Az Európai Unió
Hivatalos Lapja

C 126

61. évfolyam

Magyar nyelvű kiadás

Tájékoztatások és közlemények

2018. április 10.

Tartalom

HU

IV

(Tájékoztatások)

AZ EURÓPAI UNIÓ INTÉZMÉNYEITŐL, SZERVEITŐL, HIVATALAITÓL ÉS ÜGYNÖKSÉGEITŐL SZÁRMAZÓ TÁJÉKOZTATÁSOK

EURÓPAI KÜLÜGYI SZOLGÁLAT

Az Unió külügyi és biztonságpolitikai főképviselőjének 2017. szeptember 19-i határozata az Európai Külügyi Szolgálat biztonsági szabályairól

ADMIN(2017) 10

(2018/C 126/01)

AZ UNIÓ KÜLÜGYI ÉS BIZTONSÁGPOLITIKAI FŐKÉPVISELŐJE,

tekintettel az Európai Külügyi Szolgálat (a továbbiakban: EKSZ) szervezetének és működésének a megállapításáról szóló, 2010. július 26-i 2010/427/EU tanácsi határozatra ([1]),

tekintettel az Európai Külügyi Szolgálat biztonsági szabályairól szóló, 2011. június 15-i főképviselői határozat ([2]) 9. cikkének (6) bekezdésében említett bizottság véleményére,

mivel:

(1) Az EKSZ-nek az Európai Unió önálló, függetlenül működő szerveként a 2010/427/EU tanácsi határozat 10. cikkének (1) bekezdése szerinti biztonsági szabályokkal kell rendelkeznie.

(2) Az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: főképviselő) határoz az EKSZ működésének valamennyi biztonsági szempontjára kiterjedő biztonsági szabályzatról, annak érdekében, hogy az EKSZ hatékonyan kezelje a felelőssége alá tartozó személyzettel, a fizikai eszközeivel és a birtokában lévő információkkal, valamint a látogatóival kapcsolatos kockázatokat, továbbá hogy eleget tegyen a vonatkozó gondossági kötelezettségének.

(3) Különösen az EKSZ felelőssége alá tartozó személyzet, az EKSZ fizikai eszközei – köztük a kommunikációs és információs rendszerek –, a birtokában lévő adatok és a látogatói számára kell olyan szintű védelmet biztosítani, ami összhangban áll a Tanács, a Bizottság, a tagállamok és adott esetben nemzetközi szervezetek bevált gyakorlataival.

(4) Az EKSZ biztonsági szabályainak segítenie kell az EU-minősített adatok védelmére vonatkozó, koherensebb átfogó, általános keret kialakítását az Európai Unión belül, az Európai Unió Tanácsa (a továbbiakban: a Tanács) biztonsági szabályai és a Bizottság biztonsági rendelkezései alapján, és azokkal a lehető legkoherensebb módon.

(5) Az EKSZ, a Tanács és a Bizottság elkötelezett az iránt, hogy egyenértékű biztonsági előírásokat alkalmazzanak az EU-minősített adatok védelmére vonatkozóan.

(6) Ez a határozat nem érinti az Európai Unió működéséről szóló szerződés (EUMSZ) 15. és 16. cikkét, sem az azokat végrehajtó jogi aktusokat.

([1]) HL L 201., 2010.8.3., 30. o.
([2]) HL C 304., 2011.10.15., 7. o.

(7) Szükség van az EKSZ-en belüli biztonsági szervezet kialakítására, valamint a biztonsági feladatoknak az EKSZ szervezetén belüli felosztására.

(8) A főképviselőnek szükség esetén igénybe kell vennie a tagállamok, a Tanács Főtitkársága és a Bizottság szakértelmét.

(9) A főképviselőnek a tagállamok, a Tanács Főtitkársága és a Bizottság támogatásával meg kell tennie az e szabályok végrehajtásához szükséges valamennyi megfelelő intézkedést.

(10) Az EKSZ biztonsági hatósága az EKSZ főtitkára, és az Európai Külügyi Szolgálat főtitkára 2015. szeptember 14-i ADMIN (2015)34 határozatának 1. cikke értelmében a biztonsági hatóság biztonsággal kapcsolatos feladatait – az EKSZ biztonsági szabályaiban meghatározottakkal összhangban – a költségvetésért és igazgatásért felelős főigazgató látja el,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Tárgy és hatály

A határozat lefekteti az Európai Külügyi Szolgálat biztonsági szabályait (a továbbiakban: *az EKSZ biztonsági szabályai*).

Az Európai Külügyi Szolgálat szervezetének és működésének a megállapításáról szóló, 2010. július 26-i 2010/427/EU tanácsi határozat 10. cikkének (1) bekezdése értelmében a határozat az EKSZ teljes személyzetére és az uniós küldöttségek teljes személyzetére alkalmazandó, függetlenül az egyes személyek jogállásától vagy kinevezésének módjától, valamint meghatározza a 2. cikkben említettek szerint az EKSZ felelőssége alá tartozó személyzettel, az EKSZ helyiségeivel, a fizikai eszközeivel, a birtokában lévő adatokkal és a látogatóival kapcsolatos kockázatok hatékony kezelésére vonatkozó általános szabályozási keretet.

2. cikk

Fogalommeghatározások

E határozat alkalmazásában:

a) „Az EKSZ személyzete”: az EKSZ tisztviselői és egyéb alkalmazottai, beleértve a tagállamok diplomáciai szolgálatainak ideiglenes alkalmazottként kinevezett tagjait és a kirendelt nemzeti szakértőket, az Európai Külügyi Szolgálat szervezetének és működésének a megállapításáról szóló, 2010. július 26-i 2010/427/EU tanácsi határozat 6. cikkében meghatározottaknak megfelelően.

b) „Az EKSZ felelőssége alá tartozó személyzet”: az EKSZ székhelyén és az uniós küldöttségeken foglalkoztatott személyzete és az uniós küldöttségek teljes egyéb személyzete, függetlenül az egyes személyek jogállásától vagy kinevezésének módjától, továbbá e határozat összefüggésében a főképviselő és adott esetben az EKSZ székhelyének helyiségeiben tevékenykedő egyéb személyzet.

c) „Eltartottak”: az uniós küldöttségeken az EKSZ felelőssége alá tartozó személyzet háztartásában élő családtagok, a fogadó állam külügyminisztériumának tett bejelentésnek megfelelően.

d) „Az EKSZ helyiségei”: az EKSZ valamennyi létesítménye, beleértve az épületeket, irodákat, termeket és egyéb területeket, valamint az olyan területeket, amelyek kommunikációs és információs rendszereknek adnak helyet (beleértve az EU-minősített adatokat kezelő rendszereket), ahol az EKSZ állandó vagy ideiglenes tevékenységet folytat.

e) „Az EKSZ biztonsági érdekei”: az EKSZ felelőssége alá tartozó személyzet, az EKSZ helyiségei, az eltartottak, a fizikai eszközök, beleértve a kommunikációs és információs rendszereket, az adatok és a látogatók.

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

g) „Uniós küldöttség”: harmadik országokban és nemzetközi szervezetekben működő küldöttség az Európai Külügyi Szolgálat szervezetének és működésének megállapításáról szóló, 2010. július 26-i 2010/427/EU tanácsi határozat 1. cikkének (4) bekezdésében említettek szerint.

Egyéb meghatározások a vonatkozó mellékletekben és az A. függelékben szerepelnek.

3. cikk

Gondossági kötelezettség

1. Az EKSZ biztonsági szabályainak célja, hogy eleget tegyenek az EKSZ gondossági kötelezettségének.

2. Az EKSZ gondossági kötelezettségébe beletartozik a kellő gondosság érvényesítése az EKSZ biztonsági érdekeit érintő, észszerűen előre látható károk megelőzését célzó biztonsági intézkedések végrehajtását szolgáló valamennyi észszerű lépés megtétele során.

Ez felöleli a biztonsági és a védelmi elemeket, beleértve a vészhelyzetből vagy válságból adódóakat, azok jellegétől függetlenül.

3. Figyelembe véve a tagállamok, az uniós intézmények vagy szervek és az uniós küldöttségeken és/vagy az uniós küldöttségek helyiségeiben személyzettel rendelkező egyéb érdekelt felek gondossági kötelezettségét, vagy – amennyiben az uniós küldöttségeknek a fent említett egyéb érdekelt felek helyiségei adnak otthont – az EKSZ-re háruló ilyen kötelezettséget, az EKSZ-nek a fenti szervezetek mindegyikével igazgatási megállapodásokat kell kötnie, amelyekben ki kell térni az egyes felek szerepére, felelősségi körére, feladataira és az együttműködési mechanizmusokra.

4. cikk

Fizikai és infrastruktúra-biztonság

1. Az EKSZ megteszi az összes megfelelő (állandó vagy ideiglenes) fizikai biztonsági intézkedést – beleértve a hozzáférés-ellenőrzési intézkedéseket – az EKSZ minden helyiségében az EKSZ biztonsági érdekeinek védelmére. Az ilyen intézkedéseket figyelembe kell venni az új helyiségek kialakításánál és tervezésénél, vagy meglévő helyiségek bérlése előtt.

2. Az EKSZ felelőssége alá tartozó személyzet és az eltartottak számára biztonsági okokból különleges kötelezettségek és korlátozások írhatók elő meghatározott időszakra és meghatározott területekre vonatkozóan.

3. Az (1) és a (2) bekezdésben említett intézkedéseknek arányosnak kell lenniük a becsült kockázatokkal.

5. cikk

Riasztási fokozatok és a válsághelyzetek kezelése

1. Az I. szakasz 13. cikkének (1) bekezdése szerinti az EKSZ biztonsági hatósága felel a riasztási fokozatokra vonatkozó megfelelő intézkedések végrehajtásáért – az EKSZ-en belüli biztonságot érintő fenyegetésekre és incidensekre való felkészülés vagy az azokra való reagálás jegyében –, és a válsághelyzetek kezeléséhez szükséges intézkedésekért.

2. Az (1) bekezdésben említett riasztási fokozatokra vonatkozó intézkedéseknek arányosnak kell lenniük a biztonsági fenyegetés szintjével. A riasztási fokozatok szintjeit szoros együttműködésben határozzák meg az egyéb uniós intézmények, ügynökségek és szervek, valamint az EKSZ helyiségeinek otthont adó tagállam vagy tagállamok illetékes szolgálataival.

3. A riasztási fokozatok és a válsághelyzetek kezelése tekintetében az EKSZ biztonsági hatósága a kapcsolattartó pont.

6. cikk

A minősített adatok védelme

1. Az EU-minősített adatok védelmére az ebben a határozatban és különösen az A. mellékletben megállapított követelmények vonatkoznak. Az EU-minősített adatok birtokosai felelősek az adatok megfelelő védelméért.

2. Az EKSZ biztosítja, hogy csak olyan személyek kapjanak hozzáférést a minősített adatokhoz, akik megfelelnek az A. melléklet 5. cikkében előírt feltételeknek.

3. A főképviselő szintén meghatározza azokat a feltételeket, amelyek alapján a helyi alkalmazottak hozzáférhetnek az EU-minősített adatokhoz, az e határozat A. mellékletében előírt, az EU-minősített adatok védelmére vonatkozó szabályokkal összhangban.

4. Az EKSZ Biztonsági Igazgatósága adatbázist vezet az EKSZ felelőssége alá tartozó személyzet és az EKSZ-szel szerződéses jogviszonyban álló vállalkozók biztonsági tanúsítványának állapotáról.

5. Amennyiben a tagállamok nemzeti biztonsági minősítési jelöléssel ellátott minősített adatokat visznek be az EKSZ struktúráiba vagy hálózataiba, az EKSZ ezeket az adatokat az azonos szintű EU-minősített adatokra alkalmazandó előírásoknak megfelelően védi az e határozat B. függelékében szereplő, a biztonsági minősítésekre vonatkozó egyenértékűségi táblázatában foglaltak szerint.

6. Az EKSZ-en belül a CONFIDENTIEL UE/EU CONFIDENTIAL vagy ennél magasabb, vagy ezeknek megfelelő minősítésű adatok tárolására szolgáló helyiségeket biztonsági területként alakítják ki az e határozat A.II. mellékletében foglalt szabályoknak megfelelően, és azokat az EKSZ biztonsági hatósága hagyja jóvá.

7. Az EU-minősített adatok harmadik államokkal vagy nemzetközi szervezetekkel történő megosztására vonatkozó megállapodások vagy igazgatási megállapodások értelmében a főképviselőre háruló feladatok ellátására vonatkozó eljárások leírása e határozat A. és A.VI. mellékletében szerepel.

8. A főtitkár meghatározza, hogy az EKSZ milyen feltételek mellett oszthatja meg a birtokában lévő EU-minősített adatokat más uniós intézményekkel, szervekkel, hivatalokkal vagy ügynökségekkel. E célból kialakítanak egy megfelelő keretet, többek között intézményközi, illetve egyéb megállapodások megkötése révén, amennyiben azok szükségesnek minősülnek.

9. Ennek a keretnek biztosítania kell, hogy az EU-minősített adatok a minősítési szintjüknek megfelelő, valamint az e határozatban megállapítottakkal egyenértékű alapelveknek és minimumszabályoknak megfelelő védelemben részesüljenek.

7. cikk

Biztonsági incidensek és vészhelyzetek

1. A biztonsági incidensekre való időben történő és hatékony reagálás érdekében az EKSZ kialakítja az ilyen incidensekre és vészhelyzetekre vonatkozó jelentéstételi eljárást, amely a hét minden napján, napi huszonnégy órában működik, és kiterjed az EKSZ biztonsági érdekeit érintő bármely biztonsági incidensre vagy fenyegetésre (például baleset, konfliktus, rosszhiszemű cselekmény, bűncselekmény, emberrablás és túszejtés, egészségügyi vészhelyzet, a kommunikációs és információs rendszerrel kapcsolatos incidensek, informatikai támadások stb.).

2. Vészhelyzeti kapcsolattartási csatornákat hoznak létre az EKSZ székhelye, az uniós küldöttségek, a Tanács, a Bizottság, az EU különleges képviselői és a tagállamok között, a személyzetet érintő biztonsági incidensek és következményeik kezelésében történő támogatásnyújtás érdekében, beleértve a vészhelyzeti tervezést is.

3. A biztonsági incidensek kezelése többek között az alábbiakra terjed ki:

— a személyzetet érintő biztonsági incidensekkel kapcsolatos döntéshozatali eljárás hatékony támogatását szolgáló eljárások, beleértve a kiküldetés kivonásával vagy felfüggesztésével kapcsolatos döntéseket is, valamint

— a személyi állomány mentésére vonatkozó politika és eljárások – pl. a személyzet tagjainak eltűnése vagy emberrablás és túszejtés esetén –, figyelembe véve a tagállamok, az uniós intézmények és az EKSZ e tekintetben fennálló különleges felelősségeit. Az ilyen műveletek irányítása során esetleg felmerülő, konkrét képességek iránti igényt a tagállamok által rendelkezésre bocsátható források szem előtt tartásával mérlegelik.

4. Az EKSZ megfelelő adminisztratív intézkedéseket vezet be az uniós küldöttségeken bekövetkező biztonsági incidensekről való jelentéstételre vonatkozóan. Szükség esetén tájékoztatják a tagállamokat, a Bizottságot, az egyéb érintett hatóságot, valamint az érintett biztonsági bizottságokat.

5. Az incidenskezelési eljárásokat rendszeresen gyakorolják és felülvizsgálják.

8. cikk

A kommunikációs és információs rendszerek biztonsága

1. Az EKSZ gondoskodik a kommunikációs és információs rendszerekben kezelt adatok védelméről a bizalmas kezelésüket, sértetlenségüket, hozzáférhetőségüket, hitelességüket és letagadhatatlanságukat érintő fenyegetésekkel szemben.

2. Az EKSZ tulajdonában lévő vagy általa üzemeltetett valamennyi kommunikációs és információs rendszer védelmére vonatkozó szabályokat, biztonsági iránymutatásokat és biztonsági programot az EKSZ biztonsági hatósága hagyja jóvá.

3. A szabályok, a politika és a program összhangban állnak és végrehajtásukat szorosan összehangolják a Tanács és a Bizottság szabályaival, politikáival és programjaival és adott esetben a tagállamok által alkalmazott biztonsági politikákkal.

4. A minősített adatot kezelő valamennyi kommunikációs és információs rendszert akkreditációs eljárásnak kell alávetni. Az EKSZ a Tanács Főtitkárságával és a Bizottsággal konzultálva a biztonsági akkreditációt kezelő rendszert alkalmaz.

5. Ha az EKSZ által kezelt EU-minősített adatok védelmét kriptográfiai termékekkel biztosítják, az ilyen termékeket az EKSZ kriptográfiai jóváhagyó hatósága hagyja jóvá a Tanács Biztonsági Bizottságának ajánlása alapján.

6. Az EKSZ biztonsági hatósága a szükséges mértékig a következő információvédelmi funkciókat hozza létre:

a) információvédelmi hatóság;

b) TEMPEST-hatóság;

c) kriptográfiai jóváhagyó hatóság;

d) kriptográfiai terjesztési hatóság.

7. Minden rendszer tekintetében az EKSZ biztonsági hatósága a következő funkciókat hozza létre:

a) biztonsági akkreditációs hatóság;

b) információvédelmi üzemeltetési hatóság.

8. Az e cikk végrehajtására vonatkozó rendelkezéseket az EU-minősített adatok védelmének tekintetében az A. és az A.IV. melléklet tartalmazza.

9. cikk

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

1. A biztonsági szabályok megsértése az e határozatban foglalt biztonsági szabályokkal és/vagy az annak végrehajtásához szükséges intézkedéseket megállapító, a 21. cikk (1) bekezdésével összhangban jóváhagyott biztonsági politikákkal vagy iránymutatásokkal ellentétes cselekmény vagy mulasztás eredményeként következik be.

2. Az EU-minősített adatok illetéktelenek tudomására jutása akkor következik be, ha az adatok részben vagy egészben illetéktelen személyek vagy felek tudomására jutnak.

3. A biztonsági szabályok megsértését vagy annak gyanúját, illetve a minősített adatok illetéktelenek tudomására jutását vagy annak gyanúját minden esetben haladéktalanul jelenteni kell az EKSZ Biztonsági Igazgatóságának, amely az A. melléklet 11. cikkében előírtak alapján megteszi a szükséges intézkedéseket.

4. Az e határozatban megállapított biztonsági szabályok megsértéséért vagy a minősített adatok illetéktelenek tudomására jutásáért felelős bármely egyén a vonatkozó jogszabályok, rendelkezések és szabályzatok szerint fegyelmi és/vagy jogi eljárás alá vonható, az A. melléklet 11. cikke (3) bekezdésének megfelelően.

10. cikk

A biztonsági incidensekre, a biztonsági szabályok megsértésére és/vagy a minősített adatok illetéktelenek tudomására jutására vonatkozó ellenőrzés, valamint a korrekciós intézkedések

1. A személyzeti szabályzat ([1]) IX. melléklete 86. cikkének (fegyelmi intézkedések) sérelme nélkül az EKSZ Biztonsági Főigazgatósága biztonsági ellenőrzést végezhet:

a) EU-minősített vagy Euratom-minősített adatok, vagy nem minősített érzékeny adatok lehetséges kiszivárgása, helytelen kezelése vagy illetéktelenek tudomására jutása esetén;

b) az EKSZ és annak személyzete ellen irányuló, hírszerző szolgálatok által végrehajtott ellenséges támadások elhárítása érdekében;

c) az EKSZ és annak személyzete ellen irányuló terrorista támadások elhárítása érdekében;

d) számítástechnikai incidensek esetén;

e) az EKSZ általános biztonságát érintő vagy potenciálisan érintő egyéb incidensek – többek között bűncselekmény gyanúja – esetén.

2. Az EKSZ Biztonsági Igazgatósága, adott esetben a tagállamok és/vagy más uniós intézmények szakértőinek támogatásával, és szükség esetén az EKSZ biztonsági hatóságának engedélyével adott esetben és a megfelelő időben végrehajtja az ellenőrzések alapján szükséges korrekciós intézkedéseket.

Az EKSZ-en belüli biztonsági ellenőrzések koordinálására vonatkozó hatáskörrel kizárólag az EKSZ biztonsági hatósága által ráruházott, névre szóló megbízás alapján felhatalmazással rendelkező személyzetet lehet, jelenlegi feladatkörére tekintettel, megbízni.

3. Az ellenőrzést végző személyek hozzáférnek az ilyen ellenőrzés lefolytatásához szükséges valamennyi adathoz, és e tekintetben megkapnak minden támogatást az EKSZ valamennyi szolgálatától és teljes személyzetétől.

Az ellenőrzést végző személyek megfelelő intézkedéseket tehetnek a bizonyítékok nyomvonalának oly módon történő megóvása érdekében, amely arányos az ellenőrzés tárgyát képező kérdés súlyával.

4. Amennyiben az adatokhoz való hozzáférés személyes adatokhoz kapcsolódik, beleértve a kommunikációs és információs rendszerekben tárolt adatokat is, az ilyen hozzáférésnek összhangban kell állnia a 45/2001/EK rendelettel ([2]).

5. Amennyiben az ellenőrzéshez személyes adatokat tartalmazó adatbázis létrehozására van szükség, a fent említett rendelettel összhangban értesítik az európai adatvédelmi biztost.

11. cikk

Biztonsági kockázatkezelés

1. Védelmi biztonsági szükségleteinek meghatározása érdekében az EKSZ átfogó biztonsági kockázatértékelési módszertant alakít ki, szorosan együttműködve a Bizottság Biztonsági Igazgatóságával, valamint adott esetben a Tanács Főtitkárságának Biztonsági Hivatalával.

2. Az EKSZ biztonsági érdekeit fenyegető kockázatok folyamatként kezelendők. E folyamat célja az ismert biztonsági kockázatok meghatározása, az ilyen kockázatok elfogadható szintre csökkentését szolgáló biztonsági intézkedések kialakítása, valamint a mélységi védelem elvével összhangban álló intézkedések alkalmazása. A fenti intézkedések hatékonyságát, valamint a kockázat mértékét folyamatosan értékelni kell.

([1]) A Tanács 259/68/EGK, Euratom, ESZAK rendelete az Európai Közösségek tisztviselőinek személyzeti szabályzatáról és az Európai Közösségek egyéb alkalmazottainak alkalmazási feltételeiről, a továbbiakban: személyzeti szabályzat (HL L 56., 1968.3.4., 1. o.).

([2]) Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

3. Az e határozatban rögzített szerepek, felelősségek és feladatok nem érintik az EKSZ felelőssége alá tartozó személyzet egyes tagjainak felelősségét, különös tekintettel a harmadik országokban kiküldetésben lévő uniós személyzetre, amelynek saját védelme és biztonsága tekintetében a józan észre és ítélőképességre kell hagyatkoznia, és be kell tartania az összes alkalmazandó biztonsági szabályt, előírást, eljárást és útmutatást.

