EURÓPAI
SZÁMVEVŐSZÉK

A Számvevőszék 041–2021. számú határozata az EU-minősített adatok (EUCI) védelmét szolgáló biztonsági szabályokról

AZ EURÓPAI SZÁMVEVŐSZÉK,

TEKINTETTEL az Európai Unióról szóló szerződés 13. cikkére,

TEKINTETTEL az Európai Unió működéséről szóló szerződés 287. cikkére,

TEKINTETTEL az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról szóló, 2018. július 18-i (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendeletre,

TEKINTETTEL a Számvevőszék eljárási szabályzatának végrehajtására vonatkozó szabályok (a Számvevőszék 21–2021. számú határozata) 1. cikkének (6) bekezdésére,

TEKINTETTEL a más uniós intézmények, ügynökségek és szervek EU-minősített adatainak védelmét szolgáló biztonsági szabályokra,

TEKINTETTEL a Számvevőszék információbiztonsági politikájára (127/15 FINAL határozat) és adatminősítési politikájára (123/2020 személyzeti közlemény),

MIVEL az EUMSZ 287. cikkének (3) bekezdése alapján a Számvevőszék jogosult hozzáférni minden olyan dokumentumhoz vagy információhoz, amelyek véleménye szerint a feladatai elvégzéséhez szükségesek, beleértve az EU-minősített adatokat (EUCI) is, és ennek az intézmények közötti lojális együttműködés elvével és a hatáskör-átruházás elvével teljes összhangban kell történnie; az EU-minősített adatokhoz való hozzáférésnek az EUMSZ által biztosított jogát az EU-minősített adatok kibocsátója nem kérdőjelezheti meg, miközben a Számvevőszéket fel lehet kérni bizonyos biztonsági intézkedések bevezetésére és betartására az alábbiakban részletesen kifejtettek szerint;

MIVEL a Számvevőszék tagjait, tisztviselőit és egyéb alkalmazottait az EUMSZ 339. cikke, a személyzeti szabályzat 17. cikke és az annak alapján elfogadott jogi aktusok szerint titoktartási kötelezettség köti, még a szolgálatból való kilépésük után is;

MIVEL az EU-minősített adatok érzékeny jellege miatt kezelésük megköveteli a titoktartási kötelezettség betartását, amelyet olyan megfelelő biztonsági intézkedésekkel kell biztosítani, amelyek szavatolják ezen információk magas szintű védelmét, és amelyek egyenértékűek a többi uniós intézmény, ügynökség és szerv által elfogadott, az EU-minősített adatok védelmére vonatkozó szabályokban meghatározottakkal, azzal a feltétellel, hogy amennyiben a Számvevőszék úgy ítéli meg, hogy az ilyen biztonsági intézkedések az EU-minősített adatok jellegére és típusára tekintettel nem indokoltak, a Számvevőszék fenntartja a jogot, hogy az EU-minősített adatok

minősítési szintjének tiszteletben tartása mellett megtegye az általa megfelelőnek ítélt észrevételeket;

MIVEL a Számvevőszékkel közölt információk bizalmas jellegének, sértetlenségének és rendelkezésre állásának védelmét szolgáló biztonsági intézkedéseknek meg kell felelniük az érintett információk jellegének és típusának;

MIVEL a minősített adatokhoz való hozzáférést a Számvevőszék számára a szükséges ismeret elve alapján biztosítani kell a Szerződések, illetve a Szerződések alapján elfogadott jogi aktusok által a Számvevőszékre ruházott feladatok elvégzése céljából;

MIVEL bizonyos információk jellegére és érzékeny tartalmára tekintettel helyénvaló külön eljárást bevezetni az EU-minősített adatokat tartalmazó dokumentumok Számvevőszék általi kezelésére;

MIVEL az intézménynek biztosítania kell, hogy ezt a határozatot az összes alkalmazandó szabállyal összhangban hajtják végre, különös tekintettel a személyes adatok védelmére, a személyek, az épületek és az informatika fizikai biztonságára, valamint a dokumentumokhoz való nyilvános hozzáférésre vonatkozó rendelkezésekre;

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

1. cikk Tárgy és hatály

1) Ez a határozat meghatározza a Számvevőszék által a megbízatása gyakorlása során kezelt minősített adatok védelmére vonatkozó alapelveket és biztonsági minimumszabályokat.

2) E határozat alkalmazásában a minősített adat a következő típusú információk bármelyikét vagy mindegyikét jelenti:

a) más uniós intézmények, ügynökségek, szervek vagy hivatalok biztonsági szabályaiban meghatározott „EU-minősített adat” (EUCI), és amely az alábbi biztonsági minősítési jelölések egyikével van ellátva:

- TRÈS SECRET UE/EU TOP SECRET: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele rendkívül súlyosan sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit;
- SECRET UE/EU SECRET: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele súlyosan sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit;
- CONFIDENTIEL UE/EU CONFIDENTIAL: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit;
- RESTREINT UE/EU RESTRICTED: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele hátrányosan érintheti az Európai Unió, illetve egy vagy több tagállam érdekeit.

b) a tagállamok által rendelkezésére bocsátott minősített adat, amelynek nemzeti biztonsági minősítési jelölése megfelel az EU-minősített adatok a) pontban felsorolt biztonsági minősítési jelölései[1] valamelyikének;

c) harmadik államok vagy nemzetközi szervezetek által az Európai Számvevőszék rendelkezésére bocsátott minősített adat, amelynek biztonsági minősítési jelölése megfelel az EU-minősített adatok a) pontban felsorolt biztonsági minősítési jelölései valamelyikének, a vonatkozó információbiztonsági megállapodásokkal vagy igazgatási megállapodásokkal összhangban.

3) A Számvevőszék a RESTREINT UE/EU RESTRICTED szintű információkat saját létesítményeiben kezeli, és ennek érdekében meghoz minden szükséges védelmi intézkedést. 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.

4) Ez a határozat a Számvevőszék valamennyi szervezeti egységére és létesítményére alkalmazandó.

