2024/1418

2024.5.24.

19/2024. sz. felhatalmazáson alapuló határozat a CONFIDENTIEL UE/EUCONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kezelésére vonatkozó végrehajtási szabályokról

AZ EURÓPAI SZÁMVEVŐSZÉK IGAZGATÁSI BIZOTTSÁGA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 287. cikkére,

tekintettel az EU-minősített adatok (EUCI) védelmét szolgáló biztonsági szabályokról szóló, 41/2021. sz. európai számvevőszéki határozatra ([1]) (a továbbiakban: „41/2021. sz. határozat”),

tekintettel a Számvevőszék információbiztonsági politikájára (jelenleg a 127/15 FINAL határozat) és információosztályozási politikájára (123/20. sz. személyzeti közlemény) ([2]),

tekintettel az Igazgatási Bizottság 2024. március 18-i ülésén folytatott megbeszélésekre,

mivel a 41/2021. sz. határozat a Számvevőszék valamennyi szervezeti egységére és létesítményére alkalmazandó;

mivel a 41/2021. sz. határozat 1. cikkének (3) bekezdése értelmében intézkedéseket kell hozni annak érdekében, hogy a Számvevőszék azon alkalmazottai, akiknek magasabb szintű EU-minősített adatokhoz kell hozzáférniük, ezt más uniós intézmények, szervek vagy ügynökségek megfelelő helyiségeiben megtehessék;

mivel a 41/2021. sz. határozat 1. cikkének (3) bekezdése és 5. cikkének (6) bekezdése úgy rendelkezik, hogy a Számvevőszék szolgáltatási szintre vonatkozó megállapodást köthet egy másik luxemburgi székhelyű uniós intézménnyel annak érdekében, hogy a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítésű adatokat ezen intézményen belül egy biztonsági területen kezelhesse és tárolhassa, és 2023. szeptember 25-én egyetértési megállapodást írt alá a Bizottság Humánerőforrásügyi és Biztonsági Főigazgatóságával a Biztonsági Igazgatóság luxembourgi biztonsági területének használatáról;

mivel az EU-minősített adatok – azok teljes életciklusa során biztosított – védelme érdekében hozott intézkedéseknek arányosnak kell lenniük különösen az adatok biztonsági minősítési szintjével;

mivel a Számvevőszékkel közölt információk bizalmas jellege, sértetlensége és rendelkezésre állása védelmét szolgáló biztonsági intézkedéseknek meg kell felelniük az érintett információk jellegének és típusának;

mivel a 41/2021. sz. határozat 3. cikkének (3) bekezdése értelmében az EU-minősített adatokat fizikai biztonsági intézkedésekkel kell védeni, a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatokat pedig személyi biztonsági intézkedésekkel is védeni kell;

mivel a 41/2021. sz. határozat 10. cikkének (10) bekezdése úgy rendelkezik, hogy az Igazgatási Bizottság felhatalmazáson alapuló határozatot fogad el a végrehajtási szabályok megállapításáról, és mivel a 41/2021. sz. határozat 8. cikkének (1) bekezdése és 10. cikkének (1) bekezdése értelmében annak hatálya az EU-minősített adatok kezelésére és tárolására, illetve a biztonsági szabályok megsértésére is kiterjed;

mivel a Számvevőszék a 41/2021. sz. határozattal biztosította, hogy az EU-minősített adatok magas szintű védelmét biztosító biztonsági intézkedései egyenértékűek legyenek a többi uniós intézmény, ügynökség és szerv által az EU-minősített adatok védelmére vonatkozóan elfogadott intézkedésekkel;

mivel a Számvevőszék, valamint a Bizottság, a Tanács és az EKSZ között 2023. január 27-én egyszerűsített adminisztratív megállapodás lépett hatályba;

([1]) HL L 256., 2021.7.19., 106.o.
([2]) Letölthető innen: https://www.eca.europa.eu/hu/legal-framework.

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

1. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

1. E határozat rögzíti a CONFIDENTIEL UE/EU CONFIDENTIAL ([3]) és a SECRET UE/EU SECRET ([4]) szintű, EU-minősített adatoknak (EUCI) a 41/2021. sz. számvevőszéki határozatnak megfelelően történő kezelési feltételeit.

2. Ez a határozat a Számvevőszék valamennyi szervezeti egységére vonatkozóan, a Számvevőszék valamennyi létesítményében alkalmazandó. A határozat hatálya a Számvevőszék kamaráira és bizottságaira is kiterjed, amelyek e határozat alkalmazásában beletartoznak a „szervezeti egységek” fogalmába.

3. 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 a Számvevőszék 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 írásban elismerte az érintett adatok védelmével kapcsolatos felelősségét;

d) a személy a 41/2021. sz. határozat 4. cikkének (4) bekezdésével összhangban biztonsági tanúsítványt szerzett és a megfelelő szintig és a meghatározott időpontig hozzáférési engedélyt kapott a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatójától.

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

3. A hozzáférést az alkalmazottak egyéb kategóriáira vonatkozóan a mellékletben szereplő táblázatnak megfelelően kell visszatartani vagy engedélyezni.

([3]) A 41/2021. sz. határozat 1. cikke (2) bekezdésének a) pontja értelmében a CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű adatok „olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit”.