4. A biztonsági kockázatok megelőzése és ellenőrzése érdekében a megbízott személyzet az e határozat hatálya alá tartozó személyek tekintetében háttérellenőrzést végezhet annak megállapítása érdekében, hogy ezen személyek számára az EKSZ létesítményeihez vagy adataihoz való hozzáférés engedélyezése biztonsági fenyegetést jelent-e. E célból – és a 45/2001/EK rendelettel összhangban – az érintett megbízott személyzet: a) felhasználhatja az EKSZ rendelkezésére álló bármely információforrást, az információforrás megbízhatóságának figyelembevételével; b) megfelelően indokolt esetben hozzáférhet az EKSZ által foglalkoztatott vagy foglalkoztatni kívánt személyek vagy vállalkozók alkalmazottainak az EKSZ birtokában levő személyzeti aktájához vagy adataihoz.

5. Az EKSZ megtesz minden észszerű intézkedést biztonsági érdekei védelmének garantálása, valamint azok észszerűen előre látható károsodásának megakadályozása érdekében.

6. Az EKSZ-ben az EU-minősített adatok teljes életciklusa során biztosított védelmét szolgáló biztonsági intézkedések arányosak különösen a minősítési szinttel, az adat vagy az anyag formájával és terjedelmével, az EU-minősített információ tárolására szolgáló létesítmények elhelyezkedésével és kialakításával, valamint a rosszindulatú és/vagy bűncselekménynek minősülő tevékenységek – köztük a kémkedés, a szabotázs és a terrorizmus – jelentette fenyegetéssel, ideértve a helyi szinten észlelt fenyegetést is.

12. cikk

Biztonságtudatosság és képzés

1. Az EKSZ biztonsági hatósága biztosítja, hogy megfelelő biztonságtudatossági és képzési programok készüljenek és valósuljanak meg, és az EKSZ felelőssége alá tartozó személyzet, illetve adott esetben eltartott családtagjaik megkapják a szükséges, a tartózkodási- vagy munkahelyükön fennálló kockázatokkal arányos felvilágosítást és képzést.

2. Az EU-minősített adatokhoz való hozzáférés megadása előtt, valamint ezt követően rendszeres időközönként a személyzet a 6. cikken alapuló szabályokkal összhangban tájékoztatást kap az EU-minősített adatok védelméről, és vállalja az ezzel kapcsolatos felelősséget.

13. cikk

Az EKSZ biztonsági szervezete

1. szakasz

Általános rendelkezések

1. A főtitkár az EKSZ biztonsági hatóságaként jár el. E minőségében a főtitkár biztosítja, hogy:

a) a biztonsági intézkedéseket szükség szerint összehangolják a tagállamok illetékes hatóságaival, a Tanács Főtitkárságával és a Bizottsággal, valamint adott esetben harmadik államok illetékes hatóságaival vagy nemzetközi szervezetekkel az EKSZ tevékenysége szempontjából fontos valamennyi biztonsági kérdésben, ideértve az EKSZ biztonsági érdekeit érintő kockázatok jellegét és az ezek elleni védekezés eszközeit is;

b) a biztonsági szempontokat kezdettől teljes mértékben figyelembe vegyék az EKSZ minden tevékenysége során;

c) a minősített adatokhoz való hozzáférést csak olyan személyeknek adják meg, akik megfelelnek az A. melléklet 5. cikkében előírt feltételeknek;

d) létrehozzanak egy nyilvántartási rendszert, amely biztosítja, hogy a CONFIDENTIEL UE/EU CONFIDENTIAL vagy ennél szigorúbb minősítésű adatok EKSZ-en belüli kezelése, valamint az uniós tagállamokkal, uniós intézményekkel, szervekkel vagy ügynökségekkel, illetve az engedéllyel rendelkező egyéb címzettekkel történő közlése e határozattal összhangban történjen. Külön nyilvántartást kell vezetni az EKSZ által harmadik államok vagy nemzetközi szervezetek rendelkezésére bocsátott valamennyi EU-minősített adatról, valamint a harmadik államoktól vagy nemzetközi szervezetektől kapott valamennyi minősített adatról;

e) megvalósuljanak a 16. cikkben említett biztonsági ellenőrzések;

f) a biztonsági szabályok bármely tényleges vagy feltételezett megszegése esetében, valamint az EKSZ birtokában lévő vagy az EKSZ-től származó minősített adatok illetéktelenek tudomására jutásának vagy elvesztésének tényleges vagy feltételezett eseteiben ellenőrzésre kerül sor, és a releváns biztonsági hatóságok felkérést kapnak az ellenőrzésben való részvételre;

g) megfelelő incidens- és következménykezelési terveket és mechanizmusokat dolgozzanak ki a biztonsági incidensekre való hatékony és megfelelő időben történő reagálás érdekében;

h) megfelelő intézkedéseket hozzanak abban az esetben, ha az egyének nem tartják be az e határozatban foglaltakat;

i) megfelelő fizikai és szervezeti intézkedések garantálják az EKSZ biztonsági érdekeinek védelmét.

E tekintetben az EKSZ biztonsági hatósága:

— a Bizottsággal konzultálva meghatározza az uniós küldöttségek biztonsági kategóriáit,

— dönt – adott esetben a főképviselővel folytatott konzultációt követően – az uniós küldöttségeken dolgozó személyzet evakuálásának időpontjáról, amennyiben a biztonsági helyzet megköveteli azt,

— dönt az eltartott családtagok védelme érdekében alkalmazandó intézkedésekről, adott esetben figyelembe véve az uniós intézményekkel kötött, a 3. cikk (3) bekezdésében említettek szerinti megállapodásokat;

— jóváhagyja a kriptográfiai kommunikációra vonatkozó politikát, különösen a kriptográfiai termékek és mechanizmusok telepítésének programját.

2. Az EKSZ biztonsági hatóságát feladatainak ellátása során a költségvetésért és igazgatásért felelős főigazgatóság, az EKSZ biztonsági igazgatója, valamint adott esetben a közös biztonság- és védelempolitikai, illetve válságelhárítási főtitkár-helyettes segíti.

3. A főtitkár az EKSZ biztonsági hatóságaként eljárva, adott esetben átruházhat feladatokat ebben a tekintetben.

4. Valamennyi osztály-/részlegvezető felelős az EU-minősített adatok védelmére vonatkozó szabályok végrehajtásáért az osztályán/részlegén belül.

Miközben továbbra is felelősek a fent említett feladatokért, az egyes osztály-/részlegvezetők kijelölik az osztály biztonsági koordinátori feladatait ellátó személyzetet, amely feladatokra az osztály/részleg által kezelt EU-minősített adatok mennyiségével arányos források állnak rendelkezésre.

Az osztály biztonsági koordinátorai, amikor és amennyiben szükséges, segítik és támogatják osztály-/részlegvezetőjüket a biztonsággal kapcsolatos feladatok ellátásában, mint például:

a) további biztonsági követelmények kidolgozása, az osztály/részleg sajátos igényeinek megfelelően;

b) rendszeres biztonsági tájékoztatók az osztály/részleg munkatársai számára;

c) a szükséges ismeret elve tiszteletben tartásának biztosítása az osztályon/részlegen belül;

d) a biztonságos kódok és kulcsok naprakész listájának vezetése;

e) a biztonsági eljárások és biztonsági intézkedések fenntartása;

f) jelentéstétel mind az igazgatójuk, valamint a Biztonsági Igazgatóság felé a biztonsági szabályok megsértéséről és/vagy az EU-minősített adatok illetéktelenek tudomására jutásáról;

g) tájékoztató megbeszélés a személyzet azon tagjaival, akiknek megszűnik alkalmazotti státuszuk az EKSZ-nél;

h) rendszeres jelentéstétel a vezetőik útján az osztályt/részleget érintő biztonsági kérdésekben;

i) kapcsolattartás biztonsági kérdésekben az EKSZ Biztonsági Igazgatóságával.

Bármely olyan tevékenységről vagy kérdésről, amely hatással lehet a biztonságra, időben tájékoztatni kell az EKSZ Biztonsági Igazgatóságát.

5. Az egyes küldöttségvezetők felelősek az uniós küldöttség biztonságával kapcsolatos valamennyi intézkedés végrehajtásáért.

2. szakasz

Az EKSZ Biztonsági Igazgatósága

1. Az EKSZ-en belül létrejön egy Biztonsági Igazgatóság. A Biztonsági Igazgatóság:

a) irányítja, koordinálja, felügyeli és/vagy végrehajtja az összes biztonsági intézkedést az EKSZ felelőssége alá tartozó valamennyi létesítményben, a székhelyen, az EU-n belül és harmadik államokban;

b) biztosítja a koherenciát és következetességet e határozattal és bármely olyan tevékenység végrehajtási rendelkezéseivel, amelynek hatása lehet az EKSZ biztonsági érdekeinek védelmére;

c) a főképviselő, az EKSZ biztonsági hatósága és a főtitkárhelyettes főtanácsadójaként jár el valamennyi biztonsággal kapcsolatos kérdésben;

d) munkáját a tagállamok illetékes szolgálatai segítik, az Európai Külügyi Szolgálat szervezetének és működésének a megállapításáról szóló 2010/427/EU tanácsi határozat 10. cikkének (3) bekezdésével összhangban;

e) támogatja az EKSZ biztonsági akkreditációs hatóságának tevékenységét az EU-minősített adatokat kezelő kommunikációs és információs rendszerek, valamint az EU-minősített adatok kezelésére és tárolására engedélyezett helyiségek általános biztonsági környezetének (GSE) / helyi biztonsági környezetének (LSE) fizikai biztonságára vonatkozó értékelés elvégzése révén.

2. Az EKSZ biztonsági igazgatója felelős az alábbiakért:

a) biztosítja az EKSZ biztonsági érdekeinek átfogó védelmét;

b) kidolgozza, felülvizsgálja és frissíti a biztonsági szabályokat, valamint összehangolja a biztonsági intézkedéseket a tagállamok illetékes hatóságaival, valamint adott esetben harmadik államok illetékes hatóságaival és nemzetközi szervezetekkel, amelyek biztonsági megállapodásokkal és/vagy intézkedésekkel kapcsolódnak az EU-hoz;

c) támogatja az EKSZ Biztonsági Bizottságának eljárásait e határozat 15. cikkének (1) bekezdésével összhangban;

d) adott esetben a fenti (b) pontban említettektől eltérő partnerekkel vagy hatóságokkal is kapcsolatot tart biztonsági kérdésekben;

e) meghatározza a prioritásokat és javaslatokat terjeszt elő a biztonsággal kapcsolatos költségvetési gazdálkodásra vonatkozóan a székhelyen és uniós küldöttségeken.

3. Az EKSZ Biztonsági Igazgatóságának vezetője:

a) biztosítja, hogy a biztonsági szabályok megsértését és az EU-minősített adatok illetéktelenek tudomására jutását rögzítsék, és szükség esetén vizsgálatot indítsanak és folytassanak le;

b) rendszeresen – és amikor szükséges – találkozik a Tanács Főtitkárságának biztonsági igazgatójával és az Európai Bizottság Biztonsági Igazgatóságának igazgatójával, hogy egyeztessenek a közös érdeklődésre számot tartó kérdésekről.

4. Az EKSZ Biztonsági Igazgatósága kapcsolatba lép és szoros együttműködést folytat a következőkkel:

— a tagállami külügyminisztériumok biztonságért felelős szervezeti egységei,

— a tagállamok nemzeti biztonsági hatóságai és/vagy egyéb illetékes biztonsági hatóságai – segítségüket azon információk tekintetében veszi igénybe, amelyekre szüksége van az EKSZ-t, annak személyzetét, tevékenységeit, eszközeit és forrásait, valamint minősített adatait érintő veszélyek és fenyegetések értékeléséhez,

— az EKSZ esetleges tevékenységének helye szerinti tagállamok vagy a fogadó államok illetékes biztonsági hatóságai, az EKSZ adott állam területén levő személyzetének, tevékenységeinek, eszközeinek és forrásainak, valamint minősített adatainak védelmével kapcsolatos bármely kérdésre vonatkozóan,

— a Tanács Főtitkárságának Biztonsági Hivatala és a Bizottság Humánerőforrásügyi és Biztonsági Főigazgatóságának Biztonsági Igazgatósága, valamint adott esetben az egyéb uniós intézmények, szervek és ügynökségek biztonságért felelős szervezeti egységei,

— a harmadik államok vagy nemzetközi szervezetek biztonságért felelős szervezeti egységei, bármilyen hasznos koordináció érdekében, továbbá

— a tagállamok nemzeti biztonsági hatóságai, az EU-minősített adatok védelmével kapcsolatos kérdések tekintetében.

3. szakasz

Uniós küldöttségek

1. A küldöttségvezetők felelősek az EKSZ biztonsági érdekeinek védelmével kapcsolatos valamennyi intézkedés helyi végrehajtásáért és irányításáért az uniós küldöttségek helyiségein és hatáskörén belül.

A küldöttségvezető – szükség esetén a fogadó állam illetékes hatóságaival konzultálva – minden észszerűen megvalósítható intézkedés meghozatalával biztosítja az e célt szolgáló megfelelő fizikai és szervezeti intézkedések végrehajtását.

A küldöttségvezető kidolgozza a 2. cikk c) pontja szerinti eltartott családtagok védelme érdekében alkalmazandó biztonsági eljárásokat, adott esetben figyelembe véve a 3. cikk (3) bekezdésében említett igazgatási megállapodásokat. A küldöttségvezető jelentést tesz az EKSZ Biztonsági Igazgatósága vezetőjének a hatáskörébe tartozó valamennyi biztonsággal kapcsolatos kérdésről.

A küldöttségvezetőt e feladatok ellátásában az EKSZ Biztonsági Igazgatósága, az uniós küldöttség biztonságirányítási csapata – amely a biztonsági feladatokat és funkciókat ellátó személyzetet tömöríti –, valamint szükség esetén kiküldött biztonsági személyzet segíti.

Az uniós küldöttség a biztonsági kérdések tekintetében rendszeres kapcsolatot tart fenn és szoros együttműködést folytat a tagállamok diplomáciai misszióival.

2. Ezen túlmenően a küldöttségvezető:

— az általános eljárási standardok alapján kidolgozza az uniós küldöttség részletes biztonsági és vészhelyzeti tervét,

— az uniós küldöttség tevékenységi körében felmerülő biztonsági incidensek és vészhelyzetek kezelésére a hét minden napján huszonnégy órában hatékony rendszert működtet,

— biztosítja, hogy az uniós küldöttség teljes személyzete rendelkezzen a helyi feltételek által megkövetelt biztosítással,

— biztosítja, hogy az uniós küldöttség személyzetének valamennyi tagja megfelelő biztonsági felkészítő képzésben részesüljön az uniós küldöttségre való megérkezésekor, valamint

— biztosítja, hogy a biztonsági értékeléseket követően tett ajánlásokat végrehajtsák, és rendszeres időközönként írásos jelentést nyújt be ezek végrehajtásáról és egyéb biztonsági kérdésekről az EKSZ biztonsági hatósága számára.

3. Bár továbbra is felelős és elszámoltatható a biztonság megőrzéséért, valamint a testületi reziliencia biztosításáért, a küldöttségvezető átruházhatja biztonsággal kapcsolatos feladatainak végrehajtását a küldöttség biztonsági koordinátorára, aki a küldöttség helyettes vezetője vagy – amennyiben nem kerül sor annak kijelölésére – egy másik megfelelő személy.

Különösen a következő feladatok ruházhatók át a küldöttség biztonsági koordinátorára:

— biztonsági feladatok koordinációja az uniós küldöttségen belül,

— kapcsolattartás biztonsági kérdésekben a fogadó állam illetékes hatóságaival, valamint a megfelelő partnerekkel a tagállamok nagykövetségein és diplomáciai képviseletein,

— az EKSZ biztonsági érdekeivel kapcsolatos megfelelő biztonságirányítási eljárások végrehajtása, beleértve az EU-minősített adatok védelmét,

— a biztonsági szabályoknak és útmutatásoknak való megfelelés biztosítása,

— a személyzet tájékoztatása a rájuk vonatkozó biztonsági előírásokról, valamint a fogadó államban fennálló sajátos kockázatokról,

— kérelmek benyújtása az EKSZ biztonsági tanúsítványokért felelős igazgatóságának, azokra az álláshelyekre vonatkozóan, amelyek esetében kötelező a személyi biztonsági tanúsítvány, valamint

— a küldöttségvezetőnek, a regionális biztonsági tisztviselőnek és az EKSZ Biztonsági Igazgatóságának folyamatos tájékoztatása azokról a térségbeli incidensekről vagy fejleményekről, amelyek hatással vannak az EKSZ biztonsági érdekeinek védelmére.

4. A küldöttségvezető átruházhatja az adminisztratív vagy technikai jellegű biztonsági feladatokat az adminisztratív vezetőre vagy az uniós küldöttség személyzetének más tagjaira.

5. Az uniós küldöttség munkáját egy regionális biztonsági tisztviselő segíti. A regionális biztonsági tisztviselők az alább meghatározott szerepeket töltik be az uniós küldöttségen a megfelelő földrajzi illetékességi körükön belül.

Bizonyos körülmények között, amennyiben a fennálló biztonsági helyzet megköveteli, egy adott uniós küldöttséghez egy kijelölt regionális biztonsági tisztviselő küldhető ki, állandó ott-tartózkodással.

A regionális biztonsági tisztviselő áthelyezhető az aktuális felelősségi körén kívüli területre, akár a székhelyre is, vagy felkérhető egy állandó tartózkodással járó álláshely betöltésére a releváns biztonsági helyzet függvényében bármely országban, valamint az EKSZ Biztonsági Igazgatósága igényeinek megfelelően.

6. A regionális biztonsági tisztviselők az EKSZ helyszíni biztonságért felelős székhelyi szolgálatának közvetlen operatív ellenőrzése alá, és az alkalmazásuk helye szerinti küldöttségvezető és a helyszíni biztonságért felelős székhelyi szolgálat megosztott adminisztratív ellenőrzése alá tartoznak. A regionális biztonsági tisztviselők tanácsadással és segítségnyújtással támogatják a küldöttségvezetőt és az uniós küldöttség személyzetét az uniós küldöttség biztonságával kapcsolatos valamennyi fizikai, szervezeti és eljárási biztonsági intézkedés megszervezésében és végrehajtásában.

7. A regionális biztonsági tisztviselők tanácsadással és támogatásnyújtással segítik a küldöttségvezetőt és az uniós küldöttség személyzetét. A regionális biztonsági tisztviselő adott esetben – különösen, amennyiben állandóan ott tartózkodik – segíti az uniós küldöttséget a biztonságirányításban és a végrehajtásban, beleértve a biztonsági szerződések előkészítését, valamint az akkreditációk és biztonsági tanúsítványok kezelését.

14. cikk

KBVP-műveletek és az EU különleges képviselői

Az EKSZ Biztonsági Igazgatósága tanácsadással segíti a Válságkezelési és Tervezési Igazgatóságot (CMPD), az Európai Unió Katonai Törzsének (EUKT) főigazgatóját, a Polgári Tervezési és Végrehajtási Szolgálat (CPCC) polgári műveleti parancsnokát, valamint az EU katonai műveleti parancsnokait a KBVP-műveletek biztonsági vonatkozásai tekintetében, valamint az EU különleges képviselőit megbízásuk biztonsági vonatkozásai tekintetében, kiegészítve a Tanács által elfogadott vonatkozó szakpolitikákban e szempontból jelenleg hatályos különleges rendelkezéseket.

15. cikk

Az EKSZ Biztonsági Bizottsága

1. Létrejön az EKSZ Biztonsági Bizottsága.

A Biztonsági Bizottság elnöke az EKSZ biztonsági hatósága vagy annak kijelölt képviselője; és a Biztonsági Bizottság az elnök utasítására vagy bármely tagjának kérésére ülésezik. Az EKSZ Biztonsági Igazgatósága támogatja az elnököt ebben a tisztségében, és szükség esetén adminisztratív segítséget nyújt a bizottsági eljárásokhoz.

2. Az EKSZ Biztonsági Bizottságának tagjai az alábbiak képviselői:

— az egyes tagállamok,

— a Tanács Főtitkárságának Biztonsági Hivatala,

— a Bizottság Humánerőforrásügyi és Biztonsági Főigazgatóságának Biztonsági Igazgatósága.

Az EKSZ Biztonsági Bizottságához delegált tagállami küldöttségek az alábbiak tagjaiból állhatnak:

— a nemzeti biztonsági hatóság és/vagy a kijelölt biztonsági hatóság,

— a külügyminisztérium biztonságért felelős szervezeti egységei.

3. A Biztonsági Bizottság képviselőit, amennyiben szükségesnek ítélik, szakértők segíthetik és tanácsokkal láthatják el. Más uniós intézmények, ügynökségek vagy szervek képviselői is meghívást kaphatnak az üléseken való részvételre, ha a biztonságukat érintő kérdések kerülnek napirendre.

4. Az alábbi (5) bekezdés sérelme nélkül az EKSZ Biztonsági Bizottsága segíti az EKSZ-t, az EKSZ tevékenységeivel, a székhellyel és az uniós küldöttségekkel kapcsolatos valamennyi biztonsági kérdésről való konzultáció útján.

Az alábbi (5) bekezdés sérelme nélkül, az EKSZ Biztonsági Bizottsággal:

a) a következő kérdésekben konzultálnak:

— biztonsági politikák, iránymutatások, koncepciók vagy a biztonsággal kapcsolatos egyéb módszertani dokumentumok, különös tekintettel a minősített információk védelmére, valamint az abban az esetben végrehajtandó intézkedésekre, ha az EKSZ személyzete nem tartja be a biztonsági szabályokat,

— technikai biztonsági szempontok, amelyek befolyásolhatják a főképviselő arra vonatkozó döntését, hogy ajánlást terjesszen a Tanács elé az A. melléklet 10. cikke (1) bekezdésének a) pontjában említett adatbiztonsági megállapodások megkötésére irányuló tárgyalások megkezdésére,

— e határozat bármely módosítása;

b) konzultálhatnak vagy adott esetben tájékoztathatják az EKSZ-nek a székhelyen vagy az uniós küldöttségeken lévő személyzete és eszközei biztonságával kapcsolatos kérdésekről, a 3. cikk (3) bekezdésének sérelme nélkül;

c) tájékoztatják arról, ha EU-minősített adatok jutottak illetéktelenek tudomására vagy vesztek el az EKSZ-en belül.

5. Az EU-minősített adatok védelmével kapcsolatos, az e határozatban és annak A. mellékletében szereplő szabályok bármely módosításához az EKSZ Biztonsági Bizottságában képviselt tagállamok egyhangúlag kedvező véleményére van szükség. Az ilyen egyhangú véleményre az alábbiakat megelőzően is szükség van:

— az A. melléklet 10. cikke (1) bekezdésének b) pontjában említett igazgatási megállapodások megkötésére irányuló tárgyalások megkezdése,

— minősített adatok átadása az A.VI. melléklet 9., 11. és 12. pontjaiban említett rendkívüli körülmények között,

— felelősségvállalás az adatkibocsátásért az A. melléklet 10. cikke (6) bekezdésének utolsó mondatában említett körülmények között.