5) Ez a határozat a személyzet egyes csoportjaira vonatkozó konkrét rendelkezések kivételével a Számvevőszék tagjaira, a személyzeti szabályzat és az Európai Unió egyéb alkalmazottainak alkalmazási feltételeinek[2] hatálya alá tartozó számvevőszéki személyzetre, a Számvevőszékhez kirendelt nemzeti szakértőkre, a szolgáltatókra és azok személyzetére, a gyakornokokra és a Számvevőszék épületeihez vagy egyéb ingatlanaihoz hozzáféréssel rendelkező bármely személyre, illetve a Számvevőszék által kezelt adatokra vonatkozik.

6) Eltérő rendelkezés hiányában az EU-minősített adatokra vonatkozó rendelkezéseket azonos módon kell alkalmazni az e cikk (2) bekezdésének b) és c) pontjában említett minősített információkra.

2. cikk Fogalommeghatározások

E határozat alkalmazásában:

a) „engedély EU-minősített adatokhoz való hozzáférésre”: a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatója által valamely tagállam illetékes hatósága által ad ott bizonyosság alapján hozott azon határozat, hogy a Számvevőszék tisztviselője, egyéb tagja vagy alkalmazottja vagy egy kirendelt nemzeti szakértő – feltéve, hogy rájuk vonatkozóan meghatározták a „szükséges ismeret” esetének fennállását, és hogy megfelelő tájékoztatást kaptak ezzel kapcsolatos felelősségükről – meghatározott minősítési szintig (CONFIDENTIEL UE/EU CONFIDENTIAL vagy e fölött) és meghatározott időpontig hozzáférést kaphatnak EU-minősített adatokhoz; a fentieknek megfelelő személy megjelölése „biztonsági engedéllyel rendelkező” személy;

b) „minősítés”: egy minősítési szint hozzárendelése egy adathoz annak alapján, hogy annak engedély nélküli hozzáférhetővé tétele milyen mértékű sérelmet okozhat;

---

[1] Lásd: Az Európai Uniónak a Tanács keretében ülésező tagállamai között az Európai Unió érdekében kicserélt minősített adatok védelméről szóló, 2011. május 25-én aláírt megállapodás és annak melléklete (HL C 202., 2011.7.8., 13. o.).

[2] A módosított 31. EGK rendelet a tisztviselők személyzeti szabályzatáról és az egyéb alkalmazottak alkalmazási feltételeiről (HL 01 962R0031–01.01.2020–019.003–1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020–01-01).

c) „kriptográfiai anyag”: kriptográfiai algoritmusok, kriptográfiai hardver- és szoftvermodulok, valamint rejtjelező eszközök, beleértve a végrehajtás leírását és a kapcsolódó dokumentációt, valamint a kulcs generálására szolgáló anyagokat;

d) „a minősítés feloldása”: bármely biztonsági minősítés hatályának megszüntetése;

e) „dokumentum”: bármilyen rögzített adat, annak megjelenésétől vagy fizikai jellemzőitől függetlenül;

f) „visszaminősítés”: a minősítési szint leszállítása;

g) „telephely-biztonsági tanúsítvány”: annak az illetékes biztonsági hatóság által történő hivatalos meghatározása, hogy egy adott létesítmény biztonsági szempontból megfelelő szintű védelmet tud nyújtani meghatározott biztonsági minősítésű szintű EU-minősített adatoknak;

h) EU-minősített adat „kezelése”: minden olyan lehetséges tevékenység, amelynek az EU-minősített adat az életciklusa során ki lehet téve: az adat előállítása, nyilvántartásba vétele, feldolgozása, szállítása, visszaminősítése, a rá vonatkozó minősítés feloldása és az adat megsemmisítése. A kommunikációs és információs rendszerek (CIS) vonatkozásában kezelésnek minősül ezen felül az adatok gyűjtése, megjelenítése, átadása és tárolása;

i) „birtokos”: olyan, megfelelő engedéllyel rendelkező, a szükséges ismeret feltételének eleget tévő személy, aki minősített adat birtokában van, és ezért felel annak védelméért;

j) „információbiztonsági hatóság”: a Számvevőszék információbiztonsági tisztviselője, aki részben vagy egészben átruházhatja az e határozatban előírt feladatokat;

k) „adat”: minden írásban vagy szóban tett tájékoztatás, adathordozótól és megfogalmazótól függetlenül;

l) „anyag”: bármely közvetítő eszköz, adathordozó, illetve bármely gép vagy berendezés;

m) „kibocsátó”: bármely uniós intézmény, ügynökség vagy szerv, tagállam, harmadik állam vagy nemzetközi szervezet, amelynek fennhatósága alatt minősített adatokat hoztak létre, illetve vittek be uniós struktúrákba;

n) „személyi biztonsági tanúsítvány”: a valamely tagállam illetékes hatóságai által elvégzett biztonsági ellenőrzést követően a tagállam valamely illetékes hatósága által tett nyilatkozat, amely tanúsítja, hogy egy adott személy részére – feltéve, hogy az esetében meghatározták a „szükséges ismeretet”, és megfelelő tájékoztatást kapott az ezzel kapcsolatos felelősségéről – meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig és meghatározott időpontig hozzáférés biztosítható EU-minősített adatokhoz;

o) „személyi biztonsági tanúsítványról szóló igazolás”: a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatója által kiadott igazolás, amely megállapítja, hogy egy személy érvényes biztonsági tanúsítvánnyal vagy biztonsági engedéllyel rendelkezik, és megadja, hogy ez a személy milyen szintű EU-minősített adatokhoz férhet hozzá (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint a vonatkozó biztonsági tanúsítvány vagy engedély érvényességi idejét és az igazolás lejártának időpontját;

p) „fizikai biztonságért felelős hatóság”: a Számvevőszék biztonsági vezetője, aki felelős az EU-minősített adatok védelméhez szükséges fizikai biztonsági intézkedések és eljárások végrehajtásáért;

q) „nyilvántartási hivatal”: a Számvevőszék titkárságának igazgatása alá tartozik, és a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatójának felelősségi körébe tartozó igazgatási területen található. A hivatal felelős a Számvevőszékkel kicserélt RESTREINT UE/EU RESTRICTED adatok vagy azokkal egyenértékű adatok beérkezéséért és kiküldéséért;

r) „Nyilvántartó az EU-minősített adatok részére”: a biztonsági területen belül kialakított terület. Ezt a nyilvántartót a Számvevőszék biztonsági ellenőrzésen átesett és engedéllyel rendelkező, nyilvántartó hivatalt ellenőrző tisztviselője irányítja. A nyilvántartó felelős a Számvevőszékkel kicserélt CONFIDENTIEL UE/EU CONFIDENTIAL adatok vagy azoknál magasabb minősítésű adatok beérkezéséért és kiküldéséért;

s) „Biztonsági Akkreditációs Hatóság”: a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatója.

