II

(Nem jogalkotási aktusok)

HATÁROZATOK

A BIZOTTSÁG (EU, Euratom) 2019/1961 HATÁROZATA

(2019. október 17.)

a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kezelésére vonatkozó végrehajtási szabályokról

AZ EURÓPAI BIZOTTSÁG,

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

tekintettel az Európai Atomenergia-közösséget létrehozó szerződésre és különösen annak 106. 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]),

tekintettel az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról szóló, 2017. január 10-i (EU, Euratom) 2017/46 bizottsági határozatra ([3]),

mivel:

(1) Az (EU, Euratom) 2015/444 határozat valamennyi bizottsági szervezeti egységre vonatkozóan, a Bizottság valamennyi létesítményében alkalmazandó.

(2) Az EU-minősített adatok védelmét szolgáló biztonsági intézkedéseknek arányosnak kell lenniük különösen az adatok biztonsági minősítési szintjével.

(3) Az (EU, Euratom) 2015/444 határozat 4. cikkének (3) bekezdése, 19. cikke (1) bekezdésének c) pontja és 22. cikke értelmében a határozat végrehajtásának kiegészítése és támogatása érdekében részletesebb rendelkezéseket kell meghatározni azon végrehajtási szabályokban, amelyek olyan kérdéseket szabályoznak, mint a minősítési útmutató, az EU-minősített adatok biztonsági területen vagy adminisztratív zónán kívüli kezelésére vonatkozó kiegészítő intézkedések, valamint a kibocsátóra vonatkozó felelősségi körök.

(4) Szükség esetén az (EU, Euratom) 2015/444 határozat kiegészítését vagy támogatását célzó végrehajtási szabályokat az említett határozat 60. cikkével összhangban kell elfogadni.

(5) Az e határozat végrehajtása érdekében hozott biztonsági intézkedéseknek meg kell felelniük az (EU, Euratom) 2015/443 határozat 3. cikkében foglalt, a Bizottságon belüli biztonságra vonatkozó elveknek.

(6) A Tanács, a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője megállapodtak abban, hogy maximális következetességet biztosítanak az EU-minősített adatok védelmére vonatkozó biztonsági szabályok alkalmazása terén, figyelembe véve sajátos intézményi és szervezeti szükségleteiket, a Tanács azon üléséről készült jegyzőkönyvhöz csatolt nyilatkozatoknak megfelelően, amikor a Tanács elfogadta a 2013/488/EU tanácsi határozatot ([4]).

(7) A Bizottság 2016. május 4-én határozatot ([5]) fogadott el, amelyben felhatalmazza a Bizottság biztonsági ügyekért felelős tagját, hogy a Bizottság nevében és annak felelőssége mellett fogadja el az (EU, Euratom) 2015/444 határozat 60. cikkében előírt végrehajtási szabályokat,

([1]) HL L 72., 2015.3.17., 41. o.
([2]) HL L 72., 2015.3.17., 53. o.
([3]) HL L 6., 2017.1.11., 40. o.
([4]) A Tanács 2013/488/EU határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 274., 2013.10.15., 1. o.).
([5]) A Bizottság 2016. május 4-i határozata a biztonsággal kapcsolatos felhatalmazásról, C(2016) 2797 final.

ELFOGADTA EZT A HATÁROZATOT:

1. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) E határozat meghatározza a CONFIDENTIEL UE/EU CONFIDENTIAL ([6]) és a SECRET UE/EU SECRET ([7]) minősítésű szint EU-minősített adatainak (EUCI) az (EU, Euratom) 2015/444 határozatnak megfelelően történő kezelési feltételeit.

(2) Ez a határozat valamennyi bizottsági szervezeti egységre vonatkozóan, a Bizottság valamennyi létesítményében alkalmazandó.

2. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférés kritériumai

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatként minősített adatokhoz való hozzáférés a következők után adható:

a) meghatározásra került annak szükségessége, hogy egy személy – annak érdekében, hogy az Európai Bizottság számára szakmai funkciót vagy feladatot láthasson el – bizonyos CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz hozzáférjen;

b) a személyt tájékoztatták a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok védelmére vonatkozó szabályokról és kapcsolódó biztonsági előírásokról, valamint iránymutatásról;

c) a személy elismerte az érintett adatok védelmével kapcsolatos felelősségét; valamint

d) a személy a Bizottság Biztonsági Hatóságától felhatalmazást kapott az EU-minősített adatokhoz való hozzáféréshez a megfelelő szintig és egy meghatározott időpontig az (EU, Euratom) 2015/444 határozat 10. cikke (1) bekezdésének 3. pontjával összhangban.

(2) A Bizottság gyakornokai nem kaphatnak olyan feladatokat, amelyek CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférést igényelnek.

(3) A hozzáférést a személyzet egyéb kategóriáira vonatkozóan a mellékletben szereplő táblázatnak megfelelően kell visszatartani vagy engedélyezni.

2. FEJEZET

CONFIDENTIEL UE/EU CONFIDENTIAL ÉS SECRET UE/EU SECRET MINŐSÍTÉSŰ ADATOK LÉTREHOZÁSA

3. cikk

Kibocsátó

Míg az (EU, Euratom) 2015/444 határozat 1. cikke értelmében a kibocsátó olyan uniós intézmény, ügynökség vagy szerv, tagállam, harmadik állam vagy nemzetközi szervezet, amelynek fennhatósága alatt minősített adatokat hoztak létre és/vagy vittek be az uniós struktúrákba, a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok előkészítője nem feltétlenül egyezik meg a kibocsátó személyével.

([6]) Az (EU, Euratom) 2015/444 határozat 3. cikke értelmében a CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű adatok „olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele sértheti az Európai Unió vagy egy vagy több tagállam alapvető érdekeit”.

([7]) Az (EU, Euratom) 2015/444 határozat 3. cikke értelmében a SECRET UE/EU SECRET minősítésű adatok „olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele súlyosan sértheti az Európai Unió vagy egy vagy több tagállam alapvető érdekeit”.

4. cikk

A minősítési szint kijelölése

(1) A dokumentumot az 1. cikk szerinti adatok alapján előkészítő személyzetnek mindig meg kell vizsgálnia, hogy dokumentumukat minősíteni kell-e. Egy dokumentum EU-minősített adatként való minősítése magában foglal egy értékelést és a kibocsátó arra vonatkozó döntését, hogy a dokumentum jogosulatlan személyek részére történő közzététele sértené-e az Európai Unió, illetve egy vagy több tagállam érdekeit. Ha a szövegezőkben bármilyen kétség merül fel azzal kapcsolatban, hogy az általuk készített dokumentum CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésűnek minősül, konzultálniuk kell a felelős egységvezetővel vagy igazgatóval.

(2) Egy dokumentum legalább CONFIDENTIEL UE/EU CONFIDENTIAL minősítésűnek minősül, ha engedély nélküli hozzáférhetővé tétele többek között:

a) jelentős kárt okozna a diplomáciai kapcsolatokban, azaz hivatalos tiltakozást vagy más szankciókat von maga után;

b) sértené az egyének biztonságát vagy szabadságát;

c) kárt okozna a tagállamok vagy más adatszolgáltatók alkalmazott személyzete operatív hatékonyságában vagy biztonságában, illetve az értékes biztonsági vagy hírszerzési műveletek hatékonyságában;

d) lényegesen aláásná jelentős szervezetek pénzügyi életképességét;

e) akadályozná a súlyos bűncselekmények nyomozását, vagy megkönnyítené azok elkövetését;

f) számottevő mértékben az Unió vagy a tagállamok pénzügyi, monetáris, gazdasági és kereskedelmi érdekei ellen hatna;

g) komolyan hátráltatná a jelentős uniós szakpolitikák kidolgozását vagy működését;

h) lezárná vagy más módon zavarná jelentős mértékben a lényeges uniós tevékenységeket;

i) magasabb szinten minősített információk felfedezéséhez vezetne.