Amennyiben egyhangúlag kedvező véleményre van szükség, ez a feltétel akkor teljesül, ha a tagállamok küldöttségei nem emelnek kifogást a bizottsági eljárás során.

6. Az EKSZ Biztonsági Bizottsága teljes mértékben figyelembe veszi a Tanács és a Bizottság hatályos biztonsági politikáit és iránymutatásait.

7. Az EKSZ Biztonsági Bizottsága megkapja az EKSZ által végzett éves ellenőrzések listáját, valamint az ellenőrzésekről szóló jelentéseket, azok lezárását követően.

8. Az ülések szervezése:

— Az EKSZ Biztonsági Bizottsága évente legalább két alkalommal ülésezik. Az elnök szervezésében vagy a Biztonsági Bizottság tagjainak kérésére további ülésekre kerülhet sor, akár teljes összetételben, akár a nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságok vagy a külügyminisztérium biztonságért felelős részlegeinek részvételével.

— Az EKSZ Biztonsági Bizottsága úgy szervezi tevékenységét, hogy a biztonság konkrét területeire vonatkozó ajánlásokat tudjon tenni. A Biztonsági Bizottság szükség esetén egyéb szakértői alcsoportokat hoz létre. Meghatározza a szakértői alcsoportok feladatait, és azok jelentést tesznek tevékenységükről.

— Az EKSZ Biztonsági Bizottsága felelős a megvitatandó témák előkészítéséért. Az elnök minden ülésre ideiglenes napirendet készít. A Biztonsági Bizottság tagjai további napirendi pontokra tehetnek javaslatot.

16. cikk

Biztonsági ellenőrzések

1. Az EKSZ biztonsági hatósága biztosítja, hogy rendszeresen sor kerüljön biztonsági ellenőrzésekre az EKSZ székhelyén és az uniós küldöttségeken belül a biztonsági intézkedések megfelelőségének értékelése és e határozatnak való megfelelésük ellenőrzése érdekében. Az EKSZ Biztonsági Igazgatósága szükség esetén szakértőket jelölhet ki az EUSZ V. címének 2. fejezete alapján létrehozott uniós ügynökségeknél és szerveknél lefolytatandó biztonsági ellenőrzésekben való részvételre.

2. Az EKSZ biztonsági ellenőrzéseit az EKSZ Biztonsági Igazgatóságának felügyelete alatt és adott esetben a más uniós intézményeket vagy tagállamokat képviselő biztonsági szakértők támogatásával végzik, különösen a 3. cikk (3) bekezdésében említett megállapodásokkal összefüggésben.

3. Az EKSZ szükség esetén a tagállamok, a Tanács Főtitkársága és a Bizottság szakértelmére támaszkodhat.

Szükség esetén a harmadik államokban működő tagállami képviseleteken dolgozó biztonsági szakértők és/vagy a tagállamok diplomáciai biztonsági szervezeti egységeinek képviselői is meghívást kaphatnak az uniós küldöttség biztonsági ellenőrzésében való részvételre.

4. Az e cikk végrehajtására vonatkozó rendelkezéseket az EU-minősített adatok védelmének tekintetében az A.III. melléklet tartalmazza.

17. cikk

Értékelő látogatások

A harmadik államokban vagy nemzetközi szervezeteknél az A. melléklet 10. cikke (1) bekezdésének b) pontja szerint egy igazgatási megállapodás értelmében megosztott EU-minősített adatok védelmére bevezetett biztonsági intézkedések hatékonyságának megállapítása céljából értékelő látogatásokra kerül sor.

Az EKSZ Biztonsági Igazgatósága szakértőket jelölhet ki az olyan harmadik államokban vagy nemzetközi szervezeteknél esedékes értékelő látogatásokban való részvételre, amelyekkel az EU az A. melléklet 10. cikke (1) bekezdésének a) pontjában említett adatbiztonsági megállapodást kötött.

18. cikk

Üzletmenet-folytonossági tervezés

Az EKSZ általános üzletmenet-folytonossági tervezésének részeként az EKSZ Biztonsági Igazgatósága segít az EKSZ biztonsági hatóságának kezelni az EKSZ üzletmenet-folytonossági eljárásainak biztonsággal kapcsolatos vonatkozásait.

19. cikk

Az EU-n kívüli kiküldetésekkel kapcsolatos utazási tanácsok

Az EKSZ Biztonsági Igazgatósága biztosítja az EKSZ felelőssége alá tartozó személyzet EU-n kívüli kiküldetésekre vonatkozó utazási tanácsok elérhetőségét, az EKSZ valamennyi releváns szolgálatának – különösen a SITROOM és az INTCEN, a földrajzi szervezeti egységek és az uniós küldöttségek – forrásaira támaszkodva.

Az EKSZ Biztonsági Igazgatósága kérésre, és a fent említett forrásokra támaszkodva, konkrét utazási tanácsokat nyújt az EKSZ felelőssége alá tartozó személyzet olyan harmadik országokba irányuló missziói tekintetében, amelyek nagy kockázatot vagy fokozott kockázati szintet jelentenek.

20. cikk

Egészség és biztonság

AZ EKSZ biztonsági szabályai kiegészítik az EKSZ-nek a főképviselő által elfogadott, az egészség és biztonság védelmére vonatkozó szabályait.

21. cikk

Végrehajtás és felülvizsgálat

1. Az EKSZ biztonsági hatósága, adott esetben az EKSZ Biztonsági Bizottságával folytatott konzultációt követően, jóváhagyja az e szabályoknak az EKSZ-en belüli végrehajtásához szükséges intézkedéseket meghatározó biztonsági iránymutatásokat, és kiépíti a biztonság minden szempontjának lefedéséhez szükséges kapacitásokat, szorosan együttműködve a tagállamok illetékes biztonsági hatóságaival és az uniós intézmények releváns szolgálatainak támogatásával.

2. Az Európai Külügyi Szolgálat szervezetének és működésének a megállapításáról szóló, 2010. július 26-i 2010/427/EU tanácsi határozat 4. cikke (5) bekezdésével összhangban a Tanács Főtitkársága és a Bizottság releváns szolgálataival kötött szolgáltatási szintű megállapodások útján szükség esetén átmeneti intézkedések alkalmazhatók.

3. A főképviselő biztosítja e határozat alkalmazásának általános következetességét, és folyamatosan felülvizsgálja ezeket a biztonsági szabályokat.

4. Az EKSZ biztonsági szabályait a tagállamok illetékes biztonsági hatóságaival szorosan együttműködve hajtják végre.

5. Az EKSZ biztosítja, hogy a védelmi folyamat valamennyi szempontját figyelembe vegyék az EKSZ válságelhárítási rendszerén belül.

6. A főtitkár – biztonsági hatóságként eljárva –, valamint az EKSZ Biztonsági Igazgatóságának vezetője biztosítja e határozat végrehajtását.

22. cikk

Korábbi határozatok hatályon kívül helyezése

Ez a határozat hatályon kívül helyezi az Európai Külügyi Szolgálat biztonsági szabályairól szóló, 2013. április 19-i főképviselői határozatot ([1]), és annak helyébe lép.

23. cikk

Záró rendelkezések

Ez a határozat az aláírása napján lép hatályba.

A határozatot az *Európai Unió Hivatalos Lapjában* ki kell hirdetni.

Az EKSZ illetékes hatóságai kellő módon és időben tájékoztatják a határozat és mellékletei hatálya alá tartozó személyzet valamennyi tagját a határozat és mellékletei tartalmáról, hatálybalépéséről és esetleges későbbi módosításairól.

Kelt Brüsszelben, 2017. szeptember 19-én.

Federica MOGHERINI

az Unió külügyi és biztonságpolitikai főképviselője

([1]) HL C 190., 2013.6.29., 1. o.

A. MELLÉKLET

AZ EU-MINŐSÍTETT ADATOKRA VONATKOZÓ ELVEK ÉS NORMÁK

1. cikk

Cél, hatály és fogalommeghatározások

1. E melléklet megállapítja az EU-minősített adatok védelmére vonatkozó biztonsági alapelveket és minimumszabályokat.

2. Ezen alapelvek és minimumszabályok az EKSZ-re és az EKSZ felelőssége alá tartozó személyzetre alkalmazandók az e határozat 1., illetve 2. cikkében említettek és meghatározottak szerint.

2. cikk

Az EU-minősített adat fogalmának meghatározása, biztonsági minősítések és jelölések

1. „EU-minősített adat": bármely olyan EU biztonsági minősítéssel ellátott adat vagy anyag, amely 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) TRES SECRET UE/EU TOP SECRET: olyan adatok és anyagok, amelyek 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, amelyek engedély nélküli hozzáférhetővé tétele súlyosan sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit.

c) CONFIDENTIEL UE/EU CONFIDENTIAL: olyan adatok és anyagok, amelyek engedély nélküli hozzáférhetővé tétele sértheti az Európai Unió, illetve egy vagy több tagállam alapvető érdekeit.

d) RESTREINT UE/EU RESTRICTED: olyan adatok és anyagok, amelyek engedély nélküli hozzáférhetővé tétele hátrányosan érintheti az Európai Unió, illetve egy vagy több tagállam érdekeit.

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

3. cikk

A minősítés szabályai

1. Az EKSZ biztosítja az EU-minősített adatok megfelelő minősítését, minősített adatokként való egyértelmű azonosítását és azt, hogy minősítési szintjüket csak a szükséges ideig őrizzék meg.

2. A kibocsátó előzetes írásbeli hozzájárulása nélkül az EU-minősített adatok nem minősíthetők vissza és minősítésük nem oldható fel, továbbá a 2. cikk (3) bekezdésében említett jelölések nem módosíthatók és nem távolíthatók el.

3. Az EKSZ biztonsági hatósága az EKSZ Biztonsági Bizottságával folytatott konzultációt követően az e határozat 15. cikkének (5) bekezdésével összhangban jóváhagyja az EU-minősített adatok létrehozására vonatkozó biztonsági iránymutatásokat, amelyek gyakorlati minősítési útmutatót is tartalmaznak.

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 biztonsági minősítési jelöléssel ellátott minősített adatokat visznek be az EKSZ struktúráiba vagy hálózataiba, az EKSZ ezeket az adatokat az azonos szintű EU-minősített adatokra alkalmazandó előírásoknak megfelelően védi a B. függelékben szereplő, a biztonsági minősítésekre vonatkozó egyenértékűségi táblázatban foglaltak szerint.

Az EKSZ megfelelő eljárásokat alakít ki a következők kibocsátóira vonatkozó pontos nyilvántartás érdekében:

— az EKSZ-nek eljuttatott minősített adatok, valamint

— az EKSZ-nél keletkező minősített adatokban felhasznált forrásanyagok.

Az EKSZ Biztonsági Bizottsága tájékoztatást kap ezekről az eljárásokról.

4. Nagy mennyiségű EU-minősített adat vagy ilyen adatok gyűjteménye az egyes adatelemek esetében szükségeshez képest magasabb minősítési szintnek megfelelő védelmet tehet indokolttá.

5. cikk

Személyi biztonság az EU-minősített adatok kezelésére vonatkozóan

1. A személyi biztonság körébe olyan intézkedések alkalmazása tartozik, amelyek biztosítják, hogy csak azok a személyek kapjanak hozzáférést az EU-minősített adatokhoz:

— akik esetében teljesül a „szükséges ismeret” feltétele,

— akik számára a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítésű adatokhoz való hozzáférést engedélyezték, és akik megfelelő szintű biztonsági ellenőrzésen estek át, vagy a nemzeti jogszabályokkal és rendelkezésekkel összhangban más módon, feladatkörüknél fogva megfelelő engedélyt kaptak, valamint

— akiket tájékoztattak felelősségükről.

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

3. Az EU-minősített adatokhoz való hozzáférés engedélyezését megelőzően, majd azt követően rendszeres időközönként minden egyes személyt tájékoztatnak az EU-minősített adatok e határozat szerinti védelmével kapcsolatos felelősségéről, amelyet e személyeknek írásban kell tudomásul venniük.

4. Az e cikk végrehajtására vonatkozó rendelkezéseket az A.I. melléklet tartalmazza.

6. cikk

Az EU-minősített adatok fizikai biztonsága

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. Ezeket az intézkedéseket kockázatkezelési eljárás alapján határozzák meg.

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 az A. melléklet 8. cikkének (2) bekezdésében meghatározott kommunikációs és információs rendszereket tárolják.

4. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű EU-minősített adatok tárolására szolgáló területeket az A.II. mellékletnek megfelelően biztonsági területként határozzák meg, és az EKSZ biztonsági hatósága jóváhagyja azokat.

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

6. Az e cikk végrehajtására vonatkozó rendelkezéseket az A.II. melléklet tartalmazza.

7. cikk

A minősített adatok kezelése

1. A minősített adatok kezelése az EU-minősített adatok teljes életcikluson keresztüli ellenőrzésére szolgáló adminisztratív intézkedések alkalmazása, amelyek kiegészíti az 5., 6. és 8. cikkben meghatározott intézkedéseket, és ezáltal hozzájárulnak az ilyen adatoknak a szándékosan vagy véletlenszerűen illetéktelenek tudomására jutásától vagy elvesztésétől való elrettentéshez, annak észleléséhez és a kár helyreállításához. Ezek az intézkedések különösen az EU-minősített adatok létrehozására, nyilvántartásba vételére, másolására, fordítására, szállítására, kezelésére, tárolására és megsemmisítésére vonatkoznak.

2. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokat továbbítás előtt és kézhezvételkor biztonsági célokból nyilvántartásba veszik. Az EKSZ illetékes hatóságai gondoskodnak az erre a célra szolgáló nyilvántartási rendszer kiépítéséről. A TRES SECRET UE/EU TOP SECRET minősítésű adatokat erre kijelölt nyilvántartásokban rögzítik.

3. Az EKSZ biztonsági hatósága rendszeresen ellenőrzi azokat a szolgálatokat és helyiségeket, ahol EU-minősített adatokat kezelnek vagy tárolnak.

4. Az EU-minősített adatoknak a szolgálatok és helyiségek között történő, a fizikailag védett területeken kívüli továbbítása az alábbiak szerint történik:

a) főszabályként az EU-minősített adatokat az e határozat 7. cikke (5) bekezdésével összhangban jóváhagyott kriptográfiai termékekkel védett elektronikus úton és egyértelműen meghatározott biztonsági üzemeltetési eljárások (SecOp) szerint továbbítják;

b) amennyiben nem használják az a) pontban említett eszközöket, az EU-minősített adatok szállítása az alábbiak szerint történik:

   i. vagy az e határozat 8. cikkének (5) bekezdésével összhangban jóváhagyott kriptográfiai termékekkel védett elektronikus eszközökön (pl. USB-kulcson, CD-n, merevlemezen); vagy

   ii. bármely egyéb esetben az EKSZ biztonsági hatósága által az A.III. melléklet V. szakaszában megállapított vonatkozó védelmi intézkedésekkel összhangban előírt módon.

5. Az e cikk végrehajtására vonatkozó rendelkezéseket az A.III. melléklet tartalmazza.

8. 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 adatokat, 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 eljáráson alapul.

2. A „kommunikációs és információs rendszer” (CIS) az elektronikus formában történő információkezelést lehetővé tevő rendszer. A kommunikációs és információs rendszer magában foglalja a működéséhez szükséges valamennyi eszközt, beleértve az infrastruktúrát, a szervezetet, a személyzetet és az információforrásokat. E melléklet az EU-minősített adatokat kezelő EKSZ kommunikációs és információs rendszerekre alkalmazandó.

3. A kommunikációs és információs rendszer az információvédelem koncepciójával összhangban kezeli az EU-minősített adatokat.

4. Az EU-minősített adatokat kezelő valamennyi kommunikációs és információs rendszert akkreditálni kell. Az akkreditáció célja annak biztosítása, hogy e határozattal összhangban minden megfelelő biztonsági intézkedés végrehajtásra kerüljön, valamint az EU-minősített adatok és a kommunikációs és információs rendszer megfelelő szintű védelemben részesüljön. Az akkreditációs nyilatkozat meghatározza az adatoknak azt a megengedett legmagasabb minősítési szintjét, amelyet a kommunikációs és információs rendszer kezelhet, valamint a kapcsolódó feltételeket.

5. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokat kezelő kommunikációs és információs rendszereket olyan módon kell védeni, hogy az adatok bizalmassága nem szándékos elektromágneses kisugárzás következtében ne sérülhessen („TEMPEST biztonsági intézkedések”).

6. Amennyiben az EU-minősített adatok védelmét kriptográfiai termékek biztosítják, e termékek jóváhagyása e határozat 8. cikkének (5) bekezdésével összhangban történik.

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

8. E határozat 8. cikkének (6) bekezdése értelmében a következő információvédelmi funkciókat hozzák létre a szükséges mértékben:

a) információvédelmi hatóság;

b) TEMPEST-hatóság;

c) kriptográfiai jóváhagyó hatóság;

d) kriptográfiai terjesztési hatóság.

9. E határozat 8. cikkének (7) bekezdése értelmében minden rendszer tekintetében létrehozzák a következőket:

a) biztonsági akkreditációs hatóság;

b) információvédelmi üzemeltetési hatóság.

10. Az e cikk végrehajtására vonatkozó rendelkezéseket az A.IV. melléklet tartalmazza.

9. 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 az ilyen szerződések teljes életciklusa során. Az ilyen szerződések – főszabályként – nem járhatnak TRES SECRET UE/EU TOP SECRET minősítésű adatokhoz való hozzáféréssel.

2. Az EKSZ az EU-minősített adatokhoz való hozzáférést, illetve azok kezelését vagy tárolását magukban foglaló vagy azzal járó feladatokkal szerződés keretében olyan gazdálkodó vagy más szervezetet bízhat meg, amely valamely tagállamban vagy olyan harmadik államban van bejegyezve, amellyel az A. melléklet 10. cikkének (1) bekezdése szerinti adatbiztonsági megállapodást vagy igazgatási megállapodást kötött.

3. Az EKSZ – mint szerződő hatóság – a minősített szerződések gazdálkodó vagy egyéb szervezetek részére történő odaítélésekor gondoskodik arról, hogy az iparbiztonságnak az e határozatban és a szerződésben foglalt minimumszabályait betartsák. Az ilyen minimumszabályok betartását az érintett nemzeti biztonsági hatóság/kijelölt biztonsági hatóság útján biztosítja.

4. Egy tagállamban nyilvántartásba vett, minősített vállalkozói vagy alvállalkozói szerződésekben részt vevő vállalkozók vagy alvállalkozók, amelyeknek saját létesítményeikben CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat kell kezelniük és tárolniuk, akár e szerződések teljesítése, akár a szerződéskötést megelőző szakaszban rendelkeznek az adott tagállam nemzeti biztonsági hatósága, kijelölt biztonsági hatósága vagy egyéb illetékes biztonsági hatósága által kibocsátott, megfelelő minősítési szintű telephelybiztonsági tanúsítvánnyal.

5. A vállalkozók vagy alvállalkozók azon személyzetének, akinek a minősített szerződés teljesítéséhez CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférésre van szüksége, rendelkeznie kell az adott nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság általa nemzeti jogszabályokkal és rendelkezésekkel, valamint az A.I. mellékletben foglalt biztonsági minimumszabályokkal összhangban kibocsátott személyi biztonsági tanúsítvánnyal (PSC).

6. Az e cikk végrehajtására vonatkozó rendelkezéseket az A.V. melléklet tartalmazza.

10. cikk

A minősített adatok megosztása harmadik államokkal és nemzetközi szervezetekkel

1. Az EKSZ csak abban az esetben oszthat meg EU-minősített adatokat harmadik állammal vagy nemzetközi szervezettel, ha:

a) az EU és az adott harmadik állam vagy nemzetközi szervezet között az EUSZ 37. cikkével és az EUMSZ 218. cikkével összhangban megkötött adatbiztonsági megállapodás van hatályban; vagy

b) a főképviselő és az adott harmadik állam vagy nemzetközi szervezet illetékes hatósága között elvben legfeljebb RESTREINT UE/EU RESTRICTED minősítési szintű adatok megosztására vonatkozó, e határozat 15. cikkének (5) bekezdésével összhangban megkötött igazgatási megállapodás van hatályban; vagy

c) az EU és az adott harmadik állam között a válságkezelési KBVP-műveletek összefüggésében az EUSZ 37. cikkével és az EUMSZ 218. cikkével összhangban megkötött, részvételről szóló keretmegállapodás vagy részvételről szóló ad hoc megállapodás alkalmazandó,

és az ebben az eszközben előírt feltételek teljesülnek.

A fenti főszabályra vonatkozó kivételeket az A.VI. melléklet V. szakasza tartalmazza.

2. A (1) bekezdés b) pontjában említett igazgatási megállapodások rendelkezéseket tartalmaznak annak biztosítása érdekében, hogy amennyiben harmadik állam vagy nemzetközi szervezet EU-minősített adatot kap, az ilyen adatot a minősítési szintjének és legalább az e határozatban foglaltakkal azonos szintű minimumszabályoknak megfelelő védelemben részesítsék.

Az (1) bekezdés c) pontjában említett megállapodások alapján megosztott adatokat e megállapodások alapján és azok rendelkezéseivel összhangban az olyan KBVP-műveletekre vonatkozó adatokra kell korlátozni, amelyekben a szóban forgó harmadik állam részt vesz.

3. Ha ezt követően az Unió és a részt vevő harmadik állam vagy nemzetközi szervezet adatbiztonsági megállapodást köt, az adatbiztonsági megállapodás az EU-minősített adatok megosztása és kezelése tekintetében felülírja a részvételi keretmegállapodások, az ad hoc részvételi megállapodást és az ad hoc igazgatási megállapodások bármelyikében megállapított, a minősített adatok megosztására vonatkozó rendelkezést.

4. KBVP-művelet céljára előállított EU-minősített adatok az A.VI. melléklet 1–3. pontjával összhangban tehetők hozzáférhetővé a harmadik államok vagy nemzetközi szervezetek által az adott művelethez kirendelt személyzet számára. A KBVP-művelet helyszínén vagy kommunikációs és információs rendszerében az ilyen személyzet EU-minősített adatokhoz való hozzáférésének engedélyezésekor megfelelő intézkedéseket kell alkalmazni (beleértve a hozzáférhetővé tett EU-minősített adatok naplózását) az adatok elvesztése vagy illetéktelenek tudomására jutása kockázatának csökkentésére. Ezek az intézkedések a megfelelő tervezési vagy missziós dokumentumokban kerülnek meghatározásra.

5. A harmadik államokban vagy nemzetközi szervezeteknél az e határozat 17. cikkében említettek szerint értékelő látogatásokra kerül sor a megosztott EU-minősített adatok védelmére bevezetett biztonsági intézkedések hatékonyságának megállapítása céljából.

6. Az EKSZ birtokában lévő EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére történő átadásáról eseti alapon döntenek, az adatok jellegétől és tartalmától, a címzett számára szükséges ismerettől, valamint az EU számára jelentkező előnyök mértékétől függően.