3. cikk Az EU-minősített adatok védelmére szolgáló intézkedések

1) A Számvevőszék a számára átadott valamennyi minősített adat védelmét a kibocsátó által meghatározott minősítési szintnek megfelelő módon és e határozattal összhangban biztosítja.

2) E célból a Számvevőszék az EU-minősített adatok kezelését fizikai és adott esetben személyi biztonsági intézkedésekhez köti, beleértve az azonosított személyek hozzáférési engedélyét, valamint a kommunikációs és információs rendszerek védelmét szolgáló intézkedéseket. Ezeket az intézkedéseket a 4–6. cikk ismerteti, és azokat az EU-minősített adatok teljes életciklusa során alkalmazni kell. Ezeknek arányosnak kell lenniük az EU-minősített adatok biztonsági minősítésével, az adatok, illetve anyag formájával és mennyiségével, azon létesítmények helyével és felépítésével, ahol az EU-minősített adatokat tárolják, valamint a szándékos károkozás miatt és/vagy bűncselekményekből – a kémkedést, a szabotázst és a terrorizmust is ideértve – eredően helyi szinten fennálló fenyegetéssel.

3) 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.

4) Az EU-minősített adatok csak olyan személyeknek adhatók át, akiknek az intézményen belül ezeket ismerniük kell. Az EU-minősített adatok birtokosa köteles azokat az e határozatban előírtak szerint védeni.

5) EU-minősített adatok nem hozhatók nyilvánosságra sem szóban, sem írásban. A Számvevőszék előzetes észrevételei, jelentései, véleményei, sajtóközleményei és egyéb termékei, honlapja és intranete, szóbeli felszólalásai, a dokumentumokhoz való hozzáférés iránti kérelmekre adott válaszai[3], valamint hang- és videofelvételei nem tartalmazhatnak EU-minősített adatot vagy annak kivonatát, és nem hivatkozhatnak rá. Ha azonban a kibocsátó olyan dokumentumokat vagy információkat tett közzé, amelyek hivatkoznak EU-minősített adatokra, akkor ez a hivatkozás megemlíthető.

6) Az (5) bekezdéstől eltérve a Számvevőszék és a kibocsátó megállapodhatnak abban, hogy egy konkrét ellenőrzés kapcsán a Számvevőszék az EU-minősített adatok elemeit sokszorosíthatja vagy felhasználhatja egy dokumentumban. Ebben az esetben az említett számvevőszéki dokumentumot az egyeztető eljárást megelőzően vagy annak során először a szóban forgó EU-minősített adat kibocsátója részére kell megküldeni. Ebben a helyzetben a Számvevőszék és a kibocsátó megállapodnak abban, hogy a Számvevőszék által kiadott dokumentumot minősíteni kell-e. Amennyiben a jelentésért felelős számvevőszéki tag szükségesnek tartja, hogy – az e határozathoz kapcsolódó valamennyi biztonsági intézkedés figyelembevételével – egy részben vagy egészben minősített ellenőrzési jelentést megküldjön bizonyos címzetteknek az Európai Parlamentnél vagy a Tanácsnál, ehhez a minősített adat kibocsátójának

[3] Az Európai Számvevőszéknek a 14/2009. számú határozattal (HL C 67., 2009.3.20., 1. o.) módosított, a Számvevőszék dokumentumaihoz való nyilvános hozzáférésről szóló 12/2005. számú határozata alapján.

hozzájárulása szükséges. Az ilyen dokumentumok cseréjére vonatkozó jogi keretet és eljárást a 7. cikk határozza meg.

7) Amennyiben megbízatásának gyakorlása egy minősített dokumentum vagy adat bizonyos elemeinek szélesebb körű megosztását teszi szükségessé, a Számvevőszék – a biztonsági minősítési jelölés megfelelő figyelembevételével – konzultál a kibocsátóval, mielőtt döntést hozna ezen elemek vagy adatok felhasználásáról, ha úgy ítéli meg, hogy ehhez nyomós közérdek fűződik. Az adatokat a jelentésben csak úgy szabad felhasználni, hogy a kibocsátó érdekei ne sérüljenek. Ezt oly módon lehetne megfelelően biztosítani, hogy a kibocsátót felkérik észrevételek megtételére az információk anonimizálásának, tömörítésének, általánosításának stb. módjára nézve egy megállapodás elérése érdekében, tiszteletben tartva ugyanakkor a közzétett adatok által elsődlegesen érintettek érdekeit.

8) A Számvevőszék a kibocsátóval folytatott előzetes konzultáció és annak kifejezett írásbeli hozzájárulása nélkül nem ad át az EU-minősített adatot más uniós intézménynek, ügynökségnek, szervnek vagy hivatalnak, tagállamnak, harmadik államnak vagy nemzetközi szervezetnek.

9) Amennyiben a SECRET UE / EU SECRET vagy annál alacsonyabb minősítésű dokumentum kibocsátója nem korlátozta a dokumentum sokszorosítását vagy lefordítását, az ilyen dokumentumok a birtokos kérésére és a Számvevőszék információbiztonsági hatóságának gyakorlati munkautasításaival összhangban sokszorosíthatók vagy lefordíthatók. Az eredeti dokumentumra vonatkozó biztonsági intézkedéseket a másolatokra és a fordításokra is alkalmazni kell.

10) Ha a Számvevőszéknek szüksége van arra, hogy a hozzá érkezett minősített dokumentumot, vagy amelyhez hozzáférési engedélyt kapott, visszaminősítsék vagy a minősítését feloldják, a Számvevőszék megkérdezi a kibocsátót, hogy az rendelkezésre tudja-e bocsátani a dokumentum visszaminősített vagy feloldott minősítésű változatát.