(3) Egy adat legalább SECRET UE/EU SECRET minősítésűnek minősül, ha engedély nélküli hozzáférhetővé tétele többek között:

a) fokozná a nemzetközi feszültségeket;

b) súlyos kárt okozná a harmadik országokkal vagy nemzetközi szervezetekkel folytatott kapcsolatokban;

c) közvetlen életveszélyt okozna, illetve súlyosan sértené a közrendet vagy az egyéni biztonságot, illetőleg szabadságot;

d) súlyos károkat okozna a tagállamok vagy más adatszolgáltatók alkalmazott személyzete operatív hatékonyságának vagy biztonságának, illetve a rendkívül értékes biztonsági vagy hírszerzési műveletek folyamatos hatékonyságának;

e) jelentős kárt okozna az Unió vagy a tagállamok pénzügyi, monetáris, gazdasági vagy kereskedelmi érdekeinek;

f) magasabb szinten minősített információk felfedezéséhez vezetne.

(4) A kibocsátók dönthetnek úgy, hogy standard minősítési szintet rendelnek hozzá az általuk rendszeresen összeállított adatkategóriákhoz. Ugyanakkor biztosítaniuk kell, hogy az egyes adatok megfelelő minősítési szintet kapjanak.

5. cikk

Együttműködés a tervezetekkel

(1) Az adatokat előállításukat követően azonnal minősíteni kell. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű szintű adatokat tartalmazó személyes feljegyzéseket, előzetes tervezeteket vagy üzeneteket kezdettől fogva ekként kell megjelölni, és e határozatnak megfelelően kell őket előállítani és kezelni.

(2) Ha a végleges dokumentum már nem indokolja a kezdeti minősítési szint megadását, úgy azt vissza kell minősíteni, vagy a minősítést fel kell oldani.

6. cikk

A forrásanyag rögzítése

A 14. cikk szerinti kibocsátói ellenőrzés gyakorlásának lehetővé tétele érdekében a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok kibocsátóinak nyilvántartást kell vezetniük a minősített dokumentumok, többek között az eredetileg az uniós tagállamokból, nemzetközi szervezetektől vagy harmadik országokból származó minősített dokumentumok előállítására használt minősített forrásokról. Az aggregált minősített adatokat adott esetben oly módon kell megjelölni, hogy azokon feltüntetve maradjon az alkalmazott minősített forrásanyagok kibocsátóinak azonosítása.

7. cikk

Egy dokumentum részeinek minősítése

(1) Az (EU, Euratom) 2015/444 határozat 22. cikkének (6) bekezdésével összhangban a dokumentumok általános minősítési szintjének legalább olyan magasnak kell lennie, mint a dokumentum legmagasabb minősítéssel rendelkező összetevőjének. Ha egy dokumentumot különböző forrásokból származó adatokból állítanak össze, a kész aggregált dokumentumot a minősítési szint meghatározása céljából át kell nézni, mivel összességében magasabb szintű minősítést igényelhet, mint egyes részei külön-külön.

(2) A minősített és a nem minősített részeket tartalmazó dokumentumokat úgy kell szerkeszteni és megjelölni, hogy a különböző minősítési és/vagy érzékenységi szinteket tartalmazó elemek könnyen azonosíthatók és – szükség esetén – elkülöníthetők legyenek. Ennek lehetővé kell tennie minden egyes rész megfelelő kezelését akkor is, ha a többi elemtől külön állnak.

8. cikk

Teljes minősítési jelölés

(1) A minősítést indokolttá tevő információkat fizikai formájuktól függetlenül kell megjelölni és kezelni. A minősítési szintet egyértelműen közölni kell a címzettekkel vagy minősítési jelölés útján, ha az adatok írásos formában – akár papíron, akár eltávolítható adathordozón vagy kommunikációs és információs rendszerben (CIS) – kerülnek továbbításra, vagy bejelentés útján, ha az adatok szóban, például beszélgetés vagy előadás formájában hangzanak el. A minősített anyagokat fizikai jelöléssel kell ellátni, hogy a biztonsági minősítés könnyen azonosítható legyen.

(2) A dokumentumok esetében a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET teljes minősítési jelölést a (3) bekezdéssel összhangban nyomtatott nagybetűvel kell kitölteni, teljes egészében franciául (először franciául) és angolul. A jelölést nem szabad más nyelvekre lefordítani.

(3) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítési jelölést a következő módon kell feltüntetni:

a) a dokumentum minden oldala tetejének és aljának közepén;

b) egy vonalon szerepel a teljes minősítési jelölés, a jobbra dőlő perjel egyik oldalán sincs szóköz;

c) nagybetűvel, fekete, Times New Roman 16-os (amennyiben lehetséges, de legalább 14-es) félkövér betűtípussal, amelyet minden oldalról keret vesz körül.

(4) CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok létrehozása során:

a) minden egyes oldalon jól láthatóan szerepeltetni kell a minősítési jelölést;

b) minden egyes oldalt számozni kell;

c) a dokumentumnak hivatkozási számmal, nyilvántartási számmal és tárggyal kell rendelkeznie, amely önmagában nem lehet minősített adat, kivéve, ha akként jelölik;

d) minden mellékletet és csatolmányt – lehetőség szerint az első oldalon – fel kell sorolni; valamint

e) a dokumentumon fel kell tüntetni létrehozásának időpontját.

(5) A SECRET UE/EU SECRET jelölést lehetőség szerint pirossal kell megjelölni.

9. cikk

Rövidített C-UE/EU-C és S-UE/EU-S minősítési jelölések

A C-UE/EU-C és S-UE/EU-S rövidítések használhatók a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű dokumentum egyes részei minősítési szintjének jelölésére, vagy ha a teljes minősítési jelölés nem illeszthető be, például kisméretű eltávolítható adathordozón. A szöveg olyan szövegtörzsön alkalmazható, ahol a teljes minősítési jelölés ismételt használata körülményes. A rövidítés nem használható a teljes minősítési jelölés helyett a dokumentum fej- és láblécében.

10. cikk

Egyéb biztonsági azonosítók

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok tartalmazhatnak más jelöléseket vagy „biztonsági azonosítókat” (security designators), megnevezve például azt a mezőt, amelyre a dokumentum vonatkozik, vagy egy adott elosztást a szükséges ismeret elve alapján. Erre példa a következő:

ÁTADHATÓ LIECHTENSTEIN RÉSZÉRE

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok viselhetnek olyan biztonsági kikötést, amely külön utasításokat tartalmaz a dokumentumok kezelésére és intézésére vonatkozóan.

(3) Amennyiben lehetséges, a dokumentum első oldalán létrehozásának időpontjában fel kell tüntetni a visszaminősítés vagy a minősítés feloldásának időpontját. Például a következő jelölés alkalmazható:

SECRET UE/EU SECRET

[éééé.hh.nn.]-ig

és **RESTREINT UE/EU RESTRICTED**

ezután

11. cikk

Elektronikus adatfeldolgozás

(1) CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumokat elektronikus eszközökkel kell létrehozni, amennyiben ezek rendelkezésre állnak.

(2) CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok létrehozásakor a Bizottság személyzete a megfelelő minősítési szintre vagy magasabb minősítési szintre akkreditált kommunikációs és információs rendszert használ. A személyzet konzultál helyi biztonsági tisztviselőjével (LSO), ha bármilyen kétség merül fel azzal kapcsolatban, hogy mely kommunikációs és információs rendszer használható. A Bizottság Biztonsági Hatóságával konzultálva különleges eljárásokat lehet alkalmazni vészhelyzetben vagy meghatározott technikai konfigurációkban.

