

II

(Nem jogalkotási aktusok)

HATÁROZATOK

A TANÁCS HATÁROZATA

(2013. szeptember 23.)

az EU-minősített adatok védelmét szolgáló biztonsági szabályokról

(2013/488/EU)

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 240. cikke (3) bekezdésére,

tekintettel a Tanács eljárási szabályzatának elfogadásáról szóló, 2009. december 1-ji 2009/937/EU tanácsi határozatra ⁽¹⁾ és különösen annak 24. cikkére,

mivel:

- (1) A Tanács tevékenységének a minősített adatok kezelését igénylő valamennyi területen történő továbbfejlesztése érdekében helyénvaló egy olyan átfogó biztonsági rendszert létrehozni a minősített adatok védelmére, amely kiterjed a Tanácsra, annak Főtitkárságára és a tagállamokra.
- (2) E határozat abban az esetben alkalmazandó, amikor a Tanács, annak előkészítő szervei és a Tanács Főtitkársága (a Főtitkárság) EU-minősített adatokat kezel.
- (3) A tagállamok nemzeti jogszabályaikkal és rendelkezéseikkel összhangban és a Tanács működéséhez szükséges mértékben tiszteletben tartják ezt a határozatot, amikor illetékes hatóságaik, szerződéses vállalkozóik EU-minősített adatokat kezelnek, hogy mindegyikük biztos lehessen abban, hogy az EU-minősített adatok tekintetében egyenértékű védelem valósul meg.
- (4) A Tanács, a Bizottság és az Európai Külügyi Szolgálat (EKSZ) elkötelezett aziránt, hogy egyenértékű biztonsági előírásokat alkalmazzanak az EU-minősített adatok védelmére vonatkozóan.
- (5) A Tanács rámutat annak fontosságára, hogy adott esetben az Európai Parlamentet és más uniós intézményeket, szerveket, hivatalokat és ügynökségeket is

bevonjanak az Unió és tagállamai érdekeinek védelméhez szükséges, a minősített adatok védelmére vonatkozó titokvédelmi elvek, előírások és szabályok alkalmazásába.

- (6) A Tanácsnak – e határozattal és a hatályos intézményközi megállapodásokkal összhangban – meg kell határoznia a Tanács tulajdonában lévő EU-minősített adatok más uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel való megosztásának megfelelő kereteit.
- (7) Az Európai Unióról szóló szerződés (EUSZ) V. címének 2. fejezete alapján létrehozott uniós szerveknek és ügynökségeknek, az Europolnak és az Eurojustnak – amennyiben az őket létrehozó jogi aktus így rendelkezik – belső felépítésük keretében alkalmazniuk kell az e határozatban foglalt, az EU-minősített adatok védelmét szolgáló alapelveket és minimumszabályokat.
- (8) Az EUSZ V. címének 2. fejezete alapján létrehozott válságkezelési műveleteknek és az azokban részt vevő személyzetnek – amennyiben az e műveleteket létrehozó jogi aktus így rendelkezik – alkalmazniuk kell a Tanács által elfogadott, az EU-minősített adatok védelmét szolgáló biztonsági szabályokat.
- (9) Az EU különleges képviselőinek és munkatársaiknak – amennyiben a vonatkozó tanácsi jogi aktus így rendelkezik – alkalmazniuk kell a Tanács által elfogadott, az EU-minősített adatok védelmét szolgáló biztonsági szabályokat.
- (10) Ez a határozat nem érinti az Európai Unió működéséről szóló szerződés (EUMSZ) 15. és 16. cikkét, valamint az azokat végrehajtó jogi aktusokat.
- (11) Ez a határozat nem érinti a tagállamok fennálló gyakorlatát a nemzeti parlamenteknek az Unió tevékenységével kapcsolatos tájékoztatása tekintetében.

⁽¹⁾ HL L 325., 2009.12.11., 35. o.

- (12) Annak érdekében, hogy a Horvát Köztársaság európai uniós csatlakozására tekintettel biztosítani lehessen az EU-minősített adatok védelmét szolgáló biztonsági szabályok megfelelő időben történő alkalmazását, e határozatnak a kihirdetése napján kell hatályba lépnie,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Cél, hatály és fogalommeghatározások

- (1) Ez a határozat megállapítja az EU-minősített adatok védelmére vonatkozó alapelveket és minimumszabályokat.

- (2) Ezek az alapelvek és minimumszabályok a Tanácsra és a Főtitkárságra alkalmazandók, és azokat – vonatkozó nemzeti jogszabályaikkal és rendelkezéseikkel összhangban – a tagállamoknak is be kell tartaniuk ahhoz, hogy mindegyikük biztos lehessen abban, hogy az EU-minősített adatok tekintetében azonos szintű védelem valósul meg.

- (3) E határozat alkalmazásában az A. függelékben szereplő fogalommeghatározások alkalmazandók.

2. cikk

Az EU-minősített adat fogalmának meghatározása, minősítési szintek és minősítési jelölések

- (1) „EU-minősített adat”: bármely olyan EU biztonsági minősítéssel ellátott adat és anyag, amelynek engedély nélküli hozzáférhetővé tétele különböző mértékben sértheti az Európai Unió, illetve egy vagy több tagállam érdekeit.

- (2) Az EU-minősített adatok minősítési szintjei a következők:

- a) 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;
- b) SECRET UE/EU SECRET: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele súlyosan sértheti az Európai Unió vagy egy vagy több tagállam alapvető érdekeit;
- c) CONFIDENTIEL UE/EU CONFIDENTIAL: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele sértheti az Európai Unió vagy egy vagy több tagállam alapvető érdekeit;
- d) RESTREINT UE/EU RESTRICTED: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele hátrányosan érintheti az Európai Unió vagy egy vagy több tagállam alapvető érdekeit.

- (3) Az EU-minősített adatokat a (2) bekezdés szerinti biztonsági minősítési jelöléssel kell ellátni. Az adatok ezenkívül tartalmazhatnak az érintett tevékenységi terület és a kibocsátó azonosítására, a terjesztés, valamint a felhasználás korlátozására vagy az átadhatóságra vonatkozó jelöléseket.

3. cikk

A minősítés szabályai

- (1) Az illetékes hatóságok biztosítják az EU-minősített adatok megfelelő minősítését, minősített adatokként való egyértelmű azonosíthatóságát és azt, hogy minősítési szintjüket csak a szükséges ideig őrizték meg.

- (2) A kibocsátó előzetes írásbeli hozzájárulása nélkül nem lehet az EU-minősített adatokat visszaminősíteni vagy a minősítés alól feloldani, továbbá nem lehet azoknak a 2. cikk (3) bekezdésében említett jelöléseit módosítani vagy eltávolítani.

- (3) A Tanács az EU-minősített adatok létrehozására vonatkozó biztonsági politikát hagy jóvá, amely gyakorlati minősítési útmutatót is tartalmaz.

4. cikk

A minősített adatok védelme

- (1) Az EU-minősített adatokat e határozattal összhangban kell védeni.

- (2) Az EU-minősített adatok birtokosai felelősek az adatok e határozat szerinti védelméért.

- (3) Amennyiben a tagállamok nemzeti minősítési jelöléssel ellátott minősített adatokat visznek be az Unió struktúráiba vagy hálózataiba, a Tanács és a Tanács Főtitkársága ezeket az adatokat az azonos szintű EU-minősített adatokra alkalmazandó előírásoknak megfelelően védi a biztonsági minősítések B. függelékben szereplő egyenértékűségi táblázatában foglaltak szerint.

- (4) EU-minősített adatok összessége magasabb minősítési szintnek megfelelő védelmet tehet indokoltá, mint a részeit alkotó egyes adatoké.

5. cikk

Biztonsági kockázatkezelés

- (1) Az EU-minősített adatokat fenyegető kockázatokat folyamatként kell kezelni. A folyamat célja az ismert biztonsági kockázatok feltárása, az ilyen kockázatok elfogadható szintre történő csökkentésére irányuló biztonsági intézkedések meghatározása e határozat alapelveivel és minimumszabályaival összhangban és az intézkedések alkalmazása az „alapos védelem” A. függelékben meghatározott elvének megfelelően. A fenti intézkedések hatékonyságát folyamatosan értékelni kell.

- (2) Az EU-minősített adatok teljes életciklusuk alatti védelmét szolgáló biztonsági intézkedések arányban állnak különösen az adatok biztonsági minősítésével, az adat vagy anyag formájával és mennyiségével, az EU-minősített adatok tárolására használt létesítmények elhelyezkedésével és felépítésével, valamint a szándékos károkozás és/vagy bűncselekményekből – a kémkedést, a szabotázszt és a terrorizmust is ideértve – eredően helyi szinten fennálló fenyegetéssel.

(3) Az engedély nélküli hozzáférés és hozzáférhetővé tétel, valamint az adatok és anyagok sértetlensége vagy rendelkezésre állása megszűnésének megelőzése érdekében a szükséghelyzeti terveknek figyelembe kell venniük az EU-minősített adatok szükséghelyzet esetén való védelmének a szükségességét.

(4) Az üzletmenet-folytonossági terveknek a súlyos mulasztások vagy események által az EU-minősített adatok kezelésére és tárolására gyakorolt hatások csökkentését szolgáló megelőző és helyreállító intézkedéseket kell tartalmazniuk.

6. cikk

E határozat végrehajtása

(1) A Tanács – szükség esetén – a Biztonsági Bizottság ajánlására e határozat végrehajtását szolgáló intézkedéseket meghatározó biztonsági politikákat hagy jóvá.

(2) A Biztonsági Bizottság saját szintjén az e határozatot és a Tanács által jóváhagyott biztonsági politikákat kiegészítő vagy támogató biztonsági iránymutatásokat fogadhat el.

7. cikk

Személyi biztonság

(1) A személyi biztonság olyan intézkedések alkalmazását jelenti, amelyek biztosítják, hogy csak azon személyek kapjanak hozzáférést az EU-minősített adatokhoz:

- akiknek esetében a „szükséges ismeret” feltétele teljesül,
- akik adott esetben megfelelő szintű biztonsági ellenőrzésen átesnek, valamint
- akiket tájékoztattak felelősségükről.

(2) A személyi biztonsági tanúsítvánnyal kapcsolatos eljárások célja annak meghatározása, hogy egy adott személy számára – lojalítását, szavahihetőségét és megbízhatóságát figyelembe véve – engedélyezhető-e az EU-minősített adatokhoz való hozzáférés.

(3) A Főtitkárság személyi állománya minden olyan tagjának, akinek feladatai szükségessé teszik a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítésű EU-minősített adatokhoz való hozzáférést, illetve az ilyen adatok kezelését, az ilyen EU-minősített adatokhoz való hozzáférés engedélyezését megelőzően megfelelő szintű biztonsági ellenőrzésen kell átesnie. Az ilyen személyeknek engedélyt kell kapniuk a Főtitkárság kinevezésre jogosult hatóságától arra, hogy egy adott minősítési szintig és egy meghatározott időpontig hozzáférhessenek az EU-minősített adatokhoz.

(4) A 15. cikk (3) bekezdésében említett azon tagállami személyzetnek, amelynek feladatai szükségessé tehetik a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű EU-minősített adatokhoz való hozzáférést – az ilyen EU-minősített adatokhoz való hozzáférés engedélyezését megelőzően – megfelelő szintű biztonsági ellenőrzésen kell átesnie, vagy e

személyek számára a nemzeti jogszabályokkal és rendelkezésekkel összhangban más módon, feladatkörüknel fogva megfelelő felhatalmazást kell adni.

(5) Az EU-minősített adatokhoz való hozzáférés engedélyezését megelőzően, majd azt követően rendszeres időközönként minden egyes személyt tájékoztatni kell az EU-minősített adatok e határozat szerinti védelmével kapcsolatos felelősségről, amelyet e személyeknek tudomásul kell venni.

(6) Az e cikk végrehajtására vonatkozó rendelkezéseket az I. melléklet tartalmazza.

8. cikk

Fizikai biztonság

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

(2) A fizikai biztonsági intézkedések célja jogosulatlan személyek titokban történő vagy erőszakos behatolásának a megakadályozása, jogosulatlan cselekményektől való elrettentés, azok megakadályozása és észlelése, valamint a személyzet tagjainak megkülönböztetése az EU-minősített adatokhoz való hozzáférés tekintetében, a szükséges ismeret elve alapján. Ezek az intézkedések kockázatkezelési eljáráson alapulnak.

(3) Fizikai biztonsági intézkedéseket kell bevezetni valamennyi helyiségben, épületben, irodában, teremben és egyéb területen, ahol EU-minősített adatokat kezelnek vagy tárolnak, ideértve azon területeket is, ahol a 10. cikk (2) bekezdésében meghatározott kommunikációs és információs rendszereket tárolják.

(4) A II. mellékletnek megfelelően biztonsági területként kell meghatározni és az illetékes biztonsági hatóságnak jóvá kell hagynia azokat a területeket, ahol CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítéssel rendelkező EU-minősített adatot tárolnak.

(5) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű EU-minősített adat védelmére kizárólag jóváhagyott berendezés vagy eszköz használható fel.

(6) Az e cikk végrehajtására vonatkozó rendelkezéseket a II. melléklet tartalmazza.

9. cikk

A minősített adatok kezelése

(1) A minősített adatok kezelése az EU-minősített adatok teljes életciklusán keresztüli ellenőrzésére szolgáló adminisztratív intézkedések alkalmazása a 7., a 8. és a 10. cikkben meghatározott intézkedések kiegészítéseként, és ezáltal az ilyen adatok szándékos vagy véletlenszerű illetéktelen tudomására jutásától vagy elvesztésétől való elrettentéshez és annak észleléséhez való hozzájárulásként. Az ilyen intézkedések különösen az EU-minősített adat előállítására, nyilvántartásba vételére, másolására, fordítására, visszaminősítésére, minősítése megszüntetésére, szállítására és megsemmisítésére vonatkoznak.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat továbbítás előtt és kézhezvételkor biztonsági célokból nyilvántartásba kell venni. A Főtitkárság és a tagállamok illetékes hatóságai gondoskodnak az erre a célra szolgáló nyilvántartási rendszer kiépítéséről. A TRÈS SECRET UE/EU TOP SECRET minősítésű adatokat elkülönített nyilvántartásokban kell kezelni.

(3) Az illetékes biztonsági hatóságnak rendszeresen ellenőriznie kell azokat a szerveket és létesítményeket, ahol EU-minősített adatokat kezelnek vagy tárolnak.

(4) Az EU-minősített adatoknak a szervek és létesítmények között történő, a fizikailag védett területeken kívüli továbbítása az alábbiak szerint történik:

- a) az EU-minősített adatokat – főszabályként – a 10. cikk (6) bekezdésével összhangban jóváhagyott, kriptográfiai termékekkel védett elektronikus úton továbbítják;
- b) amennyiben nem használnak az a) pontban említett eszközöket, az EU-minősített adatok szállítása az alábbiak szerint történik:
 - i. vagy a 10. cikk (6) bekezdésével összhangban jóváhagyott kriptográfiai termékekkel védett elektronikus eszközökön (pl. USB-kulcsokon, CD-ken, merevlemezeken); vagy
 - ii. bármely egyéb esetben az illetékes biztonsági hatóság által a III. mellékletben megállapított vonatkozó védelmi intézkedésekkel összhangban előírt módon.

(5) Az e cikk végrehajtására vonatkozó rendelkezéseket a III. és a IV. melléklet tartalmazza.

10. cikk

A kommunikációs és információs rendszerekben kezelt EU-minősített adatok védelme

(1) Az információvédelem a kommunikációs és információs rendszerek tekintetében azt jelenti, hogy az ilyen rendszerek megvédik az általuk kezelt adatot, továbbá a szükséges módon, a szükséges időben, a jogszerű felhasználók ellenőrzése alatt működnek. A hatékony információvédelem biztosítja az adatok megfelelő bizalmasságát, sértetlenségét, rendelkezésre állását, letagadhatatlanságát és hitelességét. Az információvédelem kockázatkezelési eljárásokon alapul.

(2) „Kommunikációs és információs rendszer” (CIS): az elektronikus formában történő információkezelést lehetővé tevő rendszer. A CIS magában foglalja a működéséhez szükséges valamennyi eszközt, beleértve az infrastruktúrát, a szervezetet, a személyzetet és az információs forrásokat. Ezt a határozatot az EU-minősített adatokat kezelő CIS-ekre kell alkalmazni.

(3) A CIS az információvédelem koncepciójával összhangban kezeli az EU-minősített adatokat.

(4) Valamennyi CIS-t akkreditálni kell. Az akkreditáció célja, hogy biztosítva legyen, hogy e határozattal összhangban minden megfelelő biztonsági intézkedés végrehajtásra került, valamint az EU-minősített adatok és a CIS megfelelő szintű védelme biztosított. Az akkreditációs nyilatkozat meghatározza a minősített adatoknak azt a megengedett legmagasabb minősítési szintjét, amelyet a CIS kezelhet, valamint a kapcsolódó feltételeket.

(5) Biztonsági intézkedéseket kell alkalmazni a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat kezelő CIS-ek védelmére annak érdekében, hogy nem szándékos elektromágneses kisugárzás miatt a minősített adatok bizalmassága ne sérüljön („TEMPEST biztonsági intézkedések”). Ezeknek a biztonsági intézkedéseknek arányosnak kell lenniük az adatok felhasználásának kockázatával és minősítésük szintjével.

(6) Amennyiben az EU-minősített adatok védelmét kriptográfiai termékek biztosítják, e termékek jóváhagyása az alábbiak szerint történik:

- a) a SECRET UE/EU SECRET és magasabb szintű minősített adatok bizalmasságát a Tanács – mint kriptográfiai jóváhagyó hatóság (CAA) – által a Biztonsági Bizottság ajánlása alapján jóváhagyott kriptográfiai termékekkel kell védeni;
- b) a CONFIDENTIEL UE/EU CONFIDENTIAL vagy RESTREINT UE/EU RESTRICTED minősítésű adatok bizalmasságát a Tanács főtitkára (a továbbiakban: a főtitkár) – mint kriptográfiai jóváhagyó hatóság – által a Biztonsági Bizottság ajánlása alapján jóváhagyott kriptográfiai termékekkel kell védeni.

A b) pont ellenére a tagállami nemzeti rendszerekben a CONFIDENTIEL UE/EU CONFIDENTIAL vagy RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatok bizalmassága a tagállam kriptográfiai jóváhagyó hatósága által jóváhagyott kriptográfiai termékekkel is védhető.

(7) EU-minősített adatok elektronikus eszközökkel történő továbbítása során jóváhagyott kriptográfiai termékeket kell használni. E követelmény ellenére szükséghelyzet esetén vagy a IV. mellékletben meghatározott speciális technikai konfigurációk esetén különleges eljárások alkalmazhatók.

(8) A Főtitkárság és a tagállamok illetékes hatóságai létrehozzák a következő információvédelmi funkciókat:

- a) információvédelmi hatóság;
- b) TEMPEST-hatóság;
- c) kriptográfiai jóváhagyó hatóság;
- d) kriptográfiai terjesztési hatóság.

(9) A Főtitkárság és a tagállamok illetékes hatóságai minden rendszer tekintetében létrehozzák a következőket:

- a) biztonsági akkreditációs hatóság;
- b) információvédelmi üzemeltetési hatóság.

(10) Az e cikk végrehajtására vonatkozó rendelkezéseket a IV. melléklet tartalmazza.

11. cikk

Iparbiztonság

(1) Az iparbiztonság olyan intézkedések alkalmazása, amelyek célja az EU-minősített adatok védelmének vállalkozók vagy alvállalkozók általi biztosítása a minősített szerződések megkötését megelőző tárgyalások és a szerződések teljes életciklusa során. Az ilyen szerződések nem járhatnak TRÈS SECRET UE/EU TOP SECRET szintű minősített adatokhoz való hozzáféréssel.

(2) A Tanács Főtitkársága az EU-minősített adatokhoz való hozzáférést vagy azok kezelését vagy tárolását magában foglaló vagy azzal járó feladatokkal szerződés keretében olyan gazdálkodó vagy más szervezetet bízhat meg, amely valamely tagállamban vagy olyan harmadik államban van bejegyezve, amely a 13. cikk (2) bekezdésének a) vagy b) pontja szerinti megállapodást vagy igazgatási megállapodást kötött.

(3) A Főtitkárság – mint szerződő hatóság – a minősített szerződések gazdálkodó vagy egyéb szervezetek részére történő odaítélésakor gondoskodik arról, hogy az iparbiztonságnak az e határozatban és a szerződésben foglalt minimumszabályait betartsák.

(4) Az egyes tagállamok nemzeti biztonsági hatósága, kijelölt biztonsági hatósága vagy bármely egyéb illetékes hatósága a nemzeti jogszabályok és rendelkezések által lehetővé tett mértékben biztosítja, hogy a területén bejegyzett vállalkozók és alvállalkozók – a szerződéskötést megelőző tárgyalások és a minősített szerződés teljesítése során – valamennyi megfelelő intézkedést megtesznek az EU-minősített adatok védelme érdekében.

(5) Az egyes tagállamok nemzeti biztonsági hatósága, kijelölt biztonsági hatósága vagy egyéb illetékes biztonsági hatósága a nemzeti jogszabályokkal és rendelkezésekkel összhangban gondoskodik arról, hogy az adott tagállamban nyilvántartásba vett, saját létesítményeikben CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adathoz való hozzáférést igénylő minősített vállalkozói vagy alvállalkozói szerződésekben részt vevő vállalkozók vagy alvállalkozók – akár e szerződések teljesítése során, akár e szerződéseket megelőző szakaszban – rendelkeznek a megfelelő minősítési szintű telephely-biztonsági tanúsítvánnyal.

(6) Vállalkozók vagy alvállalkozók azon foglalkoztatottjai, akiknek a minősített szerződés teljesítéséhez CONFIDENTIEL

UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáféréssel kell rendelkeznie, az adott nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság személyi biztonsági tanúsítványt (PSC) bocsát ki a nemzeti jogszabályokkal és rendelkezésekkel, valamint az I. mellékletben foglalt biztonsági minimumszabályokkal összhangban.

(7) Az e cikk végrehajtására vonatkozó rendelkezéseket az V. melléklet tartalmazza.

12. cikk

Az EU-minősített adatok megosztása

(1) A Tanács meghatározza, hogy milyen feltételek mellett oszthatók meg a tulajdonában lévő EU-minősített adatok más uniós intézményekkel, szervekkel, hivatalokkal vagy ügynökségekkel. Ehhez létrehozható egy megfelelő keret, amelynek részét képezi intézményközi, illetve egyéb megállapodások megkötése, amennyiben az ennek érdekében szükséges.

(2) Ennek a keretnek biztosítania kell, hogy az EU-minősített adatok a minősítési szintjüknek megfelelő, valamint az e határozatban megállapított alapelvekkel és minimumszabályokkal egyenértékű alapelveknek és minimumszabályoknak megfelelő védelemben részesüljenek.

13. cikk

Minősített adatok harmadik államokkal és nemzetközi szervezetekkel való cseréje

(1) Amennyiben a Tanács megállapítja, hogy EU-minősített adatok harmadik állammal vagy nemzetközi szervezettel való cseréjére van szükség, akkor ehhez megfelelő eljárásrendet kell kialakítani.

(2) Az említett eljárásrend kialakításához és az átadott vagy átvett minősített adatok védelmét szolgáló kölcsönös szabályok meghatározásához:

- a) az Unió a minősített adatok megosztására és védelmére a biztonsági eljárásokról szóló megállapodásokat (a továbbiakban: az adatbiztonsági megállapodások) köt harmadik államokkal, illetve nemzetközi szervezetekkel; vagy
- b) az EU által átadni tervezett legfeljebb RESTREINT UE/EU RESTRICTED minősítési szintű adat átadására a VI. melléklet 17. pontjának megfelelően a főtitkár a Tanács Főtitkársága nevében igazgatási megállapodásokat köthet.

