kiadott biztonsági tanúsítvánnyal.

(7) A nyilvántartó hivatalt ellenőrző tisztviselő naplót vezet az EU-minősített adatokat nyilvántartó hivatalba belépő és onnan kilépő olyan munkatársakról, akik nem jogosultak kíséret nélküli hozzáférésre, és a látogatás időtartamára kíséri őket.

(8) Amennyiben a személyzet valamely tagja az EU-minősített adatokat nyilvántartó hivatalon kívül vesz át betekintésre egy dokumentumot, a nyilvántartó hivatalt ellenőrző tisztviselő megbizonyosodik arról, hogy az adott személy tisztában van a vonatkozó kompenzációs biztonsági intézkedésekkel, és a dokumentumot haladéktalanul visszaszolgáltatja, amint arra már nincs szüksége. A nyilvántartó hivatalt ellenőrző tisztviselő felhívja a személyzet tagjainak figyelmét arra, hogy az ilyen dokumentumokat a lehető leghamarabb vissza kell küldeniük.

(9) Az EU-minősített adatokat nyilvántartó hivatal futárigazolványt bocsát ki, ha a minősített dokumentumokat személyesen, kézi szállítás útján továbbítják a nyilvántartó hivatal helye szerinti országon kívül.

(10) A nyilvántartó hivatalt ellenőrző tisztviselők által betartandó, a minősített dokumentumok nyilvántartásba vételére vonatkozó részletes utasításokat biztonsági közleményben kell meghatározni.

20. cikk

Visszaminősítés és a minősítés feloldása

A nyilvántartó hivatalt ellenőrző tisztviselő segíti a kibocsátó szervezeti egységeket a nyilvántartásba vett EU-minősített adatok felülvizsgálatának folyamatában annak megállapítása érdekében, hogy az eredeti minősítési szint továbbra is megfelelő-e, illetve indokolt-e a dokumentum visszaminősítése vagy a minősítés feloldása.

21. cikk

Megsemmisítés

(1) A nyilvántartó hivatalt ellenőrző tisztviselők felelősek a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítésű adatok jóváhagyott eszközökkel történő megsemmisítéséért, adott esetben biztonsági ellenőrzésen átesett tanúk jelenlétében.

(2) A nyilvántartó hivatalt ellenőrző tisztviselők a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatok megsemmisítését rögzítik a minősített dokumentumok nyilvántartásában, és a megsemmisítésre vonatkozó tanúsítványokat megőrzik az EU-minősített adatokat nyilvántartó hivatalban.

22. cikk

További feladatok

(1) A nyilvántartó hivatalt ellenőrző tisztviselő minden szükséges segítséget megad a helyi biztonsági tisztviselőnek abban az esetben, ha a helyi biztonsági tisztviselő felügyeleti tevékenységet végez az EU-minősített adatokat nyilvántartó hivatalban.

(2) A nyilvántartó hivatalt ellenőrző tisztviselő minden feltételezett vagy tényleges biztonsági eseményt jelent a helyi biztonsági tisztviselőnek, aki pedig jelenti azokat a Bizottság Biztonsági Hatóságának.

(3) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb szintű minősített ülést szervező bizottsági szervezeti egység EU-minősített adatokat nyilvántartó hivatalának ellenőrző tisztviselője előkészíti az ülés során kezelendő EU-minősített adatokat, és egyeztet az ülés szervezőjével annak biztosítása érdekében, hogy valamennyi dokumentumot és elismervényt a vonatkozó szabályoknak megfelelően kezeljenek.

6. FEJEZET

Záró rendelkezések

23. cikk

Átláthatóság

Ezt a határozatot az Európai Bizottság személyzetének és a határozat hatálya alá tartozó minden személynek a tudomására kell hozni, és az Európai Unió Hivatalos Lapjában közzé kell tenni.

24. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon lép hatályba.

Kelt Brüsszelben, 2022. április 7-én.

a Bizottság részéről,
az elnök nevében,
Gertrud INGESTAD
főigazgató
Humánerőforrásügyi és Biztonsági Főigazgatóság