(3) Az 5. cikk által előírt CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok – beleértve a tervezeteket is – nem továbbíthatók e-mailben, szabványos nyomtatókon nyomtatott vagy lapolvasókon szkennelt formában, illetve nem továbbíthatók a személyzet tagjainak személyes eszközeire. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű dokumentumok kinyomtatására kizárólag elektromágneses sugárzástól védett önálló számítógépekhez vagy akkreditált rendszerekhez csatlakoztatott nyomtatók vagy fénymásolók használhatók.

12. cikk

Biztonsági célú nyilvántartásba vétel

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatot a terjesztés és a kézhezvétel előtt biztonsági célból nyilvántartásba kell venni. Nyilvántartásba kell venni az adatot:

— amikor az a szervezeti egységbe megérkezik, vagy elhagyja azt; valamint

— amikor az a kommunikációs és információs rendszerbe megérkezik, vagy elhagyja azt.

(2) Az ilyen nyilvántartásba vétel papíralapon vagy elektronikus iktatókönyvben is elvégezhető.

(3) Ha az adatok kezelésére elektronikusan kerül sor a kommunikációs és információs rendszerben, ezek a nyilvántartási eljárások a kommunikációs és információs rendszeren belüli folyamatok útján is elvégezhetők. Ebben az esetben a kommunikációs és információs rendszer olyan intézkedéseket tartalmaz, amelyek garantálják az iktatókönyvben szereplő bejegyzések integritását.

(4) A nyilvántartó hivatalt ellenőrző tisztviselő nyilvántartást vezet, amely legalább az alábbi információkat tartalmazza minden egyes dokumentum esetében:

a) a végleges minősített dokumentum nyilvántartásba vételének időpontja;

b) a minősítési szint;

c) adott esetben a minősítési szint lejárati időpontja;

d) a kibocsátó szervezeti egység neve;

e) a címzett vagy a címzettek;

f) a tárgy;

g) a kibocsátó szervezeti egység dokumentumának hivatkozási száma;

h) a nyilvántartási szám;

i) a szétosztott példányok száma;

j) amennyiben lehetséges, az okmány létrehozásához felhasznált források jegyzéke;

k) a dokumentum visszaminősítésének vagy minősítése megszüntetésének időpontja; valamint

l) a megsemmisítés adatai (hely, dátum, módszer, felügyelet, megsemmisítési igazolás).

13. cikk

Elosztás

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű dokumentumok küldőjének el kell döntenie, hogy a szükséges ismeret elve alapján kinek továbbítsa a szükséges adatokat. A szükséges ismeret elvének további érvényesítése érdekében elosztási jegyzéket kell készíteni.

3. FEJEZET

A MEGLÉVŐ CONFIDENTIEL UE/EU CONFIDENTIAL ÉS A SECRET UE/EU SECRET MINŐSÍTÉSŰ ADATOKKAL FOLYTATOTT MUNKA

14. cikk

A kibocsátó ellenőrzése

(1) A kibocsátónak kibocsátói ellenőrzést kell gyakorolnia az általa előállított CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok felett. A kibocsátó előzetes írásbeli hozzájárulását kell kérni, mielőtt az adatok:

a) minősítésének feloldására vagy visszaminősítésére kerül sor;

b) a kibocsátó által meghatározott céltól eltérő célra kerülnek felhasználásra;

c) harmadik ország vagy nemzetközi szervezet részére átadhatók;

d) a Bizottságon kívüli féllel, de az EU-n belül is nyilvánosságra kerülnek; vagy

e) harmadik országban található szerződéses megbízott vagy leendő szerződéses megbízott rendelkezésére bocsáthatók.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok birtokosai megfelelően felhatalmazott személyek, akik azért kaptak hozzáférést a minősített adatokhoz, hogy képesek legyenek feladataik ellátására. Ők felelősek az (EU, Euratom) 2015/444 határozatnak megfelelően az adatok helyes kezeléséért, tárolásért és védelméért. A minősített adatok kibocsátóival ellentétben a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok birtokosai nem jogosultak dönteni azok visszaminősítéséről, minősítésének feloldásáról vagy továbbadásáról.

(3) Ha a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adat kibocsátója nem azonosítható, a kibocsátói ellenőrzést a minősített adatot birtokló bizottsági szervezeti egység gyakorolja. A Bizottság biztonsági szakértői csoportjával konzultálni kell, mielőtt CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adat kiadásra kerülne valamely harmadik ország vagy nemzetközi szervezet részére.

15. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kezelésére alkalmas kommunikációs és információs rendszer (CIS)

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokat elektronikus úton kell kezelni és továbbítani, amennyiben ilyen eszközök rendelkezésre állnak. A releváns vagy magasabb minősítési szint alá tartozó adatok kezelésére kizárólag a Bizottság biztonsági akkreditációs hatósága által akkreditált kommunikációs és információs rendszer és berendezések használhatók.

(2) Amennyiben a Bizottság szervezeti egysége megfelelő eszközökkel rendelkezik az ezen a szinten minősített adatok kezelésére és továbbítására, úgy segítséget nyújt más bizottsági szerveknek az adatok megfelelő kezeléséhez és továbbküldéséhez, amennyiben erre lehetősége van.

16. cikk

Az eltávolítható adathordozókon tárolt CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokra vonatkozó egyedi intézkedések

(1) Az eltávolítható adathordozók használatát ellenőrizni kell, és azzal kapcsolatban felelősséget kell viselni. Csak a Bizottság által rendelkezésre bocsátott és a Bizottság Biztonsági Hatósága által jóváhagyott termék által titkosított eltávolítható adathordozókat szabad használni. A személyes eltávolítható adathordozók és a konferenciákon, szemináriumokon stb. ajándékként kiosztott adathordozók nem használhatók fel minősített adatok továbbítására. Amennyiben lehetséges, a Bizottság Biztonsági Hatósága által kiadott útmutatásnak megfelelően Tempest-biztos eltávolítható adathordozót kell használni.

(2) Ha a minősített dokumentumot eltávolítható adathordozón, például USB-kulcson, CD-n vagy memóriakártyán elektronikusan kezelik vagy tárolják, a minősítési jelölésnek jól láthatónak kell lennie a megjelenített adatokon, valamint a fájlnévben és az eltávolítható adathordozón.

(3) A személyzet tagjai szem előtt tartják, hogy amennyiben az eltávolítható adathordozón nagy mennyiségű minősített adatot tárolnak, az eszköz magasabb minősítési szintet igényelhet.

(4) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok eltávolítható adathordozóra, illetőleg adathordozóról történő továbbítására csak megfelelő akkreditációval rendelkező kommunikációs és információs rendszer használható.

(5) A eltávolítható adathordozókon tárolt ilyen minősítésű adatok letöltésekor különös figyelmet kell fordítani annak biztosítására, hogy az eszköz az adattovábbítást megelőzően ne tartalmazzon vírust vagy rosszindulatú szoftvert.

(6) Adott esetben az eltávolítható adathordozókat az alkalmazott titkosítási rendszerhez kapcsolódó biztonsági üzemeltetési eljárásokkal összhangban kell kezelni.