(3) A (2) bekezdésben említett adatbiztonsági vagy igazgatási megállapodások rendelkezéseket tartalmaznak annak biztosítására, hogy amennyiben a harmadik állam vagy a nemzetközi szervezet EU-minősített adatot kap, az ilyen adatot a minősítési szintjének és az e határozatban foglaltakkal legalább azonos szintű minimumszabályoknak megfelelő védelemben részesítsék.

(4) A Tanácstól származó EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére történő átadásáról szóló határozatot csak a Tanács hozhatja meg eseti alapon, az adat jellegétől és tartalmától, az átvevő számára szükséges ismeret elvétől, valamint az Unió számára jelentkező előnyök mértékétől függően. Ha az átadni kért minősített adat kibocsátója nem a Tanács, akkor a Főtitkárságnak a kibocsátó előzetes írásbeli beleegyezését kell kérnie az adat átadásához. Ha a kibocsátó nem állapítható meg, feladatkörét a Tanács látja el.

(5) A harmadik államokban vagy nemzetközi szervezeteknél az átadott vagy kicserélt EU-minősített adatok védelmére bevezetett biztonsági intézkedések hatékonyságának megállapítása céljából értékelő látogatásokra kerül sor.

(6) Az e cikk végrehajtására vonatkozó rendelkezéseket a VI. melléklet tartalmazza.

14. cikk

A biztonsági szabályok megsértése és az EU-minősített adatok illetéktelen tudomására jutása

(1) A biztonsági szabályok megsértése az e határozatban foglalt biztonsági szabályokkal ellentétes cselekmény vagy mulasztás eredményeként következik be.

(2) Az EU-minősített adatok illetéktelen tudomására jutása akkor következik be, ha az adatok a biztonsági szabályok megsértésének következtében részben vagy egészben illetéktelen személyek tudomására jutnak.

(3) A biztonsági szabályok megsértését vagy azok feltételezett megsértését minden esetben haladéktalanul jelenteni kell az illetékes biztonsági hatóságnak.

(4) Amennyiben ismert, vagy alapos okkal gyanítható, hogy EU-minősített adatok illetéktelen személy tudomására jutottak vagy elvesztek, a nemzeti biztonsági hatóság vagy egyéb illetékes hatóság a vonatkozó jogszabályokkal és más rendelkezésekkel összhangban megteszi a szükséges intézkedéseket:

a) a kibocsátó tájékoztatására;

b) annak biztosítására, hogy a tények megállapítása érdekében az esetet olyan személyek vizsgálják ki, akiket a biztonsági szabályok megsértése közvetlenül nem érint;

c) az Unió vagy a tagállamok érdekei tekintetében okozott esetleges károk felmérésére;

d) az ismételt előfordulás megelőzése érdekében; valamint

e) értesíti a megfelelő hatóságokat a megtett lépésekről.

(5) Az e határozatban megállapított biztonsági szabályokat megsértő személy a vonatkozó szabályok és rendelkezések szerint fegyelmi eljárás alá vonható. Az EU-minősített adatok illetéktelen tudomására jutásáért vagy elvesztéséért felelős személy a vonatkozó jogszabályok és rendelkezések szerint fegyelmi és/vagy jogi eljárás alá vonható.

15. cikk

Végrehajtási felelősség

(1) A Tanács minden szükséges intézkedést megtesz annak érdekében, hogy biztosítsa e határozat alkalmazásának általános összhangját.

(2) A főtitkár minden szükséges intézkedést megtesz annak érdekében, hogy az EU-minősített adatok és minden más minősített adat kezelésekor vagy tárolásakor a Tanács által igénybe vett helyszíneken és a Főtitkárságon belül a Főtitkárság tisztviselői és egyéb alkalmazottai, a Főtitkársághoz kirendelt személyek, valamint a Főtitkárság vállalkozói alkalmazzák e határozatot.

(3) A tagállamok minden megfelelő intézkedést meghoznak annak érdekében, hogy az EU-minősített adatok kezelésekor vagy tárolásakor a következő személyek betartsák e határozatot:

a) a tagállamok Európai Unió melletti állandó képviselteinek tagjai, valamint a Tanács vagy annak előkészítő szervei ülésein, valamint a Tanács egyéb tevékenységeiben részt vevő nemzeti küldöttek;

b) a tagállamok nemzeti közigazgatásában foglalkoztatottak, beleértve a közigazgatáshoz delegált szakértőket is, akár a tagállamok területén, akár külföldön teljesítenek szolgálatot;

c) az EU-minősített adatokhoz való hozzáférésre feladatkörükönél fogva megfelelően felhatalmazott egyéb személyek a tagállamokban; valamint

d) a tagállamok szerződéses vállalkozói, akár a tagállamok területén, akár külföldön.

16. cikk

A Tanács biztonsági szervezete

(1) A Tanács – az e határozat alkalmazása általános összhangjának biztosításában betöltött szerepe részeként – jóváhagyja a következőket:

- a) a 13. cikk (2) bekezdésének a) pontjában említett megállapodások;
- b) a Tanács által kibocsátott vagy a Tanács tulajdonában lévő EU-minősített adatoknak a harmadik államok vagy nemzetközi szervezetek részére történő átadását jóváhagyó vagy engedélyező határozatok, a kibocsátó beleegyezésének elvével összhangban;
- c) a Biztonsági Bizottság által ajánlott éves értékelő látogatási program a tagállamok szerveinél és létesítményeinél, valamint az e határozatot vagy az e határozatban foglalt elveket alkalmazó uniós szerveknél, ügynökségeknél és szervezeteknél, valamint harmadik államokban és nemzetközi szervezeteknél tett értékelő látogatások az EU-minősített adatok védelme érdekében tett intézkedések hatékonyságának megállapítása céljából; valamint
- d) a 6. cikk (1) bekezdésében foglaltak szerinti biztonsági politikák.

(2) A főtitkár a Főtitkárság biztonsági hatósága. E minőségében a főtitkár:

- a) végrehajtja és folyamatosan felülvizsgálja a Tanács biztonsági politikáját;
- b) a Tanács tevékenységei szempontjából lényeges minősített adatok védelmével kapcsolatos valamennyi biztonsági kérdésben egyeztet a tagállamok nemzeti biztonsági hatóságával;
- c) a 7. cikk (3) bekezdésével összhangban engedélyt ad a Főtitkárság tisztviselői, egyéb alkalmazottai és a kirendelt nemzeti szakértők számára, hogy hozzáférjenek a CONFIDENTIEL UE/EU CONFIDENTIAL vagy ennél magasabb minősítésű adatokhoz;
- d) adott esetben vizsgálatot rendel el a Tanács birtokában lévő vagy a Tanácsnál keletkezett minősített adatok tényleges vagy feltételezett illetéktelen tudomására jutása vagy elvesztése esetén, és felkéri a megfelelő biztonsági hatóságokat, hogy nyújtsanak segítséget a kivizsgálásban;
- e) rendszeres időközönként ellenőrzi a minősített adatok védelmét szolgáló, a Főtitkárság létesítményeiben érvényes biztonsági intézkedéseket;
- f) rendszeres időközönként látogatásokat tesz az e határozatot vagy az e határozatban foglalt elveket alkalmazó uniós

szerveknél, ügynökségeknél és szervezeteknél, hogy értékelje az EU-minősített adatok védelmét szolgáló biztonsági intézkedéseket;

- g) az érintett nemzeti biztonsági hatóságokkal közösen és egyetértésben rendszeres időközönként értékeli az EU-minősített adatok védelmét szolgáló, a tagállamok szerveinél és létesítményeiben érvényes biztonsági intézkedéseket;
- h) gondoskodik a biztonsági intézkedések szükséges mértékű, a tagállamok és adott esetben harmadik államok, valamint nemzetközi szervezetek minősített adatok védelméért felelős hatóságaival való koordinálásáról, az EU-minősített adatok biztonságát veszélyeztető fenyegetések jellegére és az azokkal szembeni védekezés eszközeire vonatkozóan is; valamint
- i) a 13. cikk (2) bekezdésének b) pontjában említett igazgatási megállapodásokat köt.

A Főtitkárság Biztonsági Hivatala a főtitkár rendelkezésére áll, és segíti őt e feladatok végrehajtásában.

(3) A 15. cikk (3) bekezdésének végrehajtása céljából a tagállamok:

- a) kijelölik az EU-minősített adatok védelmét szolgáló biztonsági intézkedésekért felelős nemzeti biztonsági hatóságot – amelyek jegyzékét a C. függelék tartalmazza – annak érdekében, hogy
 - i. a bármely nemzeti hatóság, szerv vagy ügynökség, vagy köz- vagy magánintézmény által belföldön vagy külföldön birtokolt EU-minősített adatok e határozatnak megfelelő védelemben részesüljenek;
 - ii. az EU-minősített adatok védelmét szolgáló biztonsági intézkedéseket rendszeres időközönként ellenőrizzék, illetve értékeljék;
 - iii. a nemzeti közigazgatásban vagy szerződéses vállalkozó által foglalkoztatott minden olyan személy, aki CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz hozzáférhet, megfelelő biztonsági ellenőrzésen essen át, vagy a nemzeti jogszabályokkal és rendelkezésekkel összhangban más módon, feladatkörénél fogva megfelelő felhatalmazást kapjon;
 - iv. szükség szerint alakítsanak ki biztonsági programokat, hogy minimálisra csökkentsék az EU-minősített adatok illetéktelen tudomására jutásának vagy elvesztésének kockázatát;
 - v. az EU-minősített adatok védelmével kapcsolatos biztonsági kérdésekről egyeztessenek más illetékes nemzeti hatóságokkal, beleértve az e határozatban említett hatóságokat is; valamint

vi. válaszoljanak különösen az azon uniós szervektől, ügynökségektől és szervezetektől, valamint az EUSZ V. címének 2. fejezete alapján létrehozott műveletek részéről, továbbá az EU különleges képviselőitől (EUKK) és munkatársaitól érkező megfelelő biztonsági tanúsítványok iránti kérelmekre, amelyek alkalmazzák e határozatot vagy az e határozatban foglalt elveket;

b) biztosítják, hogy illetékes hatóságai tájékoztassák és tanácsal lássák el kormányukat és – ez utóbbi útján – a Tanácsot az EU-minősített adatok biztonságát fenyegető veszélyek jellegéről és az azokkal szemben alkalmazandó védelmi eszközökről.

17. cikk

Biztonsági Bizottság

(1) Biztonsági Bizottság jön létre. A bizottság megvizsgálja és értékeli az e határozat alkalmazási körébe tartozó valamennyi biztonsági kérdést, és adott esetben ajánlásokat tesz a Tanácsnak.

(2) A Biztonsági Bizottság a tagállamok nemzeti biztonsági hatóságainak képviselőiből áll, és ülésein részt vesz a Bizottság és az EKSZ egy képviselője. A Biztonsági Bizottság elnöke a főtitkár vagy a kijelölt képviselője. A Biztonsági Bizottság a Tanács utasításai alapján, vagy a főtitkár vagy egy nemzeti biztonsági hatóság kérésére ülésezik.

Az e határozatot vagy az e határozatban foglalt elveket alkalmazó uniós szervek, ügynökségek és szervezetek is meghívást kaphatnak az üléseken való részvételre, ha őket érintő kérdéseket vitatnak meg.

(3) A Biztonsági Bizottságnak úgy kell megszerveznie tevékenységét, hogy a biztonság meghatározott területei tekintetében ajánlásokat tudjon tenni. A bizottság információvédelmi kérdésekkel foglalkozó csoportot és szükség esetén egyéb szakértői csoportokat hoz létre. Elkészíti a szakértői csoportok feladatmeghatározását, és tevékenységükről – adott esetben a Tanácsnak tett ajánlásokról is – jelentéseket kap.

18. cikk

A korábbi határozat hatályon kívül helyezése

(1) Ez a határozat hatályon kívül helyezi a 2011/292/EU tanácsi határozatot ⁽¹⁾, és annak helyébe lép.

(2) A 2001/264/EK ⁽²⁾ és a 2011/292/EU tanácsi határozat értelmében minősített valamennyi EU-minősített adatot továbbra is e határozat vonatkozó rendelkezéseivel összhangban kell védeni.

19. cikk

Hatálybalépés

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

Kelt Brüsszelben, 2013. szeptember 23-án.

a Tanács részéről

az elnök

V. JUKNA

⁽¹⁾ A Tanács 2011/292/EU határozata (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 141., 2011.5.27., 17. o.).

⁽²⁾ A Tanács 2001/264/EK határozata (2001. március 19.) a Tanács biztonsági szabályzatának elfogadásáról (magyar nyelvű kiadás 1. fejezet, 3. kötet, 263. o.).

*MELLÉKLETEK**I. MELLÉKLET*

Személyi biztonság

II. MELLÉKLET

Fizikai biztonság

III. MELLÉKLET

A minősített adatok kezelése

IV. MELLÉKLET

A CIS-ben kezelt EU-minősített adatok védelme

V. MELLÉKLET

Iparbiztonság

VI. MELLÉKLET

Minősített adatok cseréje harmadik államokkal és nemzetközi szervezetekkel

I. MELLÉKLET

SZEMÉLYI BIZTONSÁG

I. BEVEZETÉS

1. Ez a melléklet a 7. cikk végrehajtására vonatkozó rendelkezéseket határoz meg. Az annak meghatározására szolgáló kritériumokat állapítja meg, hogy egy adott személy – lojalitását, szavahihetőségét és megbízhatóságát figyelembe véve – engedélyt kaphat-e EU-minősített adatokhoz való hozzáférésre, és tartalmazza az e célból követendő vizsgálati és adminisztratív eljárásokat.

II. AZ EU-MINŐSÍTETT ADATOKHOZ VALÓ HOZZÁFÉRÉS ENGEDÉLYEZÉSE

2. Egy adott személy csak azt követően kaphat hozzáférést minősített adatokhoz, hogy:

- a) megállapítást nyert, hogy esetében a „szükséges ismeret” feltétele teljesül;
- b) tájékoztatást kapott az EU-minősített adatok védelmére szolgáló biztonsági szabályokról és eljárásokról, és tudomásul vette az ilyen adatok védelmével kapcsolatos felelősségét; valamint
- c) CONFIDENTIEL UE/EU CONFIDENTIAL vagy ennél magasabb minősítési szintű adatok esetén:
 - a megfelelő szintre érvényes személyi biztonsági tanúsítványt, vagy a nemzeti jogszabályokkal és rendelkezésekkel összhangban más módon, feladatkörénél fogva megfelelő felhatalmazást kapott, vagy
 - a Főtitkárság tisztségviselői, egyéb alkalmazottai, illetve kirendelt nemzeti szakértők esetében az illető a Főtitkárság kinevezésre jogosult hatóságától a 16–25. ponttal összhangban felhatalmazást kapott arra, hogy egy adott minősítési szintig és egy meghatározott időpontig hozzáférjen az EU-minősített adatokhoz.

3. Az egyes tagállamok és a Főtitkárság meghatározzák szervezeti felépítésükben azokat a beosztásokat, amelyek CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adathoz való hozzáférést tesznek szükségessé, és ezért megfelelő szintű biztonsági tanúsítványt igényelnek.

III. A SZEMÉLYI BIZTONSÁGI TANÚSÍTVÁNNYAL KAPCSOLATOS KÖVETELMÉNYEK

4. A megfelelően engedélyezett kérelem kézhezvételét követően a nemzeti biztonsági hatóságok vagy egyéb illetékes nemzeti hatóságok felelnek azért, hogy a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáférést igénylő állampolgáraik biztonsági ellenőrzését elvégezzék. Azzal összefüggésben, hogy PSC-t állítsanak ki vagy adott esetben biztosítékot adjanak annak a személynek, aki engedélyt kapna az EU-minősített adatokhoz való hozzáféréshez, az ellenőrzésre vonatkozó szabályoknak összhangban kell állniuk a nemzeti jogszabályokkal és rendelkezésekkel.
5. Ha az érintett személy tartózkodási helye egy másik tagállam vagy egy harmadik állam területén van, az illetékes nemzeti hatóságok a nemzeti jogszabályokkal és rendelkezésekkel összhangban segítséget kérnek a tartózkodási hely szerinti állam illetékes hatóságától. A tagállamok a nemzeti jogszabályokkal és rendelkezésekkel összhangban segítséget nyújtanak egymásnak a biztonsági ellenőrzések elvégzéséhez.
6. Amennyiben a nemzeti jogszabályok és rendelkezések megengedik, a nemzeti biztonsági hatóságok vagy egyéb illetékes nemzeti hatóságok elvégezhetik a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáférést igénylő külföldi állampolgárok biztonsági ellenőrzését. Az ellenőrzésre vonatkozó szabályoknak összhangban kell állniuk a nemzeti jogszabályokkal és rendelkezésekkel.

A biztonsági ellenőrzés kritériumai

7. Az adott személy lojalitásának, szavahihetőségének és megbízhatóságának a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáférést engedélyező biztonsági tanúsítvány megadása céljából történő értékelése biztonsági ellenőrzés keretében történik. Az illetékes nemzeti hatóság általános értékelést készít a biztonsági ellenőrzés eredményei alapján. Az e célra használt alapvető kritériumok magukban foglalják – a nemzeti jogszabályok és rendelkezések szerint lehetséges mértékben – annak mérlegelését, hogy az adott személy:

- a) elkövetett-e vagy megkísérelt-e elkövetni kémkedést, terrorizmust, szabotázszt, hazaárulást vagy lázadást, annak szervezésében részt vett-e vagy ahhoz segítséget nyújtott-e, vagy felbújtott-e mást annak elkövetésére;
 - b) kapcsolatban áll-e vagy állt-e kémekkel, terroristákkal, szabotőrökkel vagy ilyen cselekmények elkövetésével alaposan gyanúsítható személyekkel, vagy olyan szervezetek vagy külföldi államok képviselőivel – külföldi hírszerző szolgálatokat is beleértve –, akik veszélyt jelenthetnek az Unió és/vagy a tagállamok biztonságára, kivéve, ha ezekre a kapcsolatokra hivatalos feladatok ellátása során kapott engedélyt;
 - c) tagja-e vagy tagja volt-e olyan szervezetnek, amely erőszakos, felforgató vagy egyéb jogellenes módon többek között arra törekszik, hogy valamely tagállam kormányát megdöntse, valamely tagállam alkotmányos rendjét megváltoztassa, vagy kormányának formáját vagy politikáit megváltoztassa;
 - d) támogatója-e vagy a támogatója volt-e bármely, a c) pontban említett szervezetnek, vagy szoros kapcsolatban áll-e vagy állt-e a közelmúltban ilyen szervezetek tagjaival;
 - e) szándékosan visszatartott-e, elferdített-e vagy meghamisított-e lényeges – különösen biztonsági természetű – információt, vagy szándékosan közölt-e hamis adatot a személyi biztonsági formanyomtatvány kitöltésekor vagy a személyes elbeszélgetés alkalmával;
 - f) elítélték-e bűncselekmény vagy bűncselekmények elkövetése miatt;
 - g) alkoholfüggő-e/volt-e alkoholfüggő, fogyaszt-e/fogyasztott-e tiltott kábítószeret és/vagy visszaél-e/visszaélt-e engedélyezett kábítószerrel;
 - h) tanúsít-e vagy tanúsított-e olyan magatartást, amelynek következtében fennállhat a zsarolás vagy nyomásgyakorlás miatti sebezhetőség veszélye;
 - i) ténylegesen vagy szóban tanúsított-e becselenséget, hűtlenséget, állhatatlanságot vagy megbízhatatlanságot;
 - j) súlyosan vagy ismételten megsértette-e a biztonsági szabályokat; vagy kísérelt-e meg vagy hajtott-e végre jogosulatlan tevékenységet a CIS-ek tekintetében; valamint
 - k) ki lehet-e téve nyomásgyakorlásnak (például azért, mert egy vagy több nem uniós állampolgársággal rendelkezik, vagy olyan hozzátartozók vagy közeli kapcsolatok révén, akik veszélyeztetettek lehetnek olyan külföldi hírszerző szolgálatok, terroristacsoportok vagy egyéb felforgató szervezetek vagy személyek által, akiknek a céljai sérthetik az Unió és/vagy a tagállamok biztonsági érdekeit).
8. Adott esetben és a nemzeti jogszabályokkal és rendelkezésekkel összhangban az érintett személy pénzügyi és egészségügyi háttere is lényegesnek bizonyulhat a biztonsági ellenőrzés során.
9. Adott esetben és a nemzeti jogszabályokkal és rendelkezésekkel összhangban a házastárs, az élettárs vagy a közeli hozzátartozók viselkedése és körülményei szintén lényegesek lehetnek a biztonsági ellenőrzés során.

Az EU-minősített adatokhoz való hozzáférésre vonatkozó ellenőrzési követelmények

Biztonsági tanúsítvány első megadása

10. A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférés engedélyezéséhez szükséges első biztonsági tanúsítványnak legalább az utolsó öt évre vagy – attól függően, hogy melyik a rövidebb – 18 éves kortól az adott időpontig terjedő időszakra vonatkozó biztonsági ellenőrzésen kell alapulnia, amely az alábbiakat foglalja magában:
- a) az azon minősítési szinthez tartozó nemzeti személyi biztonsági kérdőív kitöltése, amilyen szintű EU-minősített adatokhoz az érintett személy hozzáférést igényelhet; kitöltés után a kérdőívet elküldik az illetékes biztonsági hatóságnak;

- b) a személyazonosság ellenőrzése/állampolgárság/nemzetiségi státus – a személy születési idejét és helyét, valamint személyazonosságát ellenőrizni kell. A személy jelenlegi és volt állampolgársági státusát és/vagy nemzetiségét meg kell állapítani; ennek magában kell foglalnia a külföldi forrásból kiinduló – például a korábbi lakóhellyel vagy kapcsolatokkal összefüggő – nyomásgyakorlás miatti sebezhetőség felmérését; valamint
- c) a nemzeti és helyi nyilvántartások ellenőrzése – ellenőrizni kell a nemzeti biztonsági és a központi bűnügyi nyilvántartást, amennyiben ez utóbbi létezik, és/vagy egyéb hasonló kormányzati vagy rendőrségi nyilvántartásokat. Ellenőrizni kell azoknak az illetékességgel rendelkező bűnüldöző szervezeteknek a nyilvántartásait, ahol a személy lakóhellyel rendelkezett vagy alkalmazásban állt.
11. A TRÈS SECRET UE/EU TOP SECRET minősítésű adatokhoz való hozzáférés engedélyezéséhez szükséges első biztonsági tanúsítványnak legalább az utolsó tíz évre vagy – attól függően, hogy melyik a rövidebb – 18 éves kortól az adott időpontig terjedő időszakokra vonatkozó biztonsági ellenőrzéseken kell alapulnia. Amennyiben az e) alpontban meghatározott személyes elbeszélgetésre kerül sor, az ellenőrzések legalább az utolsó hét évet vagy – attól függően, hogy melyik a rövidebb – 18 éves kortól az adott időpontig terjedő időszakot foglalják magukban. A fenti 7. pontban említett kritériumokon kívül az alábbi szempontokat kell megvizsgálni – a nemzeti jogszabályok és rendelkezések szerint lehetséges mértékben – a TRÈS SECRET UE/EU TOP SECRET PSC megadása előtt; ha a nemzeti jogszabályok és rendelkezések előírják, e szempontokat a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET PSC megadása előtt is megvizsgálhatják:
- a) pénzügyi helyzet – információt kell szerezni a személy pénzügyeiről annak megítélése érdekében, hogy súlyos pénzügyi nehézségek következtében fennáll-e külföldi vagy hazai nyomásgyakorlás miatti bármilyen sebezhetőség, illetve bármely megmagyarázhatatlan vagyongyarapodás feltárása érdekében;
- b) tanulmányok – információt kell szerezni a tizennyolcadik életév betöltésétől kezdődően vagy a vizsgálatot lefolytató hatóság által megfelelőnek ítélt időszakban látogatott iskolákban, egyetemeken és egyéb oktatási intézményekben végzett tanulmányok ellenőrzése érdekében;
- c) munkaviszony – a jelenlegi és a korábbi munkaviszonyokra vonatkozó információt kell szerezni, többek között olyan forrásokból, mint a munkáltatói nyilvántartások, a teljesítmény- vagy hatékonyságértékelések, valamint a munkáltatók vagy munkahelyi vezetők;
- d) katonai szolgálat – adott esetben meg kell vizsgálni a személy fegyveres erőknél letöltött szolgálatát és a leszerelés módját; valamint
- e) személyes elbeszélgetés – amennyiben a nemzeti jogszabály azt előírja és lehetővé teszi, személyes elbeszélgetést vagy elbeszélgetéseket kell folytatni a vizsgált személlyel. Személyes elbeszélgetést kell folytatni olyan más személyekkel is, akik képesek a személy hátterét, tevékenységeit, lojalitását, szavahihetőségét és megbízhatóságát elfogulatlanul megítélni. Amennyiben az országban kialakult gyakorlat szerint az ellenőrzés alanyának referencia-személyeket kell megjelölnie, személyes elbeszélgetést kell folytatni a referenciaszemélyekkel is, kivéve akkor, ha alaposan indokolt, hogy erre ne kerüljön sor.
12. Szükség esetén és a nemzeti jogszabályokkal és rendelkezésekkel összhangban további ellenőrzést lehet folytatni annak érdekében, hogy a személyről minden hozzáférhető lényeges információt megszerezzenek, valamint hogy a kedvezőtlen információkat bizonyítsák vagy cáfolják.