([4]) A 41/2021. sz. határozat 1. cikke (2) bekezdésének a) pontja értelmében a SECRET UE/EU SECRET minősítésű adatok „olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele súlyosan sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit”.

2. FEJEZET

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

3. cikk

Kibocsátó

Míg a 41/2021. sz. határozat 2. cikkének m) pontja értelmében a kibocsátó olyan uniós intézmény, ügynökség vagy szerv, tagállam, harmadik állam vagy nemzetközi szervezet, amelynek fennhatósága alatt minősített adatokat hoztak létre, illetve vittek be az uniós struktúrákba, a CONFIDENTIEL UE/EU CONFIDENTIAL, illetve a SECRET UE/EU SECRET minősítésű adatok előkészítője nem feltétlenül egyezik meg a kibocsátó személyével.

4. cikk

A minősítési szint kijelölése

1. Egy dokumentum legalább CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű, ha engedély nélküli hozzáférhetővé tétele többek között:

a) jelentős kárt okozhatna a diplomáciai kapcsolatokban, azaz hivatalos tiltakozást vagy egyéb szankciókat vonna maga után;

b) sérthetné az egyének biztonságát vagy szabadságát;

c) károsíthatná a tagállamok vagy más adatszolgáltatók alkalmazott személyzete operatív hatékonyságát vagy biztonságát, illetve a fontos biztonsági vagy hírszerzési műveletek eredményességét;

d) lényegesen gyengíthetné jelentős szervezetek pénzügyi életképességét;

e) akadályozhatná a súlyos bűncselekmények felderítését, vagy megkönnyítené azok elkövetését;

f) jelentősen árthatna az EU vagy a tagállamok pénzügyi, monetáris, gazdasági vagy kereskedelmi érdekeinek;

g) komolyan hátráltathatná a fő uniós szakpolitikák kidolgozását vagy működését;

h) jelentős uniós tevékenységek megszűnéséhez vagy hirtelen megszakadásához vezethetne;

i) magasabb szinten minősített adatok felfedéséhez vezethetne.

2. Egy adat legalább SECRET UE/EU SECRET minősítésű, ha engedély nélküli hozzáférhetővé tétele többek között:

a) nemzetközi feszültséget okozhatna;

b) súlyos kárt okozhatna a harmadik országokkal vagy nemzetközi szervezetekkel fenntartott kapcsolatokban;

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

d) súlyosan károsíthatná a tagállamok vagy más adatszolgáltatók alkalmazott személyzete operatív hatékonyságát vagy biztonságát, illetve a rendkívül értékes biztonsági vagy hírszerzési műveletek folyamatos eredményességét;

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

f) magasabb szinten minősített adatok felfedéséhez vezethetne.

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

5. cikk

A tervezetek kezelése

1. Az adatokat előállításukat követően azonnal minősíteni kell. A CONFIDENTIEL UE/EU CONFIDENTIAL, illetve 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, miután a dokumentum kibocsátója megerősítette, hogy ez valóban biztonságos.

6. cikk

A forrásanyag rögzítése

Az alábbi 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 lehetséges maradjon az alkalmazott minősített forrásanyagok kibocsátóinak azonosítása.

7. cikk

Egy dokumentum részeinek minősítése

1. A Számvevőszék információosztályozási szabályzatának 12. pontjával 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 az 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, illetve 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 feltüntetni, franciául és angolul (először franciául). A jelölést nem szabad más nyelvekre lefordítani.

3. A CONFIDENTIEL UE/EU CONFIDENTIAL, illetve 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 (ha lehet, 16-os, de legalább 14-es) félkövér betűtípussal, minden oldalról kerettel körülvéve.

4. A CONFIDENTIEL UE/EU CONFIDENTIAL, illetve a 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 utóbbi önmagában nem minősített adat, kivéve, ha akként jelölik;

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

e) a dokumentumon fel kell tüntetni létrehozásának időpontját.

5. Amennyiben lehetséges, a SECRET UE/EU SECRET jelölést piros színnel kell feltüntetni.

9. cikk

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

A C-UE/EU-C és S-EU/EU-S rövidítések használhatók a CONFIDENTIEL UE/EU CONFIDENTIAL, illetve 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 rövidítés olyan szövegtörzsön is alkalmazható, ahol a teljes minősítési jelölés ismételt használata körülményes lenne. 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”, 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.

Amennyiben ez lehetséges, a minősítés feloldásának időpontját a dokumentum első oldalán, annak létrehozása időpontjában kell feltüntetni. 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 ilyenek rendelkezésre állnak.

2. CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok létrehozásakor a Számvevőszék alkalmazottainak a megfelelő minősítési szintre vagy magasabb minősítési szintre akkreditált kommunikációs és információs rendszert kell használnia. Ha kétség merül fel, az alkalmazottaknak konzultálnia kell a Számvevőszék információbiztonsági tisztviselőjével.

3. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok, beleértve a tervezeteket is (lásd: 5. cikk) nem továbbíthatók e-mailben, szabványos nyomtatón nyomtatott vagy lapolvasókon szkennelt formában, illetve nem továbbíthatók az alkalmazottak személyes eszközeire. A CONFIDENTIEL UE/EU CONFIDENTIAL, illetve 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 SECRET UE/EU SECRET minősítésű adatokat a terjesztés előtt és kézhezvételkor biztonsági célból nyilvántartásba kell venni. Nyilvántartásba kell venni az adatot:

— amikor megérkezik a Bizottság luxembourgi biztonsági területére, amelynek használatára a Számvevőszék egyetértési megállapodást kötött, illetve amikor elhagyja azt;

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

2. A 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 tartalmaz olyan intézkedéseket, amelyek garantálják a bejegyzések integritását.

4. A nyilvántartást ellenőrző tisztviselő egy olyan nyilvántartást vezet, amely minden egyes dokumentumra vonatkozóan legalább a következő információkat tartalmazza:

a) a végleges minősített dokumentum nyilvántartásba vételének időpontja;

b) a minősítési szint;

c) adott esetben a minősítési szint lejáratának időpontja;

d) a kibocsátó szervezeti egység neve;

e) a címzett, illetve címzettek;

f) a tárgy;

g) a dokumentum hivatkozási száma a kibocsátó szervezeti egységnél;

h) a nyilvántartási szám;

i) a szétosztott példányok száma;

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

k) a dokumentum visszaminősítésének vagy minősítése feloldásának időpontja;

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

13. cikk

Elosztás

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

3. FEJEZET

A MEGLÉVŐ CONFIDENTIEL UE/EU CONFIDENTIAL ÉS SECRET UE/EU SECRET MINŐSÍTÉSŰ ADATKAL 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 átadásra kerülnek;

d) a Számvevőszéken kívüli, de az EU-n belüli fél számára hozzáférhetővé válnak.

2. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok birtokosai olyan megfelelően felhatalmazott személyek, akik azért kaptak hozzáférést a minősített adatokhoz, hogy képesek legyenek feladataik ellátására. Ők felelősek a 41/2021. sz. határozatnak megfelelően az ilyen adatok helyes kezeléséért, tárolásért és védelméért. A minősített adatok kibocsátóival ellentétben a CONFIDENTIEL UE/EU CONFIDENTIAL, illetve a SECRET UE/EU SECRET minősítésű adatok birtokosai nem jogosultak dönteni azok visszaminősítéséről, minősítésének feloldásáról vagy azok továbbadásáról.

3. Ha a CONFIDENTIEL UE/EU CONFIDENTIAL, illetve a SECRET UE/EU SECRET minősítésű adat kibocsátója nem azonosítható, a kibocsátói ellenőrzést a minősített adatot birtokló számvevőszéki szervezeti egység gyakorolja. Amennyiben az adat birtokosa szükségesnek ítéli a CONFIDENTIEL UE/EU CONFIDENTIAL, illetve a SECRET UE/EU SECRET információk harmadik ország vagy nemzetközi szervezet részére történő átadását, a Számvevőszék tanácsot kér valamely, ugyanazon harmadik országgal vagy nemzetközi szervezettel kötött információbiztonsági megállapodás részes feleinek egyikétől ([5]).

15. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kezelésére alkalmas kommunikációs és információs rendszerek

A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokat lehetőség szerint elektronikus úton kell kezelni és továbbítani. A 41/2021. sz. határozat 6. cikkével összhangban erre a célra csak olyan kommunikációs és információs rendszerek és berendezések használhatók, amelyeket egy másik uniós intézmény, ügynökség, szerv vagy a Számvevőszék akkreditált.

16. cikk

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

1. Az eltávolítható adathordozók, például USB-kulcsok, CD-k, DVD-k vagy memóriakártyák (beleértve az SSD-ket is ([6])) használatát szigorúan ellenőrizni és dokumentálni kell. Csak a Számvevőszék vagy más uniós intézmény, szerv vagy ügynökség által rendelkezésre bocsátott, az információbiztonsági tisztviselő által jóváhagyott és az általa jóváhagyott termékkel titkosított, eltávolítható adathordozókat szabad használni. A személyes eltávolítható adathordozók és a konferenciákon, szemináriumokon stb. ajándékként kiosztott adathordozók nem használhatók minősített adatok továbbítására. Amennyiben lehetséges, az információbiztonsági tisztviselő által kiadott útmutatásnak megfelelően Tempest-biztos eltávolítható adathordozót kell használni.

([5]) Részletesebben lásd: 35. cikk.

([6]) Az SSD félvezető alapú meghajtót, tartós állapotú meghajtót vagy szilárdtestmeghajtót jelent.

2. Ha a minősített dokumentumot eltávolítható adathordozón elektronikusan kezelik vagy tárolják, a minősítési jelölésnek jól láthatónak kell lennie az adatokon belül, valamint a fájlnévben és az eltávolítható adathordozón.

3. Az alkalmazottak 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. Az ilyen minősítésű adatok eltávolítható adathordozókra történő letöltése előtt különös figyelmet kell fordítani annak biztosítására, hogy az eszköz 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 jóváhagyott termékek vagy módszerek révén biztonságosan el kell távolítani, vagy törölni kell. Az eltávolítható adathordozókat – amikor már nincs rájuk szükség – meg kell semmisíteni, kivéve, ha azokat megfelelő széfben tárolják. Minden megsemmisítésnek vagy törlésnek a Számvevőszék biztonsági szabályaival összhangban kell történnie. A eltávolítható adathordozókról jegyzéket kell vezetni, és megsemmisítésükről nyilvántartást kell vezetni.