(7) Az eltávolítható adathordozókon tárolt, már nem szükséges, illetve a megfelelő kommunikációs és információs rendszerbe áthelyezett dokumentumokat a jóváhagyott termékeken vagy módszereken keresztül biztonságosan el kell távolítani, vagy törölni kell. Az eltávolítható adathordozókat – amennyiben már nincs rájuk szükség – meg kell semmisíteni, kivéve, ha azokat megfelelő zárt irodabútorokban tárolják. Minden megsemmisítésnek vagy törlésnek olyan módszert kell alkalmaznia, amely összhangban áll a Bizottság biztonsági szabályaival. Az eltávolítható adathordozókról jegyzéket kell vezetni, és fel kell jegyezni azok megsemmisítését.

17. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kezelése és tárolása

(1) Az (EU, Euratom) 2015/444 határozat 19. cikke (3) bekezdése a) pontjának megfelelően a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok biztonsági területen ([8]) a következőképpen kezelhetők:

(2) Az (EU, Euratom) 2015/444 határozat 19. cikke (3) bekezdésének b) pontja szerint ezek az adatok kezelhetők adminisztratív zónán ([9]) belül, feltéve, hogy az EU-minősített adat védve van az engedéllyel nem rendelkező egyének hozzáférésétől.

(3) Ezek az adatok kezelhetők biztonsági területen vagy adminisztratív zónán kívül, amennyiben az adat birtokosa vállalta, hogy eleget tesz az (EU, Euratom) 2015/444 határozat 19. cikke (3) bekezdésének c) pontja szerinti kiegészítő intézkedéseknek.

— A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok nem olvashatók nyilvános helyen.

— Az EU-minősített adatokat mindenkor a jogosult személyes ellenőrzése alatt kell tartani.

— Papíralapú dokumentumok esetében az adatok birtokosa értesítette az érintett nyilvántartást arról, hogy a minősített dokumentumokat a biztonsági területen és az adminisztratív zónán kívül kezelik.

— A dokumentumokat megfelelő széfben kell tárolni, amikor azokat nem olvassák vagy tárgyalják.

— Az irodahelység ajtaját be kell zárni, amikor a dokumentumot olvassák vagy tárgyalják.

— A dokumentum részletei nem kerülhetnek megvitatásra nem biztonságos vonalon folytatott telefonhíváson keresztül vagy e-mailben.

— A dokumentumot a birtokos nem fénymásolhatja és nem szkennelheti be. Csak a nyilvántartó készíthet további másolatokat.

— A dokumentumot adminisztratív zónán vagy biztonsági területen kívül csak a szükséges minimális ideig lehet kezelni és ideiglenesen tárolni, amely időtartamot követően vissza kell küldeni a nyilvántartásba.

([8]) Az (EU, Euratom) 2015/444 határozat 18. cikkében foglaltak szerint.
([9]) Az (EU, Euratom) 2015/444 határozat 18. cikkében foglaltak szerint.

— A dokumentum visszaszolgáltatását alá kell írni.

— Az adat birtokosa nem dobhatja ki, illetve nem semmisítheti meg a minősített dokumentumot.

(4) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatot biztonsági területen kell tárolni biztonsági tárolóeszközben vagy megerősített helyiségben.

(5) További tanács kérhető a Bizottság illetékes szervezeti egységének helyi biztonsági tisztviselőjétől (LSO).

(6) A dokumentumot érintő bármely gyanús vagy tényleges biztonsági incidenst a lehető leghamarabb jelenteni kell az LSO felé.

18. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok másolása és fordítása

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok másolására vagy fordítására az adat birtokosának utasítására kerülhet sor, feltéve, hogy a kibocsátó nem jelentett be ezzel kapcsolatos fenntartásokat. A feltétlenül szükségesnél több másolat azonban nem készíthető.

(2) Amennyiben a minősített dokumentumnak csak egy részét másolják, ugyanazokat a feltételek alkalmazandók, mint a teljes dokumentum másolásakor. A kivonatokat azonos szintű minősítéssel kell ellátni, kivéve, ha a kibocsátó kifejezetten alacsonyabb szintű vagy nem minősített jelöléssel látta el őket.

(3) Az eredeti adatokra alkalmazandó biztonsági intézkedéseket azok másolataira és fordításaira is alkalmazni kell.

19. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok szállítására vonatkozó általános elvek

(1) Lehetőség szerint a biztonsági területen vagy az adminisztratív zónán kívülre továbbítandó CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat elektronikusan, a megfelelően akkreditált eszközökkel és/vagy a jóváhagyott kriptográfiai termékekkel védett módon kell elküldeni.

(2) A rendelkezésre álló eszközöktől vagy különleges körülményektől függően a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kézzel történő szállítása papíralapú dokumentum formájában vagy eltávolítható adathordozón keresztül is történhet. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok továbbítására szolgáló eltávolítható adathordozót előnyben kell részesíteni a papíralapú dokumentumok küldésével szemben.

(3) Csak a Bizottság Biztonsági Hatósága által jóváhagyott termék által titkosított eltávolítható adathordozók használhatók. A Bizottság Biztonsági Hatósága által jóváhagyott termék által titkosítással nem védett eltávolítható adathordozókon tárolt CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat a papíralapú másolattal azonos módon kell kezelni.

(4) A szállítmány egynél több EU-minősített adatot is tartalmazhat, feltéve, hogy a szükséges ismeret elve teljesül.

(5) Az alkalmazott csomagolásnak biztosítania kell, hogy a csomag tartalma ne legyen látható. CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatot két rétegű nem átlátszó csomagolásban, például borítékban, nem átlátszó mappában vagy aktatáskában kell szállítani. A csomagolás külső oldalán nem szerepelhet a tartalom jellegére vagy minősítési szintjére utaló jelzés. A csomagolás belső rétegén fel kell tüntetni a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítést. Mindkét rétegen szerepelnie kell a meghatározott címzett nevének, beosztásának és címének, valamint egy visszaküldési címnek, amennyiben a szállítás nem végezhető el.

(6) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatokat kézzel szállító személyzetnek vagy futárszolgálatnak biztonsági engedéllyel és futárigazolvánnyal kell rendelkeznie.

(7) A boríték/csomag nem nyitható meg *szállítás közben*. A futárszolgálat biztonsági engedélye nem jogosítja fel őt arra, hogy hozzáférjen a minősített adatok tartalmához.

(8) A személyzet vagy futárok által szállított CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat tartalmazó bármely biztonsági incidenst egy következő vizsgálat céljából az illetékes bizottsági szervezeti egység helyi biztonsági tisztviselőjén keresztül be kell jelenteni a Humánerőforrásügyi és Biztonsági Főigazgatóság Biztonsági Igazgatóságának.

20. cikk

Az eltávolítható adathordozók kézi szállítása

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok szállításához használt eltávolítható adathordozókat szállítási bizonylatnak kell kísérnie, amely részletezi a minősített adatokat tartalmazó eltávolítható adathordozókat, valamint az azokon tárolt összes dokumentumot, hogy a címzett elvégezhesse a szükséges ellenőrzéseket és megerősíthesse az átvételt.

(2) Csak a benyújtandó dokumentumok tárolhatók az adathordozón. Az USB-kulcson található összes minősített adatnak például ugyanarra a címzettre kell irányulnia. A küldő fél szem előtt tartja, hogy az ilyen eszközökön tárolt nagy mennyiségű minősített adat az eszköz egészére vonatkozóan magasabb minősítési szintet igényelhet.

(3) CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok továbbítására csak a megfelelő minősítési jelöléssel ellátott eltávolítható adathordozó használható.

(4) Eltávolítható adathordozóra mentett CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat biztonsági célból nyilvántartásba kell venni.

21. cikk

CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok bizottsági épületeken belüli szállítása

(1) A személyzet egy bizottsági épületen belül szállíthat CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumokat, de a dokumentumoknak a szállítónál kell maradniuk, illetve nem olvashatók nyilvános helyen.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok nem továbbíthatók belső postával.