Az EKSZ törekszik írásbeli hozzájárulást szerezni bármely olyan szervezettől, amely az EKSZ-nél keletkezett EU-minősítésű adatok forrásanyagaként minősített adatokat szolgáltatott, az átadással szembeni kifogások kizárása érdekében.

Ha az átadásra szánt minősített adat kibocsátója nem az EKSZ, akkor az EKSZ az adat átadása előtt írásbeli beleegyezést kér a kibocsátótól.

Ha azonban az EKSZ nem tudja azonosítani a kibocsátót, akkor az EKSZ biztonsági hatósága vállalja magára a kibocsátó felelősségét, miután megkapta az EKSZ Biztonsági Bizottságában képviselt tagállamok egyhangúlag kedvező véleményét.

7. Az e cikk végrehajtására vonatkozó rendelkezéseket az A.VI. melléklet tartalmazza.

11. cikk

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

1. A biztonsági szabályok megsértését vagy annak gyanúját, illetve a minősített adatok illetéktelenek tudomására jutását vagy annak gyanúját minden esetben haladéktalanul jelentik az EKSZ Biztonsági Igazgatóságának, amely adott esetben értesíti az érintett tagállamo(ka)t, illetve az egyéb érintett feleket.

2. Amennyiben ismert vagy alapos okkal gyanítható a minősített adatok illetéktelenek tudomására jutása vagy elvesztése, az EKSZ Biztonsági Igazgatósága tájékoztatja az érintett tagállam(ok) nemzeti biztonsági hatóságát, és a vonatkozó jogszabályokkal és rendelkezésekkel összhangban minden szükséges intézkedést megtesz:

a) a bizonyítékok megőrzésére;

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

c) a kibocsátó vagy bármely más érintett fél azonnali tájékoztatására;

d) az ismételt előfordulás megelőzésére;

e) az EU vagy a tagállamok érdekei tekintetében okozott esetleges károk felmérésére; valamint

f) a megfelelő hatóságok értesítésére az adatok illetéktelenek tudomására jutásának tényleges vagy feltételezett esetével járó hatásokról és a megtett lépésekről.

3. Az EKSZ felelőssége alá tartozó személyzet e határozatban megállapított biztonsági szabályokat megsértő tagja a vonatkozó szabályok és rendelkezések szerint fegyelmi eljárás alá vonható.

A minősített adatok illetéktelenek tudomására jutásáért vagy elvesztéséért felelős bármely személy a vonatkozó jogszabályok és rendelkezések szerint fegyelmi és/vagy jogi eljárás alá vonható.

4. A biztonsági szabályok megsértésével és/vagy illetéktelenek tudomására jutásával kapcsolatos vizsgálatok alatt az EKSZ Biztonsági Igazgatóságának vezetője felfüggesztheti az adott személy hozzáférését az EU-minősített adatokhoz és EKSZ-helyiségekhez. E döntésről haladéktalanul tájékozatják a Bizottság Humánerőforrásügyi és Biztonsági Főigazgatóságának Biztonsági Igazgatóságát, a Tanács Főtitkárságának Biztonsági Hivatalát vagy az érintett tagállam(ok) nemzeti biztonsági hatóságát, illetve más érintett szervezeteket.

A.I. MELLÉKLET

SZEMÉLYI BIZTONSÁG

I. BEVEZETÉS

1. Ez a melléklet meghatározza az A. melléklet 5. cikkének végrehajtására vonatkozó rendelkezéseket. Konkrétan megállapítja az EKSZ által annak meghatározására alkalmazandó kritériumokat, hogy egy adott személy számára – lojalitását, szavahihetőségét és megbízhatóságát figyelembe véve – engedélyezhető-e az EU-minősített adatokhoz való hozzáférés, és rögzíti az e célból követendő vizsgálati és adminisztratív eljárásokat.

2. Az EU-minősített adatokhoz való hozzáféréshez szükséges „személyi biztonsági tanúsítvány" (PSC) a valamely tagállam illetékes hatóságai által elvégzett biztonsági ellenőrzést követően egy tagállami illetékes hatóság által tett nyilatkozat, amely tanúsítja, hogy egy adott személy részére – amennyiben a szükséges ismeret feltétele teljesül – meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig és meghatározott időpontig biztosítható az EU-minősített adatokhoz való hozzáférés; a fentieknek megfelelő személy „biztonsági ellenőrzésen átesett" személynek minősül.

3. A „személyi biztonsági tanúsítványról szóló igazolás" (PSCC) az EKSZ biztonsági hatósága által kiadott igazolás, amely tartalmazza, hogy az adott személy biztonsági ellenőrzésen átesett, hogy milyen szintű EU-minősített adatokhoz férhet hozzá, valamint rögzíti a vonatkozó személyi biztonsági tanúsítvány érvényességi idejét és az igazolás lejártának időpontját.

4. Az „EU-minősített adatokhoz való hozzáférés engedélyezése" az EKSZ biztonsági hatósága által e határozattal összhangban, a személyi biztonsági tanúsítvány tagállami illetékes hatóságai általi kiadását követően adott engedély, amely tanúsítja, hogy egy adott személy részére – amennyiben a szükséges ismeret feltétele teljesül – meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig és meghatározott időpontig biztosítható az EU-minősített adatokhoz való hozzáférés; a fentieknek megfelelő személy „biztonsági ellenőrzésen átesett" személynek minősül.

II. AZ EU-MINŐSÍTETT ADATOKHOZ VALÓ HOZZÁFÉRÉS ENGEDÉLYEZÉSE

5. A RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáférés esetében nem kötelező a személyi biztonsági tanúsítvány, és a hozzáférést megadják, ha:

   a) megállapítást nyert az adott személy személyzeti szabályzaton vagy szerződéses jogviszonyon alapuló kapcsolata az EKSZ-szel;

   b) megállapítást nyert, hogy esetében teljesül a „szükséges ismeret" feltétele;

   c) tájékoztatást kapott az EU-minősített adatok védelmére vonatkozó biztonsági szabályokról és eljárásokról, és írásban tudomásul vette az EU-minősített adatok védelmével kapcsolatos felelősségét e határozattal összhangban.

6. Egy adott személy számára csak akkor engedélyezhető a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokhoz való hozzáférés, ha:

   a) megállapítást nyert az adott személy személyzeti szabályzaton vagy szerződéses jogviszonyon alapuló kapcsolata az EKSZ-szel;

   b) megállapítást nyert, hogy esetében teljesül a „szükséges ismeret" feltétele;

   c) rendelkezik a megfelelő szintű személyi biztonsági tanúsítvánnyal, vagy a nemzeti jogszabályokkal és rendelkezésekkel összhangban más módon, feladatkörénél fogva megfelelő engedélyt kapott; valamint

   d) tájékoztatást kapott az EU-minősített adatok védelmére vonatkozó biztonsági szabályokról és eljárásokról, és írásban tudomásul vette az ilyen adatok védelmével kapcsolatos felelősségét.

7. Az EKSZ meghatározza szervezeti felépítésében azokat a beosztásokat, amelyek szükségessé teszik a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokhoz való hozzáférést, és ezért megfelelő szintű személyi biztonsági tanúsítványt igényelnek a fenti (4) bekezdéssel összhangban.

8. Az EKSZ személyzete nyilatkozik arról, hogy rendelkezik-e egynél több ország állampolgárságával.

A személyi biztonsági tanúsítvány iránti kérelemmel kapcsolatos eljárások az EKSZ-ben

9. Az EKSZ személyzete tekintetében az EKSZ biztonsági hatósága elküldi 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.

10. Amennyiben az adott személy több mint egy ország állampolgárságával rendelkezik, az átvilágításra irányuló kérelmet annak az országnak a nemzeti biztonsági hatóságához intézik, amelynek állampolgáraként az adott személyt felvették.

11. Amennyiben olyan személy biztonsági ellenőrzésével kapcsolatos releváns információ jut az EKSZ tudomására, aki személyi biztonsági tanúsítványért folyamodott, az EKSZ a vonatkozó szabályokkal és rendelkezésekkel összhangban értesíti erről az érintett nemzeti biztonsági hatóságot.

12. A biztonsági ellenőrzés elvégzését követően az érintett nemzeti biztonsági hatóság értesíti az EKSZ Biztonsági Igazgatóságát 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, az EKSZ biztonsági hatósága adott időpontig és megfelelő szintig engedélyezheti az érintett számára az EU-minősített adatokhoz való hozzáférést.

    b) Az EKSZ megtesz minden szükséges intézkedést a nemzeti biztonsági hatóság által meghatározott feltételek vagy korlátozások megfelelő végrehajtása érdekében. A nemzeti biztonsági hatóságot értesítik az ellenőrzés eredményéről.

    c) Amennyiben a biztonsági ellenőrzés kedvezőtlen eredménnyel zárul, az EKSZ biztonsági hatósága értesíti az érintett személyt, aki kérheti, hogy az EKSZ biztonsági hatósága hallgassa meg. Az EKSZ biztonsági hatósága felkérheti az illetékes nemzeti biztonsági hatóságot, hogy ha a nemzeti jogszabályok és rendelkezések alapján módjában áll, adjon további felvilágosítást. Ha az eredmény megerősítést nyer, nem engedélyezhető az EU-minősített adatokhoz való hozzáférés. Ebben az esetben az EKSZ megteszi a szükséges intézkedéseket annak biztosítására, hogy a kérelmezőtől megtagadják az EU-minősített adatokhoz való hozzáférést.

13. A biztonsági ellenőrzésre és a kapott eredményekre – amelyekre az EKSZ azon döntését alapozza, hogy engedélyezi-e vagy sem az EU-minősített adatokhoz való hozzáférést – az érintett tagállamban hatályos megfelelő jogszabályok és rendelkezések vonatkoznak, beleértve a jogorvoslattal kapcsolatos rendelkezéseket is. Az EKSZ biztonsági hatóságának határozata ellen a személyzeti szabályzattal összhangban lehet fellebbezni.

14. A személyes biztonsági tanúsítvány, amennyiben az annak alapját képező ellenőrzés megállapításai továbbra is érvényesek, az érintett személy által az EKSZ-ben, a Tanács Főtitkárságán vagy a Bizottságban végzett valamennyi feladat tekintetében érvényes.

15. Az EKSZ elfogadja a más uniós intézmény, szerv vagy ügynökség által adott engedélyt az EU-minősített adatokhoz való hozzáférésre, feltéve, hogy az továbbra is érvényes. Az engedély az érintett személy Bizottságban végzett valamennyi feladata tekintetében érvényes. Az érintett személyt alkalmazó uniós intézmény, szerv vagy ügynökség értesíti a megfelelő nemzeti biztonsági hatóságot a munkáltató megváltozásáról.

16. Amennyiben az adott személy szolgálati időszaka a biztonsági ellenőrzés eredményéről az EKSZ biztonsági hatóságának küldött értesítés dátumától számított 12 hónapon belül nem kezdődik meg, vagy amennyiben szolgálati jogviszonya 12 hónapig vagy annál hosszabb ideig szünetel, és ez idő alatt a személy nem áll alkalmazásban az EKSZ-nél, más uniós intézménynél, ügynökségnél vagy szervnél vagy valamely tagállami nemzeti közigazgatási szervnél, ahol szükség van minősített adatokhoz való hozzáférésre, az illetékes nemzeti biztonsági hatóságtól megerősítést kell kérni arra vonatkozóan, hogy az ellenőrzés eredménye továbbra is érvényes és helytálló.

17. Amennyiben arra vonatkozó információ jut az EKSZ tudomására, hogy egy érvényes személyi biztonsági tanúsítvánnyal rendelkező személy biztonsági kockázatot jelent, az EKSZ 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. Ha valamely nemzeti biztonsági hatóság egy EU-minősített adatokhoz való hozzáférésre jogosító, érvényes engedéllyel rendelkező személyre vonatkozóan a (12) bekezdés a) pontjával összhangban tett megállapítás visszavonásáról értesíti az EKSZ-t, az EKSZ biztonsági hatósága felkérheti az illetékes nemzeti biztonsági hatóságot, hogy – ha a nemzeti jogszabályok és rendelkezések alapján módjában áll – adjon további felvilágosítást. Ha a kedvezőtlen információk megerősítést nyernek, a fent említett engedélyt visszavonják, és a személyt kizárják az EU-minősített adatokhoz való hozzáférésből, valamint azokból a beosztásokból, amelyekben az ilyen hozzáférés lehetséges, vagy amelyekben a személy veszélyeztetheti a biztonságot.

18. Az EU-minősített adatokhoz való hozzáférésre vonatkozó engedélynek az EKSZ-személyzet tagjától való visszavonásáról szóló határozatról és adott esetben annak indokairól tájékoztatják az érintett személyt, aki kérheti az EKSZ biztonsági hatósága általi meghallgatását. A nemzeti biztonsági hatóságok által rendelkezésre bocsátott információkra az adott tagállamban hatályos megfelelő jogszabályok és rendelkezések vonatkoznak, beleértve a jogorvoslattal kapcsolatos rendelkezéseket is. Az EKSZ biztonsági hatóságának határozatai ellen a személyzeti szabályzattal összhangban lehet fellebbezni.

19. Az EKSZ-hez CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokhoz való hozzáférést igénylő beosztásba kirendelt nemzeti szakértőknek tevékenységük megkezdését megelőzően a megfelelő szintű EU-minősített adathoz való hozzáféréshez szükséges, érvényes személyi biztonsági tanúsítványt kell benyújtaniuk az EKSZ biztonsági hatóságához. A fenti eljárást a küldő tagállam folytatja le.

A személyi biztonsági tanúsítványok nyilvántartása

20. Az EKSZ nyilvántartást vezet a felelőssége alá tartozó személyzet és a vele szerződéses jogviszonyban álló vállalkozók személyzete biztonsági tanúsítványának állapotáról. E nyilvántartás tartalmazza, hogy az adott személy számára milyen minősítési szintű EU-minősített adatokhoz biztosítható hozzáférés (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint a személyi biztonsági tanúsítvány kibocsátásának dátumát és érvényességi idejét.

21. Megfelelő koordinációs eljárásokat vezetnek be a tagállamokkal és más uniós intézményekkel, ügynökségekkel és szervekkel annak biztosítása érdekében, hogy az EKSZ pontos és átfogó nyilvántartást vezessen a felelőssége alá tartozó személyzet és a vele szerződéses jogviszonyban álló vállalkozók személyzete biztonsági tanúsítványának állapotáról.

22. Az EKSZ biztonsági hatósága személyi biztonsági tanúsítványról szóló igazolást (PSCC) adhat ki, amely tartalmazza, hogy az adott személy számára milyen minősítési szintű EU-minősített adatokhoz biztosítható hozzáférés (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint a vonatkozó személyi biztonsági tanúsítvány érvényességi idejét és az igazolás lejáratának időpontját.

Mentességek a személyi biztonsági tanúsítvány követelménye alól

23. A feladatkörüknél fogva az EU-minősített adatokhoz való hozzáférésre a nemzeti jogszabályokkal és rendelkezésekkel összhangban megfelelően felhatalmazott személyeket az EKSZ Biztonsági Igazgatósága adott esetben tájékoztatja az EU-minősített adatok védelmével kapcsolatos biztonsági kötelezettségeikről.

III. BIZTONSÁGI OKTATÁS ÉS TUDATOSSÁG

24. Az EU-minősített adatokhoz való hozzáférés engedélyezése előtt valamennyi személynek írásban kell nyilatkoznia arról, hogy megértette az EU-minősített adatok védelmével kapcsolatos kötelezettségeit, valamint az EU-minősített adatok illetéktelenek tudomására jutásának következményeit. Az ilyen írásbeli nyilatkozatokról az EKSZ nyilvántartást vezet.

25. Mindazon személyekkel, akik engedéllyel rendelkeznek EU-minősített adatokhoz való hozzáférésre, vagy akiknek ilyen adatokat kell kezelniük, kezdetben, majd később rendszeres időközönként ismertetik a biztonságot fenyegető veszélyeket, és e személyeknek haladéktalanul jelenteniük kell a megfelelő biztonsági hatóságoknak bármilyen, általuk gyanúsnak vagy szokatlannak ítélt magatartást vagy tevékenységet.

26. Mindazon személyek tekintetében, akik számára engedélyezték az EU-minősített adatokhoz való hozzáférést, folyamatos személyi biztonsági ellenőrzéseket kell végezni (utógondozás) az EU-minősített adatok kezelésének ideje alatt. A folyamatos személyi biztonsági ellenőrzés a következők felelősségi körébe tartozik:

a) Az EU-minősített adatokhoz hozzáféréssel rendelkező személyek: E személyek személyesen felelnek saját biztonsággal kapcsolatos magatartásukért, és haladéktalanul jelenteniük kell a megfelelő biztonsági hatóságoknak az általuk gyanúsnak vagy szokatlannak ítélt magatartást vagy tevékenységet, valamint a személyes körülményeikben bekövetkezett bármely változást, amely hatással lehet személyi biztonsági tanúsítványukra vagy az EU-minősített adatokhoz való hozzáférésük engedélyezésére.

b) Közvetlen felettesek: A következőkért felelnek: annak biztosítása, hogy személyzetük ismerje az EU-minősített adatok védelmére vonatkozó biztonsági intézkedéseket és feladatokat, személyzetük biztonsággal kapcsolatos magatartásának figyelemmel kísérése, továbbá hogy vagy saját maguk foglalkozzanak az aggályos biztonsági kérdésekkel, vagy jelentsék a megfelelő biztonsági hatóságoknak az olyan kedvezőtlen információkat, amelyek hatással lehetnek személyzetük személyi biztonsági tanúsítványára vagy az EU-minősített adatokhoz való hozzáférésük engedélyezésére.

c) Az EKSZ biztonsági szervezetének biztonsági szereplői az e határozat 12. cikkében említettek szerint: A következőkért felelnek: megfelelő biztonságtudatossági tájékoztatók nyújtása annak érdekében, hogy a területükhöz tartozó személyzet rendszeres felvilágosítást kapjon, a magas fokú biztonsági kultúra előmozdítása felelősségi körükben, a személyzet biztonsággal kapcsolatos magatartásának figyelemmel kísérését célzó intézkedések bevezetése, valamint az olyan kedvezőtlen információk jelentése a megfelelő biztonsági hatóságoknak, amelyek hatással lehetnek az adott személyek személyi biztonsági tanúsítványára.

d) Az EKSZ és a tagállamok: Létrehozzák a szükséges kommunikációs csatornákat az olyan információk továbbítására, amelyek hatással lehetnek az adott személyek személyi biztonsági tanúsítványára vagy az EU-minősített adatokhoz való hozzáférésük engedélyezésére.

27. Valamennyi személlyel, akit nem alkalmaznak tovább az EU-minősített adatokhoz való hozzáférést megkövetelő feladatok ellátására, ismertetik az EU-minősített adatok folyamatos védelmének tiszteletben tartására vonatkozó kötelezettségét, és adott esetben az érintett személyeknek ezt írásban tudomásul kell venniük.

IV. RENDKÍVÜLI KÖRÜLMÉNYEK

28. Az EKSZ biztonsági hatósága – sürgős esetben, amennyiben azt az EKSZ érdekei kellően indokolják, és a teljes körű biztonsági ellenőrzés lezárulásáig – az érintett állampolgársága szerinti tagállam nemzeti biztonsági hatóságával folytatott konzultációt követően, valamint a kizáró tényezők hiányát ellenőrző előzetes vizsgálatok eredményétől függően egy meghatározott feladat tekintetében ideiglenesen engedélyezheti az EKSZ tisztviselői és egyéb alkalmazottai számára az EU-minősített adatokhoz való hozzáférést. A teljes körű biztonsági ellenőrzést a lehető leghamarabb el kell végezni. Az ideiglenes engedély érvényességének időtartama legfeljebb hat hónap lehet, és nem teheti lehetővé a TRES 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 illetéktelenek tudomására jutásának következményeit. Az ilyen írásbeli nyilatkozatokról az EKSZ nyilvántartást vezet.

29. Amennyiben egy adott személyt olyan beosztásba készülnek kinevezni, amelyhez az érintett által jelenleg birtokoltnál eggyel magasabb szintű személyi biztonsági tanúsítvány szükséges, a kinevezés átmeneti alapon végrehajtható, amennyiben:

a) a személy felettese írásban igazolja a magasabb szintű EU-minősített adatokhoz való sürgős hozzáférés szükségességét;

b) a hozzáférés a feladat elvégzését elősegítő, meghatározott EU-minősített adatokra korlátozódik;

c) a személy érvényes személyi biztonsági tanúsítvánnyal rendelkezik;

d) kezdeményezték a beosztáshoz szükséges szintű hozzáférés engedélyezését;

e) az illetékes hatóság megfelelően ellenőrizte, hogy a személy nem sértette meg súlyosan vagy ismétlődően a biztonsági szabályokat;

f) az EKSZ illetékes hatósága jóváhagyta a személy megbízását;

g) konzultáltak a személy személyi biztonsági tanúsítványát kibocsátó illetékes nemzeti vagy kijelölt biztonsági hatósággal, és az nem emelt kifogást; valamint

h) az illetékes nyilvántartás vagy alárendelt nyilvántartás nyilvántartásba veszi a kivételes esetet, beleértve azon adatok leírását, amelyekhez a hozzáférést jóváhagyták.

30. A fenti eljárás az annál eggyel magasabb szintű EU-minősített adatokhoz való hozzáférés megadására alkalmazandó, mint amilyen szintre vonatkozóan a személy biztonsági ellenőrzésen átesett. Ez az eljárás nem alkalmazható ismétlődő jelleggel.

31. Különösen kivételes körülmények között – például ellenséges környezetben végrehajtott kiküldetések során vagy növekvő nemzetközi feszültség idején, amennyiben a biztonsági intézkedések ezt megkívánják, különösen életmentés céljából – a főképviselő, az EKSZ biztonsági hatósága vagy a költségvetésért és igazgatásért felelős főigazgatóság lehetőség szerint írásban hozzáférést adhat CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz olyan személyek számára, akik nem rendelkeznek a szükséges személyi biztonsági tanúsítvánnyal, feltéve, hogy ez az engedély feltétlenül szükséges. A megadott engedélyt nyilvántartásba veszik, és bejegyzik azon adatok leírását, amelyekhez a hozzáférést jóváhagyták.

32. A TRES SECRET UE/EU TOP SECRET minősítésű adatok esetében az ilyen sürgősségi hozzáférés olyan uniós polgárokra korlátozódik, akik számára engedélyezték a TRES SECRET UE/EU TOP SECRET szint nemzeti megfelelőjéhez vagy a SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférést.

33. Az EKSZ Biztonsági Bizottságát tájékoztatják azokról az esetekről, amikor a (31) és (32) bekezdésben foglalt eljárást alkalmazzák.

34. Az EKSZ Biztonsági Bizottsága részére éves jelentést készítenek az e szakaszban meghatározott eljárások alkalmazásáról.