A biztonsági tanúsítvány megújítása

13. A biztonsági tanúsítvány első megadását követően, valamint feltéve, hogy az adott személy a nemzeti közigazgatásban vagy a Főtitkárságnál folyamatos szolgálati jogviszonyban áll és folyamatosan szüksége van az EU-minősített adatokhoz való hozzáférésre, a biztonsági tanúsítványt megújítás céljából – TRÈS SECRET UE/EU TOP SECRET szintű tanúsítvány esetén a tanúsítvány alapjául szolgáló utolsó biztonsági ellenőrzés eredményéről szóló értesítés időpontjától számítva legalább öt évenként, SECRET UE/EU SECRET és CONFIDENTIEL UE/EU CONFIDENTIAL szintű tanúsítvány esetén ezen időponttól számítva legalább tízévenként – felül kell vizsgálni. A biztonsági tanúsítvány megújításához szükséges valamennyi biztonsági ellenőrzésnek az előző ellenőrzés óta eltelt időszakra kell vonatkoznia.
14. A biztonsági tanúsítványok megújítása céljából a 10. és a 11. pontban foglalt követelményeket kell megvizsgálni.

15. A megújítás iránti kérelmeket időben be kell nyújtani, figyelembe véve a biztonsági ellenőrzések elvégzéséhez szükséges időtartamot. Mindazonáltal, amennyiben az érintett nemzeti biztonsági hatóság vagy más illetékes nemzeti hatóság a biztonsági tanúsítvány érvényességének lejártá előtt megkapja az annak megújítása iránti kérelmet és az ahhoz kapcsolódó személyi biztonsági kérdőívet, és a szükséges biztonsági ellenőrzés még nem zárult le, az illetékes nemzeti hatóság – amennyiben a nemzeti jogszabályok és rendelkezések megengedik – legfeljebb 12 hónapos időtartamra meghosszabbíthatja a meglévő biztonsági tanúsítvány érvényességét. Amennyiben a biztonsági ellenőrzés e 12 hónapos időszak végére sem zárult le, az érintett személyt olyan feladatokkal kell megbízni, amelyekhez nem szükséges biztonsági tanúsítvány.

Engedélyezési eljárások a Tanács Főtitkárságán

16. A Főtitkárság tisztviselői és egyéb alkalmazottai tekintetében a Főtitkárság biztonsági hatósága küldi el a kitöltött személyi biztonsági kérdőívet az érintett személy állampolgársága szerinti tagállam nemzeti biztonsági hatóságának, és kéri, hogy végezzenek olyan minősítési szintű biztonsági ellenőrzést, amilyen szintű EU-minősített adatokhoz az érintett személynek hozzá kell férnie.
17. Amennyiben olyan személy biztonsági ellenőrzésével kapcsolatos releváns információ jut a Főtitkárság tudomására, aki EU-minősített adatokhoz való hozzáférést biztosító biztonsági tanúsítványért folyamodott, a Főtitkárság a vonatkozó szabályokkal és rendelkezésekkel összhangban értesíti erről az érintett nemzeti biztonsági hatóságot.
18. A biztonsági ellenőrzés elvégzését követően az érintett nemzeti biztonsági hatóság a Biztonsági Bizottság által előírt egységes levelezési minta felhasználásával értesíti a Tanács Főtitkárságának biztonsági hatóságát a vizsgálat eredményéről.
- a) Amennyiben a biztonsági ellenőrzés során megállapítást nyer, hogy az adott személy lojalitását, szavahihetőségét és megbízhatóságát semmilyen ismert kedvezőtlen tény nem kérdőjelezi meg, a Főtitkárság kinevezésre jogosult hatósága megadhatja az érintettnek az engedélyt, és adott időpontig és meghatározott szintig engedélyezheti számára az EU-minősített adatokhoz való hozzáférést.
- b) Amennyiben a biztonsági ellenőrzés kedvezőtlen eredménnyel jár, a Főtitkárság kinevezésre jogosult hatósága értesíti az érintett személyt, aki kérheti, hogy a kinevezésre jogosult hatóság hallgassa meg. A kinevezésre jogosult hatóság felkérheti az illetékes nemzeti biztonsági hatóságot, hogy ha a nemzeti jogszabályok és rendelkezések alapján módjában áll, adjon további felvilágosítást. Ha az eredmény megerősítést nyer, az EU-minősített adatokhoz való hozzáférésre vonatkozó engedély nem adható meg.
19. A biztonsági ellenőrzésre és a kapott eredményekre az érintett tagállamban hatályos megfelelő jogszabályok és rendelkezések vonatkoznak, beleértve az esetleges jogorvoslattal kapcsolatos rendelkezéseket is. A Főtitkárság kinevezésre jogosult hatóságának határozata ellen a 259/68/EGK, Euratom, ESZAK tanácsi rendeletben ⁽¹⁾ foglalt, az Európai Unió tisztviselőinek személyzeti szabályzatával és az Európai Unió egyéb alkalmazottainak alkalmazási feltételeivel összhangban lehet fellebbezni (a továbbiakban: a személyzeti szabályzat és alkalmazási feltételek).
20. A Főtitkársághoz CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű EU-minősített adatokhoz való hozzáférést igénylő beosztásba kirendelt nemzeti szakértőknek tevékenységük megkezdését megelőzően érvényes személyi biztonsági tanúsítványról szóló igazolást (PSCC) kell benyújtaniuk a Főtitkárság biztonsági hatóságához, amelynek alapján a kinevezésre jogosult hatóságnak engedélyeznie kell az EU-minősített adatokhoz való hozzáférést.
21. A Tanács Főtitkársága elfogadja a más uniós intézmény, szerv vagy ügynökség által adott, EU-minősített adatokhoz való hozzáférést lehetővé tevő engedélyt, feltéve ha az továbbra is érvényes. Az engedély az érintett által a Főtitkárságon végzett valamennyi feladat tekintetében érvényes. Az érintett személyt alkalmazó uniós intézmény, szerv vagy ügynökség értesíti a megfelelő nemzeti biztonsági hatóságot a munkáltató megváltozásáról.
22. Amennyiben az adott személy szolgálati jogviszonya a biztonsági ellenőrzés eredményéről a Főtitkárság kinevezésre jogosult hatóságának részére küldött értesítés dátumától számított 12 hónapon belül nem kezdődik meg, vagy amennyiben a szolgálati jogviszony 12 hónapig szünetel, és ez idő alatt a személy nem áll alkalmazásban a Főtitkárságnál vagy valamely tagállam nemzeti közigazgatási szerveinél, az érintett nemzeti biztonsági hatóságtól kell kérni annak megerősítését, hogy az eredmény továbbra is érvényes és megfelelő.

⁽¹⁾ A Tanács 259/68/EGK, Euratom, ESZAK rendelete (1968. február 29.) az Európai Közösségek tisztviselőinek személyzeti szabályzatáról és az Európai Közösségek egyéb alkalmazottainak alkalmazási feltételeiről (HL L 56., 1968.3.4., 1. o., magyar nyelvű különkiadás 1. fejezet, 2. kötet, 5. o.).

23. Amennyiben olyan információ jut a Főtitkárság tudomására, hogy EU-minősített adatokhoz való hozzáférést lehetővé tevő engedéllyel rendelkező személy biztonsági kockázatot jelent, a Főtitkárság a vonatkozó szabályokkal és rendelkezésekkel összhangban értesíti erről az érintett nemzeti biztonsági hatóságot, és felfüggesztheti az EU-minősített adatokhoz való hozzáférést vagy visszavonhatja az ezt lehetővé tevő engedélyt.
24. Ha valamely nemzeti biztonsági hatóság olyan személyre vonatkozó, a 18. pont a) alpontjával összhangban tett megállapítás visszavonásáról értesíti a Főtitkárságot, aki engedéllyel rendelkezik az EU-minősített adatokhoz való hozzáférésre, a Főtitkárság kinevezésre jogosult hatósága felkérheti az illetékes nemzeti biztonsági hatóságot, hogy ha a nemzeti jogszabályok és rendelkezések alapján módjában áll, adjon további felvilágosítást. Ha a kedvezőtlen információkat megerősítik, az engedélyt vissza kell vonni, és a személyt ki kell zárni az EU-minősített adatokhoz való hozzáférésből, valamint azokból a beosztásokból, amelyekben az ilyen hozzáférés lehetséges, vagy amelyekben a személy a biztonságot veszélyeztetheti.
25. Az engedély főtitkársági tisztviselőtől vagy egyéb alkalmazottól való visszavonására vagy felfüggesztésére vonatkozó határozatot és adott esetben annak indokait közölni kell az érintett személlyel, aki kérheti a kinevezésre jogosult hatóság általi meghallgatását. A nemzeti biztonsági hatóságok által rendelkezésre bocsátott információkra az érintett tagállamban hatályos megfelelő jogszabályok és rendelkezések vonatkoznak, beleértve az esetleges jogorvoslattal kapcsolatos rendelkezéseket is. A Főtitkárság kinevezésre jogosult hatóságának határozata ellen a személyzeti szabállyal és alkalmazási feltételekkel összhangban lehet fellebbezni.

A biztonsági tanúsítványok és engedélyek nyilvántartása

26. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáférést lehetővé tevő PSC-k és engedélyek nyilvántartását az egyes tagállamok, illetve a Főtitkárság vezeti. E nyilvántartásnak tartalmaznia kell legalább az EU-minősített adatok minősítési szintjét, amelyhez az adott személy részére hozzáférés biztosítható, a biztonsági tanúsítvány kibocsátásának dátumát és érvényességének időtartamát.
27. Az illetékes biztonsági hatóság PSC-t adhat ki, amely tartalmazza, hogy az adott személy milyen szintű EU-minősített adatokhoz rendelkezik hozzáférési engedéllyel (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint tartalmazza a vonatkozó, EU-minősített adatokhoz való hozzáférést lehetővé tevő PSC vagy engedély érvényességi idejét és a tanúsítvány lejártaának időpontját.

Mentességek a PSC-re vonatkozó követelmények alól

28. A tagállamokban a feladatkörüknél fogva megfelelően felhatalmazott személyek EU-minősített adatokhoz való hozzáférést a nemzeti jogszabályokkal és rendelkezésekkel összhangban kell meghatározni; e személyeket tájékoztatni kell az EU-minősített adatok védelmével kapcsolatos biztonsági kötelezettségeikről.

IV. BIZTONSÁGI OKTATÁS ÉS TUDATOSSÁG

29. Minden biztonsági tanúsítvánnyal rendelkező személynek írásban nyilatkoznia kell arról, hogy megértette az EU-minősített adatok védelmével kapcsolatos kötelezettségeit, valamint az EU-minősített adatok illetéktelen személy tudomására jutásának következményeit. Az ilyen írásbeli nyilatkozatokról a tagállamoknak vagy adott esetben a Főtitkárságnak nyilvántartást kell vezetnie.
30. Mindazon személyekben, akik engedéllyel rendelkeznek EU-minősített adatokhoz való hozzáférésre, vagy akiknek ilyen adatokat kell kezelniük, kezdetben, majd később rendszeres időközönként tudatosítani kell a biztonságot fenyegető veszélyeket, és e személyeknek haladéktalanul jelenteniük kell a megfelelő biztonsági hatóságoknak az általuk gyanúsnak vagy szokatlannak ítélt közeledést vagy tevékenységet.
31. Bármely személyben, akit nem alkalmaznak tovább az EU-minősített adatokhoz való hozzáférést megkövetelő feladatok ellátására, tudatosítani kell az EU-minősített adatok folyamatos védelmével kapcsolatos kötelezettségét, és adott esetben az érintett személyeknek erről írásbeli nyilatkozatot kell tenniük.

V. RENDKÍVÜLI KÖRÜLMÉNYEK

32. Amennyiben a nemzeti jogszabályok és rendelkezések lehetővé teszik, a nemzeti tisztviselők az adott tagállam illetékes nemzeti hatósága által a nemzeti minősített adatokhoz való hozzáférésre vonatkozóan megadott biztonsági tanúsítvány alapján – az EU-minősített adatokhoz való hozzáférésre vonatkozó PSC megadásáig ideiglenesen – a B. függelék egyenértékűségi táblázatában szereplő megfelelő szintig hozzáférhetnek az EU-minősített adatokhoz, amennyiben erre az ideiglenes hozzáférésre az Unió érdekében szükség van. A nemzeti biztonsági hatóság tájékoztatja a Biztonsági Bizottságot arról, ha a nemzeti jogszabályok és rendelkezések nem teszik lehetővé az EU-minősített adatokhoz való ideiglenes hozzáférést.

33. A Főtitkárság kinevezésre jogosult hatósága – szükséghelyzetből adódóan, amennyiben azt a szolgálat érdekei kellően indokolják, és a teljes biztonsági ellenőrzés lezárulásáig az érintett állampolgársága szerinti tagállam nemzeti biztonsági hatóságával folytatott konzultációt követően, valamint a kizáró tényezők hiányát kereső első vizsgálatok eredményére is figyelemmel – meghatározott feladat tekintetében ideiglenes engedélyt adhat a Főtitkárság tisztviselőinek és egyéb alkalmazottainak EU-minősített adatokhoz való hozzáférésre. Az ideiglenes engedély érvényességének időtartama legfeljebb hat hónap lehet, és nem teheti lehetővé a TRÈS SECRET UE/EU TOP SECRET minősítésű adatokhoz való hozzáférést. Minden ideiglenes engedéllyel rendelkező személynek írásban nyilatkoznia kell arról, hogy megértette az EU-minősített adatok védelmével kapcsolatos kötelezettségeit, valamint az EU-minősített adatok illetéktelen tudomására jutásának következményeit. Az ilyen írásbeli nyilatkozatokról a Főtitkárságnak nyilvántartást kell vezetnie.
34. Amennyiben egy adott személyt olyan beosztásba készülnek kinevezni, amelyhez az érintett által jelenleg birtokoltnál eggyel magasabb szintű biztonsági tanúsítvány szükséges, a kinevezés ideiglenes jelleggel végrehajtható, amennyiben:
- a) a magasabb szintű EU-minősített adatokhoz való, sürgős feladat miatti hozzáférés szükségességét a személy felettese írásban igazolja;
 - b) a hozzáférés meghatározott EU-minősített adatokra korlátozódik a feladat elvégzése érdekében;
 - c) az érintett személy rendelkezik érvényes biztonsági tanúsítvánnyal vagy EU-minősített adatokhoz való hozzáférést lehetővé tevő engedéllyel;
 - d) intézkedés történt a beosztáshoz szükséges szintű hozzáférés engedélyeztetésére;
 - e) az illetékes hatóság megfelelően ellenőrizte, hogy az érintett biztonsági szabályokat súlyosan vagy ismétlődően nem sértett meg;
 - f) az érintett megbízását az illetékes hatóság jóváhagyta; valamint
 - g) a kivételes esetet – beleértve azon adat leírását, amelyhez a hozzáférést jóváhagyták – az illetékes nyilvántartó hivatal vagy alárendelt nyilvántartó hivatal feljegyzi.
35. A fenti eljárás az annál eggyel magasabb szintű EU-minősített adatokhoz való hozzáférés megadására alkalmazandó, mint amilyen szintre vonatkozóan a személy biztonsági ellenőrzését elvégezték. Ez az eljárás nem alkalmazható ismétlődő jelleggel.
36. Különösen kivételes körülmények között – például ellenséges környezetben végrehajtott missziók során vagy növekvő nemzetközi feszültség idején, amennyiben a sürgősségi intézkedések ezt megkívánják, különösen életmentés céljából – a tagállamok és a főtitkár vagy a főtitkárhelyettes lehetőség szerint írásban hozzáférést adhat CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz olyan személyek számára, akik nem rendelkeznek a szükséges biztonsági tanúsítvánnyal, feltéve, hogy ez az engedély feltétlenül szükséges, és nem merülnek fel megalapozott kétségek az érintett személy lojalitását, szavahihetőségét és megbízhatóságát illetően. A megadott engedélyt nyilvántartásba kell venni, és fel kell jegyezni, hogy milyen adatokhoz adtak hozzáférést.
37. A TRÈS SECRET UE/EU TOP SECRET minősítésű adat esetében az ilyen sürgősségi hozzáférést olyan uniós polgároknak kell korlátozni, akik a TRÈS SECRET UE/EU TOP SECRET szint nemzeti megfelelőjéhez vagy SECRET UE/EU SECRET minősítésű adatokhoz hozzáféréssel rendelkeznek.
38. A Biztonsági Bizottságot tájékoztatni kell azon esetekről, amikor a 36. és a 37. pontban foglalt eljárást ismétlődő jelleggel alkalmazzák.
39. Amennyiben egy tagállam nemzeti jogszabályai és rendelkezései szigorúbb szabályokat állapítanak meg az ideiglenes engedélyekkel, ideiglenes kinevezéssel, a minősített adatokhoz való egyszeri vagy sürgősségi hozzáféréssel kapcsolatban, az e szakaszban előírt eljárások csak a vonatkozó nemzeti jogszabályokban és rendelkezésekben foglalt korlátozásokkal alkalmazhatók.
40. A Biztonsági Bizottság részére éves jelentést kell készíteni az e szakaszban meghatározott eljárások alkalmazásáról.

VI. TANÁCSI ÜLÉSEKEN VALÓ RÉSZVÉTEL

41. A 28. pontra is figyelemmel, a Tanács vagy a Tanács előkészítő szerveinek CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat tárgyaló ülésein a részvétellel megbízott személyek csak biztonsági tanúsítványuk státusának megerősítését követően vehetnek részt. A tagállamok küldöttei esetében a PSCC-t vagy a biztonsági tanúsítvány egyéb bizonyítékát a megfelelő hatóságok továbbítják a Főtitkárság Biztonsági Hivatalának, vagy azt kivételes esetben az érintett küldött is benyújthatja. Adott esetben összesített névjegyzék használható, amely a biztonsági tanúsítvány meglétét bizonyítja.
42. Amennyiben az EU-minősített adatokhoz való hozzáférésre szóló PSC-t biztonsági okokból visszavonják egy olyan személytől, akinek feladatai megkövetelik a Tanács vagy a Tanács előkészítő szerveinek ülésein való részvételt, az illetékes hatóság tájékoztatja erről a Főtitkárságot.

VII. AZ EU-MINŐSÍTETT ADATOKHOZ VALÓ POTENCIÁLIS HOZZÁFÉRÉS

43. A futároknak, a biztonsági őröknek és a kísérőknek megfelelő szintű biztonsági ellenőrzésen kell átesniük, vagy a nemzeti jogszabályoknak és rendelkezéseknek megfelelő egyéb vizsgálaton kell átesniük, tájékoztatni kell őket az EU-minősített adatok védelmére szolgáló biztonsági eljárásokról és a rájuk bízott minősített adatok védelmét érintő feladataikról.
-

II. MELLÉKLET

FIZIKAI BIZTONSÁG

I. BEVEZETÉS

1. Ez a melléklet a 8. cikk végrehajtására vonatkozó rendelkezéseket határoz meg. Megállapítja az olyan helyiségek, épületek, irodák, termek és egyéb területek – többek között a CIS-nek helyet adó területek – fizikai védelmének minimumkövetelményeit, ahol EU-minősített adatokat kezelnek és tárolnak.
2. A fizikai biztonsági intézkedések célja az EU-minősített adatokhoz való jogosulatlan hozzáférés megakadályozása az alábbiak révén:
 - a) az EU-minősített adatok megfelelő módon való kezelésének és tárolásának a biztosítása;
 - b) a személyzet tagjainak szigorúan a szükséges ismeret elve és szükség szerint személyi biztonsági tanúsítványuk alapján történő megkülönböztetése az EU-minősített adatokhoz való hozzáférés tekintetében;
 - c) a jogosulatlan cselekményektől való elrettentés, azok megakadályozása és észlelése; valamint
 - d) behatolók titokban történő vagy erőszakos behatolásának megakadályozása vagy késleltetése.

II. FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK ÉS INTÉZKEDÉSEK

3. A fizikai biztonsági intézkedéseket az illetékes hatóságok által elvégzett fenyegetésvértékelés alapján kell megválasztani. A Főtitkárság és a tagállamok egyaránt kockázatkezelési eljárást alkalmaznak az EU-minősített adatoknak a saját területükön történő védelmére, a felmért kockázattal arányos mértékű fizikai védelem biztosítása érdekében. A kockázatkezelési folyamat figyelembe veszi az összes vonatkozó tényezőt, különösen az alábbiakat:
 - a) az EU-minősített adatok minősítési szintje;
 - b) az EU-minősített adatok megjelenési formája és mennyisége, szem előtt tartva, hogy nagy mennyiségű EU-minősített adat vagy ilyen adatok gyűjteménye szigorúbb védelmi intézkedések alkalmazását teheti szükségessé;
 - c) azon épületek vagy területek közvetlen környezete és kialakítása, ahol EU-minősített adatokat kezelnek, illetve tárolnak; valamint
 - d) az Unió vagy a tagállamok ellen tevékenykedő hírszerző szolgálatok tevékenységéből eredő fenyegetések, valamint a szabotázs, terrorizmus, felforgató tevékenységek vagy más bűncselekmények miatt fenyegető veszélyek.
4. A hatáskörrel rendelkező biztonsági hatóság a zónaszerű védelem elvének alkalmazásával meghatározza a végrehajtandó fizikai biztonsági intézkedések megfelelő kombinációját. Ezek közé az alábbiakban felsoroltak közül egy vagy több tartozhat:
 - a) kordon: fizikai akadály, amely védi a védelmet igénylő terület határát;
 - b) behatolásjelző rendszerek (IDS): behatolásjelző rendszereket a kordon nyújtotta védelem növelésére vagy termekben és épületekben a biztonsági személyzet helyett vagy annak támogatására lehet használni;
 - c) belépés-ellenőrzés: a belépés-ellenőrzés kiterjedhet egy adott helyszínre, egy adott helyszínen található épületre vagy épületekre, valamint épületen belüli területekre vagy termekre. Az ellenőrzés történhet elektronikus vagy elektromechanikus eszközökkel, a biztonsági személyzet és/vagy a recepció által vagy bármilyen más fizikai eszközzel;
 - d) biztonsági személyzet: képzett, felügyelt és – szükség esetén – megfelelő biztonsági ellenőrzésen átesett biztonsági személyzetet lehet alkalmazni többek között a titkos behatolást tervező személyek elrettentésére;
 - e) zárt láncú televízió (CCTV): nagy kiterjedésű területeken vagy körzetekben a biztonsági személyzet CCTV segítségével ellenőrizheti a biztonsági eseményeket és a behatolásjelző rendszer riasztásait;
 - f) biztonsági világítás: biztonsági világítás használható a lehetséges behatolók elrettentésére, valamint a biztonsági személyzet általi közvetlen vagy a CCTV-rendszeren keresztül közvetett, hatékony megfigyeléshez szükséges megvilágítás biztosítására; valamint
 - g) bármely más megfelelő fizikai intézkedés, amelynek célja az EU-minősített adatokhoz való jogosulatlan hozzáférés vagy az ilyen adat elvesztésének vagy megrongálódásának megakadályozása vagy észlelése.