4. cikk Személyi biztonság

1) A Számvevőszék tagjai feladatkörüknél fogva jogosultak hozzáférni valamennyi EU-minősített adathoz, és részt vehetnek olyan üléseken, ahol EU-minősített adatokat kezelnek. A tagokat tájékoztatni kell az EU-minősített adatok védelmével kapcsolatos biztonsági kötelezettségeikről, és nekik írásban el kell ismerniük az ilyen információk védelmével kapcsolatos felelősségüket.

2) A Számvevőszék alkalmazottai – legyenek tisztviselők, az egyéb alkalmazottakra vonatkozó alkalmazási feltételek hatálya alá tartozó alkalmazottak vagy kirendelt nemzeti szakértők – csak azután kaphatnak hozzáférést EU-minősített adatokhoz, miután:

   i. megállapítást nyert, hogy a „szükséges ismeret” feltétele teljesül;

   ii. tájékoztatást kaptak az EU-minősített adatok védelmére szolgáló biztonsági szabályokról és a vonatkozó biztonsági szabványokról és útmutatókról, és írásban elismerték az ilyen adatok védelmével kapcsolatos felelősségüket;

   iii. a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatok esetében biztonsági ellenőrzésen estek át, és engedélyt kaptak a hozzáférésre.

3) A 10. cikk (10) bekezdésével összhangban hozott, felhatalmazáson alapuló határozatban kell meghatározni azt az eljárást, amely alapján eldönthető, hogy a tisztviselő vagy a Számvevőszék személyzetének más tagja számára engedélyezhető-e a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű információkhoz való hozzáférés, figyelembe véve a személy

lojalitását, integritását és megbízhatóságát, és miután a 2. cikk n) pontjában említettek szerint megszerezte a tagállam illetékes hatóságainak jóváhagyását. A hozzáférési engedélyt megadó határozatot a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatója hozza meg.

4) A Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatója személyi biztonsági tanúsítványról szóló igazolásokat adhat ki, amelyek meghatározzák azt a minősítési szintet, amely tekintetében a személyek hozzáférést kaphatnak EU-minősített adatokhoz (CONFIDENTIEL UE / EU CONFIDENTIAL vagy annál magasabb minősítés), továbbá a megfelelő hozzáférési engedély érvényességi idejét és a személyi biztonsági tanúsítványról szóló igazolás lejárati dátumát.

5) Csak a fenti (2) bekezdés iii. pontjában említett engedéllyel rendelkező személyek és a fenti (1) bekezdés értelmében a Számvevőszék tagjai vehetnek részt olyan üléseken, amelyeken CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatokat kezelnek. A Számvevőszék és a kibocsátó eseti alapon gondoskodik az ilyen ülések gyakorlati lebonyolításáról.

6) A Számvevőszék olyan ülések szervezéséért felelős szervezeti egységei, ahol CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatokat kezelnek, időben tájékoztatják az információbiztonsági hatóságot az ülések időpontjáról és helyszínéről, és ismertetik vele a résztvevők listáját.

7) Minden olyan személynek, aki nem rendelkezik megfelelő engedéllyel, illetve nem bizonyított, hogy szükséges ismernie az EU-minősített adatokat, a lehető leghamarabb jelentenie kell a helyzetet az információbiztonsági hatóságnak, és gondoskodnia kell az EU-minősített adatok e határozatban megkövetelt védelméről.

5. cikk A minősített adatok védelmét szolgáló fizikai biztonsági intézkedések

1) A fizikai biztonság az EU-minősített adatokhoz való illetéktelen hozzáférés megakadályozását célzó fizikai és technikai védelmi intézkedések alkalmazását jelenti.

2) A fizikai biztonsági intézkedések célja jogosulatlan személyek titokban történő vagy erőszakos behatolásának a megakadályozása, jogosulatlan cselekményektől való elrettentés, azok megakadályozása és észlelése, valamint az alkalmazottak megkülönböztetése az EU-minősített adatokhoz való hozzáférés tekintetében, a szükséges ismeret elve alapján. Ezeket az intézkedéseket kockázatkezelési eljárás alapján, e határozattal összhangban kell meghatározni.

3) A Számvevőszék illetékes biztonsági hatóságának rendszeresen ellenőriznie kell azokat a területeket, ahol EU-minősített adatokat kezelnek vagy tárolnak.

4) Az EU-minősített adatok kezelésére és tárolására kizárólag olyan berendezések vagy eszközök használhatók, amelyek megfelelnek az uniós intézményekben, ügynökségekben vagy szervekben az EU-minősített adatok védelmére vonatkozó szabályoknak.

5) A Számvevőszék alkalmazottai a Számvevőszék létesítményein kívüli biztonsági területeken is hozzáférhetnek a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű vagy azzal egyenértékű EU-minősített adatokhoz.

6) A Számvevőszék szolgáltatásszint-megállapodást köthet valamely másik luxembourgi uniós intézménnyel annak érdekében, hogy a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatokat az adott intézmény biztonsági területén kezelhesse és

tárolhassa. A kibocsátó kifejezett beleegyezése nélkül az ilyen EU-minősített adatot nem lehet a Számvevőszék létesítményeiben kezelni vagy tárolni, és a Számvevőszék nem sokszorosíthatja vagy fordíthatja le azokat.

7) A kapott RESTREINT UE/EU RESTRICTED minősítésű adatokat a Számvevőszék nyilvántartásba veszi. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű vagy azzal egyenértékű adatoknak a Számvevőszék létesítményein kívül történő megtekintését biztonsági okokból nyilvántartásba kell venni.

8) A RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatot megfelelően zárható irodabútorokban lehet tárolni az igazgatási területen vagy a biztonsági területen. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű EU-minősített adatokat egy szolgáltatásszint-megállapodás értelmében egy másik luxembourgi uniós intézmény biztonsági területén lévő biztonsági konténerben kell tárolni.