V. AZ EKSZ SZÉKHELYÉN ÉS AZ UNIÓS KÜLDÖTTSÉGEKEN TARTOTT ÜLÉSEKEN VALÓ RÉSZVÉTEL

35. Az EKSZ székhelyén és az uniós küldöttségeken tartott, CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokat tárgyaló üléseken való részvétellel megbízott személyek csak személyi biztonsági tanúsítványuk állapotának megerősítését követően vehetnek részt. A tagállamok képviselői, a Tanács Főtitkársága és a Bizottság tisztviselői esetében a személyi biztonsági tanúsítványról szóló igazolást vagy a személyi biztonsági tanúsítvány egyéb bizonyítékát a megfelelő hatóságok továbbítják az EKSZ Biztonsági Igazgatóságának, az uniós küldöttség biztonsági koordinátorának vagy azt kivételes esetben az érintett személy is benyújthatja. Adott esetben összesített névjegyzék használható, amely a személyi biztonsági tanúsítvány meglétét bizonyítja.

36. Amennyiben az EU-minősített adatokhoz való hozzáféréshez szükséges személyi biztonsági tanúsítványt visszavonják egy olyan személytől, akinek feladatai megkövetelik az EKSZ székhelyén vagy az uniós küldöttségeken tartott, CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokat tárgyaló üléseken való részvételt, az illetékes hatóság tájékoztatja erről az EKSZ-t.

VI. AZ EU-MINŐSÍTETT ADATOKHOZ VALÓ POTENCIÁLIS HOZZÁFÉRÉS

37. Amennyiben egyes személyeket olyan körülmények között alkalmaznak, amelyek között potenciálisan CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű adatokhoz férhetnek hozzá, e személyeknek megfelelő biztonsági ellenőrzésen kell átesniük, vagy állandó kíséretet kell biztosítani számukra.

38. A futároknak, a biztonsági őröknek és a kísérőknek megfelelő szintű biztonsági ellenőrzésen, vagy a nemzeti jogszabályoknak és rendelkezéseknek megfelelő egyéb vizsgálaton kell átesniük, rendszeres időközönként tájékoztatni kell őket az EU-minősített adatok védelmét célzó biztonsági eljárásokról és az olyan minősített adatok védelmét érintő feladataikról, amelyeket rájuk bíztak vagy amelyekhez véletlen folytán hozzáférhetnek.

A.II. MELLÉKLET

AZ EU-MINŐSÍTETT ADATOK FIZIKAI BIZTONSÁGA

I. BEVEZETÉS

1. Ez a melléklet meghatározza az A. melléklet 6. cikkének végrehajtására vonatkozó rendelkezéseket. Megállapítja az olyan helyiségek, épületek, irodák, termek és egyéb területek – többek között a kommunikációs és információs rendszernek 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 biztosítása;

   b) a személyzet tagjainak 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 belépésének megakadályozása vagy késleltetése.

II. FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK ÉS INTÉZKEDÉSEK

3. Az EKSZ kockázatkezelési eljárást alkalmaz az EU-minősített adatoknak a saját helyiségein belüli védelmére, a becsült 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 formája és terjedelme, 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;

   d) az INTCEN által különösen az uniós küldöttségek jelentései alapján kidolgozott, harmadik országról szóló fenyegetésértékelés, valamint

   e) az EU-t vagy a tagállamokat célzó tevékenységet végző hírszerző szolgálatokhoz, valamint a szabotázshoz, terrorizmushoz, felforgató tevékenységekhez vagy más bűncselekményekhez kapcsolódó becsült fenyegetések.

4. Az EKSZ biztonsági hatósága a mélységi védelem elvének alkalmazásával meghatározza a végrehajtandó fizikai biztonsági intézkedések megfelelő kombinációját. Ezek egy vagy több, alább felsorolt intézkedést foglalhatnak magukban:

   a) kordon: fizikai akadály, amely védi a védelmet igénylő terület határát;

   b) behatolásjelző rendszerek: behatolásjelző rendszerek a kordon nyújtotta védelem növelésére, vagy termekben és épületekben a biztonsági személyzet helyett vagy annak támogatására használhatók;

   c) belépés-ellenőrzés: a belépés-ellenőrzés kiterjedhet egy adott helyszínre, egy adott helyszínen található épületre vagy épületekre, valamint egy épületen belüli területekre vagy termekre. Az ellenőrzés történhet elektronikus vagy elektromechanikus eszközökkel, a biztonsági személyzet és/vagy a recepciós által vagy bármilyen más fizikai eszközzel;

   d) biztonsági személyzet: képzett, felügyelt és – szükség esetén – megfelelő biztonsági ellenőrzésen átesett biztonsági személyzet alkalmazható többek között a titkos behatolást tervező személyek elrettentésére;

   e) zártláncú televízió: nagy kiterjedésű helyszíneken vagy a határterületeken a biztonsági személyzet zártláncú televízió segítségével ellenőrizheti az incidenseket és a behatolásjelző rendszer riasztásait;

f) biztonsági világítás: biztonsági világítás használható a lehetséges behatolók elrettentésére, valamint a biztonsági személyzet általi közvetlen vagy a zártláncú televíziós rendszeren keresztüli 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 EKSZ Biztonsági Igazgatósága a be- és kilépéskor átvizsgálást végezhet a nem engedélyezett anyagok bevitelétől vagy EU-minősített adatoknak a helyiségből vagy épületből történő engedély nélküli kivitelétől való elrettentés céljából.

6. Amennyiben fennáll az EU-minősített adatokba történő – akár véletlenszerű – betekintés kockázata, megfelelő intézkedéseket kell hozni annak kivédésére.

7. Az új létesítmények esetében a fizikai biztonsági követelményeket és azok funkcionális jellemzőit a létesítmények tervezése és kialakítása során meg kell határozni. A már meglevő létesítmények esetében a fizikai biztonsági követelményeket a lehető legteljesebb mértékben kell érvényesíteni.

III. AZ EU-MINŐSÍTETT ADATOK FIZIKAI VÉDELMÉRE SZOLGÁLÓ BERENDEZÉSEK

8. Az EU-minősített adatok fizikai védelmét szolgáló felszerelések (például biztonsági tárolóeszközök, iratmegsemmisítő gépek, ajtózárak, elektronikus beléptető rendszerek, behatolásjelző-rendszerek, riasztórendszerek) beszerzésekor az EKSZ biztonsági hatósága biztosítja, hogy a felszerelések megfeleljenek a jóváhagyott műszaki szabványoknak és minimumkövetelményeknek.

9. Az EU-minősített adatok fizikai védelmére szolgáló felszerelések műszaki jellemzőit az EKSZ Biztonsági Bizottsága 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 optimálisan 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 a fizikai védelemben részesülő területek – vagy azok nemzeti megfelelői – két típusa kerül kialakításra:

a) adminisztratív területek; valamint

b) biztonsági területek (köztük a technikailag biztosított biztonsági területek).

13. Az EKSZ biztonsági hatósága megállapítja, hogy egy adott terület megfelel-e az adminisztratív területként, biztonsági területként vagy technikailag biztosított biztonsági területként való kijelölés követelményeinek.

14. Adminisztratív területek esetében:

a) láthatóan elhatárolt körzetet kell meghatározni, amely lehetővé teszi a személyek és lehetőség szerint a járművek ellenőrzését;

b) a kíséret nélküli belépés csak az EKSZ Biztonsági Igazgatósága által kiadott megfelelő engedéllyel rendelkező személyek számára biztosítható; valamint

c) minden más személy számára állandó kíséretet kell biztosítani vagy a személyt ezzel egyenértékű ellenőrzésnek kell alávetni.

15. Biztonsági területek esetében:

a) láthatóan elhatárolt és védett körzetet kell kialakítani, amelybe, illetve amelyből minden be- és kilépést beléptető vagy személyazonosító rendszerrel ellenőriznek;

b) kíséret nélküli belépés kizárólag olyan személyek számára biztosítható, akik megfelelő szintű biztonsági ellenőrzésen estek át, és a szükséges ismeret elve alapján különleges engedéllyel rendelkeznek a területre való belépésre;

c) minden más személy számára állandó kíséretet kell biztosítani vagy a személyt ezzel egyenértékű ellenőrzésnek kell alávetni.

16. Amennyiben a biztosított területre való belépés lehetővé teszi az ott található minősített adatokhoz való közvetlen – bármilyen gyakorlati célt szolgáló – hozzáférést, 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 számára állandó kíséretet kell biztosítani és minden látogatónak megfelelő biztonsági ellenőrzésen kell átesnie, kivéve ha intézkedéseket tettek az EU-minősített adatokhoz való hozzáférés lehetőségének kizárására;

c) az elektronikus eszközöket a területen kívül kell hagyni.

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 behatolásjelző rendszerrel szerelik fel, használaton kívül zárva tartják, használat esetén pedig őrzik. E melléklet VI. szakaszával összhangban valamennyi kulcsot ellenőrizni kell;

b) az e területekre belépő személyeket és anyagokat ellenőrizni kell;

c) az ilyen területeket rendszeres fizikai és/vagy technikai ellenőrzéseknek vetik alá az EKSZ biztonsági hatósága 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 kommunikációs eszközök, illetve elektromos vagy elektronikus berendezések;

18. A (17) bekezdés d) pontja ellenére minden kommunikációs, elektromos vagy elektronikus berendezést – mielőtt olyan területen használnák őket, ahol SECRET UE/EU SECRET vagy magasabb minősítési szintű adatokat érintő üléseket tartanak vagy munkát végeznek, valamint ahol az EU-minősített adatokat fenyegető kockázat magasnak minősül – először az EKSZ biztonsági hatósága megvizsgál annak biztosítása érdekében, hogy ilyen berendezés révén véletlenül vagy tiltott módon ne továbbíthassanak 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 ellenőrzik, a rendes munkaidőn kívül pedig szúrópróbaszerűen ellenőrzik, amennyiben az említett területeken nem működik behatolásjelző rendszer.

20. Biztonsági területek és technikailag biztosított biztonsági területek ideiglenesen is létrehozhatók egy adminisztratív területen belül, minősített üléshez vagy más hasonló célból.

21. Minden egyes biztonsági terület tekintetében kidolgozzák a biztonsági üzemeltetési eljárásokat, amelyek az alábbiakat tartalmazzák:

a) a területen esetlegesen kezelt és tárolt EU-minősített adatok minősítési szintje;

b) az alkalmazandó megfigyelési és védelmi intézkedések;

c) a szükséges ismeret elve és biztonsági tanúsítvány alapján a területre kíséret nélkül való belépésre jogosult személyek;

d) adott esetben a kíséretre vagy az EU-minősített adatok védelmére vonatkozó eljárások minden más személy területre való belépésének engedélyezésekor;

e) bármely egyéb vonatkozó intézkedés és eljárás.

22. A biztonsági területeken biztosított helyiségeket kell kialakítani. Az EKSZ biztonsági hatósága jóváhagyja a falakat, padlókat, plafonokat, ablakokat és zárható ajtókat, amelyek az ugyanilyen minősítési szintű EU-minősített adatok tárolására jóváhagyott biztonsági tárolóeszköz által nyújtottal egyenértékű védelmet biztosítanak.

V. AZ EU-MINŐSÍTETT ADATOK KEZELÉSÉRE ÉS TÁROLÁSÁRA VONATKOZÓ FIZIKAI VÉDELMI INTÉZKEDÉSEK

23. A RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatok kezelhetők:

a) biztonsági területen;

b) adminisztratív területen, amennyiben biztosított az EU-minősített adatok védelme az engedéllyel nem rendelkező személyek általi hozzáféréssel szemben, vagy

c) biztonsági területen vagy adminisztratív területen kívül, amennyiben az adat birtokosa az A.III. melléklet (30)–(42) bekezdésével összhangban szállítja az EU-minősített adatokat, és vállalta, hogy eleget tesz az EKSZ biztonsági hatósága által az EU-minősített adatok engedéllyel nem rendelkező személyek általi hozzáférésével szembeni védelme céljából kiadott biztonsági utasításokban foglalt kiegészítő intézkedéseknek.

24. A RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatokat megfelelően zárható irodabútorokban kell tárolni az adminisztratív vagy a biztosított területen belül. Ezek az adatok ideiglenesen biztosított területen vagy igazgatási területen kívül is tárolhatók, amennyiben az adat birtokosa vállalta, hogy eleget tesz az EKSZ biztonsági hatósága által kiadott biztonsági utasításokban foglalt kiegészítő intézkedéseknek.

25. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű EU-minősített adatok kezelhetők:

a) biztonsági területen;

b) adminisztratív területen, amennyiben biztosított az EU-minősített adatok védelme az engedéllyel nem rendelkező személyek általi hozzáféréssel szemben; vagy

c) biztonsági területen vagy adminisztratív területen kívül, amennyiben az adat birtokosa:

i. az A.III. melléklet (30)–(42) bekezdésével összhangban szállítja az EU-minősített adatokat;

ii. vállalta, hogy eleget tesz az EKSZ biztonsági hatósága által az EU-minősített adatok engedéllyel nem rendelkező személyek általi hozzáférésével szembeni védelme céljából kiadott biztonsági utasításokban foglalt kiegészítő intézkedéseknek;

iii. az EU-minősített adatokat mindenkor személyes felügyelete alatt tartja; valamint

iv. papíralapú dokumentumok esetében értesítette erről az érintett nyilvántartást.

26. A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat a biztonsági területen belül kell tárolni biztonsági tárolóeszközben vagy biztosított helyiségben.

27. A TRES SECRET UE/EU TOP SECRET minősítésű adatokat biztonsági területen kell kezelni.

28. A TRES SECRET UE/EU TOP SECRET minősítésű EU-minősített adatokat a székhely biztonsági területén az alábbi módok valamelyikének megfelelően kell tárolni:

a) a (8) bekezdés szerinti biztonsági tárolóeszközben, az alábbiak közül egy vagy több kiegészítő ellenőrzés kíséretében:

i. ellenőrzésen átesett biztonsági vagy munkavégző személyzet általi folyamatos védelem vagy ellenőrzés;

ii. jóváhagyott behatolásjelző rendszer, a biztonságért felelős elhárító személyzettel együtt;

vagy

b) behatolásjelző rendszerrel ellátott biztosított helyiségben, a biztonságért felelős elhárító személyzettel együtt.

29. Az EU-minősített adatok fizikailag védett területeken kívüli szállítására vonatkozó szabályokat az A.III. melléklet tartalmazza.

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

30. Az EKSZ biztonsági hatósága meghatározza az irodák, termek, biztosított helyiségek és biztonsági tárolóeszközök kulcsainak és kombinációinak kezelésére vonatkozó eljárásokat. Ezek az eljárások biztosítják a jogosulatlan hozzáféréssel szembeni védelmet.

31. A kombinációkat kívülről meg kell tanulnia annak a lehető legkisebb számú személynek, akinek azokat ismernie kell. Az EU-minősített adatok tárolására szolgáló biztonsági tárolóeszközök és biztosított helyiségek kombinációit az alábbi esetekben meg kell változtatni:

a) új tárolóeszköz átvételekor;

b) a kombinációt ismerő személyzet minden változásakor;

c) ha azok illetéktelenek tudomására jutottak vagy ennek gyanúja merült fel;

d) ha a záron karbantartást vagy javítást végeztek; valamint

e) legalább 12 havonta.

III.A. MELLÉKLET

MINŐSÍTETT ADATOK KEZELÉSE

I. BEVEZETÉS

1. Ez a melléklet meghatározza az A. melléklet 7. cikkének végrehajtására vonatkozó rendelkezéseket. Megállapítja az EU-minősített adatok teljes életcikluson keresztüli ellenőrzésére szolgáló adminisztratív intézkedéseket, amelyek hozzájárulnak az ilyen adatok illetéktelenek tudomására jutásától vagy elvesztésétől való elrettentéshez – szándékos vagy véletlenszerű esetekben egyaránt –, annak észleléséhez és a kár helyreállításához.

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 az A. melléklet 2. cikkének (2) bekezdésével összhangban, valamint az A. melléklet 3. cikkének (3) bekezdésével összhangban jóváhagyandó biztonsági iránymutatásokra hivatkozva kell meghatározni.

5. A tagállamok EKSZ-szel megosztott minősített adatai számára ugyanolyan szintű védelmet kell biztosítani, mint az egyenértékű minősítésű EU-minősített adatok számára. E határozat B. függelékében egyenértékűségi táblázat található.

6. A biztonsági minősítést – és adott esetben azon időpontot vagy konkrét eseményt, amelyet követően a minősített adat visszaminősíthető vagy a minősítés feloldható – egyértelműen és helyesen fel kell tüntetni, attól függetlenül, hogy az EU-minősített adat papíralapú, szóbeli, elektronikus vagy más formátumú.

7. Egy adott dokumentum egyes részei (például oldalai, bekezdései, szakaszai, mellékletei, függelékei, toldalékai és csatolmányai) eltérő minősítést igényelhetnek, és ennek megfelelő jelölést kell kapniuk, az elektronikus formában történő tárolás esetén is.

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 dokumentum vagy az akta egésze legalább a legmagasabb minősítési szintű részével megegyező minősítését kap. Ha egy dokumentumot különböző forrásokból származó adatokból állítanak össze, a kész anyagot az átfogó minősítési szint meghatározása céljából át kell nézni, mivel összességében indokolt lehet az egyes részekhez képest magasabb minősítési szint.

10. A mellékleteket kísérő levél vagy feljegyzés ugyanolyan minősítést kap, mint a legmagasabb minősítési szintű melléklete. A kibocsátó megfelelő jelöléssel egyértelműen jelzi, hogy a kísérő levél vagy feljegyzés milyen szintű minősítést kap, ha a mellékleteitől elválasztják, például a következő formában:

CONFIDENTIEL UE/EU CONFIDENTIAL

Melléklet(ek) nélküli minősítés: RESTREINT UE/EU RESTRICTED

Jelölések

11. Az A. melléklet 2. cikkének (2) bekezdésében meghatározott biztonsági minősítési jelölések mellett az EU-minősített adatok további jelölésekkel láthatók el, úgymint:

a) a kibocsátó megjelölésére szolgáló azonosító;

b) figyelmeztetés, kód vagy betűszó a dokumentum által érintett tevékenységi terület, a szükséges ismeret elve alapján történő különleges továbbítási szabályok vagy a felhasználási korlátozások meghatározására;

c) az átadhatóságra vonatkozó jelölések.

12. Az EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére történő átadására vonatkozó döntést követően az EKSZ Biztonsági Igazgatósága továbbítja az érintett minősített adatokat, amelyeken szerepel az átvevő harmadik államot vagy nemzetközi szervezetet feltüntető, átadásra jogosító jelölés is.

13. Az EKSZ biztonsági hatósága el fogja fogadni az engedélyezett jelölések listáját.

Rövidített minősítési jelölések

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

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

TRES 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 adatok létrehozása

16. EU-minősített dokumentum létrehozásakor:

a) minden egyes oldalon jól láthatóan feltüntetik a minősítési szintet;

b) minden egyes oldalt megszámoznak;

c) a dokumentumot ellátják nyilvántartási számmal és tárggyal, amely önmagában nem minősített adat, kivéve ha akként jelölik;

d) a dokumentumot keltezik;

e) a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű dokumentumok minden egyes oldalán feltüntetik a példány sorszámát, ha azokat több példányban forgalmazzák.

17. Amennyiben az EU-minősített adatokra a (16) bekezdés nem alkalmazható, az e határozat értelmében kialakítandó biztonsági iránymutatásoknak megfelelő egyéb intézkedéseket kell hozni.

EU-minősített adatok visszaminősítése és a minősítés feloldása

18. Az adat létrehozásakor – amennyiben lehetséges, és különösen a RESTREINT UE/EU RESTRICTED minősítésű adat esetén – a kibocsátó jelöli, hogy egy adott időpontban vagy egy konkrét eseményt követően az EU-minősített adat visszaminősíthető-e vagy minősítése feloldható-e.

19. Az EKSZ rendszeresen felülvizsgálja a birtokában lévő EU-minősített adatokat annak megállapítása céljából, hogy minősítési szintjük továbbra is érvényes-e. Az EKSZ kialakít egy rendszert az általa kibocsátott, nyilvántartásba vett EU-minősített adatok minősítési szintjének legalább ötévenkénti felülvizsgálatára. Nincs szükség ilyen felülvizsgálatra akkor, ha a kibocsátó már kezdetben jelezte, hogy egy adott időpontban az adatot automatikusan vissza fogják minősíteni vagy a minősítését fel fogják oldani, és az adatot ennek megfelelően jelölték.

III. EU-MINŐSÍTETT ADATOK BIZTONSÁGI CÉLÚ NYILVÁNTARTÁSBA VÉTELE

20. A székhelyen központi nyilvántartást hoznak létre. Az EKSZ keretében működő, EU-minősített adatot kezelő valamennyi szervezeti egységnél létrehoznak egy, a központi nyilvántartásnak alárendelt felelős nyilvántartást annak biztosítása érdekében, hogy az EU-minősített adatok kezelése e határozattal összhangban történjen. A nyilvántartásokat az A. mellékletben meghatározott biztonsági területeken hozzák létre.

Az egyes uniós küldöttségek létrehozzák az EU-minősített adatokat rögzítő saját nyilvántartásukat.

Az EKSZ biztonsági hatósága kijelöli e nyilvántartások vezető iktatási tisztviselőjét.

21. E határozat alkalmazásában a biztonsági célú nyilvántartásba vétel (a továbbiakban: nyilvántartásba vétel) olyan eljárások alkalmazása, amelyek során rögzítésre kerül az adat életciklusa, beleértve a terjesztését és a megsemmisítését is. Kommunikációs és információs rendszer esetében a nyilvántartási eljárások a kommunikációs és információs rendszeren belüli folyamatok keretében is elvégezhetők.

22. Valamennyi CONFIDENTIEL UE/EU CONFIDENTIAL és annál magasabb minősítésű anyagot a szervezeti egységhez – köztük az uniós küldöttségekhez – való beérkezéskor vagy az onnan történő továbbításkor nyilvántartásba vesznek. A TRES SECRET UE/EU TOP SECRET minősítésű adatokat erre kijelölt nyilvántartásokban rögzítik.

23. Az EKSZ székhelyén található központi nyilvántartás a minősített adatok harmadik államokkal és nemzetközi szervezetekkel való megosztásának fő beérkezési és kiküldési pontjaként működik. A központi nyilvántartás valamennyi ilyen adatcserét rögzíti.

24. Az EKSZ biztonsági hatósága jóváhagyja az EU-minősített adatok biztonsági célú nyilvántartásba vételére vonatkozó biztonsági iránymutatásokat, e határozat 14. cikkével összhangban.

TRES SECRET UE/EU TOP SECRET nyilvántartások

25. Az EKSZ székhelyén kijelölik a TRES SECRET UE/EU TOP SECRET minősítésű adatok központi átvételéért és továbbításáért felelős hatóságként működő központi nyilvántartást. Szükség esetén ennek alárendelt nyilvántartások is kijelölhetők ezen adatok nyilvántartási célú kezelésére.