5. Az illetékes hatóság jogosult lehet a be- és kiléptetésnél átvizsgálást végezni a nem engedélyezett anyagok bevitelétől vagy EU-minősített adatoknak a helyiségből vagy épületből történő engedély nélküli kivitelétől való elrettentés céljából.
6. Amennyiben EU-minősített adatokat – akár véletlenszerűen is – rálátás veszélye fenyeget, megfelelő intézkedéseket kell hozni e veszély kivédésére.
7. Az új létesítmények esetében a fizikai biztonsági követelményeket és azok funkcionális jellemzőit már a létesítmények tervezése során meg kell határozni. A már meglévő létesítmény esetében a fizikai biztonsági követelményeket a lehető legteljesebb mértékben meg kell valósítani.

III. AZ EU-MINŐSÍTETT ADATOK FIZIKAI VÉDELMERE SZOLGÁLÓ BERENDEZÉSEK

8. Az EU-minősített adatok fizikai védelmét szolgáló felszerelések (például biztonsági tárolóeszközök, iratmegsemmisítő gépek, ajtózárok, elektronikus beléptetőrendszerek, behatolásjelző rendszerek, riasztórendszerek) beszerzésekor az illetékes hatóság biztosítja, hogy a felszerelések megfeleljenek a jóváhagyott műszaki szabványoknak és minimum-követelményeknek.
9. Az EU-minősített adatok fizikai védelmére szolgáló felszerelések műszaki jellemzőit a Biztonsági Bizottság által jóváhagyandó biztonsági iránymutatások tartalmazzák.
10. A biztonsági rendszereket rendszeres időközönként ellenőrizni kell, a felszereléseket pedig rendszeresen karban kell tartani. A karbantartás során figyelembe kell venni az ellenőrzések eredményét annak biztosítása érdekében, hogy a felszerelések továbbra is a lehető leghatékonyabban működjenek.
11. Az egyes biztonsági intézkedések és a teljes biztonsági rendszer hatékonyságát minden ellenőrzés során újra kell értékelni.

IV. FIZIKAI VÉDELEMBEN RÉSZESÜLŐ TERÜLETEK

12. Az EU-minősített adatok fizikai védelmére két típusú, fizikai védelemben részesülő terület – vagy azok nemzeti megfelelői – kerül megállapításra:

- a) igazgatási területek; valamint
- b) biztonsági területek (köztük a technikailag biztosított biztonsági területek).

E határozatban az igazgatási területekre és a biztonsági területekre – így a technikailag biztosított biztonsági területekre – való valamennyi hivatkozás egyben azok nemzeti megfelelőire való hivatkozásként is értelmezendő.

13. Az illetékes biztonsági hatóság megállapítja, hogy az adott terület megfelel-e az igazgatási területként, biztonsági területként, technikailag biztosított biztonsági területként való kijelölés követelményeinek.

14. Az igazgatási területek esetében:

- a) láthatóan elhatárolt körzetet kell meghatározni, amely lehetővé teszi a személyek és lehetőség szerint a járművek ellenőrzését;
- b) a kíséret nélküli belépést csak az illetékes hatóság megfelelő engedélyével rendelkező személyek számára lehet megadni; valamint
- c) minden más személy mellé folyamatos kíséretet kell adni vagy ezzel egyenértékű ellenőrzésnek kell alávetni.

15. A biztonsági területek esetében:

- a) láthatóan elhatárolt és védett körzetet kell meghatározni, amelyen minden be- és kilépést beléptető vagy személyazonosító rendszerrel ellenőriznek;
- b) kíséret nélküli belépés kizárólag olyan személyek számára biztosítható, akik biztonsági ellenőrzésen estek át, és a szükséges ismeret elve alapján különleges engedéllyel rendelkeznek a területre való belépésre; valamint
- c) minden más személy mellé folyamatos kíséretet kell adni vagy ezzel egyenértékű ellenőrzésnek kell alávetni.

16. Amennyiben a biztosított területre való belépés az ott található minősített adatokhoz való közvetlen – bármilyen gyakorlati célt szolgáló – hozzáférést tesz lehetővé, az alábbi kiegészítő követelményeket kell alkalmazni:
- a) az adott területen általában tárolt adatok legmagasabb minősítési szintjét egyértelműen fel kell tüntetni;
 - b) minden látogatónak különleges engedéllyel kell rendelkeznie a területre való belépéshez, minden látogató mellé folyamatos kíséretet kell rendelni, és valamennyi látogatónak megfelelő biztonsági ellenőrzésen kell átesnie, kivéve, ha intézkedéseket tettek annak biztosítására, hogy EU-minősített adatokhoz ne legyen lehetséges a hozzáférés.
17. A lehallgatás ellen védett biztonsági területek a technikailag biztosított biztonsági terület megjelölést kapják. E területekre a következő kiegészítő követelmények vonatkoznak:
- a) az ilyen területeket behatolásgelző rendszerrel szerelik fel, használaton kívül zárva tartják, használat esetén pedig őrzik. Az VI. szakasszal összhangban valamennyi kulcsot ellenőrizni kell;
 - b) az e területekre belépő személyeket és anyagokat ellenőrizni kell;
 - c) e területeket rendszeres fizikai és/vagy technikai ellenőrzéseknek kell alávetni az illetékes biztonsági hatóság előírásainak megfelelően. Ezeket az ellenőrzéseket illetéktelen behatolás vagy annak gyanúja esetén is el kell végezni; valamint
 - d) az ilyen területeken nem lehetnek engedély nélküli kommunikációs vonalak, engedély nélküli telefonvonalak és más engedély nélküli eszközök és elektromos vagy elektronikus berendezések.
18. A 17. pont d) alpontja ellenére minden kommunikációs, elektromos vagy elektronikus berendezést – mielőtt olyan területen használnák őket, ahol SECRET UE/EU SECRET vagy magasabb szintű minősített adatokat érintő üléseket tartanak vagy munkát végeznek, valamint az EU-minősített adatot fenyegető, nagy kockázatúnak értékelt veszély esetén – először az illetékes biztonsági hatóságnak meg kell vizsgálnia annak biztosítása érdekében, hogy ilyen berendezés révén véletlenül vagy tiltott módon ne közvetíthessenek értelmezhető adatokat az adott biztosított területen kívülre.
19. Azokat a biztosított területeket, ahol nem tartózkodik napi 24 órán át munkavégző személyzet, adott esetben a rendes munkaidő végén ellenőrizni, valamint a rendes munkaidőn kívül szűrőpróbaszerűen ellenőrizni kell, amennyiben az említett területeken nem működik behatolásgelző rendszer.
20. Biztonsági területeket és technikailag biztosított biztonsági területeket ideiglenesen is fel lehet állítani valamely igazgatási területen belül, minősített üléshöz vagy más hasonló célból.
21. Minden egyes biztonsági terület tekintetében ki kell dolgozni a biztonsági szabályzatot, amely az alábbiakat tartalmazza:
- a) a területen kezelt és tárolt EU-minősített adatok minősítési szintje;
 - b) a fenntartandó ellenőrzési és védelmi intézkedések;
 - c) a szükséges ismeret elve és biztonsági tanúsítvány alapján a területre kíséret nélkül való belépésre engedéllyel rendelkező személyek;
 - d) adott esetben a kíséretre vagy az EU-minősített adatok védelmére vonatkozó eljárások minden más személynek a területre való belépése engedélyezésekor; valamint
 - e) minden más vonatkozó intézkedés és eljárás.
22. A biztonsági területeken megerősített helyiségeket kell kialakítani. Az illetékes biztonsági hatóságnak ellenőriznie kell a falakat, padlókat, plafonokat, ablakokat és zárható ajtókat, amelyeknek az ugyanilyen minősítési szintű EU-minősített adat tárolásához jóváhagyott tárolóeszköz által nyújtottal egyenértékű védelmet kell biztosítaniuk.
- V. AZ EU-MINŐSÍTETT ADAT KEZELÉSÉRE ÉS TÁROLÁSÁRA VONATKOZÓ FIZIKAI VÉDELMI INTÉZKEDÉSEK
23. Az olyan EU-minősített adatot, amely RESTREINT UE/EU RESTRICTED minősítésű, az alábbi helyeken lehet kezelni:
- a) biztonsági területen;
 - b) igazgatási területen, amennyiben az EU-minősített adat védve van az engedéllyel nem rendelkező egyének hozzáféréstől; vagy
 - c) biztonsági területen vagy igazgatási területen kívül, amennyiben az adat birtokosa a III. melléklet 28–41. pontjával összhangban szállítja az EU-minősített adatot, és vállalta, hogy eleget tesz az illetékes nemzeti biztonsági hatóság által az EU-minősített adatok engedéllyel nem rendelkező személyek általi hozzáféréssel szembeni védelme céljából kiadott biztonsági utasításokban foglalt kiegészítő intézkedéseknek.

24. Az olyan EU-minősített adatot, amely RESTREINT UE/EU RESTRICTED minősítésű, megfelelően zárható irodabútorokban kell tárolni igazgatási vagy biztosított területen. Ideiglenesen biztosított területen vagy igazgatási területen kívül is lehet tárolni, amennyiben az adat birtokosa vállalta, hogy eleget tesz az illetékes biztonsági hatóság által kiadott biztonsági utasításokban foglalt kiegészítő intézkedéseknek.
25. Az olyan EU-minősített adatot, amely CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű, az alábbi helyeken lehet kezelni:
- a) biztonsági területen;
 - b) igazgatási területen, amennyiben az EU-minősített adat védve van az engedéllyel nem rendelkező egyének hozzáféréstől; vagy
 - c) biztonsági területen vagy igazgatási területen kívül, amennyiben az adat birtokosa:
 - i. a III. melléklet 28–41. pontjával összhangban szállítja az EU-minősített adatot;
 - ii. vállalta, hogy eleget tesz az illetékes nemzeti biztonsági hatóság által az EU-minősített adatok engedéllyel nem rendelkező személyek általi hozzáféréssel szembeni védelme céljából kiadott biztonsági utasításokban foglalt kiegészítő intézkedéseknek;
 - iii. az EU-minősített adatot mindenkor személyes felügyelete alatt tartja; valamint
 - iv. papíralapú dokumentumok esetében értesítette erről az érintett nyilvántartót.
26. A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatot biztonsági területen kell tárolni biztonsági tárolóeszközben vagy megerősített helyiségben.
27. A TRÈS SECRET UE/EU TOP SECRET minősítésű adatokat biztonsági területen kell kezelni.
28. A TRÈS SECRET UE/EU TOP SECRET minősítésű adatokat biztonsági területen az alábbi módok valamelyike szerint kell tárolni:
- a) a 8. pont szerinti biztonsági tárolóeszközben, az alábbiak közül legalább egy kiegészítő ellenőrzés kíséretében:
 - i. ellenőrzött biztonsági vagy munkavégző személyzet általi folyamatos védelem vagy ellenőrzés;
 - ii. jóváhagyott behatolásjelző rendszer, reagáló biztonsági személyzettel együttesen;
 - b) behatolásjelző rendszerrel ellátott megerősített helyiségben, reagáló biztonsági személyzettel együttesen.
29. Az EU-minősített adatok fizikailag védett területeken kívüli szállítására vonatkozó szabályokat a III. melléklet tartalmazza.

VI. AZ EU-MINŐSÍTETT ADATOK VÉDELMÉRE SZOLGÁLÓ KULCSOK ÉS KOMBINÁCIÓK ELLENŐRZÉSE

30. Az illetékes biztonsági hatóság meghatározza az irodák, termek, megerősített helyiségek és biztonsági tárolóeszközök kulcsainak és kombinációinak kezelésére vonatkozó eljárásokat. Ezek az eljárások a jogosulatlan hozzáféréssel szembeni védelmet biztosítják.
31. A kombinációkat kívülről meg kell tanulnia annak a lehető legkisebb számú személyzetnek, akinek azokat ismernie kell. Az EU-minősített adatok tárolására szolgáló biztonsági tárolóeszközök és megerősített helyiségek kombinációit az alábbi esetekben meg kell változtatni:
- a) új tárolóeszköz átvételekor;
 - b) a kombinációt ismerő személyzet minden változásakor;
 - c) ha azok ténylegesen illetéktelen személy tudomására jutottak vagy ennek gyanúja merült fel;
 - d) amikor a záron javítást vagy karbantartást végeztek; valamint
 - e) legalább 12 havonta.

III. MELLÉKLET

A MINŐSÍTETT ADATOK KEZELÉSE

I. BEVEZETÉS

1. Ez a melléklet a 9. cikk végrehajtására vonatkozó rendelkezéseket határoz meg. Megállapítja az EU-minősített adat teljes életciklusán keresztüli ellenőrzésére szolgáló adminisztratív intézkedéseket az ilyen adat szándékos vagy véletlenszerű illetéktelen tudomására jutásától vagy elvesztésétől való elrettentéshez és annak észleléséhez való hozzájárulás érdekében.

II. A MINŐSÍTÉS SZABÁLYAI

Minősítések és jelölések

2. Az adatokat akkor kell minősíteni, ha a titkosságuk biztosításához védelemre van szükségük.
3. Az EU-minősített adatok minősítési szintjének a megfelelő minősítési útmutató szerinti meghatározásáért és a címzettekhez történő továbbításáért az adat kibocsátója felel.
4. Az EU-minősített adatok minősítési szintjét a 2. cikk (2) bekezdésével összhangban, valamint a 3. cikk (3) bekezdésével összhangban jóváhagyandó biztonsági politikára hivatkozással kell meghatározni.
5. A minősítést és jelölést egyértelműen és helyesen fel kell tüntetni, tekintet nélkül arra, hogy az EU-minősített adat papír, szóbeli, elektronikus vagy egyéb formájú.
6. Egy adott dokumentum egyes részei (például oldalai, bekezdései, szakaszai, mellékletei, függelékei, toldalékai és csatolmányai) eltérő minősítést igényelhetnek, és ennek megfelelő jelölést kell kapniuk, többek között az elektronikus formában történő tárolásuk alkalmával.
7. A dokumentum vagy a fájl egésze a legmagasabb minősítési szintű rész minősítését kapja. Ha egy dokumentumot különböző forrásokból származó adatokból állítanak össze, a kész anyagot a minősítési szint meghatározása céljából át kell nézni, mivel összességében magasabb szintű minősítést igényelhet, mint egyes részei külön-külön.
8. A különböző minősítési szintű részeket tartalmazó dokumentumokat lehetőség szerint úgy kell szerkeszteni, hogy az eltérő minősítésű részek könnyen felismerhetők és szükség esetén leválaszthatók legyenek.
9. A mellékleteket kísérő levél vagy feljegyzés ugyanolyan minősítést kap, mint legmagasabb minősítési szintű melléklete. A kibocsátónak megfelelő jelöléssel egyértelműen jeleznie kell, hogy a kísérő levél vagy feljegyzés milyen szintű minősítést kap, ha a mellékleteitől elválasztják, például a következő formában:

CONFIDENTIEL UE/EU CONFIDENTIAL

A RESTREINT UE/EU RESTRICTED minősítésű melléklet(ek) nélkül

Jelölések

10. A 2. cikk (2) bekezdésében meghatározott minősítési jelölések mellett az EU-minősített adatok további jelölésekkel láthatók el, úgymint:
 - a) a kibocsátó megjelölésére szolgáló azonosító;
 - b) különleges kezelési utasítás, kód vagy betűszó a dokumentum által érintett tevékenységi terület vagy a szükséges ismeret elve alapján történő továbbítási vagy felhasználási korlátozások meghatározására;
 - c) a kiadhatóságra vonatkozó jelölések; vagy
 - d) adott esetben azon időpont vagy konkrét esemény, amelyet követően a minősített adat visszaminősíthető vagy a minősítés megszüntethető.

Rövidített minősítési jelölések

11. Egy adott szöveg egyes bekezdései minősítési szintjének jelölésére egységes rövidített minősítési jelölések használhatók. A rövidítések nem helyettesítik a teljesen kiírt minősítési jelöléseket.

12. Az EU-minősített dokumentumokon belül a szöveg egy oldalnál kisebb terjedelmű szakaszainak vagy részeinek minősítési szintje a következő egységes rövidítésekkel jelölhető:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

EU-minősített dokumentumok létrehozása

13. EU-minősített dokumentum létrehozásakor:

- a) minden egyes oldalon jól láthatóan szerepeltetni kell a minősítési jelölést;
- b) minden egyes oldalt számozni kell;
- c) a dokumentumnak nyilvántartási számmal és tárggyal kell rendelkeznie, amely önmagában nem minősített adat, kivéve, ha akként jelölik;
- d) a dokumentumot dátummal kell ellátni; valamint
- e) a SECRET UE/EU SECRET és magasabb minősítési szintű dokumentumok minden egyes oldalán fel kell feltüntetni a példány sorszámát, ha azokat több példányban továbbítják.

14. Amennyiben az EU-minősített adatokra a 13. pont nem alkalmazható, a 6. cikk (2) bekezdése értelmében kialakítandó biztonsági iránymutatásoknak megfelelő intézkedéseket kell hozni.

EU-minősített adatok visszaminősítése és a minősítés megszüntetése

15. Az adat létrehozásakor – amennyiben lehetséges és különösen RESTREINT UE/EU RESTRICTED minősítésű adat esetén – a kibocsátó jelöli, hogy adott időpontban vagy konkrét eseményt követően az EU-minősített adat visszaminősíthető-e vagy minősítése megszüntethető-e.
16. A Főtitkárság rendszeresen felülvizsgálja az általa őrzött EU-minősített adatokat annak megállapítására, hogy minősítésük még érvényes-e. A Főtitkárság kialakít egy rendszert az általa kibocsátott EU-minősített adatok minősítésének legalább ötévenkénti felülvizsgálatára. Nincs szükség ilyen felülvizsgálatra akkor, ha a kibocsátó már kezdetben jelezte, hogy az adatot automatikusan vissza fogják minősíteni vagy a minősítését meg fogják szüntetni, és az adatot ennek megfelelően jelölték.

III. EU-MINŐSÍTETT ADATOK BIZTONSÁGI CÉLÚ NYILVÁNTARTÁSBA VÉTELE

17. A Főtitkárság vagy a tagállamok nemzeti közigazgatásai keretében működő, EU-minősített adatot kezelő valamennyi szervezeti egységénél nyilvántartót kell kialakítani, amely biztosítja, hogy az EU-minősített adatok kezelése e határozattal összhangban történjen. A nyilvántartókat a II. mellékletben meghatározott biztonsági területeken kell létrehozni.
18. E határozat alkalmazásában a biztonsági célú nyilvántartásba vétel (a továbbiakban: a nyilvántartásba vétel) olyan eljárások alkalmazása, amelyek során rögzítésre kerül az anyag életciklusa, beleértve a továbbítását és a megsemmisítését is.
19. Valamennyi CONFIDENTIEL UE/EU CONFIDENTIAL és annál magasabb minősítésű anyagot a szervezeti egységhez való beérkezés vagy onnan történő elküldés alkalmával külön erre a célra szolgáló nyilvántartásokban kell kezelni.
20. A Főtitkárság központi nyilvántartója nyilvántartást vezet a Tanács és a Főtitkárság által harmadik államok és nemzetközi szervezetek részére átadott valamennyi minősített adatról, valamint a harmadik államoktól vagy nemzetközi szervezetektől érkezett valamennyi minősített adatról.
21. CIS esetében a végrehajtandó nyilvántartási eljárások a CIS-beli folyamatok keretében is elvégezhetők.
22. A Tanács jóváhagyja az EU-minősített adatoknak biztonsági célú nyilvántartásba vételére vonatkozó biztonsági politikát.

TRÈS SECRET UE/EU TOP SECRET nyilvántartók

23. A tagállamokban és a Főtitkárságon ki kell jelölni a TRÈS SECRET UE/EU TOP SECRET minősítésű adatok központosított kézhezvételével és elosztásával megbízott központi nyilvántartót. Szükség esetén ennek alárendelt nyilvántartók is kijelölhetők ezen adatok nyilvántartására és kezelésére.
24. Az alárendelt nyilvántartók nem továbbíthatnak közvetlenül TRÈS SECRET UE/EU TOP SECRET dokumentumokat az ugyanazon TRÈS SECRET UE/EU TOP SECRET minősítéssel rendelkező, központi nyilvántartóhoz tartozó többi alárendelt nyilvántartó számára vagy kifelé e központi nyilvántartó kifejezett írásbeli jóváhagyása nélkül.

IV. EU-MINŐSÍTETT DOKUMENTUMOK MÁSOLÁSA ÉS FORDÍTÁSA

25. TRÈS SECRET UE/EU TOP SECRET minősítésű dokumentumok kizárólag a kibocsátó előzetes írásbeli hozzájárulásával másolhatók vagy fordíthatók le.
26. Amennyiben a SECRET UE/EU SECRET és ennél alacsonyabb minősítésű dokumentumok kibocsátója a másolásra vagy fordításra vonatkozóan nem szabott korlátozásokat, e dokumentumok a titokbirtokos utasítására másolhatók vagy fordíthatók.
27. Az eredeti dokumentumra vonatkozó biztonsági intézkedéseket a másolatokra és a fordításokra is alkalmazni kell.

V. EU-MINŐSÍTETT ADATOK SZÁLLÍTÁSA

28. Az EU-minősített adatok szállítására a 30–41. pontban szereplő védelmi intézkedések vonatkoznak. Az EU-minősített adatok elektronikus eszközökön történő szállítása során – a 9. cikk (4) bekezdésétől eltérően – az alább előírt védelmi intézkedéseket – az elvesztés vagy az illetéktelen tudomására jutás kockázatának minimalizálása érdekében – kiegészíthetik az illetékes biztonsági hatóság által előírt, megfelelő technikai ellenintézkedések.
29. A Főtitkárság és a tagállamok illetékes biztonsági hatóságai utasításokat bocsátanak ki az EU-minősített adatok e határozattal összhangban történő szállítására vonatkozóan.

Épületen vagy zárt épületcsoporton belüli szállítás

30. A valamely épületen vagy zárt épületcsoporton belül szállított EU-minősített adatokat az azok tartalmába való betekintés megakadályozása érdekében le kell takarni.
31. TRÈS SECRET UE/EU TOP SECRET minősítésű adatokat adott épületen vagy zárt épületcsoporton belül lezárt borítékban kell szállítani, amelyen kizárólag a címzett neve tüntethető fel.

Az Unión belül

32. Az Unión belül épületek vagy létesítmények között szállított EU-minősített adatokat oly módon kell becsomagolni, hogy azok védettek legyenek az illetéktelen hozzáféréstől.
33. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatoknak az Unión belüli szállítása az alábbi módok valamelyikén történik:

a) katonai, kormányzati vagy diplomáciai futár, az esetnek megfelelően;

b) kézi szállítás, amennyiben:

i. az EU-minősített adat a szállítást végző személy birtokában marad, kivéve, ha azt a II. mellékletben foglalt követelményekkel összhangban tárolják;

ii. az EU-minősített adatot tartalmazó csomagot útközben nem nyitják ki vagy olvassák nyilvános helyen;

iii. az érintett személyeket tájékoztatják a biztonsággal kapcsolatos felelősségükről; valamint

iv. az érintetteket szükség esetén futárigazolvánnyal látják el;

c) postaszolgálatok vagy kereskedelmi futárszolgálatok, feltéve, hogy:

i. azokat a megfelelő nemzeti biztonsági hatóság a nemzeti jogszabályokkal és rendelkezésekkel összhangban jóváhagyta; valamint

ii. azokat a 6. cikk (2) bekezdése értelmében kialakítandó biztonsági iránymutatásokban meghatározandó minimális követelményeknek megfelelő védelmi intézkedéseket alkalmaznak.