9) A nyilvántartó hivatalon kívül az EU-minősített adatokat a következőképpen kell átadni a szervezeti egységek és létesítmények között:

   a) az EU-minősített adatokat – főszabályként – a 6. cikk (8) bekezdésével összhangban jóváhagyott, kriptográfiai termékekkel védett elektronikus úton továbbítják;

   b) ha nem az a) pont szerint továbbítják, akkor az EU-minősített adatokat a 6. cikk (8) bekezdésével összhangban jóváhagyott, kriptográfiai termékekkel védett adathordozón (USB, CD, merevlemez) vagy papíralapon, nem átlátszó lezárt borítékban kell továbbítani.

10) A RESTREINT UE/EU RESTRICED minősítésű adatokat a birtokos a Számvevőszékben alkalmazandó archiválási szabályok szerint megsemmisítheti. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű információkat a nyilvántartó hivatalt ellenőrző tisztviselő csak akkor semmisíti meg, ha a birtokos vagy egy illetékes hatóság a Számvevőszéknél alkalmazandó archiválási szabályokkal összhangban erre utasítást ad. A SECRET UE/EU SECRET minősítésű dokumentumokat legalább a megsemmisítendő dokumentum minősítési szintjének megfelelő biztonsági tanúsítvánnyal rendelkező tanú jelenlétében kell megsemmisíteni. A nyilvántartó hivatalt ellenőrző tisztviselő és a tanú, amennyiben tanú jelenléte szükséges, aláírja a megsemmisítésről szóló jegyzőkönyvet, amelyet a nyilvántartásban iktatnak. A nyilvántartó hivatalt ellenőrző tisztviselő legalább öt évig megőrzi a nyilvántartást a CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok megsemmisítéséről.

11) A fizikai biztonságért felelős hatóság és az információbiztonsági hatóság a helyi körülmények figyelembevételével közös tervet készít az EU-minősített adatok válsághelyzetben történő védelmére, beleértve szükség szerint az információk veszélyhelyzet esetén történő megsemmisítésére vagy evakuálására vonatkozó terveket is. A két hatóság adott esetben az általa megfelelőnek ítélt utasítások kiadásával akadályozza meg,hogy az EU-minősített adatok illetéktelen személyek kezébe kerüljenek.

12) Amennyiben az EU-minősített adatot fizikailag kell szállítani, a Számvevőszék betartja a kibocsátó által előírt, a szállítás során az engedély nélküli hozzáférhetővé tétellel szembeni védelemre vonatkozó intézkedéseket.

13) A melléklet tartalmazza a fizikai biztonsági intézkedéseket arra az esetre, ha RESTREINT UE/EU RESTRICTED minősítésű adatokat igazgatási területeken kezelnek és tárolnak.

6. cikk Az EU-minősített adatok védelme a kommunikációs és információs rendszerekben

1) E cikk alkalmazásában „kommunikációs és információs rendszer” minden olyan rendszer, amely lehetővé teszi az EU-minősített adatok elektronikus formában történő kezelését.

A kommunikációs és információs rendszer magában foglalja a működéséhez szükséges valamennyi eszközt, beleértve az infrastruktúrát, a szervezetet, a személyzetet és az információs forrásokat.

2) „Jogszerű felhasználó” az a számvevőszéki tag, tisztviselő, egyéb alkalmazott vagy kirendelt nemzeti szakértő, akinek megalapozott és elismert szüksége van egy adott információs rendszerhez való hozzáférésre.

3) A Számvevőszék biztosítékot nyújt arra, hogy rendszerei megfelelő mértékben védik az általuk kezelt információkat, és a jogszerű felhasználók ellenőrzése mellett akkor és úgy működnek, ahogyan és amikor kell. Ennek érdekében garantálják a megfelelő szintű:

- hitelességet: annak garanciáját, hogy az információ valódi és jóhiszemű forrásokból származik;
- rendelkezésre állást: az engedéllyel rendelkező szervezet kérelemére megvalósuló hozzáférhetőséget és felhasználhatóságot;
- bizalmas jelleget: annak garanciáját, hogy az információ nem hozzáférhető illetéktelen személy, szervezet vagy folyamat részére;
- sértetlenséget: az eszközök és információk pontosságának és teljességének védettségét;
- letagadhatatlanságot: egy cselekmény vagy esemény megtörténtének bizonyíthatóságát annak érdekében, hogy ezt az eseményt vagy cselekményt később ne lehessen letagadni.

Ez a biztosíték egy kockázatkezelési eljáráson alapul. A „kockázat” annak valószínűsége, hogy egy adott fenyegetés kihasználja valamely szervezet vagy az általa használt rendszerek bármelyikének belső, illetve külső sebezhetőségét, és ezáltal kárt okoz az adott szervezetnek, illetve kárt tesz annak tárgyi eszközeiben vagy immateriális javaiban. Mérőszáma a fenyegetések bekövetkezése valószínűségének, illetve hatásának kombinációja. A kockázatkezelési eljárás a következő lépésekből áll: a fenyegetések és sebezhetőségek azonosítása, kockázatértékelés, kockázatkezelés, kockázatelfogadás és kockázatkommunikáció.

- A „kockázatértékelés” a fenyegetések és sebezhetőségek azonosításából, valamint a kapcsolódó kockázatelemzésből, azaz a valószínűség és a hatás értékeléséből áll.
- A „kockázatkezelés” a kockázat (megfelelő technikai, fizikai, szervezeti vagy eljárási intézkedések kombinálásával történő) enyhítése, megszüntetése, csökkentése, illetve annak átruházása vagy figyelemmel kísérése.
- A „kockázatelfogadás” az azt elfogadó döntés,hogy a kockázatkezelést követően továbbra is létezik fennmaradó kockázat.
- A „fennmaradó kockázat” a biztonsági intézkedések végrehajtását követően is fennálló kockázat, tekintve, hogy nem lehet minden fenyegetést elhárítani és minden sebezhetőséget megszüntetni.
- A „kockázatkommunikáció” a kommunikációs és információs rendszer felhasználói közösségei körében a kockázatokkal kapcsolatos tudatosság növelése, a jóváhagyó hatóságok tájékoztatása a kockázatokról és jelentéstétel azokról a működtető hatóságok részére.