22. cikk

CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok Unión belüli szállítása

(1) A személyzet vagy a Bizottság futárai az Unión belül bárhol szállíthatnak CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat, feltéve, hogy azok megfelelnek a következő előírásoknak:

a) a nem átlátszó, dupla falú borítékok vagy csomagolások a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok továbbítására szolgálnak. A külső oldalon nem szerepelhet a tartalom jellegére vagy minősítési szintjére utaló jelzés;

b) a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatoknak a szállító birtokában kell maradniuk; valamint

c) a boríték vagy csomag nem nyitható meg *szállítás közben*, és az adatok nem olvashatók nyilvános helyen.

(2) A nyilvántartó személyzet azon tagjai, akik CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatot kívánnak küldeni az Unión belül más helyszínekre, intézkedhetnek arról, hogy azt az alábbi eszközök egyikével továbbítsák:

— a szállítmányt nyomon követő nemzeti postai szolgáltatások vagy a személyes kézi szállítást biztosító kereskedelmi futárszolgáltatások révén, feltéve, hogy megfelelnek az e határozat 24. cikkében meghatározott követelményeknek;

— katonai, kormányzati vagy diplomáciai futárszolgálattal.

(3) Azon alkalmazottak, akik SECRET UE/EU SECRET minősítésű adatokat kívánnak küldeni más tagállamoknak az Európai Unióban, nyilvántartó hivataluknál intézkedhetnek az adatoknak katonai, kormányzati vagy diplomáciai futárszolgálat, de nem postai vagy kereskedelmi futárok útján történő továbbítása ügyében.

(4) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatokat szállító bizottsági személyzetnek vagy hivatalos bizottsági futároknak minden egyes szállítmányra vonatkozóan az illetékes szervezeti egység nyilvántartási hivatala által kiállított futárigazolvánnyal kell rendelkezniük, amely igazolja, hogy a szállító jogosult a szállítmány szállítására.

23. cikk

Harmadik ország területéről származó vagy oda irányuló CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok szállítása

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatokat az Unió területe és egy harmadik ország területe között személyesen, kézi szállítás útján lehet továbbítani.

(2) A nyilvántartó személyzet intézkedhet katonai vagy diplomáciai futár által végzendő szállításról.

(3) CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű, papíralapú vagy eltávolítható adathordozón szállított dokumentumok kézi szállítása során a személyzetnek a következő kiegészítő intézkedések mindegyikének meg kell felelnie:

— Ha a minősített adatokat tömegközlekedéssel szállítják, a dokumentumot a szállító által személyesen felügyelt aktatáskába vagy zsákba kell helyezni. Minősített dokumentum csomagmegőrzőben nem helyezhető el.

— A csomagolás belső részén hivatalos pecsétnek kell állnia annak jelzésére, hogy az hivatalos szállítmány, és nem kell biztonsági ellenőrzésen átesnie.

— A szállítónak futárigazolvánnyal kell rendelkeznie, amely igazolja, hogy a szállító jogosult a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű, az illetékes szervezeti egység nyilvántartása által kiállított csomag szállítására.

24. cikk

Kereskedelmi futárok által végzett szállítás

(1) E határozat alkalmazásában a „kereskedelmi futárok” elnevezés alatt értendők az olyan belföldi postai szolgáltatásokat és kereskedelmi futárszolgálatot végző vállalatok, amelyek adattovábbítási szolgáltatásukat díjfizetés ellenében vagy személyesen kézi szállítással, vagy személyes nyomon követéssel nyújtják.

(2) A kereskedelmi futárok CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű adatot is továbbíthatnak egy tagállamon belül vagy egyik tagállamból egy másik tagállamba. A kereskedelmi futárok a SECRET UE/EU SECRET minősítésű adatot csak az adott tagállamon belül, de külföldön nem továbbíthatják.

(3) A kereskedelmi futárszolgálatokat utasítani kell arra, hogy CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű szállítmányt csak a nyilvántartó hivatalt ellenőrző tisztviselő, a megfelelő felhatalmazással rendelkező helyettesítő személy vagy a tervezett címzett részére szállíthassanak.

(4) A kereskedelmi futárok alvállalkozó szolgáltatásait is igénybe vehetik. Az e határozatnak való megfelelésért vállalt felelősséget azonban továbbra is a futárszolgálat viseli.

(5) A nyilvántartásba vett szállítási okmányok elektronikus továbbítását biztosító kereskedelmi futárok által nyújtott szolgáltatások nem használhatók CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok esetében.

25. cikk

Az EU-minősített adatok kereskedelmi futárok által végzett szállításra történő előkészítése

(1) Minősített szállítmányok előkészítése során a küldőnek szem előtt kell tartania, hogy a kereskedelmi futárszolgálatok CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű szállítmányokat csak a címzett, a megfelelően felhatalmazott helyettes, a nyilvántartó hivatalt ellenőrző tisztviselő vagy megfelelően felhatalmazott helyettese, illetőleg recepciós részére kézbesítenek.

(2) Ha az ilyen adatokat jóváhagyott kereskedelmi futárszolgálat küldi el, a szállítmányt a következők szerint kell előkészíteni és csomagolni:

a) A szállítmányt dupla falú borítékban (ahol a belső réteg kialakítása egyértelművé teszi, ha megkísérelték kinyitni a borítékot) vagy más megfelelően biztonságos csomagolóanyag felhasználásával kell küldeni.

b) A minősítési szintnek jól láthatónak kell lennie a belső borítékon vagy a csomagolás belső rétegén.

c) A borítékon vagy a csomagolás külső oldalán nem szerepelhet a minősítésre utaló jelzés.

d) Mind a belső, mind a külső borítékon vagy a csomagolás rétegeiben egyértelműen fel kell tüntetni a tervezett címzett nevét, és tartalmaznia kell a visszaküldési címet is.

e) A nyilvántartási űrlapot a belső borítékban vagy a csomagolás belső rétegében kell elhelyezni, hogy a címzett azt kitöltse és visszaküldje. A nyilvántartási űrlapnak, amely önmagában nem lehet minősített adat, tartalmaznia kell a dokumentum hivatkozási számát, dátumát és a másolat sorszámát, a tárgyát azonban nem.

f) A boríték külső részén vagy a külső csomagoláson fel kell tüntetni az átvételi elismervényeket. Az átvételi elismervény, amely önmagában nem minősített, tartalmazza a hivatkozási számot, a dátumot és a dokumentum másolatának sorszámát, de a tárgyat nem.

g) A futárszolgálatnak meg kell szereznie és át kell adnia a feladó részére a küldemény aláírt és az adatok egyezőségét igazoló átvételi elismervényét, illetve a futárnak meg kell kapnia az átvételi elismervényeket vagy csomagszámokat.

(3) A feladó a szállítás előtt felveszi a kapcsolatot a megnevezett címzettel annak érdekében, hogy megállapodjanak a szállítás megfelelő napjáról és időpontjáról.

(4) A feladó kizárólagos felelősséggel tartozik minden, kereskedelmi futárszolgálattal feladott szállítmányért. Abban az esetben, ha a szállítmány elveszett, vagy kiszállítása nem történik meg időben, a feladó köteles azt jelenteni a Bizottság Biztonsági Hatóságának, amely nyomon követi a biztonsági incidenst.

26. cikk

Egyéb különleges kezelési feltételek

(1) Az adatbiztonsági megállapodásban vagy igazgatási megállapodásokban meghatározott bármely fuvarozási feltételnek teljesülnie kell. Kétség esetén a személyzetnek konzultálnia kell saját nyilvántartási hivatalukkal vagy a Humánerőforrásügyi és Biztonsági Főigazgatóság Biztonsági Igazgatóságával.