Egyik tagállamból másikba történő szállítás esetén a c) alpont rendelkezései kizárólag a CONFIDENTIEL UE/EU CONFIDENTIAL adatokra alkalmazandók.

34. A RESTREINT UE/EU RESTRICTED minősítésű adatok postaszolgálatokkal, illetve kereskedelmi futárszolgálatokkal is szállíthatók. Az ilyen adatok szállításához futárigazolvány nem szükséges.
35. Az olyan CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű anyagokat (pl. gépek vagy berendezések), amelyek a 33. pontban említett módon nem szállíthatók, kereskedelmi fuvarozók az V. mellékletnek megfelelően szállítmánycént szállítják.
36. TRÈS SECRET UE/EU TOP SECRET minősítésű adatok szállítása az Unión belül épületek vagy létesítmények között az adott esetben megfelelően katonai, kormányzati vagy diplomáciai futár révén történik.

Szállítás az Unióból valamely harmadik állam területére

37. Az Unióból valamely harmadik állam területére szállított EU-minősített adatot úgy kell becsomagolni, hogy az védve legyen az illetéktelen hozzáféréstől.
 38. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatoknak az Unióból valamely harmadik állam területére történő szállítása az alábbi módok valamelyikén történik:
 - a) katonai vagy diplomáciai futár;
 - b) kézi szállítás, amennyiben:
 - i. a csomag hivatalos pecséttel van ellátva, vagy oly módon van becsomagolva, amelyből kiderül, hogy az hivatalos küldemény és nem képezi vámvizsgálat vagy biztonsági ellenőrzés tárgyát;
 - ii. a szállítást végző személyek a csomagot azonosító és őket a csomag szállítására felhatalmazó futárigazolvánnyal rendelkeznek;
 - iii. az EU-minősített adat a szállítást végző személy birtokában marad, kivéve, ha azt a II. mellékletben foglalt követelményekkel összhangban tárolják;
 - iv. az EU-minősített adatot tartalmazó csomagot útközben nem nyitják ki vagy olvassák nyilvános helyen; valamint
 - v. az érintett személyeket tájékoztatják biztonsági felelősségi körükről.
 39. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű, az Unió által harmadik ország vagy nemzetközi szervezet részére átadott adatok szállítását a 13. cikk (2) bekezdésének a), illetve b) pontja szerinti adatbiztonsági megállapodások vagy igazgatási megállapodások vonatkozó rendelkezéseivel összhangban kell végezni.
 40. RESTREINT UE/EU RESTRICTED minősítésű adatok postaszolgálatok vagy kereskedelmi futárszolgálatok révén is szállíthatók.
 41. TRÈS SECRET UE/EU TOP SECRET minősítésű adatoknak az Unióból harmadik állam területére történő szállítása katonai vagy diplomáciai futár útján történik.
- #### **VI. EU-MINŐSÍTETT ADATOK MEGSEMISÍTÉSE**
42. A már nem szükséges EU-minősített dokumentumok – az archiválásra vonatkozó szabályok és rendelkezések sérelme nélkül – megsemmisíthetők.
 43. A dokumentumok birtokosainak vagy az illetékes hatóságnak az utasítására a felelős nyilvántartó hivatal semmisíti meg azokat a dokumentumokat, amelyekre a 9. cikk (2) bekezdésével összhangban nyilvántartásba vétel vonatkozik. Az iktatókönyveket és egyéb nyilvántartásokat ennek megfelelő módon aktualizálni kell.
 44. A SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET minősítésű dokumentumok esetében a megsemmisítést tanú jelenlétében kell végrehajtani, akinek a megsemmisítendő dokumentum minősítési szintjével legalább megegyező minősítésű adatok megismerésére jogosító személyi biztonsági tanúsítvánnyal kell rendelkeznie.
 45. Az ügykezelő és – amennyiben annak jelenléte kötelező – a tanú aláírja a megsemmisítési jegyzőkönyvet, amelyet a nyilvántartóban kell iktatni. A nyilvántartó a megsemmisítési jegyzőkönyveket TRÈS SECRET UE/EU TOP SECRET minősítésű dokumentumok esetében legalább tíz évig, a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok esetében pedig legalább öt évig őrzi meg.

46. A minősített dokumentumokat – ideértve a RESTREINT UE/EU RESTRICTED minősítéssel rendelkezőket is – a vonatkozó uniós vagy az ezzel egyenértékű szabványoknak, vagy a tagállamok által a nemzeti műszaki szabványokkal összhangban jóváhagyott szabványoknak megfelelően kell megsemmisíteni, megakadályozandó az adott dokumentum egészének vagy egy részének helyreállítását.
47. Az EU-minősített adatok tárolására szolgáló számítógépes adathordozókat a IV. melléklet 37. pontjával összhangban kell megsemmisíteni.
48. Vészhelyzet esetén, ha illetéktelen hozzáférés közvetlen kockázata áll fenn, a tulajdonosnak meg kell semmisítenie az EU-minősített adatokat úgy, hogy azokat sem részben, sem egészben ne lehessen helyreállítani. A nyilvántartásba vett EU-minősített adatok vészhelyzeti megsemmisítéséről tájékoztatni kell az adatok kibocsátóját és a származási nyilvántartót.

VII. ÉRTÉKELŐ LÁTOGATÁSOK

49. Az „értékelő látogatás” kifejezést a továbbiakban:

- a) a 9. cikk (3) bekezdése és a 16. cikk (2) bekezdésének e), f) és g) pontja szerinti ellenőrzések vagy értékelő látogatások; vagy
- b) a 13. cikk (5) bekezdése szerinti értékelő látogatások megjelölésére kell alkalmazni,

amelyek célja az EU-minősített adatok védelme tekintetében végrehajtott intézkedések hatékonyságának az értékelése.

50. Értékelő látogatásokat kell végezni többek között a következők céljából:

- a) az EU-minősített adatok védelme tekintetében az e határozatban megállapított minimumszabályok tiszteletben tartásának a biztosítása;
- b) a biztonság fontosságának és a hatékony kockázatkezelésnek a hangsúlyozása az ellenőrzött szervezeteken belül;
- c) ellenintézkedések ajánlása a minősített adatok bizalmas jellegének, sértetlenségének vagy rendelkezésre állásának sérülése által okozott hatás enyhítésére; valamint
- d) a biztonsági hatóságok folyamatban lévő biztonsági oktatási és tudatosságnövelő programjainak erősítése.

51. A Tanács minden naptári év végéig elfogadja a következő évre vonatkozó, a 16. cikk (1) bekezdésének c) pontjában előírt értékelő látogatási programot. Az egyes értékelő látogatások tényleges időpontja az érintett uniós szervvel vagy ügynökséggel, tagállammal, harmadik állammal vagy nemzetközi szervezettel egyetértésben kerül meghatározásra.

Az értékelő látogatások lefolytatása

52. Az értékelő látogatások célja a meglátogatott szervezet vonatkozó szabályainak, rendelkezéseinek és eljárásainak, valamint annak az ellenőrzése, hogy a szervezetnél alkalmazott gyakorlatok megfelelnek-e az e határozatban és a minősített adatoknak az adott szervezettel való cseréjére vonatkozó rendelkezésekben foglalt alapelveknek és minimumszabályoknak.
53. Az értékelő látogatások végrehajtása két szakaszban történik. Maga a látogatás előtt – adott esetben – előkészítő ülésre kerül sor az érintett szervezettel. Ezen előkészítő ülést követően az értékelő látogatást végző csoport – az érintett szervezettel egyetértésben – részletes értékelő látogatási programot dolgoz ki, amely a biztonság valamennyi területére kiterjed. Az értékelő látogatást végző csoportnak hozzáféréssel kell rendelkeznie minden olyan helyszínhez, ahol EU-minősített adatot kezelnek, különösen a nyilvántartókhoz és a CIS kapcsolódási pontjaihoz.
54. A tagállamok nemzeti közigazgatásában, harmadik államokban és nemzetközi szervezeteknél tett értékelő látogatásokat a meglátogatott szervezet, a harmadik állam vagy a nemzetközi szervezet tisztviselőivel teljes mértékben együttműködve kell végezni.
55. Az e határozatot vagy az e határozatban foglalt elveket alkalmazó uniós szerveknél, ügynökségeknél és szervezeteknél tett értékelő látogatásokat azon nemzeti biztonsági hatóság szakértői segítségével kell végrehajtani, amelynek területén a szerv vagy az ügynökség található.
56. Az e határozatot vagy az e határozatban foglalt elveket alkalmazó uniós szerveknél, ügynökségeknél és szervezeteknél, valamint a harmadik államoknál és nemzetközi szervezeteknél tett értékelő látogatások esetében a nemzeti biztonsági hatóság szakértőinek segítségét és hozzájárulását lehet kérni, a Biztonsági Bizottság által meghatározandó részletes szabályokkal összhangban.

Jelentések

57. Az értékelő látogatás végeztével a főbb következtetéseket és ajánlásokat ismertetni kell a meglátogatott szervezettel. Ezt követően jelentést kell készíteni az értékelő látogatásról. Amennyiben korrekciós intézkedéseket javasolnak és ajánlásokat fogalmaznak meg, úgy a jelentésnek elegendő adatot kell tartalmaznia a levont következtetések alátámasztására. A jelentést továbbítani kell a meglátogatott szervezet megfelelő hatósága részére.

58. A tagállamok nemzeti közigazgatásában végrehajtott értékelő látogatások esetében:

- a) az érintett nemzeti biztonsági hatósághoz eljuttatják az értékelő látogatásról szóló jelentés tervezetét, a benne szereplő tények helyességének és annak ellenőrzésére, hogy az nem tartalmaz RESTREINT UE/EU RESTRICTED szintnél magasabb minősítésű adatokat; valamint
- b) amennyiben az érintett tagállam nemzeti biztonsági hatósága nem kéri, hogy az értékelési jelentéseket ne terjesszék általánosan, úgy azokat el kell juttatni a Biztonsági Bizottsághoz. A jelentésnek RESTREINT UE/EU RESTRICTED minősítésűnek kell lennie.

A Főtitkárság biztonsági hatóságának (Biztonsági Hivatalának) felelőssége mellett rendszeresen jelentést kell készíteni a tagállamokban egy adott időszakban végrehajtott értékelő látogatásból levont tanulságok kiemelése céljából, amely jelentést a Biztonsági Bizottságnak meg kell vizsgálnia.

59. A harmadik államokban és nemzetközi szervezeteknél tett értékelő látogatások esetében a jelentést a Biztonsági Bizottságnak kell továbbítani. A jelentésnek legalább RESTREINT UE/EU RESTRICTED minősítésűnek kell lennie. A nyomon követő látogatás során valamennyi korrekciós intézkedést ellenőrizni kell, és ezen intézkedésekről jelentést kell tenni a Biztonsági Bizottságnak.

60. Az e határozatot vagy az e határozatban foglalt elveket alkalmazó uniós szerveknél, ügynökségeknél és szervezeteknél tett értékelő látogatások esetén, az értékelő látogatásokról szóló jelentéseket el kell küldeni a Biztonsági Bizottságnak. Az értékelő látogatásról szóló jelentés tervezetét eljuttatják az érintett ügynökséghez vagy szervhez a benne szereplő tények helyességének és annak ellenőrzésére, hogy az nem tartalmaz RESTREINT UE/EU RESTRICTED szintnél magasabb minősítésű adatokat. A nyomon követő látogatás során valamennyi korrekciós intézkedést ellenőrizni kell, és ezen intézkedésekről jelentést kell tenni a Biztonsági Bizottságnak.

61. A Főtitkárság biztonsági hatósága az 50. pontban meghatározott célok érdekében rendszeres ellenőrzéseket folytat a Főtitkárság szervezeti egységeinél.

Ellenőrző lista

62. A Főtitkárság biztonsági hatósága (a Biztonsági Hivatal) az értékelő látogatás során használandó, az ellenőrizendő elemeket tartalmazó listát készít és azt frissíti. Ezt az ellenőrző listát továbbítani kell a Biztonsági Bizottság részére.

63. Az ellenőrző lista kitöltéséhez szükséges adatokat – különösen a látogatás során – az ellenőrzött szervezet biztonsági vezetőitől kell beszerezni. Az ellenőrző listát a részletes kitöltést követően az ellenőrzött szervvel egyetértésben minősíteni kell. E lista nem képezi az ellenőrzési jelentés részét.

IV. MELLÉKLET

A CIS-BEN KEZELT EU-MINŐSÍTETT ADATOK VÉDELME

I. BEVEZETÉS

1. Ez a melléklet a 10. cikk végrehajtására vonatkozó rendelkezéseket határoz meg.
2. A CIS-ben folytatott műveletek biztonsága és helyes működése tekintetében alapvető fontosságúak az információvédelem következő jellemzői és szempontjai:

Hitelesség:	annak garanciája, hogy az információ valódi és jóhiszemű forrásokból származik;
Rendelkezésre állás:	az engedéllyel rendelkező szervezet kérelemére megvalósuló hozzáférhetőség és felhasználhatóság;
Bizalmasság:	annak garanciája, hogy az információ nem hozzáférhető illetéktelen személy, szervezet vagy folyamat részére;
Sértetlenség:	az információk és eszközök hitelességének és teljességének védelme;
Letagadhatatlanság:	egy cselekmény vagy esemény megtörténtének bizonyíthatósága annak érdekében, hogy ezt a cselekedetet vagy eseményt később ne lehessen letagadni.

II. INFORMÁCIÓVÉDELMI ELVEK

3. Az alábbiakban foglalt rendelkezések képezik az EU-minősített adatokat kezelő minden CIS biztonságosságának alapját. E rendelkezések végrehajtásának részletes követelményeit az információvédelmi biztonsági előírások és biztonsági iránymutatások határozzák meg.

Biztonsági kockázatkezelés

4. A biztonsági kockázatkezelés a CIS meghatározásának, kialakításának, működtetésének és fenntartásának szerves részét képezi. A kockázatkezelést (értékelés, tulajdonképpeni kezelés, elfogadás, kommunikáció) ismétlődő folyamatként kell elvégezni, a rendszertulajdonosok, projekthatóságok, működtető hatóságok és biztonsági jóváhagyó hatóságok képviselőivel közösen, egy kipróbált, átlátható és teljes mértékben érthető kockázatértékelési folyamat alkalmazásával. A CIS alkalmazási körét és eszközeit a kockázatkezelési folyamat kezdetekor egyértelműen meg kell határozni.
5. Az illetékes hatóságoknak át kell tekinteniük a CIS-t fenyegető potenciális veszélyeket, valamint naprakész és pontos, az aktuális működési környezetet tükröző fenyegetésértékeléssel kell rendelkezniük. A változó információtechnológiai környezettel való lépéstartás érdekében folyamatosan frissíteniük kell a sebezhetőségi kérdésekkel kapcsolatos ismereteiket, és rendszeresen felül kell vizsgálniuk a sebezhetőségi értékeléseket.
6. A biztonsági kockázatkezelés célja olyan biztonsági intézkedések alkalmazása, melyek eredményeképpen kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a fennmaradó biztonsági kockázatok között.
7. Egy adott CIS akkreditálásának vonatkozásában a megfelelő biztonsági akkreditációs hatóság által meghatározott különös követelményeknek, nagyságrendnek és részletességnek arányban kell állnia a valamennyi vonatkozó tényező figyelembevételével – a CIS-ben kezelt EU-minősített adatok minősítési szintjét is beleértve – megállapított kockázattal. Az akkreditáció magában foglalja a fennmaradó kockázat hivatalos megállapítását és a fennmaradó kockázatnak a felelős hatóság általi elfogadását.

Biztonság a CIS teljes életciklusán keresztül

8. A biztonság a CIS teljes életciklusa alatt követelmény, az indítástól kezdve egészen a működésből való kivonásig.
9. Az életciklus minden szakaszára meg kell állapítani a CIS-ben érintett egyes résztvevők biztonsági szerepét és a biztonság tekintetében a többi résztvevővel folytatott interakcióját.
10. A CIS-t – a technikai és nem technikai biztonsági intézkedéseket is beleértve – az akkreditációs folyamat során biztonsági tesztelésnek kell alávetni a kellő biztonsági szintről való meggyőződés érdekében, valamint annak ellenőrzése céljából, hogy azt helyesen telepítették, integrálták és konfigurálták.

11. A biztonsági értékeléseket, ellenőrzéseket és felülvizsgálatokat a CIS működése és karbantartása során, valamint rendkívüli körülmények felmerülése esetén rendszeresen ismételni kell.
12. A CIS biztonsági dokumentációja az életciklusa alatt a változás- és konfigurációkezelés szerves részeként folyamatosan fejlődik.

Legjobb gyakorlat

13. A Főtitkárság és a tagállamok együttműködnek a CIS-ben kezelt EU-minősített adatok védelmére vonatkozó legjobb gyakorlat kialakítása érdekében. A legjobb gyakorlatra vonatkozó iránymutatások tartalmazzák a CIS-szel kapcsolatos, az adott fenyegetésekkel és sebezhetőségekkel szemben bizonyítottan hatékony technikai, fizikai, szervezeti és eljárási biztonsági intézkedéseket.
14. A CIS-ben kezelt EU-minősített adatok védelme az információvédelemben részt vevő – az Unión belüli és kívüli – szervezetek által levont tanulságokra épül.
15. A legjobb gyakorlat terjesztése és azt követő végrehajtása hozzájárul a Főtitkárság és az EU-minősített adatot kezelő tagállamok által működtetett, különböző CIS-ek azonos biztonsági szintjének eléréséhez.

Mélységi védelem

16. A CIS-t fenyegető veszélyek enyhítése érdekében technikai és nem technikai biztonsági intézkedéseket kell végrehajtani, melyek többszörös biztonsági réteget alkotnak. E rétegek az alábbiak:
 - a) *elrettetés*: a CIS megtámadását tervező bármely ellenség elrettentését célzó biztonsági intézkedések;
 - b) *megelőzés*: a CIS megtámadásának megakadályozását célzó biztonsági intézkedések;
 - c) *észlelés*: a CIS megtámadásának észlelését célzó biztonsági intézkedések;
 - d) *ellenálló képesség*: a támadás hatásának az információk vagy CIS-eszközök minimumára való korlátozását és a további kár megelőzését célzó biztonsági intézkedések; valamint
 - e) *helyreállítás*: a CIS biztonságos helyzetének helyreállítását célzó biztonsági intézkedések.

Az ilyen biztonsági intézkedések szigorúságának mértékét kockázatfelmérés alapján kell meghatározni.

17. A nemzeti biztonsági hatóságnak vagy az egyéb illetékes hatóságnak biztosítania kell, hogy:
 - a) rendelkezésre álljanak kiberbiztonsági képességek a szervezeti vagy a nemzeti határokon esetlegesen átnyúló fenyegetésekre való reagálásra; valamint
 - b) a reagálások összehangoltak legyenek, továbbá a fenyegetésekre, az eseményekre és az ezekkel kapcsolatos kockázatra vonatkozó információk megosztásra kerüljenek (számítógépes sürgősségi helyzetű válaszadási képességek).

A minimalitás és a legkisebb kiváltság elve

18. A szükségtelen kockázat elkerülése érdekében kizárólag a működési követelmények teljesítéséhez alapvetően szükséges funkcionálisokat, eszközöket és szolgáltatásokat kell végrehajtani.
19. A CIS felhasználói és az automatizált folyamatok kizárólag a feladataik elvégzéséhez szükséges hozzáférésekkel, kiváltságokkal vagy engedélyekkel rendelkezhetnek a balesetek, hibák vagy a CIS-erőforrások illetéktelen felhasználásából eredő károk korlátozása érdekében.
20. A CIS által végrehajtott nyilvántartási eljárásokat – szükség esetén – az akkreditációs folyamat részeként ellenőrizni kell.

Információvédelmi tudatosság

21. A CIS biztonsága védelmének első vonalát a kockázatok és a rendelkezésre álló biztonsági intézkedések ismerete képezi. A CIS életciklusában érintett valamennyi személynek – a felhasználókat is beleértve – tudatában kell lennie különösen annak, hogy:
 - a) a biztonsági hiányosságok jelentősen károsíthatják a CIS-t;
 - b) az összekapcsolódásból és egymásrautaltságból adódóan másokat milyen károk érhetnek; valamint
 - c) a rendszerben és folyamatokban betöltött szerepeik szerint személyesen felelősek és elszámoltathatók a CIS biztonságáért.

22. A biztonsággal kapcsolatos felelősség ismeretének biztosítása érdekében valamennyi érintett személy – beleértve a vezető tisztviselőket és a CIS-felhasználókat is – számára kötelező információvédelmi oktatást és tudatosságnövelő képzést kell szervezni.

Az IT biztonsági termékek értékelése és jóváhagyása

23. A biztonsági intézkedések – védelmi szintként meghatározott – szükséges megbízhatósági szintjét a kockázatkezelési eljárás eredménye alapján és a vonatkozó biztonsági előírásokkal és biztonsági iránymutatásokkal összhangban kell meghatározni.
24. A védelmi szintet nemzetközileg elismert vagy nemzeti szinten jóváhagyott folyamatok és módszerek alkalmazásával kell ellenőrizni. Ez elsősorban értékelés, ellenőrzés és auditálás lehet.
25. Az EU-minősített adatok védelmére szolgáló kriptográfiai termékeket valamely tagállam nemzeti kriptográfiai jóváhagyó hatósága (CAA) értékeli és jóváhagyja.
26. A Tanács vagy a főtitkár általi jóváhagyásra irányuló ajánlást megelőzően, a 10. cikk (6) bekezdésének megfelelően ezeket az EU-minősített adat védelmére szolgáló kriptográfiai termékeket a berendezés tervezésében vagy gyártásában részt nem vevő tagállam megfelelő minősítéssel rendelkező hatósága (AQUA) általi második értékelésnek kell alávetni, amelyen azoknak meg kell felelniük. A második értékelés során a vizsgálat részletessége az érintett termékek által védendő EU-minősített adat tervezett legmagasabb minősítési szintjétől függ. A Tanács a kriptográfiai termékek értékelésére és jóváhagyására vonatkozó biztonsági politikát hagy jóvá.
27. A Tanács vagy a főtitkár – konkrét működési indokok alapján, adott esetben – a Biztonsági Bizottság ajánlására figyelmen kívül hagyhatja az e melléklet 25. és a 26. pontjában foglalt követelményeket, és meghatározott időtartamra ideiglenes jóváhagyást biztosíthat a 10. cikk (6) bekezdésében foglalt eljárással összhangban.
28. A Tanács – a Biztonsági Bizottság ajánlása alapján eljárva – elfogadhatja a valamely harmadik állam vagy nemzetközi szervezet kriptográfiai termékeire vonatkozó értékelési, kiválasztási és jóváhagyási eljárást, és ennek megfelelően az adott harmadik államnak vagy nemzetközi szervezetnek átadott EU-minősített adatok védelme tekintetében jóváhagyottnak tekintheti ezeket a kriptográfiai termékeket.
29. A megfelelő minősítéssel rendelkező hatóság valamely tagállam kriptográfiai jóváhagyó hatósága, amely a Tanács által meghatározott szempontok alapján akkreditációt nyert az EU-minősített adatok védelmére szolgáló kriptográfiai termékek második értékelésének elvégzésére.
30. A Tanács a nem kriptográfiai IT biztonsági termékek minősítésére és jóváhagyására vonatkozó biztonsági politikát hagy jóvá.

Adattovábbítás biztonságos és igazgatási területeken belül

31. E határozat rendelkezései ellenére, amennyiben az EU-minősített adatok továbbítása biztonságos területekre vagy igazgatási területekre korlátozódik, rejtjelezetlen továbbítás vagy alacsonyabb szintű rejtjelezés alkalmazható a kockázatkezelési folyamat eredményére alapozva és a biztonsági akkreditációs hatóság jóváhagyásával.