17. cikk

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

1. A 41/2021. határozat 5. cikkének (5) és (6) bekezdésével összhangban a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokat biztonsági területen kell kezelni ([7]). Az ilyen információkhoz a Számvevőszék alkalmazottai egy másik uniós intézmény biztonsági területein is hozzáférhetnek.

2. A 41/2021. sz. határozat 5. cikkének (6) bekezdése értelmében és a kibocsátó kifejezett beleegyezése esetén ezek az információk kivételesen a Számvevőszék igazgatási területén ([8]) is kezelhetők, feltéve, hogy az EU-minősített adatokhoz jogosulatlan személyek nem férhetnek hozzá.

3. Válsághelyzetben vagy vészhelyzet esetén ezek az információk a biztonsági területen és az adminisztratív zónán kívül is kezelhetők, feltéve, hogy a birtokos megelőzően vállalja, hogy kompenzációs intézkedéseket alkalmaz, amelyek legalább a következőket foglalják magukban:

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

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

— Papíralapú dokumentumok esetében a birtokos a lehető leghamarabb és a válsághelyzet vagy vészhelyzet jellegétől függően értesíti az EU-minősített adatok nyilvántartóját arról, hogy a minősített dokumentumokat a biztonsági területen és az adminisztratív zónán kívül kezelik.

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

— A helyiség 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. További másolatokat csak az EU-minősített adatok nyilvántartója bocsáthat rendelkezésre.

([7]) Az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2015. március 13-i (EU, Euratom) 2015/444 bizottsági határozat (HL L 72., 2015.3.17., 53. o.) 18. cikke szerint.

([8]) A 41/2021. sz. határozat mellékletének fogalommeghatározása szerint.

— A dokumentumokat adminisztratív zónán vagy biztonsági területen kívül csak a szükséges minimális ideig lehet kezelni és ideiglenesen tárolni, amely időtartamot követően azokat vissza kell szolgáltatni az EU-minősített adatok nyilvántartójának.

— A dokumentum visszaszolgáltatását aláírással kell igazolni.

— Minősített dokumentumot annak birtokosa nem dobhat ki, illetve nem semmisíthet meg.

4. A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat biztonsági területen kell tárolni biztonsági tárolóeszközben vagy megerősített helyiségben.

5. További tanács az információbiztonsági tisztviselőtől kérhető.

6. A dokumentumot érintő bármely feltételezett vagy tényleges biztonsági incidenst a lehető leghamarabb jelenteni kell az információbiztonsági tisztviselőnek.

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 adatok birtokosának utasítására kerülhet sor, feltéve, hogy a kibocsátó ezt kifejezetten jóváhagyta és nem jelentett be ezzel kapcsolatos fenntartásokat. A feltétlenül szükségesnél több másolat azonban nem készíthető. A Számvevőszék arra is felkérheti a kibocsátót, hogy bocsásson rendelkezésre angol nyelvű fordítást a dokumentumból.

2. Amennyiben a minősített dokumentumnak csak egy része kerül sokszorosításra, ugyanazok a feltételek alkalmazandók, mint ha ugyanez a teljes dokumentumot érintené. Azonos szintű minősítéssel kell ellátni a kivonatokat is, kivéve, ha a kibocsátó azokat kifejezetten alacsonyabb szintű minősítéssel, illetve „nem minősített” jelöléssel látta el.

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 a 17. cikk (2) bekezdésével összhangban elektronikusan, megfelelően akkreditált eszközökkel, illetve jóváhagyott kriptográfiai termékekkel védett módon kell elküldeni.

2. A rendelkezésre álló eszközöktől vagy a konkrét körülményektől függően a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kézzel történő szállítása papíralapú dokumentum formájában vagy eltávolítható adathordozó révén is történhet. CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok továbbításakor a papíralapú dokumentumok küldésével szemben előnyben kell részesíteni az eltávolítható adathordozók használatát.

3. A 41/2021. határozat 6. cikkének (8) bekezdésével összhangban az eltávolítható adathordozókat a Tanács, vagy a Tanács főtitkára által kriptojóváhagyó hatóságként jóváhagyott termék, vagy ilyen híján a más uniós intézmények, ügynökségek és szervek által az EU-minősített adatok védelmére jóváhagyott termék révén titkosítani kell. Az így jóváhagyott termék alkalmazásával történő titkosítással nem védett eltávolítható adathordozókon tárolt CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokat a papíralapú információkkal 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. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatot két rétegű nem átlátszó csomagolásban, például borítékban, nem átlátszó mappában vagy aktatáskában kell szállítani. A csomagolás külső oldalát le kell zárni és azon 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 szándékolt címzett nevének, beosztásának és címének, valamint egy visszaküldési címnek, amennyiben a szállítmány nem kézbesíthető.

6. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatokat kézzel szállító alkalmazottaknak, illetve futárszolgálatnak biztonsági engedéllyel és futárigazolvánnyal kell rendelkeznie.