26. Az alárendelt nyilvántartások a központi nyilvántartás kifejezett írásbeli jóváhagyása nélkül nem továbbíthatnak közvetlenül TRES SECRET UE/EU TOP SECRET minősítésű dokumentumokat az ugyanazon TRES SECRET UE/EU TOP SECRET központi nyilvántartásnak alárendelt többi nyilvántartás számára vagy külső feleknek.

IV. EU-MINŐSÍTETT DOKUMENTUMOK MÁSOLÁSA ÉS FORDÍTÁSA

27. A TRES SECRET EU/EU TOP SECRET minősítésű dokumentumok nem másolhatók vagy fordíthatók a kibocsátó előzetes írásbeli hozzájárulása nélkül.

28. Amennyiben a SECRET UE/EU SECRET és ennél alacsonyabb minősítésű dokumentumok kibocsátója a másolásra vagy fordításra vonatkozóan nem határozott meg korlátozásokat, e dokumentumok az adatbirtokos utasítására másolhatók vagy fordíthatók.

29. Az eredeti dokumentumra vonatkozó biztonsági intézkedések a másolatokra és a fordításokra is alkalmazandók. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű dokumentumokról kizárólag a vonatkozó (alárendelt) nyilvántartás készíthet másolatot biztonságos másológéppel. A másolatokat nyilvántartásba kell venni.

V. EU-MINŐSÍTETT ADATOK SZÁLLÍTÁSA

30. Az EU-minősített adatok szállítására a (32)–(42) bekezdésben szereplő védelmi intézkedések vonatkoznak. Az EU-minősített adatok elektronikus eszközökön történő szállítása során – az A. melléklet 7. cikkének (4) bekezdésétől eltérően – az elvesztés vagy az illetéktelenek tudomására jutás kockázatának minimalizálása érdekében az alább meghatározott védelmi intézkedéseket kiegészíthetik az EKSZ biztonsági hatósága által előírt, megfelelő technikai ellenintézkedések.

31. Az EKSZ biztonsági hatósága utasításokat bocsát ki az EU-minősített adatok e határozattal összhangban történő szállítására vonatkozóan.

Épületen vagy zárt épületcsoporton belül

32. A valamely épületen vagy zárt épületcsoporton belül szállított EU-minősített adatokat a tartalmukba való betekintés megakadályozása érdekében el kell takarni.

33. TRES SECRET UE/EU TOP SECRET minősítésű adatokat adott épületen vagy zárt épületcsoporton belül megfelelő biztonsági ellenőrzésen átesett személyeknek kell szállítaniuk egy lezárt borítékban, amelyen kizárólag a címzett neve tüntethető fel.

Az Európai Unión belül

34. Az EU-n belül épületek vagy létesítmények között szállított EU-minősített adatokat úgy kell becsomagolni, hogy azok védettek legyenek az illetéktelen hozzáféréstől.

35. A legfeljebb SECRET UE/EU SECRET minősítési szintű adatok EU-n 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 szállító személy birtokában marad, kivéve, ha azt az A.II. mellékletben foglalt követelményekkel összhangban tárolják;

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

iii. az érintett személyek megfelelő szintű biztonsági ellenőrzésen estek át, és tájékoztatást kaptak a biztonsággal kapcsolatos felelősségükről;

iv. az érintettek számára szükség esetén futárigazolványt állítanak ki;

c) postaszolgálatok vagy kereskedelmi futárszolgálatok, feltéve, hogy:

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

ii. azok az e határozat 21. cikkének (1) bekezdése szerinti biztonsági iránymutatásokban meghatározandó minimumkövetelményeknek megfelelő védelmi intézkedéseket alkalmaznak.

Egyik tagállamból a másikba történő szállítás esetén a c) pont rendelkezései kizárólag a CONFIDENTIEL UE/EU CONFIDENTIAL és annál alacsonyabb minősítésű adatokra alkalmazandók.

36. Az olyan CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű anyagokat (pl. gépek vagy berendezések), amelyek a (34) bekezdésben említett módon nem szállíthatók, kereskedelmi fuvarozók rakományként szállítják az A.V. mellékletnek megfelelően.

37. A TRES SECRET UE/EU TOP SECRET minősítésű adatok EU-n belüli szállítása épületek vagy létesítmények között az adott esetnek megfelelően katonai, kormányzati vagy diplomáciai futár révén történik.

Az EU-ból egy harmadik állam területére, vagy harmadik államokban található uniós szervezeti egységek között

38. Az EU-ból egy harmadik állam területére, vagy harmadik államokban található uniós szervezeti egységek között szállított EU-minősített adatokat úgy kell becsomagolni, hogy védve legyenek az illetéktelen hozzáféréstől.

39. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatoknak az EU-ból valamely harmadik állam területére, valamint a legfeljebb SECRET UE/EU SECRET minősítési szintű EU-minősített adatoknak a harmadik államokban lévő uniós szervezeti egységek között 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 szállító személy birtokában marad, kivéve, ha azt az A.II. mellékletben foglalt követelményekkel összhangban tárolják;

iv. az EU-minősített adatot tartalmazó csomagot útközben nem nyitják ki és nem olvassák nyilvános helyen; valamint

v. az érintett személyek megfelelő szintű biztonsági ellenőrzésen estek át, és tájékoztatást kaptak a biztonsággal kapcsolatos felelősségükről.

40. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű, az EU által harmadik állam vagy nemzetközi szervezet részére átadott adatok szállítása az A. melléklet 10. cikkének (2) bekezdése szerinti adatbiztonsági megállapodások vagy igazgatási megállapodások vonatkozó rendelkezéseivel összhangban történik.

41. A RESTREINT UE/EU RESTRICTED minősítésű adatok az EU-ból valamely harmadik állam területére postaszolgálatok vagy kereskedelmi futárszolgálatok révén is szállíthatók.

42. A TRES SECRET UE/EU TOP SECRET minősítésű adatoknak az EU-ból harmadik állam területére, vagy harmadik államokban lévő uniós szervezeti egységek között történő szállítása katonai vagy diplomáciai futár útján történik.

VI. EU-MINŐSÍTETT ADATOK MEGSEMMISÍTÉSE

43. A már nem szükséges EU-minősített dokumentumok – az archiválásra vonatkozó szabályok és rendelkezések sérelme nélkül – megsemmisíthetők.

44. A dokumentumok birtokosának vagy az illetékes hatóságnak az utasítására a felelős nyilvántartás semmisíti meg azokat a dokumentumokat, amelyeket az A. melléklet 7. cikkének (2) bekezdésével összhangban nyilvántartásba kell venni. Az iktatókönyveket és az egyéb nyilvántartási adatokat ennek megfelelően aktualizálják.

45. A SECRET UE/EU SECRET vagy TRES SECRET UE/EU TOP SECRET minősítésű dokumentumok esetében a megsemmisítést tanú jelenlétében hajtják végre, aki a megsemmisítendő dokumentum minősítési szintjével legalább megegyező szintre vonatkozó személyi biztonsági tanúsítvánnyal rendelkezik.

46. Az ügykezelő és – amennyiben annak jelenléte kötelező – a tanú aláírja a megsemmisítési tanúsítványt, amelyet iktatnak a nyilvántartásban. A nyilvántartás a megsemmisítési tanúsítványokat TRES SECRET UE/EU TOP SECRET minősítésű dokumentumok esetében legalább tíz évig, CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű dokumentumok esetében pedig legalább öt évig megőrzi.

47. A minősített dokumentumokat – köztük a RESTREINT UE/EU RESTRICTED minősítéssel rendelkezőket – a vonatkozó uniós vagy azzal egyenértékű szabványoknak, vagy a tagállamok által a nemzeti műszaki szabványokkal összhangban jóváhagyott szabványoknak megfelelően kell megsemmisíteni, ezáltal megakadályozva az adott dokumentum egészének vagy egy részének helyreállítását.

48. Az EU-minősített adatok tárolására szolgáló számítógépes adathordozókat az EKSZ biztonsági hatósága által jóváhagyott eljárásokkal összhangban kell megsemmisíteni.

VII. BIZTONSÁGI ELLENŐRZÉSEK

Az EKSZ biztonsági ellenőrzései

49. Az EKSZ biztonsági ellenőrzései e határozat 16. cikkével összhangban a következőket ölelik fel:

a) általános biztonsági ellenőrzések, amelyek célja az EKSZ-székhely, az uniós küldöttségek és valamennyi azokhoz tartozó vagy azokhoz kapcsolódó helyiség általános biztonsági szintjének felmérése, különösen az EKSZ biztonsági érdekeinek védelmében végrehajtott biztonsági intézkedések hatékonyságának értékelése érdekében;

b) EU-minősített adatokra vonatkozó biztonsági ellenőrzések, amelyek célja az EKSZ-székhelyen és az uniós küldöttségeken az EU-minősített adatok védelmében végrehajtott intézkedések hatékonyságának – rendszerint akkreditáció céljából történő – értékelése.

Ilyen ellenőrzéseket többek között különösen a következők céljából kell végezni:

i. az EU-minősített adatok védelme tekintetében az e határozatban megállapított minimumszabályok tiszteletben tartásának biztosítása;

ii. a biztonság fontosságának és a hatékony kockázatkezelésnek a hangsúlyozása az ellenőrzött szervezeteken belül;

iii. ellenintézkedések ajánlása a minősített adatok bizalmas jellegének, sértetlenségének vagy rendelkezésre állásának sérülése által okozott hatás enyhítésére; valamint

iv. a biztonsági hatóságok folyamatban lévő biztonsági oktatási és tudatosságnövelő programjainak előmozdítása.

Az EKSZ biztonsági ellenőrzéseinek lefolytatása és az ezekről szóló jelentéstétel

50. Az EKSZ biztonsági ellenőrzéseit az EKSZ Biztonsági Igazgatóságának ellenőrző csoportja végzi, szükség esetén más uniós intézmények vagy a tagállamok biztonsági szakértőinek támogatásával.

Az ellenőrző csoport hozzáféréssel rendelkezik minden olyan helyszínhez, ahol EU-minősített adatokat kezelnek, különösen a nyilvántartásokhoz és a kommunikációs és információs rendszerek kapcsolódási pontjaihoz.

51. Az EKSZ biztonsági ellenőrzéseit az uniós küldöttségeken szükség esetén a tagállamok harmadik országokban működő nagykövetségein dolgozó biztonsági tisztviselők segítségével végezhetik.

52. Az EKSZ biztonsági hatósága minden naptári év végéig elfogadja az EKSZ következő évre vonatkozó biztonsági ellenőrzési programját.

53. Az EKSZ biztonsági hatósága szükség esetén a fenti programban nem szereplő biztonsági ellenőrzéseket is végezhet.

54. A biztonsági ellenőrzés végeztével a fő következtetéseket és ajánlásokat ismertetik az ellenőrzött szervezettel. Ezt követően az ellenőrző csoport jelentést készít az ellenőrzésről. Amennyiben korrekciós intézkedéseket javasolnak és ajánlásokat fogalmaznak meg, úgy a jelentésnek elegendő adatot kell tartalmaznia a levont következtetések alátámasztására. A jelentést továbbítják az EKSZ biztonsági hatósága és az ellenőrzött szervezet vezetője részére.

Az EKSZ Biztonsági Igazgatóságának felelőssége alatt rendszeresen jelentés készül az adott időszakban végrehajtott ellenőrzésekből levont tanulságok bemutatása céljából, amely jelentést az EKSZ Biztonsági Bizottsága megvizsgálja.

Az EUSZ V. címének 2. fejezete alapján létrehozott uniós ügynökségeknél és szerveknél végzett biztonsági ellenőrzések lefolytatása és az ezekről szóló jelentéstétel

55. Az EKSZ Biztonsági Bizottsága szükség esetén szakértőket jelölhet ki az EUSZ V. címének 2. fejezete alapján létrehozott uniós ügynökségeknél és szerveknél biztonsági ellenőrzéseket végző közös uniós ellenőrző csoportokban való részvételre.

Az EKSZ biztonsági ellenőrzései során használt ellenőrző lista

56. Az EKSZ Biztonsági Igazgatósága összeállítja és naprakészen tartja az EKSZ biztonsági ellenőrzései során használandó, az ellenőrizendő elemeket tartalmazó ellenőrző listát. Az ellenőrző listát továbbítják az EKSZ Biztonsági Bizottsága részére.

57. Az ellenőrző lista kitöltéséhez szükséges adatokat – különösen az ellenőrzés során – az ellenőrzött szervezet biztonsági vezetőitől kell beszerezni. Az ellenőrző listát a részletes kitöltést követően az ellenőrzött szervezettel egyetértésben minősítik. E lista nem képezi az ellenőrzési jelentés részét.

A.IV. MELLÉKLET

A KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZERBEN KEZELT EU-MINŐSÍTETT ADATOK VÉDELME

I. BEVEZETÉS

1. Ez a melléklet meghatározza az A. melléklet 8. cikkének végrehajtására vonatkozó rendelkezéseket.

2. A kommunikációs és információs rendszerekben (CIS) végzett műveletek biztonsága és helyes működése érdekében 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 pontosságának és teljességének védelme;
letagadhatatlanság:	egy cselekmény vagy esemény megtörténtének bizonyíthatósága annak érdekében, hogy ezt a cselekményt vagy eseményt később ne lehessen letagadni.

II. INFORMÁCIÓVÉDELMI ELVEK

3. Az alábbiakban foglalt rendelkezések képezik az EU-minősített adatokat kezelő bármely kommunikációs és információs rendszer biztonságosságának alapját. E rendelkezések végrehajtásának részletes követelményeit az információvédelmi biztonsági iránymutatások határozzák meg.

Biztonsági kockázatkezelés

4. A biztonsági kockázatkezelés a kommunikációs és információs rendszer meghatározásának, kialakításának, működtetésének és fenntartásának szerves része. A kockázatkezelést (értékelés, tulajdonképpeni kezelés, elfogadás és kommunikáció) ismétlődő folyamatként kell elvégezni, a rendszertulajdonosok, a projekthatóságok, a működtető hatóságok és a biztonsági jóváhagyó hatóságok képviselőivel közösen, egy bevált, átlátható és teljes mértékben érthető kockázatértékelési eljárást alkalmazva. A kommunikációs és információs rendszer alkalmazási körét és eszközeit a kockázatkezelési folyamat kezdetekor egyértelműen meg kell határozni.

5. Az EKSZ illetékes hatóságai áttekintik a kommunikációs és információs rendszert fenyegető potenciális veszélyeket, valamint naprakész és pontos, az aktuális működési környezetet tükröző fenyegetésértékelést készítenek. 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 kielégítő egyensúlyt teremtenek a felhasználók igényei és a fennmaradó biztonsági kockázatok között.

7. Egy adott kommunikációs és információs rendszer akkreditálása tekintetében a megfelelő biztonsági akkreditációs hatóság (SAA) olyan konkrét követelményeket, hatókört és részletességet határoz meg, amelyek arányban állnak a valamennyi vonatkozó tényezőt – köztük a kommunikációs és információs rendszerben kezelt EU-minősített adatok minősítési szintjét – figyelembe véve megállapított kockázattal. Az akkreditáció magában foglalja a fennmaradó kockázat hivatalos megállapítását és a fennmaradó kockázatnak a felelős hatóság általi elfogadását.

Biztonság a kommunikációs és információs rendszer teljes életciklusán keresztül

8. A biztonság a kommunikációs és információs rendszer teljes életciklusa alatt követelmény, az indulástól kezdve egészen a működésből való kivonásig.

9. Az életciklus minden szakasza tekintetében meg kell állapítani a kommunikációs és információs rendszerben érintett egyes felek biztonsági szerepét és a többi résztvevővel folytatott interakcióját.

10. A kommunikációs és információs rendszereket – a technikai és nem technikai biztonsági intézkedéseket is beleértve – az akkreditációs folyamat során biztonsági tesztelésnek kell alávetni a végrehajtott biztonsági intézkedések kellő biztonsági szintjéről való meggyőződés érdekében, valamint annak ellenőrzése céljából, hogy azokat helyesen telepítették, integrálták és konfigurálták.

11. A biztonsági értékeléseket, ellenőrzéseket és felülvizsgálatokat a kommunikációs és információs rendszer működése és karbantartása során, valamint rendkívüli körülmények felmerülése esetén rendszeresen ismételni kell.

12. A kommunikációs és információs rendszer biztonsági dokumentációja az életciklusa alatt a változás- és konfigurációkezelés szerves részeként folyamatosan fejlődik.

Bevált gyakorlat

13. Az EKSZ együttműködik a Tanács Főtitkárságával, a Bizottsággal és a tagállamokkal a kommunikációs és információs rendszerben kezelt EU-minősített adatok védelmére vonatkozó bevált gyakorlat kialakítása érdekében. A bevált gyakorlatra vonatkozó iránymutatások tartalmazzák a kommunikációs és információs rendszerrel kapcsolatos, az adott fenyegetésekkel és sebezhetőségekkel szemben bizonyítottan hatékony technikai, fizikai, szervezeti és eljárási biztonsági intézkedéseket.

14. A kommunikációs és információs rendszerben kezelt EU-minősített adatok védelme az információvédelemben részt vevő – az EU-n belüli és kívüli – szervezetek által levont tanulságokra épül.

15. A bevált gyakorlat terjesztése és azt követő végrehajtása hozzájárul az EKSZ által működtetett, EU-minősített adatokat kezelő különböző kommunikációs és információs rendszerek azonos biztonsági szintjének eléréséhez.

Mélységi védelem

16. A kommunikációs és információs rendszert fenyegető veszélyek enyhítése érdekében technikai és nem technikai biztonsági intézkedéseket hajtanak végre, amelyek többszörös biztonsági réteget alkotnak. E rétegek az alábbiak:

a) *elrettentés*: a kommunikációs és információs rendszer elleni támadást tervező bármely ellenség elrettentését célzó biztonsági intézkedések;

b) *megelőzés*: a kommunikációs és információs rendszer elleni támadás megakadályozását célzó biztonsági intézkedések;

c) *észlelés*: a kommunikációs és információs rendszer elleni támadás észlelését célzó biztonsági intézkedések;

d) *ellenálló képesség*: a támadás hatásának az információk vagy kommunikációs és információs rendszerbeli eszközök minimumára való korlátozását és a további kár megelőzését célzó biztonsági intézkedések; valamint

e) *helyreállítás*: a kommunikációs és információs rendszer biztonságos helyzetének helyreállítását célzó biztonsági intézkedések.

Az ilyen biztonsági intézkedések szigorúságának és alkalmazhatóságának mértékét kockázatértékelés alapján kell meghatározni.

17. Az EKSZ illetékes hatóságai biztosítják, hogy képesek legyenek a szervezeti vagy nemzeti határokon esetlegesen átnyúló eseményekre való reagálásra, a válaszintézkedések összehangolása, valamint az ilyen incidensekről és a kapcsolódó kockázatokról való információcsere érdekében (számítógépes vészhelyzet-reagálási képesség).

A minimalitás és a legkisebb kiváltság elve

18. A szükségtelen kockázat elkerülése érdekében kizárólag a működési követelmények teljesítéséhez szükséges funkcionalitásokat, eszközöket és szolgáltatásokat kell végrehajtani.

19. A kommunikációs és információs rendszer felhasználói és az automatizált folyamatok kizárólag a feladataik elvégzéséhez szükséges hozzáférésekkel, kiváltságokkal vagy engedélyekkel rendelkezhetnek a balesetek, hibák vagy a kommunikációs és információs rendszer erőforrásainak illetéktelen felhasználásából eredő károk korlátozása érdekében.

20. A kommunikációs és információs rendszer által végrehajtott nyilvántartási eljárásokat – szükség esetén – az akkreditációs folyamat részeként ellenőrzik.

Információvédelmi tudatosság

21. A kommunikációs és információs rendszer biztonsága védelmének első vonalát a kockázatok és a rendelkezésre álló biztonsági intézkedések ismerete képezi. A kommunikációs és információs rendszer életciklusában érintett valamennyi személynek – a felhasználókat is beleértve – tudatában kell lennie különösen annak, hogy:

a) a biztonsági hiányosságok jelentősen károsíthatják a kommunikációs és információs rendszert és az egész szervezetet;

b) az összekapcsolásból és egymásra utaltságból adódóan milyen károk érhetnek másokat; valamint

c) a rendszerben és folyamatokban betöltött szerepük szerint személyesen felelősek és elszámoltathatók a kommunikációs és információs rendszer biztonságáért.

22. A biztonsággal kapcsolatos felelősség ismeretének biztosítása érdekében a személyzet valamennyi érintett tagja – köztük a felső vezetés és a kommunikációs és információs rendszer felhasználói – számára kötelező információvédelmi oktatást és tudatosságnövelő képzést kell szervezni.

Az információtechnológiai 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 határozzák meg.

24. A védelmi szintet nemzetközileg elismert vagy nemzeti szinten jóváhagyott folyamatok és módszerek alkalmazásával ellenőrzik. Ezek elsősorban az értékelést, ellenőrzést és auditot foglalják magukban.

25. Az EU-minősített adatok védelmére szolgáló kriptográfiai termékeket valamely tagállam nemzeti kriptográfiai jóváhagyó hatósága (CAA) értékeli és hagyja jóvá.

26. Az EKSZ kriptográfiai jóváhagyó hatósága általi jóváhagyásra irányuló ajánlást megelőzően, az e határozat 8. cikke (5) bekezdésének megfelelően, az ilyen kriptográfiai termékeknek sikeresen át kell esniük a berendezés tervezésében vagy gyártásában részt nem vevő tagállam megfelelő minősítéssel rendelkező hatósága (AQUA) által végzett második értékelésen. A második értékelés során a vizsgálat részletessége az érintett termékek által védendő EU-minősített adatok tervezett legmagasabb minősítési szintjétől függ.

27. Az EKSZ kriptográfiai jóváhagyó hatósága – konkrét operatív indokok alapján – a Tanács Biztonsági Bizottságának ajánlása nyomán figyelmen kívül hagyhatja a (25) és a (26) bekezdésben foglalt követelményeket, és meghatározott időtartamra ideiglenes jóváhagyást biztosíthat e határozat 8. cikkének (5) bekezdésével összhangban.

28. A megfelelő minősítéssel rendelkező hatóság valamely tagállam kriptográfiai jóváhagyó hatósága, amely a Tanács által meghatározott szempontok alapján akkreditációt szerzett az EU-minősített adatok védelmére szolgáló kriptográfiai termékek második értékelésének elvégzésére.

29. A főképviselő jóváhagyja a nem kriptográfiai információtechnológiai biztonsági termékek minősítésére és jóváhagyására vonatkozó biztonsági politikát.

Adattovábbítás biztonságos területeken belül

30. E határozat rendelkezései ellenére, amennyiben az EU-minősített adatok továbbítása biztonságos területekre vagy adminisztratív területekre korlátozódik, titkosítás nélküli továbbítás vagy alacsonyabb szintű titkosítás alkalmazható a kockázatkezelési folyamat eredményére alapozva és a biztonsági akkreditációs hatóság jóváhagyásával.