A CIS-ek biztonságos összekapcsolása

32. E határozat alkalmazásában a rendszerek összekapcsolása két vagy több információtechnológiai rendszer adatok és egyéb információforrások megosztása (pl. kommunikáció) céljából történő, egyirányú vagy többirányú, közvetlen összekapcsolását jelenti.
33. A CIS valamennyi vele összekapcsolt információtechnológiai rendszert bizalmasan kezel, és a minősített adatok cseréjének ellenőrzése céljából védelmi intézkedéseket hajt végre.
34. A CIS más információtechnológiai rendszerrel való minden összekapcsolása tekintetében a következő alapkövetelményeknek kell eleget tenni:
- a) az ilyen összekapcsolások üzleti vagy üzemeltetési követelményeit az illetékes hatóságok határozzák meg és hagyják jóvá;
 - b) az összekapcsolást kockázatkezelési és akkreditációs eljárásnak kell alávetni, és ahhoz az illetékes biztonsági akkreditációs hatóság (SAA) jóváhagyása szükséges; valamint
 - c) valamennyi CIS körzethatárán határvédelmi szolgáltatásokat (BPS) kell létesíteni.

35. Akkreditált CIS nem kapcsolható össze nem védett vagy nyilvános hálózattal, kivéve, ha a CIS jóváhagyott, a CIS és a nyilvános hálózat között e célból telepített határvédelmi szolgáltatással rendelkezik. Az ilyen összekapcsolásra vonatkozó biztonsági intézkedéseket az illetékes CIS információvédelmi hatóságnak felül kell vizsgálnia, és az illetékes biztonsági akkreditációs hatóságnak jóvá kell hagynia.

Amennyiben a nem védett vagy nyilvános hálózatot kizárólag adatközzétítésre használják, és az adatokat a 10. cikknek megfelelően jóváhagyott kriptográfiai termékkel kódolták, az ilyen kapcsolat nem tekintendő összekapcsolásnak.

36. Tilos a TRÈS SECRET UE/EU TOP SECRET minősítésű adatok kezelésére akkreditált CIS közvetlen vagy kaszkád módon való összekapcsolása nem védett vagy nyilvános hálózattal.

Számítógépes adathordozók

37. A számítógépes adathordozókat az illetékes biztonsági hatóság által jóváhagyott eljárásokkal összhangban meg kell semmisíteni.
38. A számítógépes adathordozókat a 6. cikk (2) bekezdése szerint kidolgozandó biztonsági iránymutatásokkal összhangban kell újrafelhasználni vagy visszaminősíteni, továbbá e politikával összhangban kell a minősítésüket megszüntetni.

Szükséghelyzet

39. Az e határozatban foglalt rendelkezések ellenére, szükséghelyzetben – például fenyegető vagy ténylegesen fennálló válság-, konfliktus- vagy háborús helyzetben – vagy rendkívüli üzemeltetési körülmények között az alábbiakban leírt különös eljárások alkalmazhatók.
40. EU-minősített adatok az illetékes hatóság beleegyezésével továbbíthatók alacsonyabb minősítési szintre jóváhagyott kriptográfiai termékek felhasználásával vagy rejtjelezés nélkül, amennyiben a késedelem által okozott kár egyértelműen meghaladná a minősített adatok illetéktelen hozzáférhetővé tétele által okozott kárt, és ha:
- a) a küldő, illetve az átvevő nem rendelkezik az előírt rejtjelezési lehetőséggel vagy egyáltalán rejtjelezési lehetőséggel; valamint
 - b) a minősített anyag más eszközökkel nem továbbítható időben.
41. A 39. pontban meghatározott körülmények esetén továbbított minősített adat nem látható el olyan jelöléssel vagy jelzéssel, amely azt a nem minősített adatoktól vagy elérhető kriptográfiai eszköz által védhető adattól megkülönbözteti. Az átvevőket késedelem nélkül, egyéb módon értesíteni kell a minősítési szintről.
42. Amennyiben a 39. pontban említett eljárás alkalmazására kerül sor, jelentést kell tenni az illetékes hatóságnak és a Biztonsági Bizottságnak.

III. INFORMÁCIÓVÉDELMI FELADATKÖRÖK ÉS HATÓSÁGOK

43. A tagállamok és a Főtitkárság a következő információvédelmi feladatköröket állapítják meg. E feladatkörök nem igényelnek külön szervezeti egységeket. Külön megbízatással kell rendelkezniük. Mindazonáltal, e feladatkörök és az azokat kísérő felelősségi körök ugyanazon szervezeti egységen belül kombinálhatók vagy integrálhatók, vagy különböző szervezeti egységek között lehet őket megosztani, feltéve, hogy elkerülhető a belső összeférhetetlenség vagy a feladatok ütközése.

Információvédelmi hatóság

44. Az információvédelmi hatóság felelős az alábbiakért:
- a) információvédelmi biztonsági politikák és biztonsági iránymutatások kidolgozása és azok hatékonyságának és helyénvalóságának figyelemmel kísérése;
 - b) a kriptográfiai termékekkel kapcsolatos technikai információk védelme és igazgatása;
 - c) annak biztosítása, hogy az EU-minősített adatok védelmére kiválasztott információvédelmi intézkedések megfeleljenek a jogosultságot és kiválasztást szabályozó, vonatkozó politikáknak;
 - d) annak biztosítása, hogy a kriptográfiai termékek kiválasztása a jogosultságot és kiválasztást szabályozó politikáknak megfelelően történjen;
 - e) az információvédelemmel kapcsolatos képzés és tudatosságnövelés koordinálása;
 - f) konzultáció a rendszerszolgáltatóval, a biztonsági szereplőkkel és a felhasználók képviselőivel az információvédelmi biztonsági politikák és biztonsági iránymutatások tekintetében; valamint
 - g) megfelelő szakértelem rendelkezésre állásának biztosítása a Biztonsági Bizottság információvédelmi kérdésekkel foglalkozó szakértői csoportjában.

TEMPEST-hatóság

45. A TEMPEST-hatóság felelős azért, hogy a CIS megfeleljen a TEMPEST-politikáknak és -iránymutatásoknak. Megadja a jóváhagyást a működési környezetükben meghatározott minősítési szintig EU-minősített adatok védelmére szolgáló berendezésekre és termékekre vonatkozó TEMPEST-ellenintézkedésekre.

Kriptográfiai jóváhagyó hatóság

46. A kriptográfiai jóváhagyó hatóság (CAA) felel annak biztosításáért, hogy a kriptográfiai termékek megfeleljenek a nemzeti kriptográfiai politikának vagy a Tanács kriptográfiai politikájának. A kriptográfiai termékek tekintetében megadja a jóváhagyást arra, hogy azok működési környezetükben meghatározott minősítési szintig EU-minősített adatokat részesítsenek védelemben. A tagállamok tekintetében a CAA felel továbbá a kriptográfiai termékek értékeléséért is.

Kriptográfiai terjesztési hatóság

47. A kriptográfiai terjesztési hatóság (CDA) felelős az alábbiakért:

- a) az EU kriptográfiai anyag igazgatása és könyvelése;
- b) annak biztosítása, hogy valamennyi EU kriptográfiai anyag könyvelése, biztonságos kezelése, tárolása és terjesztése tekintetében a megfelelő eljárásokat alkalmazzák és csatornákat hozzak létre; valamint
- c) az EU kriptográfiai anyag továbbításának biztosítása az azt felhasználó egyénektől vagy szolgáltatóktól, vagy azok felé.

Biztonsági akkreditációs hatóság

48. Minden egyes rendszer biztonsági akkreditációs hatósága a következő feladatokat látja el:

- a) annak biztosítása, hogy a CIS megfeleljen a vonatkozó biztonsági politikáknak és biztonsági iránymutatásoknak, jóváhagyási tanúsítvány kiadása arról, hogy a CIS működési környezetében meghatározott minősítési szintig EU-minősített adatokat kezelhet, az akkreditáció feltételeinek és azon kritériumoknak a meghatározása, amelyek esetében ismételt jóváhagyás szükséges;
- b) biztonsági akkreditációs folyamat létrehozása a vonatkozó politikákkal összhangban, egyértelműen megállapítva a jóváhagyási feltételeket a felelőssége alá tartozó CIS tekintetében;
- c) biztonsági akkreditációs stratégia kialakítása, amely a megkövetelt biztonsági szinttel arányosan meghatározza az akkreditációs eljárás részletességének mértékét;
- d) a biztonsággal kapcsolatos dokumentáció, többek között a kockázatkezelés és fennmaradó kockázat megállapítása, a rendszerspecifikus biztonsági követelmények (a továbbiakban: az SSRS) megállapítása, a biztonsági végrehajtás ellenőrzési dokumentációja és a biztonsági üzemeltetési eljárások (a továbbiakban: a SecOP) megvizsgálása és jóváhagyása, és annak biztosítása, hogy az összhangban álljon a Tanács biztonsági szabályaival és politikájával;
- e) a CIS-szel kapcsolatos biztonsági intézkedések végrehajtásának ellenőrzése biztonsági értékelések, ellenőrzések vagy felülvizsgálatok végrehajtása vagy támogatása révén;
- f) biztonsági követelmények meghatározása (pl. személyi biztonsági tanúsítványok szintjei) a CIS tekintetében betöltött szenzitív beosztások tekintetében;
- g) a CIS biztonságát szolgáló engedélyezett kriptográfiai és TEMPEST-termékek kiválasztásának jóváhagyása;
- h) CIS másik CIS-szel való összekapcsolódásának jóváhagyása, vagy adott esetben a közös engedélyezésben való részvétel; valamint
- i) a rendszerszolgáltatóval, a biztonsági szereplőkkel és a felhasználók képviselőivel való konzultálás a biztonsági kockázatkezelés tekintetében – különös tekintettel a fennmaradó kockázatra –, valamint a jóváhagyási tanúsítvány kiadási feltételei tekintetében.

49. A Főtitkárság biztonsági akkreditációs hatósága felel a Főtitkárság hatáskörében működő valamennyi CIS akkreditálásáért.

50. A tagállamok érintett biztonsági akkreditációs hatósága felel a tagállamok hatáskörében működő CIS-ek és azok rendszerelemeinek akkreditálásáért.

51. Közös biztonsági akkreditációs bizottság (SAB) felel a mind a Főtitkárság, mind a tagállamok biztonsági akkreditációs hatóságai hatáskörébe tartozó CIS akkreditálásáért. A SAB az egyes tagállamok biztonsági akkreditációs hatóságainak képviselőiből áll, és ülésein részt vesz a Bizottság biztonsági akkreditációs hatóságának egy képviselője. A CIS-hez kapcsolódó egyéb szervezetek meghívást kapnak az adott rendszerrel foglalkozó ülésekre.

A SAB elnöke a Főtitkárság biztonsági akkreditációs hatóságának a képviselője. A SAB a CIS-hez kapcsolódó intézmények, tagállamok és más szervezetek biztonsági akkreditációs hatóságai képviselőinek konszenzusos határozatai alapján jár el. Rendszeres időközönként jelentést tesz tevékenységeiről a Biztonsági Bizottságnak, és azt valamennyi akkreditációs tanúsítványról értesíti.

Információvédelmi üzemeltetési hatóság

52. Minden egyes rendszer információvédelmi üzemeltetési hatósága felelős az alábbiakért:

- a) biztonsági dokumentáció kidolgozása a biztonsági politikákkal és biztonsági iránymutatásokkal összhangban, különösen a rendszerspecifikus biztonsági követelmények megállapítása (SSRS), ideértve a fennmaradó kockázat megállapítását, a biztonsági üzemeltetési eljárásokat (SecOP) és a CIS akkreditációs folyamatának részét képező kriptográfiai tervet;
- b) részvétel a rendszerspecifikus technikai biztonsági intézkedések, eszközök és szoftverek kiválasztásában és tesztelésében, a végrehajtásuk felügyelete és annak biztosítása, hogy azokat a vonatkozó biztonsági dokumentációnak megfelelően, biztonságosan telepítsék, konfigurálják és tartsák karban;
- c) részvétel a TEMPEST biztonsági intézkedések és eszközök kiválasztásában, amennyiben az a rendszerspecifikus biztonsági követelmények szerint szükséges, és annak biztosítása, hogy azokat a TEMPEST-hatósággal együttműködésben, biztonságosan telepítsék és tartsák karban;
- d) a biztonsági üzemeltetési eljárások végrehajtásának és alkalmazásának ellenőrzése és szükség esetén a működési biztonsággal kapcsolatos felelősségnek a rendszertulajdonosra ruházása;
- e) a kriptográfiai termékek kezelése, biztosítva a kriptográfiai és ellenőrzött elemek védelmét és – adott esetben – biztosítva a kriptográfiai változók generálását;
- f) biztonsági elemzések felülvizsgálatának és tesztelésének a kivitelezése, különösen a vonatkozó kockázati jelentéseknek a biztonsági akkreditációs hatóság (SAA) előírásai szerinti elkészítése céljából;
- g) CIS-specifikus információvédelmi képzés nyújtása; valamint
- h) CIS-specifikus biztonsági intézkedések végrehajtása és működtetése.

V. MELLÉKLET

IPARBIZTONSÁG

I. BEVEZETÉS

1. Ez a melléklet a 11. cikk végrehajtására vonatkozó rendelkezéseket határoz meg. A melléklet meghatározza a Főtitkárság által odaítélt minősített szerződések megkötését megelőző tárgyalások és a szerződések teljes életciklusa során a gazdálkodó vagy más szervezetekre alkalmazandó általános biztonsági rendelkezéseket.
2. A Tanács az iparbiztonságra vonatkozó iránymutatásokat hagy jóvá, amely felvázolja különösen a telephely-biztonsági tanúsítványokra, a biztonsági mellékletre, a látogatásokra, az EU-minősített adatok továbbítására és szállítására vonatkozó részletes követelményeket.

II. A MINŐSÍTETT SZERZŐDÉSEKBEN TALÁLHATÓ BIZTONSÁGI ELEMEL

Biztonsági minősítési jegyzék (SCG)

3. A pályázati felhívás kiírását vagy a minősített szerződés odaítélését megelőzően a Főtitkárság szerződő hatóságként meghatározza a pályázók és vállalkozók részére nyújtandó bármely adat biztonsági minősítését, valamint a vállalkozó által létrehozandó bármely adat biztonsági minősítését. E célból a Főtitkárság elkészíti a szerződés teljesítése során alkalmazandó SCG-t.
4. A minősített szerződés különféle elemeire vonatkozó biztonsági minősítések meghatározása érdekében az alábbi elveket kell alkalmazni:
 - a) az SCG elkészítése során a Főtitkárságnak figyelembe kell vennie valamennyi vonatkozó biztonsági szempontot, köztük a nyújtott adathoz rendelt és az adat kibocsátója által a szerződéshez való használatra jóváhagyott biztonsági minősítést;
 - b) a szerződés minősítésének általános szintje nem lehet alacsonyabb bármely elemének legmagasabb minősítési szintjénél; valamint
 - c) adott esetben a Főtitkárság kapcsolatba lép a tagállamok nemzeti biztonsági hatóságaival/kijelölt biztonsági hatóságaival vagy más érintett illetékes biztonsági hatósággal, egy szerződés teljesítése során a vállalkozók által létrehozott vagy azok részére nyújtott adat minősítését érintő bármilyen változás esetén és az SCG bármilyen további változása esetén.

Biztonsági melléklet (SAL)

5. A szerződésspecifikus biztonsági követelményeket biztonsági mellékletben (SAL) kell leírni. Adott esetben a SAL tartalmazza az SCG-t, és a minősített vállalkozói vagy alvállalkozói szerződésnek szerves részét képezi.
6. A SAL tartalmazza a vállalkozók és alvállalkozók részére az e határozatban foglalt minimumszabályok teljesítését előíró rendelkezéseket. A minimumszabályok be nem tartása elegendő indokot jelenthet a szerződés felbontására.

Program-/projektbiztonsági utasítás (PSI)

7. Az EU-minősített adatokhoz való hozzáférést, vagy azok kezelését vagy tárolását magában foglaló program vagy projekt hatályának függvényében a program vagy projekt irányítására kijelölt szerződő hatóság külön PSI-t dolgozhat ki. A PSI-hez a tagállamoknak a programban/projektben részt vevő nemzeti biztonsági hatósága/kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatóság általi jóváhagyás szükséges, és a PSI-k további biztonsági követelményeket tartalmazhatnak.

III. LÉTESÍTMÉNYI BIZTONSÁGI ELLENŐRZÉS (FSC)

8. Az FSC-t a tagállam nemzeti biztonsági hatósága/kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatósága bocsátja ki annak jelzésére, hogy – a nemzeti jogszabályokkal és rendelkezésekkel összhangban – egy gazdálkodó vagy más szervezet képes az EU-minősített adatnak a telephelyükön, megfelelő minősítési szinten (CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET) való védelmére. A tanúsítványt be kell mutatni a Tanács Főtitkárságának mint a szerződő hatóságnak, mielőtt egy vállalkozó, alvállalkozó vagy potenciális vállalkozó vagy alvállalkozó számára az EU-minősített adathoz való hozzáférést biztosítanának vagy engedélyeznének.

9. Az FSC kiállításakor a megfelelő NSA vagy DSA legalább:
- a) értékeli a gazdálkodó vagy egyéb szervezet feddhetetlenségét;
 - b) értékeli a szervezet tulajdonlását, ellenőrzését, valamint hogy fennáll-e olyan indokolatlan befolyás, amely biztonsági kockázatnak tekinthető;
 - c) ellenőrzi, hogy a gazdálkodó vagy egyéb szervezet létesített-e olyan helyszíni biztonsági rendszert, amely a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok vagy anyagok – az e határozatban foglalt követelmények szerinti – védelméhez szükséges minden megfelelő biztonsági intézkedésre kiterjed;
 - d) ellenőrzi, hogy azon vezetők, tulajdonosok és alkalmazottak személyi biztonsági státusát, akiknek CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adathoz hozzáféréssel kell rendelkezniük, az e határozatban megállapított rendelkezéseknek megfelelően határozták-e meg; valamint
 - e) ellenőrzi, hogy a gazdálkodó vagy egyéb szervezet kinevezett-e biztonsági megbízottat (FSO), aki felelősséggel tartozik a vezetőknek a biztonsági kötelezettségeknek a szervezeten belül történő érvényesítéséért.
10. Adott esetben a Főtitkárság szerződő hatóságként értesíti a megfelelő nemzeti vagy kijelölt biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot, hogy a szerződést megelőző szakaszban vagy a szerződés teljesítéséhez FSC-re van szükség. FSC-re vagy PSC-re akkor van szükség a szerződéskötés előtti szakaszban, ha a pályázati eljárás során CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatot kell átadni.
11. A szerződő hatóság nem köthet minősített szerződést a megfelelőnek tartott pályázóval azt megelőzően, hogy kézhez kapná az érintett vállalkozó vagy alvállalkozó bejegyzésének helye szerinti tagállam nemzeti biztonsági hatósága/kijelölt biztonsági hatósága által kiállított megerősítést arról, hogy szükség szerint megfelelő FSC-vel rendelkeznek.
12. Az FSC-t kibocsátó nemzeti vagy kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság az FSC-t érintő bármely változásról értesíti a Főtitkárságot mint szerződő hatóságot. Alvállalkozói szerződés esetén a nemzeti vagy kijelölt biztonsági hatóságot, illetve bármely egyéb illetékes biztonsági hatóságot ennek megfelelően tájékoztatni kell.
13. Az FSC-nek az adott nemzeti vagy kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság általi visszavonása elegendő indokot szolgáltat a Főtitkárságnak mint szerződő hatóságnak a minősített szerződés megszüntetésére vagy a pályázónak a versenyből való kizárására.

IV. MINŐSÍTETT VÁLLALKOZÓI ÉS ALVÁLLALKOZÓI SZERZŐDÉSEK

14. Amikor egy pályázó részére a szerződést megelőző szakaszban EU-minősített adatot adnak át, a pályázati felhívásnak tartalmaznia kell egy olyan kitélet, amely azt a pályázót, aki végül nem nyújtja be pályázatát, vagy akit nem választanak ki, arra kötelezi, hogy adott időn belül valamennyi minősített dokumentumot szolgáltatassa vissza.
15. Amint sor kerül egy minősített vállalkozói vagy alvállalkozói szerződés odaítélésére, a Főtitkárság szerződő hatóságként értesíti a vállalkozó vagy alvállalkozó nemzeti vagy kijelölt biztonsági hatóságát vagy bármely más illetékes biztonsági hatóságot a minősített szerződés biztonsági előírásairól.
16. Amennyiben egy ilyen szerződést megszüntetnek, a Főtitkárság szerződő hatóságként (és/vagy a nemzeti vagy kijelölt biztonsági hatóság vagy adott esetben bármely más illetékes biztonsági hatóság, alvállalkozói szerződés esetén) késedelem nélkül értesíti azon tagállam nemzeti vagy kijelölt biztonsági hatóságát vagy bármely más illetékes biztonsági hatóságát, amelyben a vállalkozót vagy alvállalkozót bejegyezték.
17. Általános szabály, hogy a vállalkozó vagy alvállalkozó a minősített vállalkozói vagy alvállalkozói szerződés lejártát követően köteles valamennyi EU-minősített adatot visszaszolgáltatni a szerződő hatóságnak.

18. Az EU-minősített adatoknak a szerződés teljesítése során vagy a szerződés lejártával történő megsemmisítésére vonatkozó egyedi rendelkezéseket a SAL-ban kell lefektetni.
19. Amennyiben a vállalkozó vagy alvállalkozó engedélyt kap az EU-minősített adatok megtartására a szerződés lejártát követően, továbbra is be kell tartani az e határozatban foglalt minimumszabályokat, és a vállalkozónak vagy alvállalkozónak védenie kell az EU-minősített adatok bizalmasságát.
20. A pályázati kiírás és a szerződés határozza meg azon feltételeket, amelyek szerint a vállalkozó alvállalkozói szerződést köthet.
21. Mielőtt a vállalkozó a minősített szerződés bármely részére alvállalkozókat szerződtetne, ehhez engedélyt kér a Főtitkárságtól mint szerződő hatóságtól. Nem köthető alvállalkozói szerződés az olyan nem uniós államban bejegyzett gazdálkodó vagy más szervezetekkel, amely nem kötött adatbiztonsági megállapodást az Unióval.
22. A vállalkozó felel annak biztosításáért, hogy minden alvállalkozói tevékenységet az e határozatban foglalt minimumszabályokkal összhangban folytassanak, és az alvállalkozó részére nem ad át EU-minősített adatot vagy anyagot az azt kibocsátó előzetes írásbeli engedélye nélkül.
23. A vállalkozó vagy az alvállalkozó által létrehozott vagy kezelt EU-minősített adatok tekintetében a kibocsátót megillető jogokat a szerződő hatóság gyakorolja.

V. MINŐSÍTETT SZERZŐDÉSEKKEL KAPCSOLATOS LÁTOGATÁSOK

24. Amennyiben a Főtitkárság, a vállalkozók vagy az alvállalkozók személyzetének valamely minősített szerződés teljesítéséhez egymás telephelyén CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adathoz kell hozzáférnie, a látogatásokat a nemzeti vagy kijelölt biztonsági hatóságokkal vagy bármely más érintett illetékes biztonsági hatósággal összeköttetésben kell megszervezni. Egyes meghatározott projektekre vonatkozóan azonban a nemzeti vagy kijelölt biztonsági hatóságok megállapodhatnak egy olyan eljárásról, amely alapján közvetlenül meg lehet szervezni e látogatásokat.
25. Minden látogatónak megfelelő PSC-vel kell rendelkeznie, és teljesítenie kell a „szükséges ismeret” feltételét a Főtitkárság szerződésével kapcsolatos EU-minősített adatokhoz való hozzáféréshez.
26. A látogatók csak a látogatás céljához kapcsolódó EU-minősített adatokhoz kapnak hozzáférést.