7. A borítékok és a csomagok nem nyithatók meg szállítás közben. A futárszolgálat biztonsági engedélye nem jogosítja fel őt arra, hogy hozzáférjen a minősített adatok tartalmához.

8. A 41/2021. sz. határozat 5. cikkének (12) bekezdése értelmében a kibocsátó további fizikai biztonsági intézkedéseket is előírhat, hogy a szállítás során az információhoz ne lehessen jogosulatlanul hozzáférni.

9. Az alkalmazottak vagy futárok által szállított CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat tartalmazó bármely feltételezett vagy tényleges biztonsági incidenst kivizsgálás céljából haladéktalanul be kell jelenteni az információbiztonsági tisztviselőnek.

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 részletesen leírja a minősített adatokat tartalmazó eltávolítható adathordozókat, valamint az azokon tárolt összes dokumentumot, hogy a címzett elvégezhesse a szükséges ellenőrzéseket és megerősíthesse az átvételt.

2. Az eszközökön csak az éppen szállított EU-minősített adatok tárolhatók. Az ugyanazon eszközön található összes minősített adat címzettjének ugyanannak kell lennie. A küldő feleknek szem előtt kell tartaniuk, hogy az egyazon eszközön 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. Az 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 szállítása a szervezeti egységeken és a Számvevőszék épületein belül

1. A biztonsági engedéllyel rendelkező alkalmazottak a szervezeti egységeken és a Számvevőszék épületein belül szállíthatnak 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 belső postával nem továbbíthatók.

22. cikk

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

1. A Számvevőszék vagy más kibocsátó uniós intézmények, ügynökségek és szervek alkalmazottai, illetve 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) CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok nem átlátszó, dupla falú borítékban vagy csomagolásban továbbíthatók. A külső oldalt le kell zárni és azon 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.

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 minősítésű adatokat kívánnak küldeni az Unión belül más helyszínekre, intézkedhetnek úgy, hogy azokat az alábbi eszközök egyikével továbbítsák:

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

b) katonai, kormányzati vagy diplomáciai futárszolgálattal, a Nyilvántartási Hivatal alkalmazottaival együttműködve.

3. Azon alkalmazottak, akik SECRET UE/EU SECRET minősítésű adatokat kívánnak küldeni más uniós tagállamoknak, a nyilvántartást ellenőrző tisztviselővel együttműködve intézkedhetnek úgy, hogy azokat katonai, kormányzati vagy diplomáciai futárszolgálat útján továbbítsák, de postai vagy kereskedelmi futárok útján nem.

4. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatokat szállító számvevőszéki alkalmazottaknak vagy hivatalos bizottsági futároknak minden egyes szállítmányra vonatkozóan futárigazolvánnyal kell rendelkezniük. Az igazolványt a nyilvántartást ellenőrző tisztviselő állítja ki, és az igazolja, hogy a szállító jogosult a szállítmány továbbítására.

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, a Számvevőszék vagy más kibocsátó uniós intézmények, ügynökségek és szervek alkalmazottai általi kézi szállítás útján is lehet továbbítani.

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

3. CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű, papíralapú vagy eltávolítható adathordozón szállított dokumentumok kézi szállítása során az alkalmazottaknak mindegyik következő kiegészítő intézkedésnek meg kell felelnie:

— Ha a minősített adatokat tömegközlekedéssel szállítják, a dokumentumot a szállító által személyesen felügyelt aktatáskába vagy kézitáskába kell helyezni. Minősített dokumentum csomagtérben 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 a nyilvántartást ellenőrző tisztviselő által kiállított futárigazolvánnyal kell rendelkeznie, amely igazolja, hogy a szállító jogosult a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű csomag szállítására.

24. cikk

Kereskedelmi futárok által végzett szállítás

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

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

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

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

25. cikk

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

1. Minősített szállítmányok előkészítésekor a küldőknek szem előtt kell tartaniuk, hogy a kereskedelmi futárszolgálatok CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű küldeményeket csak a nyilvántartást ellenőrző tisztviselőnek, megfelelően felhatalmazott helyettesének vagy a szándékolt címzettnek szállíthatnak.

2. A jóváhagyott kereskedelmi futárszolgálat révén küldött információszállítmányokat a következőképpen kell előkészíteni és csomagolni:

a) A szállítmányt nem átlátszó, dupla falú borítékban (ahol a belső réteg kialakítása egyértelművé teszi, ha a borítékot megkísérelték felnyitni) 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 külső csomagolást le kell zárni, és azon nem szerepelhet a minősítésre utaló jelzés.

d) Mind a belső, mind a külső borítékon, illetve a csomagolás rétegein egyértelműen fel kell tüntetni egy személy nevét a szándékolt címzettnél, valamint egy visszaküldési címet is.

e) A belső borítékban vagy a csomagolás belső rétegében el kell helyezni egy nyilvántartási űrlapot, 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 példány sorszámát, a tárgyát azonban nem tartalmazhatja.

f) A külső borítéknak vagy csomagolásnak tartalmaznia kell egy átvételi elismervényt. Az átvételi elismervény, amely önmagában nem minősített dokumentum, tartalmazza a hivatkozási számot, a dátumot és a dokumentum példányának sorszámát, annak tárgyát azonban nem tartalmazhatja.