(2) A kettős csomagolásra vonatkozó követelmény alól mentesség adható a jóváhagyott kriptográfiai termékekkel védett minősített adatok esetében. A címzés céljából és mivel az eltávolítható adathordozó explicit biztonsági minősítési jelöléssel rendelkezik, az adathordozót legalább egy hagyományos borítékban kell szállítani, de további fizikai védelmi intézkedések is szükségesek lehetnek, például hogy azt buborékos fóliával bélelt borítékban kell elhelyezni.

4. FEJEZET

MINŐSÍTETT ÜLÉSEK

27. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű ülésre való felkészülés

(1) Azokat az üléseket, amelyeken CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET adatokat kell megvitatni, csak a megfelelő vagy annál magasabb szintű akkreditált ülésteremben lehet tartani. Amennyiben ilyen nem áll rendelkezésre, a személyzet kikéri a Bizottság Biztonsági Hatóságának tanácsát.

(2) Általános szabályként a napirendeket nem kell minősítéssel ellátni. Amennyiben az ülés napirendje minősített dokumentumokat említ, magát a napirendet nem lehet automatikusan minősíteni. A napirendi pontokat úgy kell megfogalmazni, hogy azok ne veszélyeztessék az Unió, illetve egy vagy több tagállam érdekeinek védelmét.

(3) Az ülés szervezőinek emlékeztetniük kell a résztvevőket arra, hogy a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű napirendi ponttal kapcsolatban benyújtott észrevételeket ne hagyományos, nyílt e-mailben vagy egyéb olyan módon küldjék, amely nem került az e határozat 11. cikkével összhangban akkreditálásra.

(4) Az ülések zavartalan működésének elősegítése érdekében az ülések szervezői törekednek úgy csoportosítani a napirenden lévő CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű tételeket, hogy azok egymást kövessék. A minősített kérdések tárgyalása során csak olyan személyek lehetnek jelen, akiknél érvényesül a szükséges ismeret elve, akik átestek a megfelelő szintű biztonsági ellenőrzésen és adott esetben engedéllyel rendelkeznek.

(5) A meghívó felhívja a résztvevők figyelmét arra, hogy az ülésen minősített témákat tárgyalnak, és megfelelő biztonsági intézkedéseket kell alkalmazni.

(6) A résztvevőket emlékeztetni kell arra, hogy a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű tételek tárgyalása során a hordozható elektronikus eszközöket az üléstermen kívül kell hagyni.

(7) Az ülések előtt a szervezők összeállítják a résztvevők teljes listáját.

28. cikk

A résztvevőknek a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű ülés adataihoz való hozzáférése

(1) Az ülések szervezői kötelesek tájékoztatni a Bizottság Biztonsági Hatóságát minden olyan külső látogatóról, aki CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű ülésen vesz részt a Bizottság helyiségeiben.

(2) A résztvevők kötelesek igazolni, hogy érvényes személyi biztonsági tanúsítvánnyal rendelkeznek a megfelelő szinten ahhoz, hogy részt vehessenek a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű napirendi pontokat taglaló vitán.

29. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű ülésteremben lévő elektronikus berendezések

(1) Minősített adatok továbbításakor csak az e határozat 11. cikke szerinti akkreditált informatikai rendszerek használhatók, például CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat bemutató előadások vagy videokonferenciák esetében.

(2) Az elnök gondoskodik arról, hogy a nem engedélyezett hordozható elektronikus eszközök az üléstermen kívül maradjanak.

30. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű ülés során követendő eljárások

(1) A minősített vita megkezdésekor az elnök bejelenti, hogy a csoport áttér minősített üzemmódba. Az ajtóknak zárva kell lenniük.

(2) A vita kezdetén csak a szükséges számú iratot kell aláírni és szükség esetén átadni a résztvevők és a tolmácsok részére.

(3) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok nem maradhatnak őrizetlenül az ülés szünetében.

(4) Az ülés végén a résztvevőket és a tolmácsokat emlékeztetik arra, hogy ne hagyják őrizetlenül azokat a minősített adatokat tartalmazó dokumentumokat vagy feljegyzéseket, amelyeket az ülésen készítettek. Az ülés végén a résztvevők által nem igényelt CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű dokumentumokat és minden esetben valamennyi tolmács dokumentumait alá kell írni és vissza kell küldeni a nyilvántartó hivatalt ellenőrző tisztviselő részére, hogy azokat a megfelelő iratmegsemmisítő-gépekben megsemmisítse.

(5) Az ülés során rögzíteni kell a résztvevők listáját, valamint a tagállamokkal megosztott és a harmadik országokkal vagy nemzetközi szervezetekkel szóban közölt minősített adatok jegyzékét annak érdekében, hogy azokat feltüntessék az eljárás eredményében.

31. cikk

Tolmácsok és fordítók

CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz kizárólag azon tolmácsok és fordítók férhetnek hozzá, akik átestek a megfelelő szintű biztonsági ellenőrzésen és engedéllyel rendelkeznek, az Európai Unió tisztviselőinek személyzeti szabályzata és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételek hatálya alá tartoznak, vagy szerződéses kapcsolatban állnak a Bizottsággal.

5. FEJEZET

A CONFIDENTIEL UE/EU CONFIDENTIAL ÉS A SECRET UE/EU SECRET MINŐSÍTÉSŰ ADATOK MEGOSZTÁSA ÉS CSERÉJE

32. cikk

A kibocsátó beleegyezése

Ha az átadni vagy megosztani kért minősített adat vagy az abban esetlegesen jelen lévő forrásanyag kibocsátója nem a Bizottság, akkor a Bizottság EU-minősített adatot birtokló szervezeti egységének a kibocsátó előzetes írásbeli beleegyezését kell kérnie az adat átadásához. Ha a kibocsátó nem azonosítható, a minősített adatot birtokló bizottsági szervezeti egység gyakorolja a kibocsátói ellenőrzést.

33. cikk

CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok más uniós szervekkel való megosztása

(1) CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok csak akkor oszthatók meg más uniós intézménnyel, ügynökséggel, szervvel vagy hivatallal, ha a címzett esetében teljesül a szükséges ismeret elve, és az adott szerv a Bizottsággal megfelelő jogi megállapodást kötött.

(2) Általános szabályként a minősített adatok más uniós intézményekkel, ügynökségekkel, szervekkel és hivatalokkal való cseréjének fő beérkezési és kiküldési helye a Bizottságon belül a Főtitkárság által irányított EU-minősített adatokat nyilvántartó hivatal. A Bizottság Biztonsági Hatóságával konzultálni kell, ha olyan biztonsági, szervezeti vagy működési okok állnak fenn, amelyek miatt az EU-minősített adatokat nyilvántartó helyi nyilvántartó hivatalok az érintett szervezeti egység hatáskörébe tartozó ügyek tekintetében az adatok beérkeztetése és kiküldése szempontjából megfelelőbbek lehetnek.

34. cikk

CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok tagállamokkal való cseréje

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokat meg lehet osztani a tagállamokkal, ha a címzett esetében teljesül a szükséges ismeret elve, és biztonsági ellenőrzésen esett át.

(2) A tagállamok azonos szintű nemzeti minősítési jelöléssel ([10]) ellátott és a Bizottság rendelkezésére bocsátott minősített adatait a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokkal megegyező szintű védelemben kell részesíteni.

35. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok harmadik országokkal és nemzetközi szervezetekkel való cseréje

(1) CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adat csak akkor bocsátható ki harmadik ország vagy nemzetközi szervezet számára, ha a címzett esetében teljesül a szükséges ismeret elve, és az adott ország vagy nemzetközi szervezet megfelelő jogi vagy igazgatási keretrendszerrel rendelkezik, ilyen például a Bizottsággal kötött adatbiztonsági megállapodás vagy igazgatási megállapodás. Az ilyen megállapodás vagy intézkedés rendelkezései elsőbbséget élveznek e határozat rendelkezéseivel szemben.

(2) Általános szabályként a Főtitkárság által irányított, EU-minősített adatokat nyilvántartó hivatal valamennyi CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősített adatnak a Bizottság és harmadik országok és nemzetközi szervezetek közötti cseréjének fő beérkezési és kiküldési helye. A Bizottság Biztonsági Hatóságával konzultálni kell, ha olyan biztonsági, szervezeti vagy működési okok állnak fenn, amelyek miatt az EU-minősített adatokat nyilvántartó helyi nyilvántartó hivatalok az érintett szervezeti egység hatáskörébe tartozó ügyek tekintetében az adatok beérkeztetése és kiküldése szempontjából megfelelőbbek lehetnek.

(3) A harmadik országtól vagy nemzetközi szervezettől kapott minősített adatokat biztonsági okokból nyilvántartásba kell venni. A személyzet ezért kapcsolatba lép a nyilvántartóval, ha a szokásos nyilvántartási körön kívülről kap minősített adatokat.

(4) A nyomonkövethetőség biztosítása érdekében rögzíteni kell a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatot:

— amikor az a szervezeti egységbe megérkezik, vagy elhagyja azt; valamint

— amikor az a kommunikációs és információs rendszerbe megérkezik, vagy elhagyja azt.

(5) Az ilyen nyilvántartásba vétel papíralapon vagy elektronikus iktatókönyvben is elvégezhető.

(6) Az akkreditált kommunikációs és információs rendszerben kezelt minősített adatokra vonatkozó nyilvántartási eljárásokat a kommunikációs és információs rendszeren belüli folyamatok is elvégezhetik. Ebben az esetben a kommunikációs és információs rendszer olyan intézkedéseket tartalmaz, amelyek garantálják az iktatókönyvben szereplő bejegyzések integritását.

(7) A harmadik országoktól vagy nemzetközi szervezetektől kapott minősített adatok ugyanolyan szintű védelmet élveznek, mint az adott adatbiztonsági megállapodásban vagy igazgatási intézkedésben rögzítetteknek megfelelően az azonos minősítési jelöléssel ellátott EU-minősített adatok.

36. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok kivételes eseti megosztása

(1) Ha a Bizottság vagy valamelyik szervezeti egysége úgy ítéli meg, hogy kivételes igény merült fel CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok harmadik országnak, nemzetközi szervezetnek vagy uniós intézménynek történő átadására, de nem létezik adatbiztonsági megállapodás vagy igazgatási intézkedés, a kivételes *ad hoc* adatátadási eljárást kell követni.

([10]) A tagállami jelölések egyenértékűségi táblázatát az (EU, Euratom) 2015/444 határozat I. melléklete határozza meg.

(2) A Bizottság szervezeti egységei felveszik a kapcsolatot a Bizottság Biztonsági Hatóságával, amely konzultál a Bizottság biztonsági szakértői csoportjával.

(3) A Bizottság biztonsági szakértői csoportjával folytatott konzultációt követően a Bizottság a Bizottság biztonsági ügyekért felelős tagjának javaslata alapján engedélyezheti az érintett adatok kiadását.

6. FEJEZET

A CONFIDENTIEL UE/EU CONFIDENTIAL ÉS A SECRET UE/EU SECRET MINŐSÍTÉSŰ ADATOK ÉLETTARTAMÁNAK VÉGE

37. cikk

Mikor van szükség az adatok visszaminősítésére vagy minősítésének feloldására?

(1) Az adatok minősítése csak addig lesz érvényben, amíg azok védelmet igényelnek. Az adatok visszaminősítése a biztonsági minősítés szintjének csökkentését jelenti. A minősítés feloldása azt jelenti, hogy az adatokat már nem kell a továbbiakban minősítettnek tekinteni. Az adat létrehozásakor – amennyiben lehetséges – a kibocsátó jelöli, hogy egy adott időpontban vagy egy konkrét eseményt követően az EU-minősített adat visszaminősíthető-e, vagy minősítése megszüntethető-e. Ellenkező esetben a kibocsátónak legalább ötévente felül kell vizsgálnia az adatokat, és értékelnie kell a kockázatokat annak megállapítása érdekében, hogy az eredeti minősítési szint továbbra is megfelelő-e.

(2) A bizottsági dokumentumok visszaminősítését vagy minősítésének feloldását eseti alapon is el lehet végezni, például a nyilvános hozzáférés iránti kérelem alapján.

38. cikk

A visszaminősítésért és a minősítés feloldásáért vállalt felelősség

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok visszaminősítésére vagy minősítésének feloldására nem kerülhet sor a kibocsátó engedélye nélkül.

(2) A Bizottság szervezeti egysége, amely minősített dokumentumot hoz létre, felelős annak eldöntéséért, hogy a minősítés visszaminősíthető-e, illetve feloldható-e. A Bizottságon belül a minősítés visszaminősítésére és feloldására irányuló összes kérelmet illetően a kibocsátó szervezeti egység vezetőjével vagy igazgatójával kell konzultálni. Ha az érintett szervezeti egység különböző forrásokból származó minősített adatokat gyűjt össze, először ki kell kérnie minden, forrásanyagot benyújtó fél – többek között a tagállamok, egyéb uniós szervek, harmadik országok vagy nemzetközi szervezetek – hozzájárulását.

(3) Amennyiben a kibocsátó bizottsági szervezeti egység már nem áll rendelkezésre, és felelősségi körét egy másik szolgálat vette át, a minősítés visszaminősítésével és feloldásával kapcsolatos döntést ez a szolgálat hozza meg. Ha a kibocsátó szervezeti egység már nem áll rendelkezésre, és felelősségi körét egy másik szolgálat nem vette át, a minősítés visszaminősítésével vagy feloldásával kapcsolatos döntést a címzett főigazgatóságok egységvezetői vagy igazgatói közösen hozzák meg.

(4) A visszaminősítésért vagy a minősítés feloldásáért felelős szervezeti egység együtt dolgozik a megfelelő nyilvántartóval a visszaminősítésről vagy a minősítés feloldásáról szóló gyakorlati intézkedések kidolgozásán.

39. cikk

Nem minősített érzékeny adatok

Amennyiben egy dokumentum felülvizsgálatának eredményeként olyan döntés születik, hogy fel kell oldani annak minősítését, mérlegelni kell, hogy a dokumentumon fel kell-e tüntetni az (EU, Euratom) 2015/443 határozat 9. cikke szerinti, „nem minősített érzékeny adat” információterjesztési jelölést.

40. cikk

Hogyan jelölendő, hogy a dokumentum minősítése visszaminősítésre vagy feloldásra került?

(1) Az eredeti minősítési jelölést minden oldal tetején és alján látható módon – az elektronikus formátumokra vonatkozó „áthúzás” funkcióval vagy a nyomtatott dokumentumok esetében kézzel – át kell húzni (és nem kell eltávolítani).

(2) Az első oldalra (fedőlapra) a „visszaminősített” vagy a „minősítés feloldva” pecsétet kell rányomni, és azon fel kell tüntetni a visszaminősítésért vagy a minősítés feloldásáért felelős hatóság adatait és a megfelelő időpontot.

(3) A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok eredeti címzettjeit tájékoztatni kell a visszaminősítésről vagy a minősítés feloldásáról. Az eredeti címzettek felelősek azért, hogy tájékoztassák azon további címzetteket, akiknek elküldték, illetve lemásolták az eredeti CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat.