VI. EU-MINŐSÍTETT ADATOK TOVÁBBÍTÁSA ÉS SZÁLLÍTÁSA

27. Az EU-minősített adatok elektronikus úton történő továbbítása tekintetében a 10. cikk és a IV. melléklet vonatkozó rendelkezéseit kell alkalmazni.
28. Az EU-minősített adatok szállítására a III. melléklet vonatkozó rendelkezéseit kell alkalmazni, a nemzeti jogszabályokkal és rendelkezésekkel összhangban.
29. Az EU-minősített adatok szállítmányként való szállítása biztonsági előírásainak meghatározása során az alábbi elveket kell alkalmazni:
 - a) a szállítás valamennyi szakasza alatt garantálni kell a biztonságot, a kiindulási helytől a végső úti célig;
 - b) egy adott szállítmányra megállapított védelmi szintet az abban foglalt anyag legmagasabb minősítési szintje határozza meg;
 - c) a szállítást végző vállalatok megfelelő szintű FSC-vel rendelkeznek. Ilyen esetekben a szállítmányt kezelő személyzetnek biztonsági ellenőrzésen kell átesnie az I. melléklettel összhangban;
 - d) a SECRET UE/EU SECRET vagy CONFIDENTIEL UE/EU CONFIDENTIEL adatként minősített anyag bármilyen, határokon átnyúló szállítását megelőzően a feladó szállítási tervet készít, amelyet az érintett nemzeti vagy kijelölt biztonsági hatóságok vagy más illetékes biztonsági hatóságok jóváhagynak;

- e) az útvonalak lehetőség szerint közvetlenek, és a szállítást a körülmények engedte lehető leggyorsabban hajtják végre; valamint
- f) az útvonalak lehetőség szerint kizárólag tagállamokon keresztül vezetnek. Nem uniós tagállamokon keresztül vezető útvonalakon kizárólag mind a feladó, mind a címzett államának nemzeti vagy kijelölt biztonsági hatósága vagy más illetékes biztonsági hatósága által kiadott jóváhagyást követően lehet haladni.

VII. EU-MINŐSÍTETT ADAT ÁTADÁSA HARMADIK ÁLLAMOKBAN MŰKÖDŐ VÁLLALKOZÓK RÉSZÉRE

- 30. Az EU-minősített adat harmadik államokban működő vállalkozók vagy alvállalkozók részére való átadása a Főtitkárság mint szerződő hatóság és azon érintett harmadik állam nemzeti vagy kijelölt biztonsági hatósága vagy más illetékes biztonsági hatósága által elfogadott biztonsági intézkedésekkel összhangban történik, ahol a vállalkozót bejegyezték.

VIII. A RESTREINT UE/EU RESTRICTED MINŐSÍTÉSŰ ADATOK

- 31. A Főtitkárság mint szerződő hatóság adott esetben a tagállam nemzeti vagy kijelölt biztonsági hatóságával összeköttetésben a szerződéses rendelkezések alapján ellenőrzéseket végezhet a vállalkozók/alvállalkozók létesítményeiben annak ellenőrzése céljából, hogy a RESTREINT UE/EU RESTRICTED szintű minősítéssel rendelkező adatok védelméhez szükséges, a szerződésben előírt biztonsági intézkedéseket megvalósították.
- 32. A nemzeti jogszabályok és rendelkezések szerint szükséges mértékben a Tanács Főtitkárságának mint szerződő hatóságnak értesítenie kell a nemzeti vagy kijelölt biztonsági hatóságokat vagy bármely más illetékes biztonsági hatóságot a RESTREINT UE/EU RESTRICTED minősítésű adatot tartalmazó szerződésekről és alvállalkozói szerződésekről.
- 33. A RESTREINT UE/EU RESTRICTED minősítésű adatot magukban foglaló, a Főtitkárság által odaítélt szerződések esetén az FSC, illetve PSC nem kötelező a vállalkozók, alvállalkozók és alkalmazottaik számára.
- 34. A Főtitkárság mint szerződő hatóság megvizsgálja azon szerződésekre kiírt pályázati felhívásokra érkezett válaszokat, amelyek RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáférést igényelnek, a nemzeti jogszabályok és rendelkezések értelmében az FSC-vel és a PSC-vel kapcsolatban esetleg meglévő bármely követelmény sérelme nélkül.
- 35. Azon feltételeknek, amelyek alapján a vállalkozó alvállalkozót szerződttethet, összhangban kell lenniük a 21. ponttal.
- 36. Amennyiben egy adott szerződés RESTREINT UE/EU RESTRICTED minősítési szintű adatok vállalkozó által működtetett CIS-ben (kommunikációs és információs rendszer) való kezelésére is kiterjed, a Főtitkárság mint szerződő hatóság biztosítja, hogy a szerződés vagy alvállalkozói szerződés meghatározza a CIS akkreditálásához szükséges, valamennyi kockázati tényezőre kiterjedő technikai és adminisztratív követelményeket. Az ilyen CIS akkreditációjának hatályáról a szerződő hatóság és az érintett nemzeti vagy kijelölt biztonsági hatóság állapodik meg.

VI. MELLÉKLET

MINŐSÍTETT ADATOK CSERÉJE HARMADIK ÁLLAMOKKAL ÉS NEMZETKÖZI SZERVEZETEKSEL

I. BEVEZETÉS

1. Ez a melléklet a 13. cikk végrehajtására vonatkozó rendelkezéseket határoz meg.

II. A MINŐSÍTETT ADATOK CSERÉJÉT SZABÁLYOZÓ KERETEK

2. Amennyiben a Tanács a minősített adatok cseréjének hosszú távú szükségességét állapítja meg:

— adatbiztonsági megállapodást kell kötni, vagy

— igazgatási megállapodást kell kötni

a 13. cikk (2) bekezdésének és a III. és IV. szakasznak megfelelően és a Biztonsági Bizottság ajánlása alapján.

3. Amikor KBVP-művelet céljára előállított EU-minősített adatoknak ilyen műveletben részt vevő harmadik államok vagy nemzetközi szervezetek részére történő átadására kerül sor, és amennyiben a 2. pontban említett keretszabályok egyike sem létezik, EU-minősített adatoknak a részt vevő harmadik állammal vagy nemzetközi szervezettel való cseréjét az V. szakasszal összhangban az alábbiak szabályozzák:

— a részvételtől szóló keretmegállapodás,

— a részvételtől szóló *ad hoc* megállapodás, vagy

— a fentiek hiányában *ad hoc* igazgatási megállapodás.

4. A 2. és 3. pontban említett keretszabályozás hiányában, és amennyiben az EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére való átadásáról rendkívüli *ad hoc* alapon, a VI. szakasznak megfelelően döntenek, írásbeli biztosítékot kell kérni az érintett harmadik államtól vagy nemzetközi szervezettől annak biztosítására, hogy az a részére átadott EU-minősített adatokat az e határozat alapelveinek és minimumszabályainak megfelelő védelemben részesíti.

III. ADATBIZTONSÁGI MEGÁLLAPODÁSOK

5. Az adatbiztonsági megállapodások megállapítják a minősített adatoknak az Unió és harmadik államok vagy nemzetközi szervezetek közötti cseréjére irányadó alapelveket és minimumszabályokat.
6. Az adatbiztonsági megállapodások rendelkeznek technikai végrehajtási szabályokról is, amelyeket az érintett uniós intézmények és szervek illetékes biztonsági hatóságai és a szóban forgó harmadik állam vagy nemzetközi szervezet illetékes biztonsági hatósága közösen alakítanak ki. A végrehajtási szabályok figyelembe veszik az érintett harmadik állam vagy nemzetközi szervezet hatályos biztonsági szabályai, struktúrái és eljárásai által biztosított védelmi szintet. Azokat a Biztonsági Bizottságnak jóvá kell hagynia.
7. Adatbiztonsági megállapodás keretében EU-minősített adatok elektronikus eszközökkel történő cseréje nem megengedett, kivéve, ha a megállapodás vagy a vonatkozó technikai végrehajtási szabályok erről kifejezetten rendelkeznek.
8. Amikor a Tanács adatbiztonsági megállapodást köt, mindkét félnek a minősített adatok cseréjének fő beérkezési és kiküldési helyeként működő nyilvántartó hivatalt kell kijelölnie.
9. Az érintett harmadik állam vagy nemzetközi szervezet biztonsági szabályai, struktúrái és eljárásai hatékonyságának megállapítása céljából értékelő látogatásokra kerül sor az érintett harmadik állammal vagy nemzetközi szervezettel való kölcsönös megállapodás alapján. Az ilyen értékelő látogatásokat a III. melléklet vonatkozó rendelkezéseivel összhangban kell lebonyolítani, és a látogatások során az alábbiak értékelését kell elvégezni:

a) a minősített adatok védelmére alkalmazandó szabályozási keret;

b) a harmadik állam vagy nemzetközi szervezet biztonsági politikájának és a biztonság szervezésének bármely sajátos jellemzője, amely befolyásolhatja az esetlegesen kicserélt minősített adatok szintjét;

c) a ténylegesen hatályos biztonsági intézkedések és eljárások; valamint

d) az átadandó EU-minősített adatok szintjére vonatkozó biztonsági ellenőrzési eljárások.

10. Az Unió nevében értékelő látogatást végző csoport értékeli, hogy a kérdéses harmadik államban vagy nemzetközi szervezetben fennálló biztonsági szabályok és eljárások megfelelőek-e az EU-minősített adatokhoz igazodó szintű védelemre.
11. E látogatások megállapításait jelentésbe kell foglalni, amelynek alapján a Biztonsági Bizottság az érintett harmadik féllel papírformátumban és adott esetben elektronikus úton kicserélhető EU-minősített adatok legmagasabb szintjét, valamint az adott féllel folytatott csere különös feltételeit meghatározza.
12. A hatályos biztonsági rendszer jellegének és hatékonyságának megállapítása érdekében minden erővel törekedni kell a teljes biztonsági értékelő látogatásnak az érintett harmadik államban vagy nemzetközi szervezetben való lebonyolítására azt megelőzően, hogy a Biztonsági Bizottság jóváhagyja a végrehajtási szabályokat. Amennyiben azonban ez nem lehetséges, a Tanács Főtitkárságának Biztonsági Hivatala a rendelkezésére álló információk alapján a lehető legteljesebb jelentést készíti a Biztonsági Bizottság számára, amelyben tájékoztatást ad az adott harmadik államban vagy nemzetközi szervezetben alkalmazandó biztonsági szabályokról és a biztonság megszervezésének módjáról.
13. Az értékelő látogatásról szóló jelentést vagy – e jelentés hiányában – a 12. pontban említett jelentést továbbítani kell a Biztonsági Bizottságnak, amelynek azt megfelelőnek kell ítélnie, mielőtt az EU-minősített adatokat ténylegesen átadják az adott harmadik államnak vagy nemzetközi szervezetnek.
14. Az uniós intézmények és szervek illetékes biztonsági hatóságainak közölniük kell a harmadik állammal vagy nemzetközi szervezettel a papírformátumban vagy elektronikus eszközök révén megosztható EU-minősített adatok legmagasabb minősítési szintjét, valamint azt az időpontot, amelytől az Unió készen áll arra, hogy a megállapodás keretében EU-minősített adatokat adjon át.
15. Adott esetben nyomon követő értékelő látogatásokat kell tenni, különösen, ha:
 - a) növelni kell az átadható EU-minősített adatok szintjét;
 - b) az EU-t értesítették a harmadik fél biztonsági szabályainak olyan alapvető megváltozásáról, amely hatással lehet az EU-minősített adatoknak a harmadik állam vagy nemzetközi szervezet általi védelmére; vagy
 - c) olyan súlyos eseményre került sor, amely az EU-minősített adatokhoz való jogosulatlan hozzáférést okozott.
16. Az adatbiztonsági megállapodás hatálybalépését és azt követően, hogy sor került a minősített adatoknak az érintett harmadik állammal vagy nemzetközi szervezettel való cseréjére, a Biztonsági Bizottság – különösen valamely nyomon követő értékelő látogatás alapján – dönthet úgy, hogy módosítja a papírformátumban vagy elektronikus úton kicserélhető EU-minősített adatok legmagasabb szintjét.

IV. IGAZGATÁSI MEGÁLLAPODÁSOK

17. Amennyiben harmadik állammal vagy nemzetközi szervezettel általános szabályként legfeljebb RESTREINT UE/EU RESTRICTED minősítési jelölésű adatok hosszú távú cseréjére van szükség, és amennyiben a Biztonsági Bizottság megállapította, hogy az érintett fél nem rendelkezik kellőképpen fejlett biztonsági rendszerrel ahhoz, hogy lehetséges legyen az adatbiztonsági megállapodás megkötése, a főtitkár – a Tanács általi jóváhagyás függvényében – a Tanács Főtitkársága nevében igazgatási megállapodást köthet a szóban forgó harmadik állam vagy nemzetközi szervezet megfelelő hatóságaival.
18. Amennyiben működési okokból gyorsan kell kialakítani a minősített adatok cseréjének keretét, a Tanács kivételesen határozhat úgy, hogy magasabb minősítési szintű adatok cseréjére vonatkozóan igazgatási megállapodást köt.
19. Az igazgatási megállapodást általában levélváltás formájában kötik.
20. Le kell folytatni a 9. pontban említett értékelő látogatást, és a jelentést – vagy annak hiányában a 12. pontban említett jelentést – továbbítani kell a Biztonsági Bizottságnak, amelynek azt megfelelőnek kell ítélnie azt megelőzően, hogy az EU-minősített adatot ténylegesen átadják az adott harmadik államnak vagy nemzetközi szervezetnek.
21. Igazgatási megállapodás keretében az EU-minősített adatok elektronikus eszközökkel történő cseréje csak akkor megengedett, ha a megállapodás erről kifejezetten rendelkezik.

V. MINŐSÍTETT ADATOK CSERÉJE KBVP-MŰVELETEK KERETÉBEN

22. Harmadik államok és nemzetközi szervezetek KBVP-műveletekben való részvételét részvételi keretmegállapodások szabályozzák. E megállapodások a KBVP-művelet céljára előállított EU-minősített adatoknak a részt vevő harmadik államok vagy nemzetközi szervezetek részére történő átadására vonatkozó rendelkezéseket is tartalmaznak. A kicserélhető EU-minősített adatok legmagasabb minősítési szintje polgári KBVP-műveletek esetén a RESTREINT UE/EU RESTRICTED szint, míg katonai KBVP-műveletek esetén a CONFIDENTIEL EU/EU CONFIDENTIAL szint, kivéve, ha az adott KBVP-művelet létrehozásáról szóló határozat más szintet határoz meg.
23. Az adott KBVP-művelet vonatkozásában megkötött *ad hoc* részvételi megállapodások a KBVP-művelet céljára előállított EU-minősített adatoknak a részt vevő harmadik állam vagy nemzetközi szervezet részére történő átadására vonatkozó rendelkezéseket is tartalmaznak. A kicserélhető EU-minősített adatok legmagasabb minősítési szintje polgári KBVP-műveletek esetén a RESTREINT UE/EU RESTRICTED szint, míg katonai KBVP-műveletek esetén a CONFIDENTIEL EU/EU CONFIDENTIAL szint, kivéve, ha az adott KBVP-művelet létrehozásáról szóló határozat más szintet határoz meg.
24. Adatbiztonsági megállapodás hiányában és a részvételi megállapodás megkötéséig a művelet céljából létrehozott EU-minősített adatoknak a műveletben részt vevő harmadik állam vagy nemzetközi szervezet részére történő átadására a főképviselő által kötött igazgatási megállapodás az irányadó, illetve arra a VI. szakasszal összhangban történő *ad hoc* átadásról szóló döntésnek kell vonatkoznia. EU-minősített adatok megosztására kizárólag ilyen megállapodás keretében kerülhet sor mindaddig, amíg a harmadik állam vagy a nemzetközi szervezet részvétele csak tervezett. A kicserélhető EU-minősített adatok legmagasabb minősítési szintje polgári KBVP-műveletek esetén a RESTREINT UE/EU RESTRICTED szint, míg katonai KBVP-műveletek esetén a CONFIDENTIEL EU/EU CONFIDENTIAL szint, kivéve, ha az adott KBVP-művelet létrehozásáról szóló határozat más szintet határoz meg.
25. A 22–24. pontban említett, a minősített adatokra vonatkozó, a részvételi keretmegállapodásba, az *ad hoc* megállapodásba és az *ad hoc* igazgatási megállapodásba illesztendő rendelkezések előírják, hogy az adott harmadik állam vagy nemzetközi szervezet biztosítja, hogy a művelethez kirendelt személyi állománya az EU-minősített adatokat a Tanács Biztonsági Szabályzatának és az illetékes hatóságok, köztük a művelet parancsnoki lánc által adott további iránymutatásoknak megfelelően védi.
26. Ha ezt követően az Unió és a részt vevő harmadik állam vagy nemzetközi szervezet adatbiztonsági megállapodást köt, az adatbiztonsági megállapodás az EU-minősített adatok cseréje és kezelése tekintetében hatálytalanít minden részvételi keretmegállapodásban megállapított, a minősített adatok megosztására vonatkozó rendelkezést, *ad hoc* részvételi megállapodást és *ad hoc* igazgatási megállapodást.
27. Harmadik állammal vagy nemzetközi szervezettel kötött részvételi keretmegállapodás, *ad hoc* részvételi megállapodás vagy *ad hoc* igazgatási megállapodás keretében EU-minősített adatok elektronikus eszközökkel történő cseréje nem megengedett, kivéve, ha a szóban forgó megállapodás erről kifejezetten rendelkezik.
28. KBVP-művelet céljára előállított EU-minősített adatok a 22–27. ponttal összhangban tehetők a harmadik állam vagy nemzetközi szervezet részéről az adott művelethez kirendelt személyi állomány által hozzáférhetővé. A KBVP-művelet helyszínén vagy CIS-ében az ilyen személyzet EU-minősített adatokhoz való hozzáféréseinek engedélyezésekor megfelelő intézkedéseket kell alkalmazni (pl. a hozzáférhetővé tett EU-minősített adatok naplózása) az adatok elvesztése vagy illetéktelen tudomására jutása kockázatának csökkentésére. Ezeket az intézkedéseket a megfelelő tervezési vagy missziós dokumentumokban kell meghatározni.
29. Adatbiztonsági megállapodás hiányában, konkrét és sürgős műveleti igény esetén az EU-minősített adatoknak a KBVP-művelet fogadó állama részére történő átadása tekintetében irányadó lehet a főképviselő által kötött igazgatási megállapodás is. Erről a lehetőségről a KBVP-művelet létrehozásáról szóló határozatban rendelkezni kell. Az ilyen körülmények között átadott EU-minősített adatok a KBVP-művelet céljaira létrehozott adatokra korlátozódnak, és minőségük legfeljebb RESTREINT UE/EU RESTRICTED lehet, hacsak a KBVP-művelet létrehozásáról szóló határozat magasabb szintű minősítést nem ír elő. Az ilyen *ad hoc* igazgatási megállapodás értelmében a fogadó államnak vállalnia kell az EU-minősített adatok olyan minimumszabályok szerinti védelmét, amelyek nem kevésbé szigorúak az e határozatban megállapítottaknál.
30. Adatbiztonsági megállapodás hiányában a KBVP-műveletben részt vevő harmadik államoktól és nemzetközi szervezetektől eltérő, releváns harmadik államok és nemzetközi szervezetek részére történő EU-minősített adatok átadása tekintetében irányadó lehet a főképviselő által kötött igazgatási megállapodás is. Adott esetben erről a lehetőségről és az ehhez kapcsolódó feltételekről a KBVP-művelet létrehozásáról szóló határozatban kell rendelkezni. Az ilyen körülmények között átadott EU-minősített adatok a KBVP-művelet céljaira létrehozott adatokra korlátozódnak, és minőségük legfeljebb RESTREINT UE/EU RESTRICTED lehet, hacsak a KBVP-művelet létrehozásáról szóló határozat magasabb szintű minősítést nem ír elő. Az ilyen *ad hoc* igazgatási megállapodás értelmében az érintett harmadik államnak vagy nemzetközi szervezetnek vállalnia kell az EU-minősített adatok olyan minimumszabályok szerinti védelmét, amelyek nem kevésbé szigorúak az e határozatban megállapítottaknál.

31. Az EU-minősített adatoknak a 22., a 23. és a 24. pont összefüggésében való átadására vonatkozó rendelkezések végrehajtása előtt nincs szükség végrehajtási szabályok meghozatalára vagy értékelő látogatásokra.

VI. EU-MINŐSÍTETT ADATOK RENDKÍVÜLI AD HOC ÁTADÁSA

32. Amennyiben a III–V. szakasz szerinti keret nem létezik, ám a Tanács vagy előkészítő szerveinek egyike úgy ítéli meg, hogy EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére való átadásának rendkívüli szükségessége merült fel, a Főtitkárság:
- a) a lehetséges mértékben ellenőrzi, hogy az adott harmadik állam vagy nemzetközi szervezet biztonsági hatóságainak biztonsági szabályai, struktúrái és eljárásai garantálni tudják, hogy a részére átadott EU-minősített adatok az e határozatban foglaltaknál nem kevésbé szigorú szabályoknak megfelelő védelemben részesüljenek; valamint
 - b) felkéri a Biztonsági Bizottságot, hogy a rendelkezésre álló információk alapján adjon ki ajánlást az EU-minősített adatokat átvevő harmadik állam vagy nemzetközi szervezet biztonsági szabályainak, struktúráinak és eljárásainak megbízhatósága tekintetében.
33. Amennyiben a Biztonsági Bizottság ajánlása támogatja az EU-minősített adatok átadását, az ügyet az Állandó Képviselők Bizottsága (COREPER) elé kell utalni, amely meghozza az adatok átadására vonatkozó döntést.
34. Ha a Biztonsági Bizottság ajánlása nem támogatja az EU-minősített adatok átadását:
- a) a KKBP/KBVP területéhez kapcsolódó kérdéseket a Politikai és Biztonsági Bizottság tárgyalja meg, és határozatra vonatkozó ajánlást fogalmaz meg a COREPER számára;
 - b) minden egyéb kérdésről a COREPER tárgyal és hoz döntést.
35. Amennyiben célszerűnek ítéli, valamint a kibocsátó előzetes írásbeli jóváhagyására is figyelemmel, a COREPER dönthet úgy, hogy a minősített adatok csak részben vagy kizárólag előzetes visszaminősítés esetén vagy a minősítés előzetes feloldásával adhatók át, vagy hogy az átadandó adatokat a forrásra vagy az eredeti EU minősítési szintre való utalás nélkül kell előkészíteni.

36. Az EU-minősített adatok átadására vonatkozó döntést követően a Főtitkárság továbbítja az érintett dokumentumot, amelyen szerepel az átvevő harmadik államot vagy nemzetközi szervezetet feltüntető átadásra jogosító jelölés is. A tényleges átadást megelőzően vagy annak alkalmával az adott harmadik fél írásban kötelezettséget vállal az átvett EU-minősített adatoknak az e határozatban megállapított alapelvek és minimumszabályok szerinti védelmére.

VII. EU-MINŐSÍTETT ADATOK HARMADIK ÁLLAMOK VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE VALÓ ÁTADÁSÁRA VONATKOZÓ FELHATALMAZÁS

37. Amennyiben létezik a minősített adatok harmadik államokkal vagy nemzetközi szervezetekkel való cseréjének 2. pont szerinti kerete, a Tanács határozatot hoz, amelyben a főtitkárt felhatalmazza az EU-minősített adatoknak az érintett harmadik állam vagy nemzetközi szervezet részére történő, a kibocsátó beleegyezésének elvével összhangban álló átadására. A főtitkár átruházhatja ezt a felhatalmazást a Főtitkárság valamely vezető tisztviselőjére.
38. Amennyiben létezik a 2. pont első francia bekezdése szerinti adatbiztonsági megállapodás, a Tanács határozhat úgy, hogy engedélyezi a főképviselőnek, hogy a közös kül- és biztonságpolitika területéhez tartozó, a Tanácstól származó EU-minősített adatokat adjon át az érintett harmadik államnak vagy nemzetközi szervezetnek azt követően, hogy megkapta az ezekben szereplő forrásanyagok kibocsátójától a hozzájárulást. A főképviselő átruházhatja ezt a felhatalmazást az EKSZ vezető tisztviselőire vagy az EUKK-kra.
39. Amennyiben létezik a minősített adatok harmadik államokkal vagy nemzetközi szervezetekkel való cseréjének 2. vagy 3. pont szerinti kerete, a főképviselő felhatalmazást kap EU-minősített adatoknak a KBVP-művelet létrehozásáról szóló együttes fellépéssel és a kibocsátó beleegyezésének elvével összhangban álló átadására. A főképviselő átruházhatja ezt a felhatalmazást az EKSZ vezető tisztviselőire, az uniós művelet, haderő vagy misszió vezetőire vagy az uniós küldöttségek vezetőire.