A kommunikációs és információs rendszerek biztonságos összekapcsolása

31. 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.

32. A kommunikációs és információs rendszer valamennyi vele összekapcsolt információtechnológiai rendszert nem megbízhatóként kezel, és a minősített adatok cseréjének ellenőrzése céljából védelmi intézkedéseket hajt végre.

33. A kommunikációs és információs rendszer más információtechnológiai rendszerrel való bármely összekapcsolása esetében 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 kommunikációs és információs rendszer körzethatárán határvédelmi szolgáltatásokat (BPS) kell végrehajtani.

34. Akkreditált kommunikációs és információs rendszer nem kapcsolható össze nem védett vagy nyilvános hálózattal, kivéve, ha a kommunikációs és információs rendszer jóváhagyott, a közte és a nyilvános hálózat között e célból telepített határvédelmi szolgáltatással rendelkezik. Az ilyen összekapcsolásra vonatkozó biztonsági intézkedéseket az illetékes információvédelmi hatóság felülvizsgálja, és az illetékes biztonsági akkreditációs hatóság jóváhagyja.

Amennyiben a nem védett vagy nyilvános hálózatot kizárólag adatközvetítésre használják, és az adatokat az e határozat 8. cikke (5) bekezdésének megfelelően jóváhagyott kriptográfiai termékkel titkosították, az ilyen kapcsolat nem tekintendő összekapcsolásnak.

35. Tilos a TRES SECRET UE/EU TOP SECRET minősítésű adatok kezelésére akkreditált kommunikációs és információs rendszer közvetlen vagy lépcsőzetes összekapcsolása nem védett vagy nyilvános hálózattal.

Számítógépes adathordozók

36. A számítógépes adathordozókat az EKSZ biztonsági hatósága által jóváhagyott eljárásokkal összhangban kell megsemmisíteni.

37. A számítógépes adathordozókat az e határozat 8. cikkének (2) bekezdése szerint kidolgozandó biztonsági iránymutatásokkal összhangban kell újrafelhasználni, visszaminősíteni vagy minősítését feloldani.

Veszélyhelyzet

38. Az e határozatban foglalt rendelkezések ellenére veszélyhelyzetben – például fenyegető vagy ténylegesen fennálló válság-, konfliktus- vagy háborús helyzetben – vagy rendkívüli üzemeltetési körülmények között korlátozott ideig az alábbiakban leírt különös eljárások alkalmazhatók.

39. EU-minősített adatok az illetékes hatóság beleegyezésével továbbíthatók alacsonyabb minősítési szintre jóváhagyott kriptográfiai termékek felhasználásával vagy titkosítás nélkül, amennyiben a késedelem által okozott kár egyértelműen meghaladná a minősített adatok hozzáférhetővé tétele által okozott kárt, és ha:

a) a küldő, illetve az átvevő nem rendelkezik az előírt titkosítási eszközzel vagy egyáltalán nem rendelkezik titkosítási eszközzel; valamint

b) a minősített anyag más eszközökkel nem továbbítható időben.

40. A (39) bekezdésben meghatározott körülmények között továbbított minősített adat nem látható el olyan jelöléssel vagy jelzéssel, amely azt a nem minősített adatoktól vagy elérhető kriptográfiai eszköz által védhető adattól megkülönbözteti. A címzetteket késedelem nélkül, egyéb módon értesíteni kell a minősítési szintről.

41. Amennyiben a (39) bekezdésben említett eljárás alkalmazására kerül sor, ezt követően jelentést kell tenni az EKSZ Biztonsági Igazgatóságának és így az EKSZ Biztonsági Bizottságának is. A jelentés minden egyes EU-minősített adatra vonatkozóan megjelöli legalább a küldőt, a címzettet és a kibocsátót.

III. INFORMÁCIÓVÉDELMI FELADATKÖRÖK ÉS HATÓSÁGOK

42. Az EKSZ-nél a következő információvédelmi feladatköröket hozzák létre. E feladatkörök nem igényelnek külön szervezeti egységeket. Külön megbízatással kell rendelkezniük. Mindazonáltal, e feladatkörök és a hozzájuk tartozó felelősségi körök ugyanazon szervezeti egységen belül kombinálhatók vagy integrálhatók, vagy különböző szervezeti egységek között megoszthatók, feltéve, hogy ez nem vezet belső összeférhetetlenséghez vagy a feladatok ütközéséhez.

Információvédelmi hatóság (IAA)

43. Az információvédelmi hatóság felelős az alábbiakért:

a) információvédelmi biztonsági iránymutatások kidolgozása, és azok hatékonyságának és relevanciájának 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 iránymutatásoknak;

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

e) az információvédelemmel kapcsolatos képzés és tudatosságnövelés koordinálása;

f) konzultáció a rendszerszolgáltatóval, a biztonsági szereplőkkel és a felhasználók képviselőivel az információvédelmi biztonsági iránymutatások tekintetében; valamint

g) megfelelő szakértelem rendelkezésre állásának biztosítása az EKSZ Biztonsági Bizottságának információvédelmi kérdésekkel foglalkozó szakértői alcsoportjában.

TEMPEST-hatóság

44. A TEMPEST-hatóság felelős azért, hogy a kommunikációs és információs rendszerek megfeleljenek a TEMPEST-politikáknak és -iránymutatásoknak. Jóváhagyja a TEMPEST-ellenintézkedéseket azokra a berendezésekre és termékekre vonatkozóan, amelyek működési környezetükben meghatározott minősítési szintig biztosítják az EU-minősített adatok védelmét.

Kriptográfiai jóváhagyó hatóság (CAA)

45. A kriptográfiai jóváhagyó hatóság felel annak biztosításáért, hogy a kriptográfiai termékek megfeleljenek a vonatkozó kriptográfiai iránymutatásoknak. Jóváhagyja a kriptográfiai termékeket, amelyek működési környezetükben meghatározott minősítési szintig biztosítják az EU-minősített adatok védelmét.

Kriptográfiai terjesztési hatóság (CDA)

46. A kriptográfiai terjesztési hatóság a következőkért felelős:

a) az uniós kriptográfiai anyagok igazgatása és könyvelése;

b) annak biztosítása, hogy valamennyi uniós kriptográfiai anyag könyvelése, biztonságos kezelése, tárolása és terjesztése tekintetében megfelelő eljárásokat alkalmazzanak és megfelelő csatornákat hozzanak létre; valamint

c) az uniós kriptográfiai anyagok továbbításának biztosítása az azokat felhasználó egyénektől vagy szolgálatoktól, vagy azok felé.

Biztonsági akkreditációs hatóság (SAA)

47. Az egyes rendszerek biztonsági akkreditációs hatósága a következőkért felelős:

a) annak biztosítása, hogy a kommunikációs és információs rendszer megfeleljen a vonatkozó biztonsági iránymutatásoknak, jóváhagyási tanúsítvány kiadása arról, hogy a kommunikációs és információs rendszer 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 iránymutatásokkal összhangban, egyértelműen megállapítva a felelőssége alá tartozó kommunikációs és információs rendszerre vonatkozó jóváhagyási feltételeket;

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 kockázatkezelésre és a fennmaradó kockázatra vonatkozó dokumentumok, a rendszerspecifikus biztonsági követelményeket megállapító dokumentum (a továbbiakban: SSRS), a biztonsági végrehajtás ellenőrzési dokumentációja és a biztonsági üzemeltetési eljárások (a továbbiakban: SecOP) – megvizsgálása és jóváhagyása, valamint annak biztosítása, hogy az összhangban álljon az EKSZ biztonsági szabályaival és iránymutatásaival;

e) a kommunikációs és információs rendszerrel kapcsolatos biztonsági intézkedések végrehajtásának ellenőrzése biztonsági értékelések, ellenőrzések vagy felülvizsgálatok végrehajtása vagy támogatása révén;

f) biztonsági követelmények meghatározása (pl. személyi biztonsági tanúsítványok szintjei) a kommunikációs és információs rendszer szempontjából érzékeny beosztások tekintetében;

g) a kommunikációs és információs rendszer biztonságát szolgáló engedélyezett kriptográfiai és TEMPEST-termékek kiválasztásának jóváhagyása;

h) kommunikációs és információs rendszer másik kommunikációs és információs rendszerrel való összekapcsolásának jóváhagyása, vagy adott esetben a közös jóváhagyási eljárásban való részvétel; valamint

i) konzultáció a rendszerszolgáltatóval, a biztonsági szereplőkkel és a felhasználók képviselőivel a biztonsági kockázatkezelésről – különös tekintettel a fennmaradó kockázatra –, valamint a jóváhagyási tanúsítvány kiadási feltételeiről.

48. Az EKSZ biztonsági akkreditációs hatósága felel az EKSZ hatáskörében működő valamennyi kommunikációs és információs rendszer akkreditálásáért.

Biztonsági akkreditációs bizottság (SAB)

49. Közös biztonsági akkreditációs bizottság (SAB) felel a mind az EKSZ, mind a tagállamok biztonsági akkreditációs hatóságainak hatáskörébe tartozó kommunikációs és információs rendszerek akkreditálásáért. A biztonsági akkreditációs bizottság az egyes tagállamok biztonsági akkreditációs hatóságainak képviselőiből áll, és ülésein részt vesz a Főtitkárság és a Bizottság biztonsági akkreditációs hatóságának egy képviselője. A kommunikációs és információs rendszerekhez kapcsolódó egyéb szervezetek meghívást kapnak az adott rendszerrel foglalkozó ülésekre.

A biztonsági akkreditációs bizottság elnöke az EKSZ biztonsági akkreditációs hatóságának a képviselője. A biztonsági akkreditációs bizottság a kommunikációs és információs rendszerhez kapcsolódó intézmények, tagállamok és más szervezetek biztonsági akkreditációs hatóságai képviselőinek konszenzusos döntése alapján jár el. Rendszeres időközönként jelentést tesz tevékenységeiről az EKSZ Biztonsági Bizottságának, és azt valamennyi akkreditációs tanúsítványról értesíti.

Információvédelmi üzemeltetési hatóság

50. Az egyes rendszerek információvédelmi üzemeltetési hatósága felelős az alábbiakért:

a) biztonsági dokumentáció kidolgozása a biztonsági iránymutatásokkal – különösen a rendszerspecifikus biztonsági követelményeket megállapító dokumentummal (**SSRS**) – összhangban, ideértve a fennmaradó kockázat megállapítását, a biztonsági üzemeltetési eljárásokat (**SecOP**) és a kriptográfiai tervet, a kommunikációs és információs rendszer akkreditációs folyamatának keretében;

b) részvétel a rendszerspecifikus technikai biztonsági intézkedések, eszközök és szoftverek kiválasztásában és tesztelésében, a végrehajtásuk felügyelete és annak biztosítása érdekében, 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 értelmében 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 felelősség átruházása a rendszertulajdonosra;

e) a kriptográfiai termékek igazgatása és kezelése, biztosítva a kriptográfiai és ellenőrzött elemek felügyeletét, és – adott esetben – biztosítva a kriptográfiai változók generálását;

f) biztonsági elemzések felülvizsgálata és tesztelése, különösen a vonatkozó kockázati jelentések előkészítése céljából, a biztonsági akkreditációs hatóság előírásai szerinti;

g) adott kommunikációs és információs rendszerre vonatkozó specifikus információvédelmi képzés nyújtása;

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

A.V. MELLÉKLET

IPARBIZTONSÁG

I. BEVEZETÉS

1. Ez a melléklet meghatározza az A. melléklet 9. cikkének végrehajtására vonatkozó rendelkezéseket. Meghatározza az EKSZ által odaítélt minősített szerződések megkötését megelőző tárgyalások és a szerződések teljes életciklusa során a gazdálkodó vagy más szervezetekre alkalmazandó általános biztonsági rendelkezéseket.

2. Az EKSZ biztonsági hatósága jóváhagyja az iparbiztonságra vonatkozó iránymutatásokat, amelyek felvázolják különösen a telephelybiztonsági tanúsítványokra, a biztonsági vonatkozások záradékára, a látogatásokra, valamint az EU-minősített adatok továbbítására és szállítására vonatkozó részletes követelményeket.

II. A MINŐSÍTETT SZERZŐDÉSEKBEN TALÁLHATÓ BIZTONSÁGI ELEMEK

Minősítési útmutató (SCG)

3. A pályázati felhívás kiírását vagy a minősített szerződés odaítélését megelőzően az EKSZ szerződő hatóságként meghatározza a pályázók és vállalkozók részére nyújtandó bármely adat biztonsági minősítését, valamint a vállalkozó által létrehozandó bármely adat biztonsági minősítését. E célból az EKSZ 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 az EKSZ-nek figyelembe kell vennie az összes vonatkozó biztonsági szempontot, köztük a megosztott adatra vonatkozó és az adat kibocsátója által a szerződéshez való használat céljából jóváhagyott biztonsági minősítést;

   b) a szerződés minősítésének általános szintje nem lehet alacsonyabb bármely elemének legmagasabb minősítési szintjénél; valamint

   c) adott esetben az EKSZ 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 számukra nyújtott adat minősítését érintő bármilyen változás esetén, valamint az SCG bármilyen további változása esetén.

Biztonsági vonatkozások záradéka (SAL)

5. A szerződésspecifikus biztonsági követelményeket a SAL-ban rögzítik. Adott esetben a SAL tartalmazza az SCG-t, és a minősített vállalkozói vagy alvállalkozói szerződés szerves részét képezi.

6. A SAL tartalmazza a vállalkozók és/vagy alvállalkozók részére az e határozatban foglalt minimumszabályok teljesítését előíró rendelkezéseket. A minimumszabályok be nem tartása elegendő indokot jelenthet a szerződés felbontására.

Program-/projektbiztonsági utasítások (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 kidolgozhatja az adott programra/projektre vonatkozó biztonsági utasításokat (PSI). 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 további biztonsági követelményeket tartalmazhat.

III. TELEPHELYBIZTONSÁGI TANÚSÍTVÁNY (FSC)

8. Az EKSZ Biztonsági Igazgatóságának kérésére az érintett tagállam nemzeti biztonsági hatósága/kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatósága FSC-t bocsát ki annak jelzésére, hogy – a nemzeti jogszabályokkal és rendelkezésekkel összhangban – egy gazdálkodó vagy más szervezet képes az EU-minősített adatok megfelelő minősítési szinten (CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET) való védelmére a létesítményein belül. Az FSC EKSZ-nek történő bemutatásáig a vállalkozó, alvállalkozó vagy potenciális vállalkozó vagy alvállalkozó számára nem biztosítják vagy engedélyezik az EU-minősített adatokhoz való hozzáférést.

9. Adott esetben az EKSZ szerződő hatóságként értesíti a megfelelő nemzeti biztonsági hatóságot/kijelölt biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot arról, 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.

10. Az EKSZ szerződő hatóságként nem köthet minősített szerződést a megfelelőnek tartott pályázóval azt megelőzően, hogy szükség esetén kézhez kapná az érintett vállalkozó vagy alvállalkozó bejegyzésének helye szerinti tagállam nemzeti biztonsági hatósága/kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatósága által kiállított megerősítést a megfelelő FSC kibocsátásáról.

11. Az EKSZ szerződő hatóságként felkéri az FSC-t kibocsátó nemzeti biztonsági hatóságot/kijelölt biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot, hogy értesítse az EKSZ-t az FSC-t érintő bármely kedvezőtlen információról. Alvállalkozói szerződés esetén a nemzeti biztonsági hatóságot/kijelölt biztonsági hatóságot, illetve bármely egyéb illetékes biztonsági hatóságot ennek megfelelően tájékoztatni kell.

12. Az FSC-nek az adott nemzeti biztonsági hatóság/kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság általi visszavonása elegendő indokot szolgáltat az EKSZ-nek mint szerződő hatóságnak a minősített szerződés felbontására vagy a pályázó versenyből való kizárására.

IV. A VÁLLALKOZÓK SZEMÉLYZETÉNEK SZEMÉLYI BIZTONSÁGI TANÚSÍTVÁNYA (PSC)

13. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű EU-minősített adatokhoz való hozzáférést igénylő munkát végző, vállalkozók alkalmazásában álló személyzet valamennyi tagja esetében megfelelő biztonsági ellenőrzést kell végezni, és teljesülnie kell a „szükséges ismeret” feltételének. Bár a PSC megléte nem előfeltétele a RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatokhoz való hozzáférésnek, az ilyen hozzáféréshez is teljesülnie kell a „szükséges ismeret” feltételének.

14. A vállalkozók személyzetére vonatkozó PSC-kérelmeket a szervezetért felelős nemzeti biztonsági hatósághoz/kijelölt biztonsági hatósághoz kell benyújtani.

15. Az EKSZ hangsúlyozza azon vállalkozóknak, akik harmadik állambeli állampolgárt kívánnak foglalkoztatni egy EU-minősített adatokhoz való hozzáférést megkövetelő beosztásban, hogy az érintett személyt alkalmazó szervezet helye szerinti tagállam nemzeti biztonsági hatósága/kijelölt biztonsági hatósága felelős annak megállapításáért, hogy e határozat szerint az érintett személynek megadható-e az ilyen adatokhoz való hozzáférés, valamint annak megerősítéséért, hogy a kibocsátónak hozzájárulását kellett adnia az ilyen hozzáférés engedélyezése előtt.

V. MINŐSÍTETT VÁLLALKOZÓI ÉS ALVÁLLALKOZÓI SZERZŐDÉSEK

16. Amikor egy pályázó részére a szerződést megelőző szakaszban EU-minősített adatot adnak át, a pályázati felhívásnak tartalmaznia kell egy olyan kitételt, miszerint az a pályázó, aki végül nem nyújtja be pályázatát, vagy akit nem választanak ki, köteles adott időn belül valamennyi minősített dokumentumot visszaszolgáltatni.

17. Amint sor kerül egy minősített vállalkozói vagy alvállalkozói szerződés odaítélésére, az EKSZ szerződő hatóságként értesíti a vállalkozó vagy alvállalkozó nemzeti biztonsági hatóságát/kijelölt biztonsági hatóságát vagy bármely más illetékes biztonsági hatóságát a minősített szerződésre vonatkozó biztonsági rendelkezésekről.

18. Amennyiben egy ilyen szerződést felmondanak vagy az lejár, az EKSZ szerződő hatóságként (és/vagy a nemzeti biztonsági hatóság/kijelölt biztonsági hatóság vagy adott esetben bármely más illetékes biztonsági hatóság, alvállalkozói szerződés esetén) késedelem nélkül értesíti azon tagállam nemzeti biztonsági hatóságát/kijelölt biztonsági hatóságát vagy bármely más illetékes biztonsági hatóságát, amelyben a vállalkozót vagy alvállalkozót bejegyezték.

19. Általános szabály, hogy a vállalkozó vagy alvállalkozó a minősített vállalkozói vagy alvállalkozói szerződés felmondását vagy lejártát követően köteles valamennyi EU-minősített adatot visszaszolgáltatni a szerződő hatóságnak.

20. Az EU-minősített adatoknak a szerződés teljesítése során vagy a szerződés felmondásával vagy lejártával történő megsemmisítésére vonatkozó egyedi rendelkezéseket a SAL-ban kell lefektetni.

21. Amennyiben a vállalkozó vagy alvállalkozó engedélyt kap az EU-minősített adatok megtartására a szerződés felmondását vagy lejártát követően, a vállalkozónak vagy alvállalkozónak továbbra is eleget kell tennie az e határozatban foglalt minimumszabályoknak, és védenie kell az EU-minősített adatok bizalmasságát.

22. A pályázati felhívás és a szerződés határozza meg azon feltételeket, amelyek szerint a vállalkozó alvállalkozói szerződést köthet.

23. Mielőtt a vállalkozó a minősített szerződés bármely részére alvállalkozót szerződtetne, ehhez engedélyt kér az EKSZ-től mint szerződő hatóságtól. Nem köthető alvállalkozói szerződés az olyan harmadik országokban bejegyzett ipari vagy más szervezettel, amely nem kötött adatbiztonsági megállapodást az EU-val.

24. A vállalkozó felel annak biztosításáért, hogy minden alvállalkozói tevékenység az e határozatban foglalt minimumszabályokkal összhangban valósuljon meg, és az alvállalkozó részére nem ad át EU-minősített adatot a szerződő hatóság előzetes írásbeli engedélye nélkül.

25. A vállalkozó vagy az alvállalkozó által létrehozott vagy kezelt EU-minősített adatok tekintetében a kibocsátót megillető jogokat a szerződő hatóság gyakorolja.

VI. MINŐSÍTETT SZERZŐDÉSEKKEL KAPCSOLATOS LÁTOGATÁSOK

26. Amennyiben az EKSZ-nek, a vállalkozóknak vagy az alvállalkozóknak egy minősített szerződés teljesítéséhez CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adathoz kell hozzáférniük egymás létesítményeiben, a látogatásokat a nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságok vagy bármely más érintett illetékes biztonsági hatóság bevonásával kell megszervezni. Ez nem érinti a nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságoknak azon jogát, hogy egyes konkrét projektekre vonatkozóan megállapodjanak az ilyen látogatások közvetlen megszervezését lehetővé tevő eljárásról.

27. Minden látogatónak megfelelő PSC-vel kell rendelkeznie, és teljesítenie kell a „szükséges ismeret” feltételét az EKSZ szerződésével kapcsolatos EU-minősített adatokhoz való hozzáférés tekintetében.

28. A látogatók csak a látogatás céljához kapcsolódó EU-minősített adatokhoz kapnak hozzáférést.

VII. EU-MINŐSÍTETT ADATOK TOVÁBBÍTÁSA ÉS SZÁLLÍTÁSA

29. Az EU-minősített adatok elektronikus úton történő továbbítása tekintetében az A. melléklet 8. cikkében és az A.IV. mellékletben foglalt vonatkozó rendelkezéseket kell alkalmazni.

30. Az EU-minősített adatok szállítására az A.III. melléklet vonatkozó rendelkezéseit kell alkalmazni, a nemzeti jogszabályokkal és rendelkezésekkel összhangban.

31. A minősített anyagok szállítmányként való szállítására vonatkozó biztonsági előírások meghatározása során az alábbi elveket kell alkalmazni:

    a) a szállítás valamennyi szakasza alatt garantálni kell a biztonságot, a kiindulási helytől a rendeltetési helyig;

    b) az adott szállítmányra megállapított védelmi szintet az abban foglalt anyag legmagasabb minősítési szintje határozza meg;

    c) a szállítást végző vállalatoknak megfelelő szintű FSC-vel kell rendelkezniük, amennyiben a vállalkozó létesítményeiben tárolnak minősített adatokat. A szállítmányt kezelő személyzetnek minden esetben megfelelő biztonsági ellenőrzésen kell átesnie az A.I. melléklettel összhangban;

d) a CONFIDENTIEL UE/EU CONFIDENTIEL vagy SECRET UE/EU SECRET minősítésű anyag határokon keresztüli bármilyen szállítását megelőzően a feladó szállítási tervet készít, amelyet az EKSZ – adott esetben mind a feladó, mind a címzett államának nemzeti biztonsági hatóságaival/kijelölt biztonsági hatóságaival vagy bármely más érintett illetékes biztonsági hatósággal egyeztetve – jóváhagy;

e) lehetőség szerint közvetlen útvonalakat kell használni, és a szállítást a körülményekhez képest a lehető leggyorsabban kell végrehajtani;

f) lehetőség szerint kizárólag a tagállamokat érintő útvonalakat kell használni. Az uniós tagállamoktól eltérő államokon keresztül vezető útvonalak kizárólag az EKSZ vagy mind a feladó, mind a címzett államának bármely más illetékes biztonsági hatósága által kiadott engedély birtokában alkalmazhatók.