4) Az EU-minősített adatok kezelésére használt valamennyi elektronikus eszköznek és berendezésnek meg kell felelnie az EU-minősített adatok védelmére vonatkozó szabályoknak. Előnyben részesülnek azok az elektronikus eszközök és berendezések, amelyeket egy másik uniós intézmény, ügynökség vagy szerv már akkreditált. Az eszközök biztonságosságát azok teljes életciklusa alatt garantálni kell.

5) A Számvevőszéknek az EU-minősített adatok kezelésére szolgáló kommunikációs és információs rendszerét egy megfelelő hatóság akkreditálja. E célból a Számvevőszék szolgáltatásszint-megállapodásra törekszik egy olyan uniós intézmény biztonsági akkreditációs hatóságával, amely képes akkreditálni az EU-minősített adatokat kezelő kommunikációs és

információs rendszert, hogy az akkreditációs nyilatkozatot adjon a Számvevőszék kommunikációs és információs rendszerében kezelhető RESTREINT UE/EU RESTRICTED minősítésű információkról, valamint a működés megfelelő feltételeiről. A szolgáltatásszint-megállapodás az akkreditációs eljárás során alkalmazandó szabványokra is hivatkozik, és azt a 10. cikk (3) bekezdésében meghatározott eljárással összhangban kell megkötni.

6) Amennyiben a Számvevőszéknek saját akkreditációs eljárást kell kialakítania a kommunikációs és információs rendszere számára, az e határozat 10. cikkének (10) bekezdésében említett, felhatalmazáson alapuló határozat állapítja meg az eljárást azon szabványokkal összhangban, amelyek az EU más intézményeiben, ügynökségeiben és szerveiben az EU-minősített adatokat kezelő kommunikációs és információs rendszer akkreditációs eljárására vonatkoznak.

7) Az akkreditációs akták és dokumentáció elkészítése az alkalmazandó szabványoknak megfelelően teljes mértékben a kommunikációs és információs rendszer tulajdonosának feladata.

8) Amennyiben az EU-minősített adatokat kriptográfiai termékekkel védik, a Számvevőszék előnyben részesíti a Tanács vagy a Tanács főtitkára által kriptográfiai jóváhagyó hatóságként jóváhagyott termékeket, vagy ilyen híján a más uniós intézmények, ügynökségek és szervek által az EU-minősített adatok védelmére jóváhagyott termékeket.

9) A RESTREINT UE/EU RESTRICTED minősítésű információkat csak olyan elektronikus eszközökön (például munkaállomásokon, nyomtatókon, fénymásolókon) lehet kezelni, amelyek az igazgatási területen vagy a biztonsági területen találhatók. A RESTREINT UE/EU RESTRICTED minősítésű információkat kezelő elektronikus eszközöket el kell különíteni más számítógépes hálózatoktól, és megfelelő fizikai vagy technikai intézkedésekkel kell védeni.

10) Az EU-minősített adatokat kezelő kommunikációs és információs rendszer tervezésében, fejlesztésében, vizsgálatában, üzemeltetésében, irányításában vagy használatában részt vevő minden számvevőszéki alkalmazott minden olyan potenciális biztonsági hiányosságról, incidensről, a biztonság megsértéséről, illetve az adatok illetéktelen tudomására jutásáról értesíti az információbiztonsági tisztviselőt, amely a kommunikációs és információs rendszer, illetve az abban foglalt EU-minősített adatok védelmére hatással lehet.

7. cikk A minősített adatok cseréjére és az ilyen adatokhoz való hozzáférés lehetővé tételére irányuló eljárás

1) Amennyiben a Szerződések vagy a Szerződések alapján elfogadott jogi aktusok erre kötelezik őket, az uniós intézmények, ügynökségek, szervek és hivatalok, valamint a nemzeti hatóságok saját kezdeményezésükre vagy az elnök, a jelentést készítő tag(ok) vagy a főtitkár írásbeli kérésére az alábbi eljárás szerint hozzáférést biztosítanak a Számvevőszék számára az EU-minősített adatokhoz.

2) A hozzáférési kérelmeket a Számvevőszék nyilvántartási hivatalán keresztül kell megküldeni az érintett intézményeknek.

3) Szükség esetén a Számvevőszék igazgatási megállapodást köt az EU-minősített adatok vagy azzal egyenértékű információk cseréjének gyakorlati vonatkozásairól.

4) Az ilyen igazgatási megállapodások megkötése céljából a Számvevőszék minden szükséges információt megad a kibocsátónak az információbiztonsági rendszeréről. Szükség esetén értékelő látogatás szervezhető.

5) Ezeket az igazgatási megállapodásokat az Európai Unióról szóló szerződés 13. cikkében meghatározott hatáskör-átruházás és lojális együttműködés elvével teljes összhangban kell megkötni. A megállapodásokat a 10. cikk (4) bekezdésében megállapított eljárásnak megfelelően kell megkötni.

6) Amennyiben egy adott uniós intézménnyel, szervvel vagy ügynökséggel, harmadik állammal vagy nemzetközi szervezettel nem kötöttek igazgatási megállapodást a minősített információknak a Számvevőszék részére történő átadásáról, a Számvevőszék a kapott minősített információk védelmére vonatkozó kötelezettségvállalási nyilatkozatot ír alá.

8. cikk A biztonsági szabályok megsértése, a minősített adatok elvesztése vagy illetéktelen tudomására jutása

1) A biztonsági szabályok megsértése bármely olyan cselekmény vagy mulasztás, amely az e határozatban foglalt biztonsági szabályokkal és azok végrehajtási szabályaival ellentétes.

2) Az illetéktelen tudomására jutás akkor következik be, ha a biztonsági szabályok megsértésének következtében adatok részben vagy egészben ismertté válnak illetéktelen személyek előtt.

3) A biztonsági szabályok megsértését vagy feltételezett megsértését minden esetben haladéktalanul jelenteni kell a Számvevőszék információbiztonsági hatóságának.