(4) A Bizottság Történeti Irattár Szolgálatát tájékoztatni kell a minősítés feloldásáról hozott valamennyi határozatról.

(5) A minősített adatok valamennyi fordításáról ugyanolyan, a visszaminősítésre vagy a minősítés feloldására irányuló eljárást kell alkalmazni, mint az eredeti nyelvi változat esetében.

41. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok részleges visszaminősítése vagy a minősítés feloldása

(1) Lehetőség van a visszaminősítésre vagy a minősítés részleges feloldására (pl. mellékletek, csak néhány bekezdés). Az eljárásnak meg kell egyeznie egy teljes dokumentum visszaminősítésével vagy minősítésének feloldásával.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok minősítésének részleges feloldása („adat-eltávolítás") esetén a feloldott minősítésű kivonatot fel kell mutatni.

(3) A továbbra is minősített részek helyébe a következők lépnek:

RÉSZ, AMELYNEK MINŐSÍTÉSE NEM OLDANDÓ FEL

vagy magában a szövegtörzsben, ha a továbbra is minősített rész egy bekezdés részét képezi, vagy bekezdésként, ha a továbbra is minősített rész egy vagy több konkrét bekezdés.

(4) Külön meg kell említeni a szövegben, ha a teljes melléklet minősítését nem lehet feloldani, és ezért nem szerepelt a kivonatban.

42. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok rutinszerű megsemmisítése és törlése

(1) A Bizottság nem halmoz fel nagy mennyiségű minősített adatot.

(2) Az egyes kibocsátó szervezeti egységeknek legalább ötévente felül kell vizsgálniuk a megsemmisítésre vagy törlésre szánt dokumentumokat. Rendszeres időközönként felülvizsgálatot kell végezni mind a papíron, mind a CIS-ben tárolt adatok tekintetében.

(3) A személyzet nem semmisítheti meg a továbbiakban már nem szükséges CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű dokumentumok nyomtatott változatát, hanem ehelyett fel kell kérni a nyilvántartó hivatalt ellenőrző tisztviselőt, hogy az eredeti dokumentumra vonatkozó archiválási követelmények figyelembevételével semmisítse meg a dokumentumokat.

(4) A személyzet nem köteles tájékoztatni a kibocsátót, ha törli a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű dokumentumok másolatát.

(5) A minősített adatokat tartalmazó dokumentumtervezetekre a megsemmisítés ugyanazon módszerei vonatkoznak, mint a véglegesített minősített dokumentumokra.

(6) CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok megsemmisítésére csak jóváhagyott iratmegsemmisítő-gépek használhatók. A DIN 66399 5. szintű iratmegsemmisítő-gépek alkalmasak CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű dokumentumok megsemmisítésére. A DIN 66399 6. szintű iratmegsemmisítő-gépek alkalmasak SECRET UE/EU SECRET minősítésű dokumentumok megsemmisítésére.

(7) A jóváhagyott iratmegsemmisítő-gépekből származó hulladék szokásos irodai hulladékként kezelhető.

(8) A nyilvántartó hivatalt ellenőrző tisztviselő megsemmisítési igazolásokat állít ki, és ennek megfelelően frissíti az iktatókönyveket és egyéb nyilvántartási adatokat.

(9) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatokat tartalmazó összes adathordozón és eszközön lévő adatokat az élettartamuk vége előtt véglegesen eltávolítják. Az elektronikus adatokat olyan módon kell megsemmisíteni vagy törölni az információs technológiai forrásokból és a kapcsolódó adathordozókból, amely észszerű biztosítékot nyújt arra, hogy az adatok végleg törlődtek. Az adatmegsemmisítés során megsemmisülnek a tárolóeszközről származó adatok, és ezzel együtt az összes címke, jelzés és tevékenységi napló is.

(10) A számítógépes adathordozót a helyi biztonsági tisztviselőnek vagy helyi informatikai biztonsági tisztviselőnek és/vagy a nyilvántartó hivatalt ellenőrző tisztviselőnek kell átadni megsemmisítés és ártalmatlanítás céljából.

43. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok eltávolítása és megsemmisítése

(1) Az osztályvezető kidolgozza, jóváhagyja és szükség esetén aktiválja az EU-minősített adatok megőrzése érdekében szükséges vészkiürítési és megsemmisítési terveket, amennyiben fennáll annak jelentős kockázata, hogy ezen adatok válsághelyzetben illetéktelen kezekbe kerülhetnek. Fontossági sorrendben és a vészhelyzet jellegétől függően figyelembe kell venni a következőket:

1. az EU-minősített adatok alternatív biztonságos helyre történő mozgatása, amennyiben lehetséges, ugyanazon épületen belüli biztonsági területen;

2. EU-minősített adatok biztonságos helyre történő átmentése, amennyiben lehetséges, egy másik épületben lévő biztonsági területen, lehetőség szerint a Bizottság egyik épületében;

3. EU-minősített adatok megsemmisítése, lehetőség szerint a jóváhagyott megsemmisítési eszközökkel.

(2) A vészhelyzeti tervek aktiválása esetén először a SECRET UE/EU SECRET minősítésű adatokat, majd azt követően a CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű adatokat kell áthelyezni vagy megsemmisíteni.

(3) A vészhelyzeti evakuálási és megsemmisítési tervek operatív részletei RESTREINT UE/EU RESTRICTED minősítésűnek minősülnek. Minden egyes, CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat tároló széfben másolatot kell őrizni, amely vészhelyzet esetén hozzáférhető.

44. cikk

Archiválás

(1) Az archiválás szükségességéről és annak időpontjáról, valamint a kapcsolódó gyakorlati intézkedésekről szóló határozatok összhangban állnak a Bizottság dokumentumkezelésre vonatkozó szakpolitikájával.

(2) CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok nem küldhetők az Európai Unió Firenzei Történeti Irattárába.

7. FEJEZET

ZÁRÓ RENDELKEZÉSEK

45. 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.

46. cikk

Hatálybalépés

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

Kelt Brüsszelben, 2019. október 17-én.

a Bizottság részéről,
az elnök nevében,
Günther OETTINGER
a Bizottság tagja

MELLÉKLET

CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz – szükség szerint – a szakmai feladatok ellátása érdekében hozzáféréssel rendelkező személyzet kategóriái

A Bizottság személyzetének kategóriái	C-UE/EU- C és S-UE/EU-S minősítésű adatokhoz való hozzáférés	Feltételek
Tisztviselők	Igen	Ellenőrzés + tájékoztató (briefing) + a kézhezvétel elismerése + engedélyezés + a szükséges ismeret elve
Ideiglenes alkalmazottak	Igen	Ellenőrzés + tájékoztató (briefing) + a kézhezvétel elismerése + engedélyezés + a szükséges ismeret elve
Szerződéses alkalmazottak	Igen	Ellenőrzés + tájékoztató (briefing) + a kézhezvétel elismerése + engedélyezés + a szükséges ismeret elve
Kirendelt nemzeti szakértők (knsz)	Igen	Kizárólag abban az esetben, ha tevékenységük megkezdését megelőzően az uniós tagállamok biztonsági ellenőrzést végeztek + a Bizottság által tartott tájékoztató + a kézhezvétel elismerése + a Bizottság általi engedélyezés + a szükséges ismeret elve
Gyakornokok	Nem	Kivétel nélkül
Bármely egyéb személyzeti kategória (átmenetileg foglalkoztatott, külsős munkatársak stb.)	Nem	Kivételek kérdésében konzultáljon a Bizottság Biztonsági Hatóságával