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, és megállapodik vele 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 jelenteni ezt az információbiztonsági tisztviselőnek és a nyilvántartást ellenőrző tisztviselőnek, akik megteszik a biztonsági incidens által szükségessé tett lépéseket.

26. cikk

Egyéb különleges kezelési feltételek

1. Az adatbiztonsági megállapodásban vagy igazgatási megállapodásokban meghatározott bármely további szállítási feltételnek teljesülnie kell. Kétség esetén az alkalmazottaknak konzultálniuk kell az információbiztonsági tisztviselővel és a nyilvántartást ellenőrző tisztviselővel.

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 lezárt, nem átlátszó borítékban kell szállítani, adott esetben további fizikai védelmi intézkedések megtételével, például buborékos fóliával bélelt borítékban történő elhelyezéssel.

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 vitatnak meg, csak a megfelelő vagy annál magasabb szintű akkreditált üléstermében lehet megtartani. A Számvevőszék egy másik uniós intézmény biztonsági területén is használhat üléstermeket. Amennyiben ilyen nem áll rendelkezésre, az alkalmazottak kikérik az információbiztonsági tisztviselő tanácsát.

2. Általános szabályként az ülések napirendjét nem kell minősítéssel ellátni. Ha az ülés napirendje minősített dokumentumokat említ, maga a napirend nem kap automatikusan minősítést. 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 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, valamint átestek a megfelelő szintű biztonsági ellenőrzésen és rendelkeznek megfelelő engedéllyel.

5. A meghívóban is fel kell hívni a résztvevők figyelmét arra, hogy az ülésen minősített témákat tárgyalnak, és hogy ennek megfelelő biztonsági intézkedésekre fog sor kerülni.

6. Az ülés szervezőinek emlékeztetniük kell a résztvevőket 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 ülés szervezői előre elkészítik a résztvevők teljes listáját. A 41/2021. sz. határozat 4. cikkének (6) bekezdésével összhangban kellő időben tájékoztatják az információbiztonsági tisztviselőt az ülések dátumáról, időpontjáról, helyszínéről és a résztvevők listájáról.

28. cikk

A résztvevők hozzáférése a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű ülésekhez

1. Az ülés szervezőinek tájékoztatniuk kell az információbiztonsági tisztviselőt és a nyilvántartást ellenőrző tisztviselőt a Számvevőszék által szervezett CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű ülésen részt vevő minden külső látogatóról.

2. A résztvevők kötelesek igazolni, hogy megfelelő szintű érvényes személyi biztonsági tanúsítvánnyal rendelkeznek 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 ülés termében lévő elektronikus berendezések

CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok közlésekor csak az e határozat 11. cikke szerinti akkreditált informatikai rendszerek használhatók, például előadások vagy videokonferenciák során.

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 átáll minősített üzemmódra. Az ajtóknak zárva kell lenniük.

2. A résztvevők és adott esetben a tolmácsok részére aláírás ellenében csak a szükséges számú iratot kell a vita kezdetén kiadni.

3. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok az ülés szüneteiben sem maradhatnak őrizetlenül.

4. Az ülés végén a résztvevőket és a tolmácsokat emlékeztetni kell arra, hogy ne hagyják őrizetlenül a minősített adatokat tartalmazó dokumentumokat, illetve az ülés alatt készített minősített feljegyzéseket. Az ülés végén a résztvevők által nem igényelt CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű dokumentumokat és a tolmácsok által használt valamennyi dokumentumot aláírással vissza kell szolgáltatni a nyilvántartást ellenőrző tisztviselőnek, hogy az a megfelelő iratmegsemmisítő-gépekben megsemmisítse azokat ([9]).

5. Az ülés során listát kell készíteni a résztvevőkről, valamint vázlatosan fel kell jegyezni, hogy milyen minősített adatokat osztottak meg a tagállamokkal, illetve közöltek szóban harmadik országokkal vagy nemzetközi szervezetekkel, hogy mindezt jegyzőkönyvezni lehessen az ülés eredményei között.

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 ([10]) hatálya alá tartoznak, vagy szerződéses kapcsolatban állnak a Számvevőszékkel vagy egy másik uniós intézménnyel.

([9]) Részletesebben lásd: a 42. cikk (6) bekezdése.

([10]) A módosított 31. EGK rendelet a tisztviselők személyzeti szabályzatáról és az egyéb alkalmazottak alkalmazási feltételeiről (HL 45., 1962.6.14., 1385/62. o.) (ELI: http://data.europa.eu/eli/reg/1962/31(1)/2023-01-01).

5. FEJEZET

A CONFIDENTIEL UE/EU CONFIDENTIAL ÉS 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 Számvevőszék, akkor a Számvevőszék 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 számvevőszéki 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 Számvevőszékkel megfelelő jogi megállapodást kötött.

2. Általános szabályként a minősített adatok más uniós intézményekkel, ügynökségekkel, szervekkel és hivatalokkal történő cseréjének fő beérkezési és kiküldési helye a Számvevőszéken belül az EU-minősített adatok nyilvántartója.