*Függelék**A. függelék*

Fogalommeghatározások

B. függelék

Minősítési jelölések egyenértékűségi táblázata

C. függelék

A nemzeti biztonsági hatóságok (NSA-k) jegyzéke

D. függelék

A rövidítések jegyzéke

A. függelék

FOGALOMMEGHATÁROZÁSOK

E határozat alkalmazásában:

„akkreditáció”: a biztonsági akkreditációs hatóság (SAA) arra vonatkozó hivatalos nyilatkozatát megelőző eljárás, miszerint a rendszer alkalmas arra, hogy működési környezetében meghatározott minősítési szinten, konkrét biztonsági üzemmódban és elfogadható kockázati szinten működjön, feltételezve azt, hogy jóváhagyott műszaki, fizikai, szervezeti és eljárási biztonsági intézkedéseket alkalmaznak;

„javak”: valamely szervezet, szokásos tevékenységei és azok folytonossága szempontjából értéket képviselő elemek összessége, beleértve a szervezet misszióját támogató információforrásokat is;

„engedély EU-minősített adatokhoz való hozzáférésre”: a Főtitkárság kinevezésre jogosult hatósága által valamely tagállam illetékes hatósága általi azon megállapítás alapján hozott határozat, hogy a Főtitkárságon dolgozó tisztviselő, egyéb alkalmazott vagy kirendelt nemzeti szakértő – feltéve, hogy az esetében meghatározták a „szükséges ismeretet”, és megfelelő tájékoztatást kapott az ezzel kapcsolatos felelősségéről – meghatározott minősítési szintig (CONFIDENTIEL UE/EU CONFIDENTIAL vagy e fölött) és meghatározott időpontig hozzáférést kaphat EU-minősített adatokhoz;

„a CIS életciklusa”: a CIS létezésének teljes időtartama, amely magában foglalja a következőket: javaslat, javaslat elfogadása, tervezés, követelményelemzés, kidolgozás, kifejlesztés, tesztelés, végrehajtás, üzemelés és karbantartás, valamint leállítás;

„minősített szerződés”: a Főtitkárság által egy adott vállalkozóval árubeszerzés, munkálatok elvégzése vagy szolgáltatásnyújtás céljából kötött szerződés, amelynek teljesítése EU-minősített adatokhoz való hozzáférést vagy ilyen adatok létrehozását teszi szükségessé vagy foglalja magában;

„minősített alvállalkozói szerződés”: a Főtitkárság által egy másik vállalkozóval (azaz alvállalkozóval) áruellátás, munkálatok elvégzése vagy szolgáltatásnyújtás céljából kötött szerződés, amelynek teljesítése EU-minősített adatokhoz való hozzáférést vagy ilyen adatok létrehozását teszi szükségessé vagy foglalja magában;

„kommunikációs és információs rendszer (CIS)”: lásd a 10. cikk (2) bekezdését;

„vállalkozó”: szerződéskötési képességgel rendelkező természetes vagy jogi személy;

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

„kriptográfiai termék”: olyan termék, amelynek elsődleges és fő feladata, hogy egy vagy több kriptográfiai mechanizmuson keresztül biztonsági szolgáltatásokat (bizalmasság, sértetlenség, rendelkezésre állás, hitelesség, letagadhatatlanság) nyújtson;

„KBVP-művelet”: az EUSZ V. címének II. fejezete szerint létrehozott katonai vagy polgári válságkezelési művelet;

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

„mélységi/arányos védelem”: többszintű védelembe szervezett biztonsági intézkedések alkalmazása;

„kijelölt biztonsági hatóság (DSA)”: egy adott tagállam nemzeti biztonsági hatóságának (NSA) felelős hatóság, amelynek feladata az ipari és egyéb szervezetek tájékoztatása az iparbiztonságot érintő ügyekre vonatkozó nemzeti politikáról, valamint iránymutatás és segítségnyújtás biztosítása a politikák végrehajtása során. A DSA feladatait az NSA vagy bármely más illetékes hatóság is elvégezheti;

„dokumentum”: bármilyen rögzített adat, fizikai formájától vagy jellemzőitől függetlenül;

„visszaminősítés”: a minősítési szint leszállítása.

„EU-minősített adat (EUCI)”: lásd a 2. cikk (1) bekezdését;

„telephely-biztonsági tanúsítvány”: annak az NSA vagy DSA által történő hivatalos meghatározása, hogy egy adott létesítmény biztonsági szempontból megfelelő szintű védelmet tud-e nyújtani meghatározott biztonsági minősítésű szintű EU-minősített adatoknak;

EU-minősített adat „kezelése”: minden olyan lehetséges tevékenység, amelynek az EU-minősített adat életciklusa során ki lehet téve. Beletartozik az adat előállítása, feldolgozása, szállítása, visszaminősítése, a rá vonatkozó minősítés feloldása és az adat megsemmisítése. A CIS-szel összefüggésben ezenfelül az adat gyűjtését, megjelenítését, átadását és tárolását is tartalmazza;

„birtokos”: olyan, megfelelő engedéllyel rendelkező, a „szükséges ismeret” feltételének eleget tévő személy, aki EU-minősített adat birtokában van, és ennek megfelelően felel annak védelméért;

„ipari vagy egyéb szervezet”: árubeszerzésben, munkálatok elvégzésében vagy szolgáltatásnyújtásban érintett szervezet; ez magában foglalhat ipari, kereskedelmi, szolgáltatói, tudományos, kutatási, oktatási vagy fejlesztési tevékenységet végző szervezeteket, vagy önálló vállalkozói tevékenységet végző személyt;

„iparbiztonság”: lásd a 11. cikk (1) bekezdését;

„információvédelem”: lásd a 10. cikk (1) bekezdését;

„összekapcsolás”: lásd a IV. melléklet 32. pontját;

„a minősített adatok kezelése”: lásd a 9. cikk (1) bekezdését;

„anyag”: dokumentum, adathordozó, vagy bármely készre gyártott vagy gyártás alatt álló gép vagy berendezés;

„kibocsátó”: olyan uniós intézmény, szerv vagy ügynökség, tagállam, harmadik állam vagy nemzetközi hatóság, amelynek fennhatósága alatt minősített adatokat hoztak létre és/vagy vittek be az uniós struktúrákba;

„személyi biztonság”: lásd a 7. cikk (1) bekezdését;

„személyi biztonsági tanúsítvány (PSC)”: 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 meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig és meghatározott időpontig hozzáférés biztosítható EU-minősített adatokhoz;

„személyi biztonsági tanúsítványról szóló igazolás (PSCC)”: valamely illetékes hatóság által kiadott igazolás, amely tartalmazza, hogy az adott személy biztonsági ellenőrzésen átesett, és biztonsági tanúsítványról szóló igazolással vagy a kinevezésre jogosult hatóságtól származó, az EU-minősített adatokhoz való hozzáférést lehetővé tevő engedéllyel rendelkezik, továbbá azt, hogy milyen szintű EU-minősített adatokhoz férhet hozzá (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint a vonatkozó PSC érvényességi idejét és a tanúsítvány lejártának időpontját;

„fizikai biztonság”: lásd a 8. cikk (1) bekezdését;

„adott programra/projektre vonatkozó biztonsági utasítások (PSI)”: adott programra/projektre alkalmazandó biztonsági eljárások felsorolása a biztonsági eljárások egységesítése céljából. A felsorolás a program/projekt teljes időtartama alatt felülvizsgálható;

„nyilvántartásba vétel”: lásd a III. melléklet 18. pontját;

„fennmaradó kockázat”: biztonsági intézkedések végrehajtását követően fennmaradó kockázat, tekintve, hogy nem lehet minden fenyegetést elhárítani és minden sebezhetőséget megszüntetni;

„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. Mérése a fenyegetések bekövetkezése valószínűségének és hatásának kombinációjával történik.

- „kockázattelfogadás”: a kockázatkezelést követően fennmaradó kockázat további meglétéhez való hozzájárulásra vonatkozó határozat,
- „kockázattértékelés”: a fenyegetések és sebezhetőségek azonosításából, valamint a kapcsolódó kockázatelemzésből, azaz a valószínűség és a hatás elemzéséből áll,
- „kockázatkommunikáció”: a CIS felhasználói közösségei körében a kockázatokkal kapcsolatos tudatosság növelése, a jóváhagyó hatóságok tájékoztatása a kockázatokról és jelentéstétel azokról a működtető hatóságok részére,
- „kockázatkezelés”: a kockázat (megfelelő technikai, fizikai, szervezeti vagy eljárási intézkedések kombinálásával történő) enyhítése, megszüntetése, csökkentése, illetve annak átruházása vagy figyelemmel kísérése;

„biztonsági vonatkozások záradéka (SAL)”: különös szerződéses feltételek szerződő hatóság által összeállított jegyzéke, amely szerves részét képezi az EU-minősített adathoz való hozzáférést vagy ilyen adat létrehozását magában foglaló minősített szerződésnek, és amely meghatározza a biztonsági követelményeket vagy a szerződésnek a biztonsági védelmet igénylő elemeit;

„minősítési útmutató (SCG)”: olyan dokumentum, amely – az alkalmazandó biztonsági minősítési szint meghatározása mellett – leírja egy program vagy szerződés minősített elemeit. Az SCG kiterjeszthető a program vagy szerződés teljes időtartamára, az egyes információk pedig újraosztályozhatók, illetve alacsonyabb szintbe sorolhatók; amennyiben létezik SCG, az a SAL része kell, hogy legyen;

„biztonsági ellenőrzés”: valamely tagállam illetékes hatósága által a nemzeti jogszabályokkal és rendelkezésekkel összhangban lefolytatott vizsgálati eljárás, amelynek célja annak megállapítása, hogy egy adott személy tekintetében nem ismeretes olyan kizáró információ, amely megakadályozná, hogy meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig EU-minősített adatokhoz való hozzáférést lehetővé tévő PSC-t vagy engedélyt kapjon;

„biztonsági üzemmód”: a CIS működési feltételeinek meghatározása a kezelt adatok minősítése, valamint a felhasználók biztonsági tanúsítványának szintje, hivatalos hozzáférési engedélye és a szükséges ismeret elve alapján. Minősített adatok kezelése vagy továbbítása négy üzemmódban történhet: kizárólagos, domináns, megosztott és többszintű üzemmód:

- „kizárólagos üzemmód”: olyan üzemmód, amelyben a CIS-hez hozzáféréssel rendelkező minden személy a CIS-ben kezelt adatok legmagasabb minősítési szintjének megfelelő biztonsági tanúsítvánnyal rendelkezik, és a CIS-ben kezelt minden adat tekintetében egységes elvet alkalmaznak a szükséges ismeretre vonatkozóan,
- „domináns üzemmód”: olyan üzemmód, amelyben a CIS-hez hozzáféréssel rendelkező minden személy a CIS-ben kezelt adatok legmagasabb minősítési szintjének megfelelő biztonsági tanúsítvánnyal rendelkezik, ugyanakkor a CIS-ben kezelt adatok ismeretére nincs a CIS-hez hozzáféréssel rendelkező minden személynek egységesen szüksége; az adathoz való hozzáférésre vonatkozó jóváhagyást megadhatja egyetlen személy,
- „megosztott üzemmód”: olyan üzemmód, amelyben a CIS-hez hozzáféréssel rendelkező minden személy a CIS-ben kezelt adatok legmagasabb minősítési szintjének megfelelő biztonsági tanúsítvánnyal rendelkezik, ugyanakkor a CIS-ben kezelt minden adathoz való hozzáférésre nincsen a CIS-hez hozzáféréssel rendelkező minden személynek hivatalos engedélye; a hivatalos engedély feltételezi, hogy létezik a hozzáférés engedélyezésének egy hivatalos központi irányítása, amely nem azonos azzal, hogy egyetlen személy határoz a hozzáférés megadásáról,
- „többszintű üzemmód”: olyan üzemmód, amelyben a CIS-hez hozzáféréssel rendelkező személyek közül nem mind-egyik rendelkezik a CIS-ben kezelt adatok legmagasabb minősítési szintjének megfelelő biztonsági tanúsítvánnyal, és a CIS-ben kezelt adatok ismeretére nincs a CIS-hez hozzáféréssel rendelkező minden személynek egységesen szüksége;

„biztonsági kockázatkezelési eljárás”: egy adott szervezet vagy az általa használt bármely rendszer biztonságát esetleg érintő, bizonytalan események azonosítására, ellenőrzésére és minimálisra csökkentésére irányuló folyamat egésze. Ez kiterjed valamennyi kockázati vonatkozású tevékenységre, az értékelést, kezelést, elfogadást és kommunikációt is beleértve;

„TEMPEST”: az illetéktelen tudomására jutást lehetővé tevő elektromágneses kisugárzások felderítése, vizsgálata és ellenőrzése, valamint a visszaszorításukra irányuló intézkedések;

„fenyegetés”: egy adott szervezet számára vagy az általa használt bármely rendszerben esetlegesen károsodást eredményező, nem kívánt esemény lehetséges okozása; e fenyegetések lehetnek véletlenszerűek vagy szándékosak (rosszindulatiak), és azokat fenyegető elemek, potenciális célpontok és támadási módszerek jellemezhetik;

„sebezhetőség”: bármilyen jellegű sérülékenység, amelyet egy vagy több fenyegetés kihasználhat. A sebezhetőség oka lehet hiányosság, vagy az összefüggő ellenőrzés gyengeségével, hiányosságával vagy következtetlenségével, továbbá lehet technikai, eljárási, fizikai, szervezeti vagy üzemeltetési jellegű.

B. függelék

MINŐSÍTÉSI JELÖLÉSEK EGYENÉRTÉKŰSÉGI TÁBLÁZATA

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgium	Très Secret (Loi 1998.12.11.) Zeet Geheim (Wet 1998.12.11.)	Secret (Loi 1998.12.11.) Geheim (Wet 1998.12.11.)	Confidentiel (Loi 1998.12.11.) Vertrouwelijk (Wet 1998.12.11.)	lásd az ⁽¹⁾ lábjegyzetet
Bulgária	Строго секретно	Секретно	Поверително	За служебно ползване
Cseh Köztársaság	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánia	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Németország	STRENG GEHEIM	GEHEIM	VS ⁽²⁾ – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Észtország	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Írország	Top Secret	Secret	Confidential	Restricted
Görögország	Άκρως Απόρρητο röv.: ΑΑΠ	Απόρρητο röv.: (ΑΠ)	Εμπιστευτικό röv.: (ΕΜ)	Περιορισμένης Χρήσης röv.: (ΠΧ)
Spanyolország	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Franciaország	Très Secret Défense	Secret Défense	Confidentiel Défense	lásd a ⁽³⁾ lábjegyzetet
Horvátország	VRLO	TAJNO/TAJNO	POVJERLJIVO	OGRANIČENO
Olaszország	Segretissimo	Segreto	Riservatissimo	Riservato
Ciprus	Άκρως Απόρρητο röv.: (ΑΑΠ)	Απόρρητο röv.: (ΑΠ)	Εμπιστευτικό röv.: (ΕΜ)	Περιορισμένης Χρήσης röv.: (ΠΧ)
Lettország	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litvánia	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Magyarország	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Málta	L-Oghla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ⁽⁴⁾
Hollandia	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Ausztria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lengyelország	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugália	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Románia	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Szlovénia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Szlovákia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finnország	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Svédország ⁽⁵⁾	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDEN- TIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Egyesült Királyság	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

⁽¹⁾ A „Diffusion Restreinte/Beperkte Verspreiding” Belgiumban nem biztonsági minősítés. Belgium a „RESTREINT UE/EU RESTRICTED” minősítésű információt az Európai Unió Tanácsának biztonsági szabályzatában leírt előírásoknál és eljárásoknál nem kevésbé szigorú módon kezeli és védi.

⁽²⁾ Németország: VS = Verschlusssache.

⁽³⁾ Franciaország nem alkalmazza a „RESTREINT” minősítést nemzeti rendszerében. Franciaország a „RESTREINT UE/EU RESTRICTED” minősítésű információt az Európai Unió Tanácsának biztonsági szabályzatában leírt előírásoknál és eljárásoknál nem kevésbé szigorú módon kezeli és védi.

⁽⁴⁾ Málta esetében a máltai és az angol nyelvű jelzések egyaránt használhatók.

⁽⁵⁾ Svédország: a felső sorban feltüntetett biztonsági minősítési megjelöléseket a védelmi hatóságok, az alsó sorban feltüntetetteket az egyéb hatóságok alkalmazzák.

C. függelék

A NEMZETI BIZTONSÁGI HATÓSÁGOK (NSA-K) JEGYZÉKE

BELGIUM Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Titkársági telefonszám: +32 25014542 Fax +32 25014596 E-mail: nvo-ans@diplobel.fed.be	ÉSZTORSZÁG National Security Authority Department Estonian Ministry of Defence (Észt Védelmi Minisztérium Nemzeti Biztonságfelügyeleti Osztály) Sakala 1 15094 Tallinn Tel. +372 7170019, +372 7170117 Fax +372 7170213 E-mail: nsa@mod.gov.ee
BULGÁRIA State Commission on Information Security (Állami Információbiztonsági Bizottság) 90 Cherkovna Str. 1505 Sofia Tel. +359 29333600 Fax +359 29873750 E-mail: dksi@government.bg Honlap: www.dksi.bg	ÍRORSZÁG National Security Authority Department of Foreign Affairs 76 – 78 Harcourt Street Dublin 2 Tel. +353 14780822 Fax +353 14082959
CSEH KÖZTÁRSASÁG Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Fax +420 257283110 E-mail: czech.nsa@nbu.cz Honlap: www.nbu.cz	GÖRÖGORSZÁG Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλ. +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227-231 HOLARGOS STG 1020 ATHENS Tel. +30 2106572045 +30 2106572009 Fax +30 2106536279 +30 2106577612
DÁNIA Politiets Efterretningstjeneste (Dán Biztonsági Hírszerző Szolgálat) Klausdalsbrovej 1 2860 Søborg Tel. +45 33148888 Fax +45 33430190 Forsvarets Efterretningstjeneste (Dán Védelmi Hírszerző Szolgálat) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Fax +45 33931320	SPANYOLORSZÁG Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n 28023 Madrid Tel. +34 913725000 Fax +34 913725808 E-mail: nsa-sp@areatec.com
NÉMETORSZÁG Bundesministerium des Innern Referat OS III 3 Alt-Moabit 101 D D-11014 Berlin Tel. +49 30186810 Fax +49 30186811441 E-mail: oesIII3@bmi.bund.de	FRANCIAORSZÁG Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Fax +33 171758200

HORVÁTOR SZÁG Ured Vijeća za nacionalnu sigurnost Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Fax +385 14686049 www.uvns.hr	LUXEMBURG Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 (központi szám) +352 24782253 (közvetlen szám) Fax +352 24782243
OLASZORSZÁG Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se. Via di Santa Susanna, 15 00187 Roma Tel. +39 0661174266 Fax +39 064885273	MAGYARORSZÁG Nemzeti Biztonsági Felügyelet 1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel. +36 17952303 Fax +36 17950344 Postai cím: 1357 Budapest, PO Box 2 E-mail: nbf@nbf.hu Honlap: www.nbf.hu
CIPRUS ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel. +357 22807569, +357 22807643, +357 22807764 Fax +357 22302351 E-mail: cynsa@mod.gov.cy	ΜΑΛΤΑ Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Fax +356 25695321
LETTOR SZÁG National Security Authority Constitution Protection Bureau of the Republic of Latvia (A Lett Köztársaság Alkotmányvédelmi Hivatalának Nemzeti Biztonsági Hatósága) P.O. Box 286 LV-1001 Riga Tel. +371 67025418 Fax +371 67025454 E-mail: ndi@sab.gov.lv	HOLLANDIA Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Fax +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Fax +31 703187522
LITVÁNIA Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (A Litván Köztársaság Titokvédelmi Koordinációs Bizottsága Nemzeti Biztonsági Hatóság) Gedimino 40/1 LT-01110 Vilnius Tel. +370 70666701, +370 70666702 Fax +370 70666700 E-mail: nsa@vds.lt	AUSZTRIA Informationssicherheitskommission Bundeskansleramt Ballhausplatz 2 1014 Wien Tel. +43 1531152594 Fax +43 1531152615 E-mail: ISK@bka.gv.at

LENGYELORSZÁG Agencja Bezpieczeństwa Wewnętrznego – ABW (Belső Biztonsági Ügynökség) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857360 Fax +48 225858509 E-mail: nsa@abw.gov.pl Honlap: www.abw.gov.pl	SZLOVÁKIA Národný bezpečnostný úrad (Nemzeti Biztonsági Hatóság) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel. +421 268692314 Fax +421 263824005 Honlap: www.nbusr.sk
PORTUGÁLIA Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel. +351 213031710 Fax +351 213031711	FINNORSZÁG National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 16055890 Fax +358 916055140 E-mail: NSA@formin.fi
ROMÁNIA Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS) Minősített Információk Nemzeti Nyilvántartó Hivatala) Str. Mureș nr. 4, sector 1 012275 București Tel. +40 212245830 Fax +40 212240714 E-mail: nsa.romania@nsa.ro Honlap: www.orniss.ro	SVÉDORSZÁG Utrikesdepartementet (Külgymisztérium) UD-RS S-10339 Stockholm Tel. +46 84051000 Fax +46 87231176 E-mail: ud-nsa@foreign.ministry.se
SZLOVÉNIA Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel. +386 14781390 Fax +386 14781399 E-mail: gp.uvtp@gov.si	EGYESÜLT KIRÁLYSÁG UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Tel. 1 +44 2072765645 Tel. 2 +44 2072765497 Fax +44 2072765651 E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

D. függelék

A RÖVIDÍTÉSEK JEGYZÉKE

Betűszó	Jelentés
AQUA	megfelelő minősítéssel rendelkező hatóság
BPS	határvédelmi szolgálatok
CAA	kriptográfiai jóváhagyó hatóság
CCTV	zárt láncú televízió
CDA	kriptográfiai terjesztési hatóság
CFSP	közös kül- és biztonságpolitika (KKBP)
CIS	az EU-minősített adatokat kezelő kommunikációs és információs rendszer
COREPER	az Állandó Képviselők Bizottsága
CSDP	közös biztonság- és védelempolitika (KBVP)
DSA	kijelölt biztonsági hatóság
ECSD	az Európai Bizottság Biztonsági Igazgatósága
EUCI	EU-minősített adat
EUSR	az EU különleges képviselője (EUKK)
FSC	telephely-biztonsági tanúsítvány
GSC	a Tanács Főtitkársága
IA	információvédelem
IAA	információvédelmi hatóság
IDS	behatolásjelző rendszer
IT	információtechnológia
NSA	nemzeti biztonsági hatóság
PSC	személyi biztonsági tanúsítvány
PSCC	személyi biztonsági tanúsítványról szóló igazolás
PSI	a programra/a projektre vonatkozó biztonsági utasítások
SAA	biztonsági akkreditációs hatóság
SAB	Biztonsági Akkreditációs Bizottság
SAL	biztonsági vonatkozások záradéka
SecOPs	biztonsági üzemeltetési eljárások
SCG	biztonsági minősítési útmutató
SSRS	rendszerspecifikus biztonsági követelmények megállapítása
TA	TEMPEST-hatóság