4) Amennyiben ismert, vagy alapos okkal gyanítható, hogy EU-minősített adatok illetéktelen személy tudomására jutottak vagy elvesztek, az információbiztonsági hatóság tájékoztatja a humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatót és a Számvevőszék főtitkárát. A humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgató haladéktalanul tájékoztatja a kibocsátó megfelelő biztonsági hatóságát. A Számvevőszék fent említett igazgatója vizsgálatot folytat le, és tájékoztatja a Számvevőszék főtitkárát és a kezdeményező biztonsági hatóságát az eredményekről, valamint a helyzet megismétlődésének megakadályozása érdekében hozott intézkedésekről. A Számvevőszék valamely tagjának érintettsége esetén a Számvevőszék elnöke felelős azért, hogy a Számvevőszék főtitkárával együttműködve intézkedjen.

5) A Számvevőszék bármely tisztviselője vagy egyéb alkalmazottja, aki felelős az e határozatban és annak végrehajtási szabályaiban megállapított biztonsági szabályok megsértéséért, az Európai Unió személyzeti szabályzatában és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben előírt szankciókkal sújtható.

6) A Számvevőszék azon tagja, aki nem tartja be e határozat rendelkezéseit, a Szerződés 286. cikkének (6) bekezdésében előírt intézkedésekkel és szankciókkal sújtható.

7) Az EU-minősített adatok elvesztéséért vagy illetéktelen tudomására jutásáért felelős személy a vonatkozó jogszabályok és rendeletek szerint fegyelmi, illetve jogi eljárás alá vonható.

9. cikk Biztonság külső beavatkozás esetén

1) A Számvevőszék az EU-minősített adatokhoz való hozzáféréssel járó vagy azokhoz való hozzáférést igénylő feladatok elvégzésével – szerződésük alapján – valamely uniós tagállamban bejegyzett vállalkozókat bízhat meg. Ez különösen a kommunikációs és információs rendszerek, valamint a számítógépes hálózat karbantartásával kapcsolatban fordulhat elő.

2) Külső beavatkozás esetén a Számvevőszék meghozza az e cikk (3) bekezdésében említett valamennyi szükséges biztonsági intézkedést, beleértve a telephely-biztonsági tanúsítvány

bekérését is annak biztosítása érdekében, hogy a jelöltek és az ajánlattevők az ajánlattételi és beszerzési eljárás teljes időtartama alatt, illetve a vállalkozók és alvállalkozók a szerződés teljes időtartama alatt védjék az EU-minősített adatokat. Az ajánlatkérő szerv gondoskodik arról, hogy a szerződésekben megemlítsék az e határozatban megállapított biztonsági minimumszabályokat, hogy kötelezzék a vállalkozókat azok betartására.

3) Az EU-minősített adatokhoz való hozzáféréssel járó szerződésekre és alvállalkozói szerződésekre, szerződési hirdetményekre, telephely-biztonsági tanúsítvány használatát előíró körülményekre vonatkozó iránymutatásra, program vagy projektbiztonsági utasításokra, a biztonsági vonatkozások záradékára, a látogatásokra, az EU-minősített adatok ilyen szerződések és alvállalkozói szerződések alapján történő továbbítására és szállítására vonatkozó biztonsági szabályoknak, beszerzési eljárásoknak, sablonoknak és mintáknak meg kell felelniük az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2015. március 13-i (EU, Euratom) 2015/444 bizottsági határozatban az Európai Bizottság által a minősített szerződésekre megállapított szabályoknak, sablonoknak és mintáknak.

<u>10. cikk</u> A határozat végrehajtása és az ahhoz kapcsolódó felelősségi körök

1) A Számvevőszék szervezeti egységei a felelősségi körükben minden szükséges intézkedést megtesznek azért, hogy az EU-minősített adatok és minden más minősített adat kezelésekor vagy tárolásakor ezen határozat és a vonatkozó végrehajtási szabályok alkalmazásra kerüljenek.

2) A főtitkár a kinevezésre jogosult hatóság és a munkaszerződések megkötésére jogosult hatóság az összes tisztviselő és egyéb alkalmazott tekintetében. A főtitkár a humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatóra ruházhatja a tisztviselők és más alkalmazottak CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatokhoz való hozzáférési engedélyének megadásával, a Biztonsági Akkreditációs Hatóságként ellátott feladatainak elvégzésével, valamint a Számvevőszék titkársága felett az EU-minősített adatok kezelése tekintetében gyakorolt felügyelettel kapcsolatos felelősségét.

3) A főtitkár hatáskörébe tartozik a szolgáltatásiszint-megállapodások megkötése a Számvevőszék kommunikációs és információs eszközeinek és rendszereinek akkreditációjáról, egy másik uniós intézményben lévő biztonsági terület használatáról, valamint az EU-minősített adatokhoz való hozzáféréssel kapcsolatos személyi biztonsági tanúsítványok kérelmezési eljárásáról.

4) A humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgató illetékes abban, hogy az uniós intézményekkel, ügynökségekkel és egyéb szervekkel olyan igazgatási megállapodásokat kössön az EU-minősített adatok cseréjére vonatkozóan, amelyekre a Számvevőszéknek megbízatása teljesítéséhez szüksége van. Az igazgató harmadik államokkal vagy nemzetközi szervezetekkel is igazgatási megállapodásokat köthet a kapott minősített információk védelméről.

5) A humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgató jogosult aláírni minden olyan kötelezettségvállalási nyilatkozatot, amely a rendkívüli *ad hoc* átadás keretében szolgáltatott EU-minősített adatok védelmére vonatkozik.

6) A Számvevőszék információbiztonsági tisztviselője információbiztonsági hatóságként jár el. Az információbiztonsági tisztviselőnek és azoknak a személyeknek, akikre feladatai egy részét vagy egészét átruházza, megfelelő biztonsági tanúsítvánnyal kell rendelkezniük. Az információbiztonsági hatóság a humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatósággal, az információkért, munkahelyért és innovációért felelős igazgatósággal és az ellenőrzés-minőségi bizottság igazgatóságával szoros

együttműködésben látja el feladatait (lásd különösen: 4., 6. és 8. cikk). Az információbiztonsági hatóság felelős továbbá az információbiztonsággal kapcsolatos képzésekért és tájékoztató ülésekért, valamint az e határozatnak való megfelelés időszakos ellenőrzéséért, beleértve a külső beavatkozás esetét és a megfelelés biztosítása érdekében meghozandó intézkedéseket is.