34. cikk

CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok tagállamokkal történő 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 ([11]) ellátott és a Számvevőszék 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 történő 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 ehhez megfelelő jogi vagy igazgatási keretrendszerrel rendelkezik, amilyen például a Számvevőszékkel kötött adatbiztonsági megállapodás vagy igazgatási megállapodás. Az ilyen megállapodás vagy intézkedés rendelkezései elsőbbséget élveznek e határozat rendelkezéseivel szemben.

2. Általános szabályként valamennyi CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősített adat a Számvevőszék, illetve harmadik országok és nemzetközi szervezetek közötti cseréjének fő beérkezési és kiküldési helye az EU-minősített adatok nyilvántartója.

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

3. A harmadik országtól vagy nemzetközi szervezettől kapott minősített adatokat biztonsági okokból nyilvántartásba kell venni. Az alkalmazottaknak ezért kapcsolatba kell lépnie az EU-minősített adatok nyilvántartójával, 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;

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

5. A nyilvántartásba vétel végezhető papíralapon, vagy elektronikus iktatókönyvben.

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

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

36. cikk

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

1. Ha a Számvevőszék 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 megfelelő adatbiztonsági megállapodás vagy igazgatási intézkedés, a kivételes eseti adatátadási eljárást kell követni.

2. A Számvevőszék szervezeti egységei kapcsolatba lépnek az információbiztonsági tisztviselővel és a kibocsátóval. A Számvevőszék tanácsot kér valamely, ugyanazon harmadik országgal, nemzetközi szervezettel vagy uniós szervezettel kötött információbiztonsági megállapodás részes feleinek egyikétől.

3. E konzultációt követően a Számvevőszék testülete a főtitkár javaslata alapján engedélyezheti az érintett információk 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 adott időpontban vagy 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 számvevőszéki dokumentumok visszaminősítését vagy minősítésének feloldását eseti alapon is el lehet végezni, például nyilvános hozzáférés iránti kérelem alapján.

38. cikk

A visszaminősítésért és a minősítés feloldásáért viselt 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. Annak eldöntéséért, hogy valamely dokumentum visszaminősíthető-e, illetve minősítése feloldható-e, a Számvevőszék azon szervezeti egysége felelős, amely a minősített dokumentumot létrehozta. A Számvevőszéken belül a dokumentum visszaminősítésére és a minősítés feloldására irányuló összes kérelmet illetően a kibocsátó szervezeti egység vezetőjével, igazgatójával, vagy a feladatfelelőssel kell konzultálni. Ha az érintett szervezeti egység különböző forrásokból származó minősített adatokat gyűjt össze, először ki kell kérnie minden, forrásanyagot rendelkezésre bocsátó fél – többek között a tagállamok, egyéb uniós szervek, harmadik országok vagy nemzetközi szervezetek – hozzájárulását.

3. Amennyiben a kibocsátó számvevőszéki szervezeti egység már nem létezik, és felelősségi körét egy másik szervezeti egység vette át, a visszaminősítéssel és feloldással kapcsolatos döntést ez az egység hozza meg. Ha a kibocsátó szervezeti egység már nem létezik, és felelősségi körét nem vette át egy másik szervezeti egység, a visszaminősítéssel vagy feloldással kapcsolatos döntést a Számvevőszék igazgatói közösen hozzák meg.

4. A visszaminősítésért vagy a minősítés feloldásáért felelős szervezeti egységnek együtt kell működnie az EU-minősített adatok nyilvántartójával a visszaminősítésről vagy a minősítés feloldásáról szóló gyakorlati intézkedések kapcsán.

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 a Számvevőszék információosztályozási politikájának ([12]) 16. pontja, illetve a nem EU-minősített adatok osztályozásáról és kezeléséről szóló iránymutatásainak 4. pontja szerinti „nem minősített érzékeny adat” információterjesztési jelölést.

40. cikk

Hogyan jelölendő, hogy a dokumentum 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 (nem pedig 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 Számvevőszék Irattárát tájékoztatni kell valamennyi, minősítés feloldásáról hozott határozatról.

5. A visszaminősítés vagy a minősítés feloldása kapcsán a minősített adatok valamennyi fordítására ugyanolyan eljárást kell alkalmazni, mint az eredeti nyelvi változat esetében.

([12]) Letölthető innen: https://www.eca.europa.eu/hu/legal-framework.

41. cikk

A CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű adatok részleges visszaminősítése vagy a minősítés részleges 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 esetén feloldott minősítésű kivonatot kell készíteni.

3. A feloldott minősítésű kivonatban a továbbra is minősített részek helyébe a következő szöveg lép:

FEL NEM OLDANDÓ MINŐSÍTÉSŰ RÉSZ

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

4. Külön meg kell említeni a szövegben, ha egy teljes melléklet minősítését nem lehet feloldani, és ezért az nem szerepel a kivonatban.

42. cikk

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

1. A Számvevőszék nem halmoz fel nagy mennyiségű minősített adatot.

2. Az egyes kibocsátó szervezeti egységeknek legalább ötévente felül kell vizsgálniuk a dokumentumokat megsemmisítés vagy törlés szempontjából. Erre rendszeres időközönként sort kell keríteni mind a papíron, mind a kommunikációs és információs rendszerben tárolt adatok tekintetében.