7) A biztonsági vezető felelős a fizikai biztonsági intézkedésekért (különösen az 5. cikk).

8) A Számvevőszék titkárságán létrehozott nyilvántartási hivatal a RESTREINT UE/EU RESTRICTED minősítésű adatok beérkezési és kiküldési helye, amelyeket a Számvevőszék más uniós intézményekkel, ügynökségekkel és szervekkel, valamint a tagállamokkal cserélhet ki. A harmadik országok és nemzetközi szervezetek ezzel egyenértékű adatainak beérkezési és kiküldési helyeként is szolgál. A nyilvántartási hivatal szervezeti felépítését egy felhatalmazáson alapuló határozatban határozzák meg. A nyilvántartási hivatal vezetőjének fő feladatai:

   a) a RESTREINT UE/EU RESTRICTED minősítésű információk beérkezésének és kiküldésének nyilvántartásba vétele;

   b) a RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatok nyilvántartására, kezelésére, tárolására és megtekintésére szolgáló elkülönített igazgatási területek kezelése.

9) Egy másik uniós intézményben lévő biztonsági terület használatáról szóló, szolgáltatásiszint-megállapodás keretében egy nyilvántartást kell létrehozni. Ez a Számvevőszék titkárságán a Számvevőszék humán erőforrásokért, pénzügyekért és általános szolgáltatásokért felelős igazgatójának felelősségi körében létrehozott nyilvántartás a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatok beérkezési és kiküldési helye, amely adatokat a Számvevőszék más uniós intézményekkel, ügynökségekkel és szervekkel, valamint a tagállamokkal cserélhet ki. A harmadik országok és nemzetközi szervezetek ezzel egyenértékű adatainak beérkezési és kiküldési helyeként is szolgál. Megfelelő széfekkel és egyéb biztonsági berendezésekkel kell felszerelni, amelyek alkalmasak a CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű adatok védelmére. A nyilvántartás szervezeti felépítését egy felhatalmazáson alapuló határozatban határozzák meg. A nyilvántartást ellenőrző tisztviselőnek megfelelő biztonsági tanúsítvánnyal kell rendelkeznie, és a következő fő feladatokat kell ellátnia:

   a) az EU-minősített adatok nyilvántartásával, megtekintésével, megőrzésével, sokszorosításával, fordításával, továbbításával, küldésével és adott esetben megsemmisítésével kapcsolatos műveletek irányítása;

   b) az EU-minősített adatok védelmével összefüggő, felhatalmazáson alapuló határozatban meghatározott egyéb feladatok ellátása.

10) Az igazgatási bizottság felhatalmazáson alapuló határozatot fogad el e határozat végrehajtási szabályainak megállapításáról. Az információbiztonsági tisztviselő meghatározza az információbiztonsági iránymutatásokat. Az ellenőrzés-minőségi bizottság ellenőrzési iránymutatásokat dolgoz ki.

<u>11. cikk</u> Hatálybalépés

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

Kelt Luxembourgban, 2021. június 3-án.

A Számvevőszék nevében

Klaus-Heiner Lehne
elnök

Melléklet: AZ EU-MINŐSÍTETT ADATOKRA VONATKOZÓ IGAZGATÁSI TERÜLETEKKEL KAPCSOLATOS FIZIKAI BIZTONSÁGI INTÉZKEDÉSEK

MELLÉKLET

AZ EU-MINŐSÍTETT ADATOKRA VONATKOZÓ IGAZGATÁSI TERÜLETEKKEL KAPCSOLATOS FIZIKAI BIZTONSÁGI INTÉZKEDÉSEK

1) Ez a melléklet a határozat 5. cikkének végrehajtására vonatkozó szabályokat tartalmazza. Ezek a minimumszabályok a Számvevőszéken belül a RESTREINT UE/EU RESTRICTED minősítésű adatokat érintő igazgatási területek fizikai védelmére vonatkoznak: ezek a RESTREINT UE/EU RESTRICTED minősítésű adatok rögzítésére, tárolására és megtekintésére kijelölt területek.

2) Az igazgatási területeken a fizikai biztonsági intézkedések célja, hogy az alábbiak szerint megakadályozzák az illetéktelen hozzáférést ezekhez a területekhez:

   a) láthatóan elhatárolt körzetet kell meghatározni, amely lehetővé teszi a személyi ellenőrzést;

   b) a kíséret nélküli belépést csak a Számvevőszék információbiztonsági hatósága vagy más illetékes hatóság megfelelő engedélyével rendelkező személyek számára lehet engedélyezni;

   c) minden más személy mellé folyamatos kíséretet kell adni vagy ezzel egyenértékű ellenőrzést kell biztosítani.

3) A Számvevőszék információbiztonsági hatósága kivételesen hozzáférést adhat engedéllyel nem rendelkező személyek számára, többek között az igazgatási területen végzett munka céljából, feltéve, hogy ez nem jár együtt az EU-minősített adatokhoz való hozzáféréssel, amelyeknek elzárva kell maradniuk. Ezek a személyek csak az információbiztonsági hatóság vagy a nyilvántartó hivatalt ellenőrző tisztviselő kíséretében és folyamatos felügyelete mellett léphetnek be.

4) Az információbiztonsági hatóság meghatározza az összes igazgatási terület és biztonságos bútor kulcsainak, illetve kombinációinak kezelésére vonatkozó eljárásokat. Ezen eljárások célja a jogosulatlan hozzáférés elleni védelem.

5) A kombinációkat kívülről meg kell tanulnia annak a lehető legkisebb számú egyénnek, akinek azokat ismernie kell. A RESTREINT UE/EU RESTRICTED minősítésű adatok tárolására szolgáló biztonságos bútorok kombinációit az alábbi esetekben meg kell változtatni:

   - új biztonságos bútor átvételekor;
   - a kombinációt ismerő személyzet minden változásakor;
   - ha a kombinációk illetéktelen tudomására jutottak vagy ennek gyanúja merült fel;
   - ha a záron karbantartást vagy javítást végeztek;
   - legalább 12 havonta.

6) E szabályok betartásáért az információbiztonsági hatóság és a biztonsági vezető felelős.