3. Az alkalmazottak nem semmisíthetik meg a továbbiakban már nem szükséges CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű dokumentumok nyomtatott példányait, hanem fel kell kérniük a nyilvántartást ellenőrző tisztviselőt, hogy a dokumentumokat az eredeti dokumentumra vonatkozó archiválási követelmények figyelembevételével semmisítse meg.

4. Az alkalmazottak nem kötelesek tájékoztatni a kibocsátót, ha törli a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a SECRET UE/EU SECRET minősítésű dokumentumok másolatait.

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 CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű dokumentumok megsemmisítésére a DIN 66399 5. szintű iratmegsemmisítő-gépek alkalmasak. A SECRET UE/EU SECRET minősítésű dokumentumok megsemmisítésére a DIN 66399 6. szintű iratmegsemmisítő-gépek alkalmasak.

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

8. A nyilvántartást ellenőrző tisztviselő megsemmisítési igazolásokat állít ki, és ennek megfelelően frissíti az iktatókönyveket és egyéb nyilvántartási adatokat.

9. Az élettartamának végét elérő valamennyi, CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET adatokat tartalmazó adathordozót és eszközt megfelelően meg kell tisztítani. Az elektronikus adatokat olyan módon kell megsemmisíteni vagy törölni az informatikai eszközökből és a kapcsolódó adathordozókból, amely észszerű biztosítékot nyújt arra, hogy az adatok végleg törlődtek. Az adatmegsemmisítés során meg kell semmisíteni a tárolóeszközről származó valamennyi adatot, és ezzel együtt az összes címkét, jelzést és tevékenységi naplót is.

10. A számítógépes adathordozókat a nyilvántartást ellenőrző tisztviselő tájékoztatását követően az információbiztonsági 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 vészhelyzet esetén

1. A Számvevőszék és a Bizottság Humánerőforrásügyi és Biztonsági Főigazgatósága közötti, a biztonsági terület használatáról szóló egyetértési megállapodás értelmében a Bizottság által a minősített adatok védelmére kidolgozott vészhelyzeti eljárást kell alkalmazni. Szükség esetén a Bizottság Biztonsági Igazgatóságának luxemburgi helyi biztonsági tisztviselője hozzáférhet a Számvevőszék széfjéhez, hogy alkalmazza a Bizottság által megállapított vészhelyzeti eljárást, és aktiválja a vészhelyzeti evakuálási és megsemmisítési terveket, amennyiben fennáll annak jelentős kockázata, hogy az EU-minősített adatok válsághelyzetben illetéktelen kezekbe kerülhetnek. Fontossági sorrendben és a vészhelyzet jellegétől függően a következő lehetőségeket kell mérlegelni:

i. az EU-minősített adatok alternatív biztonságos helyre történő áthelyezése, amennyiben lehetséges, ugyanazon épületen belüli biztonsági területre;

ii. az EU-minősített adatok biztonságos helyre történő átmentése, amennyiben lehetséges, egy másik épületben – lehetőség szerint egy uniós intézmény épületében – lévő biztonsági területre;

iii. az EU-minősített adatok megsemmisítése, lehetőség szerint a jóváhagyott megsemmisítési eszközök egyikével.

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 maguk is RESTREINT UE/EU RESTRICTED minősítésűnek minősülnek. Minden egyes, CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat tároló széfben másolatot kell őrizni, hogy az vészhelyzet esetén hozzáférhető legyen.

44. cikk

Archiválás

1. Az archiválás szükségességéről és annak időpontjáról, valamint a kapcsolódó gyakorlati intézkedésekről szóló határozatoknak összhangban kell lenniük a Számvevőszék információbiztonsági, információosztályozási és archiválási politikájával.

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 a Számvevőszék alkalmazottainak és a határozat hatálya alá tartozó minden személynek tudomására kell hozni, és az *Európai Unió Hivatalos Lapjában* közzé kell tenni.

46. cikk

Hatálybalépés

Ez a határozat az Igazgatási Bizottság általi elfogadását követően, az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon lép hatályba.

Kelt Luxembourgban, 2024. március 19-én.

az Európai Számvevőszék Igazgatási Bizottsága nevében
az elnök
Tony MURPHY

MELLÉKLET

CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz – szükség szerint – a feladataik ellátása érdekében hozzáféréssel rendelkező alkalmazottak kategóriái

A Számvevőszék személyi állományának kategóriái	A CONFIDENTIEL UE/EU CONFIDENTIAL ÉS A SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférés	Feltételek
Számvevőszéki tagok	igen	Tájékoztató (briefing) + a kézhezvétel elismerése
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
Az uniós tagállamok kirendelt nemzeti szakértői	igen	Kizárólag abban az esetben, ha tevékenységük megkezdését megelőzően az uniós tagállamok elvégezték biztonsági ellenőrzésüket + a Számvevőszék által tartott tájékoztató + a kézhezvétel elismerése + a Számvevőszék általi engedélyezés + a szükséges ismeret elve
Gyakornokok	nem	Kivétel nélkül
Az alkalmazottak bármely egyéb kategóriája (átmenetileg foglalkoztatott, külsős munkatársak stb.)	nem	Kivétel nélkül