VIII. EU-MINŐSÍTETT ADATOK ÁTADÁSA HARMADIK ÁLLAMOKBAN MŰKÖDŐ VÁLLALKOZÓKNAK

32. Az EU-minősített adatok olyan harmadik államokban működő vállalkozók vagy alvállalkozók részére való átadása, amelyeknek érvényes biztonsági megállapodása van az EU-val, az EKSZ mint szerződő hatóság és a vállalkozó bejegyzési helye szerinti harmadik állam nemzeti biztonsági hatósága/kijelölt biztonsági hatósága által elfogadott biztonsági intézkedésekkel összhangban történik.

IX. A RESTREINT UE/EU RESTRICTED MINŐSÍTÉSŰ ADATOK KEZELÉSE ÉS TÁROLÁSA

33. Az EKSZ mint szerződő hatóság adott esetben a tagállam nemzeti biztonsági hatóságával/kijelölt biztonsági hatóságával egyeztetve a szerződésben foglalt rendelkezések alapján látogatásokat tehet a vállalkozók/alvállalkozók létesítményeibe annak ellenőrzése céljából, hogy meghozták-e a RESTREINT UE/EU RESTRICTED minősítési szintű adatok védelméhez szükséges, szerződésben előírt biztonsági intézkedéseket.

34. A nemzeti jogszabályok és rendelkezések szerint szükséges mértékben az EKSZ-nek mint szerződő hatóságnak értesítenie kell a nemzeti biztonsági hatóságokat/kijelölt biztonsági hatóságokat vagy bármely más illetékes biztonsági hatóságot a RESTREINT UE/EU RESTRICTED minősítésű adatot tartalmazó szerződésekről és alvállalkozói szerződésekről.

35. A RESTREINT UE/EU RESTRICTED minősítésű adatot magukban foglaló, az EKSZ által odaítélt szerződések esetében az FSC, illetve PSC nem kötelező a vállalkozók, alvállalkozók és személyzetük számára.

36. Az EKSZ mint szerződő hatóság megvizsgálja az olyan 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.

37. Azon feltételeknek, amelyek alapján a vállalkozó alvállalkozót szerződtethet, összhangban kell állniuk a (22)–(24) bekezdéssel.

38. Amennyiben egy adott szerződés RESTREINT UE/EU RESTRICTED minősítésű adatoknak a vállalkozó által működtetett kommunikációs és információs rendszerben való kezelésére is kiterjed, az EKSZ mint szerződő hatóság biztosítja, hogy a szerződésben vagy alvállalkozói szerződésben szerepeljenek a kommunikációs és információs rendszer akkreditálásához szükséges, az összes releváns tényező alapján megállapított kockázattal arányos technikai és adminisztratív követelmények. Az ilyen kommunikációs és információs rendszer akkreditációjának hatályáról a szerződő hatóság és az érintett nemzeti biztonsági hatóság/kijelölt biztonsági hatóság állapodik meg.

A.VI. MELLÉKLET

MINŐSÍTETT ADATOK CSERÉJE HARMADIK ÁLLAMOKKAL ÉS NEMZETKÖZI SZERVEZETEKKEL

I. BEVEZETÉS

1. Ez a melléklet meghatározza az A. melléklet 10. cikkének végrehajtására vonatkozó rendelkezéseket.

II. A MINŐSÍTETT ADATOK CSERÉJÉT SZABÁLYOZÓ KERETEK

2. Az EKSZ EU-minősített adatokat cserélhet harmadik államokkal vagy nemzetközi szervezetekkel az A. melléklet 10. cikkének (1) bekezdésének értelmében.

Az EUMSZ 218. cikkében előírt feladatok ellátása terén a főképviselő támogatása érdekében:

a) az EKSZ érintett földrajzi vagy tematikus szervezeti egysége az EKSZ Biztonsági Igazgatóságával konzultálva adott esetben megállapítja a minősített adatok harmadik államokkal vagy nemzetközi szervezetekkel való cseréjének hosszú távú szükségességét;

b) az EKSZ Biztonsági Igazgatósága az EKSZ érintett földrajzi szervezeti egységével konzultálva adott esetben a főképviselő elé terjeszti a Tanács számára benyújtandó javaslatok szövegének tervezetét az EUMSZ 218. cikkének (3), (5) és (6) bekezdésével összhangban;

c) az EKSZ Biztonsági Igazgatósága támogatja a főképviselőt a tárgyalások folyamán, egyeztetve a Bizottság és a Tanács Főtitkársága érintett szolgálataival;

d) a harmadik államokkal a válságkezelési KBVP-műveletekben való részvételükre vonatkozóan kötött egyezmények és megállapodások összefüggésében, az A. melléklet 10. cikke (1) bekezdésének c) pontjában említettek szerint, az EKSZ Válságkezelési és Tervezési Igazgatósága az EKSZ érintett szolgálataival konzultálva adott esetben a főképviselő elé terjeszti a Tanács számára benyújtandó javaslatok szövegének tervezetét az EUMSZ 218. cikkének (3), (5) és (6) bekezdésével összhangban, és támogatja a főképviselőt a tárgyalások folyamán, egyeztetve a Bizottság és a Tanács Főtitkársága érintett szolgálataival.

3. Amennyiben az adatbiztonsági megállapodások rendelkeznek technikai végrehajtási szabályokról is, amelyeket az EKSZ Biztonsági Igazgatósága – a Bizottság Humánerőforrásügyi és Biztonsági Főigazgatóságának Biztonsági Igazgatóságával, valamint a Tanács Főtitkárságának Biztonsági Hivatalával egyeztetve – és a szóban forgó harmadik állam vagy nemzetközi szervezet illetékes biztonsági hatósága közösen alakít ki, az ilyen megállapodások figyelembe veszik az érintett harmadik állam vagy nemzetközi szervezet hatályos biztonsági szabályai, struktúrái és eljárásai által biztosított védelmi szintet.

4. Amennyiben az EKSZ esetében harmadik állammal vagy nemzetközi szervezettel elvileg legfeljebb RESTREINT UE/EU RESTRICTED minősítésű adatok hosszú távú cseréjére van szükség, és amennyiben megállapítást nyert, hogy az érintett fél nem rendelkezik kellőképpen fejlett biztonsági rendszerrel az adatbiztonsági megállapodás megkötéséhez, a főképviselő – miután megkapta az EKSZ Biztonsági Bizottságának egyhangúlag kedvező véleményét e határozat 15. cikkének (5) bekezdésével összhangban – igazgatási megállapodást köthet a szóban forgó harmadik állam vagy nemzetközi szervezet illetékes biztonsági hatóságaival.

5. Az EU-minősített adatok elektronikus eszközökkel történő cseréje harmadik állammal vagy nemzetközi szervezettel nem megengedett, kivéve ha az adatbiztonsági megállapodás vagy igazgatási megállapodás erről kifejezetten rendelkezik.

6. A minősített adatok cseréjéről szóló igazgatási megállapodás értelmében mind az EKSZ, mind a harmadik állam vagy nemzetközi szervezet kijelöli a minősített adatok cseréjének fő beérkezési és kiküldési pontjaként működő nyilvántartást. Az EKSZ esetében ezt a szerepet az EKSZ központi nyilvántartása tölti be.

7. Az igazgatási megállapodás megkötésére főszabályként levélváltás formájában kerül sor.

III. ÉRTÉKELŐ LÁTOGATÁSOK

8. Az e határozat 17. cikkében említett értékelő látogatásokra az érintett harmadik állammal vagy nemzetközi szervezettel való kölcsönös megállapodás alapján kerül sor, és a látogatások során az alábbiakat értékelik:

   a) a minősített adatok védelmére alkalmazandó szabályozási keret;

   b) a harmadik állam vagy nemzetközi szervezet biztonsági jogszabályainak, előírásainak, politikájának vagy eljárásainak bármely sajátos jellemzője, amely befolyásolhatja a kicserélhető minősített adatok legmagasabb szintjét;

   c) a minősített adatok védelmére vonatkozó hatályos biztonsági intézkedések és eljárások; valamint

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

9. Nem kerülhet sor EU-minősített adatok cseréjére értékelő látogatás előtt, valamint azt megelőzően, hogy a felek meghatározzák a kicserélhető minősített adatok szintjét, az ilyen adatok számára biztosítandó védelem szintjének egyenértékűsége alapján.

   Amennyiben az értékelő látogatást megelőzően a minősített adatok cseréjét indokoló kivételes vagy sürgős ok jut a főképviselő tudomására, az EKSZ a következők szerint jár el:

   a) először a kibocsátó írásbeli beleegyezését kéri arról, hogy nem emel kifogást az átadással kapcsolatban;

   b) az EKSZ biztonsági hatóságához fordul, amely az EKSZ Biztonsági Bizottságában képviselt tagállamok egyhangúlag kedvező véleményének kézhezvételét követően dönthet az átadásról.

   Ha az EKSZ nem tudja azonosítani a kibocsátót, a kibocsátó felelősségét az EKSZ biztonsági hatósága vállalja magára, miután megkapta az EKSZ Biztonsági Bizottságában képviselt tagállamok egyhangúlag kedvező véleményét.

IV. EU-MINŐSÍTETT ADATOK HARMADIK ÁLLAMOK VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE VALÓ ÁTADÁSÁNAK ENGEDÉLYEZÉSE

10. Amennyiben létezik a minősített adatok harmadik államokkal vagy nemzetközi szervezetekkel való cseréjének az A. melléklet 10. cikkének (1) bekezdése szerinti kerete, az EU-minősített adatoknak az érintett harmadik állam vagy nemzetközi szervezet részére történő átadásáról az EKSZ biztonsági hatósága határoz, amely ezt a feladatot átruházhatja az EKSZ valamely vezető tisztviselőjére vagy a felügyelete alatt álló más személyre.

11. Ha az átadni kért minősített adatok – köztük adott esetben az azokban foglalt forrásanyagok – kibocsátója nem az EKSZ, akkor az EKSZ először a kibocsátó írásbeli beleegyezését kéri, hogy az nem emel kifogást az átadással kapcsolatban. Ha az EKSZ nem tudja azonosítani a kibocsátót, a kibocsátó felelősségét az EKSZ biztonsági hatósága vállalja magára, miután megkapta az EKSZ Biztonsági Bizottságában képviselt tagállamok egyhangúlag kedvező véleményét.

V. EU-MINŐSÍTETT ADATOK RENDKÍVÜLI AD HOC ÁTADÁSA

12. Az A. melléklet 10. cikkének (1) bekezdésében említett keretek egyikének hiányában, és amennyiben az Európai Unió, illetve egy vagy több tagállam érdekei politikai, operatív vagy sürgősségi okokból megkövetelik az EU-minősített adatok átadását, az EU-minősített adatok kivételesen átadhatók harmadik államnak vagy nemzetközi szervezetnek, miután meghozták a következő intézkedéseket.

   Az EKSZ Biztonsági Igazgatósága a fenti (11) bekezdésben említett feltételek teljesülésének biztosítását követően:

   a) a lehetséges mértékben ellenőrzi az adott harmadik állam vagy nemzetközi szervezet biztonsági hatóságaival együttműködve, hogy az adott harmadik állam vagy nemzetközi szervezet biztonsági szabályai, struktúrái és eljárásai garantálni tudják-e, hogy a részére átadott EU-minősített adatok az e határozatban foglaltaknál nem kevésbé szigorú szabályoknak megfelelő védelemben részesüljenek;

b) felkéri az EKSZ Biztonsági Bizottságát, hogy a rendelkezésre álló információk alapján alakítsa ki véleményét az EU-minősített adatokat átvevő harmadik állam vagy nemzetközi szervezet biztonsági szabályainak, struktúráinak és eljárásainak megbízhatóságáról;

c) az EKSZ biztonsági hatóságához fordul, amely az EKSZ Biztonsági Bizottságában képviselt tagállamok egyhangúlag kedvező véleményének kézhezvételét követően dönthet az átadásról.

13. Az A. melléklet 10. cikkének (1) bekezdésében említett keretek egyikének hiányában a szóban forgó harmadik fél írásban vállalja az EU-minősített adatok megfelelő védelmének biztosítását.

A. függelék

Fogalommeghatározások

E határozat alkalmazásában:

„akkreditáció”: a biztonsági akkreditációs hatóság (SAA) arra vonatkozó hivatalos nyilatkozatának kiadásával záruló eljárás, hogy a rendszer alkalmas arra, hogy működési környezetében meghatározott minősítési szinten, konkrét biztonsági üzemmódban és elfogadható kockázati szinten működjön, feltételezve a jóváhagyott műszaki, fizikai, szervezeti és eljárási biztonsági intézkedések alkalmazását;

„eszköz”: valamely szervezet, a szervezet szokásos tevékenységei és azok folytonossága szempontjából értéket képviselő valamennyi elem, beleértve a szervezet misszióját támogató információforrásokat is;

„EU-minősített adatokhoz való hozzáférésre vonatkozó engedély”: a valamely tagállam illetékes hatóságai által elvégzett biztonsági ellenőrzést követően, e határozatnak megfelelően az EKSZ biztonsági hatósága által adott engedély, amely tanúsítja, hogy egy adott személy részére – amennyiben esetében a szükséges ismeret feltétele teljesül – meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig és meghatározott időpontig hozzáférés biztosítható EU-minősített adatokhoz – lásd az A.I. melléklet 2. cikkét;

„biztonsági szabályok megsértése”: az e határozatban foglalt biztonsági szabályokkal és/vagy a határozat végrehajtásához szükséges intézkedéseket megállapító biztonsági politikákkal vagy iránymutatásokkal ellentétes egyéni cselekmény vagy mulasztás;

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

„minősített szerződés”: az EKSZ 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”: az EKSZ-szel szerződéses viszonyban álló vállalkozó által egy másik vállalkozóval (azaz alvállalkozóval) árubeszerzés, 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”: az elektronikus formában történő információkezelést lehetővé tevő bármely rendszer. A kommunikációs és információs rendszer magában foglalja a működéséhez szükséges valamennyi eszközt, beleértve az infrastruktúrát, a szervezetet, a személyzetet és az információforrásokat; – lásd az A. melléklet 8. cikkének (2) bekezdését;

„EU-minősített adatok illetéktelenek tudomására jutása”: az EU-minősített adatok teljes vagy részleges felfedése illetéktelen személyek vagy szervezetek számára – lásd a 9. cikk (2) bekezdését;

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

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

„KBVP-művelet”: az EUSZ V. címének 2. fejezete szerinti katonai vagy polgári válságkezelési művelet;

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

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

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

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

„visszaminősítés”: a minősítési szint leszállítása;

„EU-minősített adat”: bármely olyan EU biztonsági minősítéssel ellátott adat vagy anyag, amelynek engedély nélküli hozzáférhetővé tétele különböző mértékben sértheti az Európai Unió, illetve egy vagy több tagállam érdekeit – lásd a 2. cikk f) pontját;

„telephelybiztonsági tanúsítvány”: annak a nemzeti biztonsági hatóság vagy kijelölt biztonsági hatóság által történő hivatalos meghatározása, hogy egy adott létesítmény biztonsági szempontból megfelelő szintű védelmet tud-e nyújtani meghatározott biztonsági minősítésű szintű EU-minősített adatoknak, valamint hogy a telephelynek az EU-minősített adatokhoz hozzáférést igénylő személyzete átesett-e a megfelelő biztonsági ellenőrzésen, és kapott-e tájékoztatást az EU-minősített adatokhoz való hozzáféréshez és azok védelméhez szükséges vonatkozó biztonsági követelményekről;

EU-minősített adat „kezelése”: minden olyan lehetséges tevékenység, amelynek az EU-minősített adat életciklusa során ki lehet téve. Beletartozik az adatok létrehozása, feldolgozása, szállítása, visszaminősítése, minősítésük feloldása és megsemmisítése. A kommunikációs és információs rendszerrel összefüggésben ezenfelül az adatok gyűjtését, megjelenítését, átadását és tárolását is magában foglalja;

„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”: 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. – lásd az A. melléklet 9. cikkének (1) bekezdését;

„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 eljáráson alapul – lásd az A. melléklet 8. cikkének (1) bekezdését;

„összekapcsolás”: e határozat alkalmazásában két vagy több információtechnológiai rendszer egyirányú vagy többirányú, közvetlen összekapcsolása adatok és egyéb információforrások megosztása (pl. kommunikáció) céljából – lásd az A.IV. melléklet (31) bekezdését;

„minősített adatok kezelése”: az EU-minősített adatok teljes életcikluson keresztüli ellenőrzésére szolgáló adminisztratív intézkedések alkalmazása az 5., 6. és 8. cikkben meghatározott intézkedések kiegészítéseként, és ezáltal hozzájárulva az ilyen adatok illetéktelenek tudomására jutásától vagy elvesztésétől való elrettentéshez – szándékos és véletlenszerű esetekben egyaránt –, annak észleléséhez és a kár helyreállításához. Ezek az intézkedések különösen az EU-minősített adat létrehozására, nyilvántartásba vételére, másolására, fordítására, szállítására, kezelésére, tárolására és megsemmisítésére vonatkoznak – lásd az A. melléklet 7. cikkének (1) bekezdését;

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

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

„személyi biztonság”: olyan intézkedések alkalmazása, amelyek biztosítják, hogy csak azon személyek kapjanak hozzáférést az EU-minősített adatokhoz:

— akik esetében teljesül a „szükséges ismeret” feltétele,

— akik átestek a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítési szintű információkhoz való hozzáféréshez szükséges megfelelő szintű biztonsági ellenőrzésen, vagy a nemzeti jogszabályokkal és rendelkezésekkel összhangban más módon, feladatkörüknél fogva megfelelő hozzáférési engedélyt kaptak, valamint

— akiket tájékoztattak felelősségükről –

lásd az A. melléklet 5. cikkének (1) bekezdését;

„személyi biztonsági tanúsítvány” (PSC) EU-minősített dokumentumokhoz való hozzáféréshez: a valamely tagállam illetékes hatóságai által elvégzett biztonsági ellenőrzést követően a tagállam illetékes hatósága által tett nyilatkozat, amely tanúsítja, hogy egy adott személy részére – amennyiben esetében a szükséges ismeret feltétele teljesül – meghatározott (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) szintig és meghatározott időpontig hozzáférés biztosítható EU-minősített adatokhoz; a fentieknek megfelelő személy megjelölése „biztonsági ellenőrzésen átesett” személy;

„személyi biztonsági tanúsítványról szóló igazolás” (PSCC): egy illetékes hatóság által kiadott igazolás, amely tartalmazza, hogy az adott személy biztonsági ellenőrzésen átesett, és érvényes személyi biztonsági tanúsítvánnyal vagy a Biztonsági Igazgatóság vezetője által kiadott, az EU-minősített adatokhoz való hozzáférést lehetővé tevő engedéllyel rendelkezik, továbbá feltünteti, hogy az érintett személy milyen szintű (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb) EU-minősített adatokhoz férhet hozzá, valamint a vonatkozó személyi biztonsági tanúsítvány érvényességi idejét és a tanúsítvány lejártának időpontját;

„fizikai biztonság”: az EU-minősített adatokhoz való illetéktelen hozzáférés megakadályozását célzó fizikai és technikai védelmi intézkedések alkalmazása – lásd az A. melléklet 6. cikkét;

„adott programra/projektre vonatkozó biztonsági utasítások” (PSI): adott programra/projektre alkalmazandó biztonsági eljárások jegyzéke, amely a biztonsági eljárások egységesítését szolgálja. A jegyzék a program/projekt teljes időtartama alatt felülvizsgálható;

„nyilvántartásba vétel”: olyan eljárások alkalmazása, amelyek során rögzítésre kerül az adat életciklusa, beleértve a továbbítását és a megsemmisítését is – lásd az A.III. melléklet (21) bekezdését;

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

„kockázat”: annak a lehetősége, hogy egy adott fenyegetés kihasználja egy szervezet vagy az általa használt bármely rendszer belső és külső sebezhetőségét, és ezáltal kárt okoz az adott szervezetnek, valamint annak tárgyi eszközeiben vagy immateriális javaiban. Mérése a fenyegetések bekövetkezése valószínűségének és hatásának kombinációjával történik.

„kockázatelfogadás”: a kockázatkezelést követően fennmaradó kockázat további meglétéhez való hozzájárulásra vonatkozó döntés;

„kockázatértékelés”: a fenyegetések és sebezhetőségek azonosításából, valamint a kapcsolódó kockázatelemzésből, azaz a valószínűség és a hatás elemzéséből áll;

„kockázatkommunikáció”: a számítógépes információs rendszer felhasználói közösségei körében a kockázatokkal kapcsolatos tudatosság növelése, a jóváhagyó hatóságok tájékoztatása a kockázatokról, valamint a kockázatokról való jelentéstétel a működtető hatóságok részére;

„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;

„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): a különös szerződéses feltételeknek a szerződő hatóság által összeállított jegyzéke, amely szerves részét képezi az EU-minősített adathoz való hozzáférést vagy ilyen adat létrehozását magában foglaló minősített szerződésnek, és meghatározza a szerződés biztonsági követelményeit vagy biztonsági védelmet igénylő elemeit – lásd az A.V. melléklet II. szakaszát;

„minősítési útmutató” (SCG): olyan dokumentum, amely leírja egy program vagy szerződés minősített elemeit, és meghatározza az alkalmazandó biztonsági minősítési szintet. Az SCG kiterjeszthető a program vagy szerződés teljes időtartamára, az egyes adatelemek pedig újra- vagy visszaminősíthetők; amennyiben létezik SCG, az a SAL részét képezi – lásd az A.V. melléklet II. szakaszát;

„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 nemzeti vagy uniós személyi biztonsági tanúsítványt kapjon;

„biztonsági üzemeltetési eljárások” (SecOP): az elfogadandó biztonsági politika végrehajtásának, a követendő biztonsági üzemeltetési eljárásoknak és a személyzet feladatkörének leírása;

„nem minősített érzékeny adat”: olyan adat vagy anyag, amelyet az EKSZ-nek védelemben kell részesítenie a Szerződésekben vagy az azok végrehajtása során elfogadott jogi aktusokban megállapított jogi kötelezettségekből adódóan, és/vagy a szóban forgó adat érzékeny jellege miatt. A nem minősített érzékeny adatok közé tartoznak többek között az EUMSZ 339. cikkében említett, szakmai titoktartás követelménye alá eső adatok és anyagok, az 1049/2001/EK európai parlamenti és tanácsi rendeletnek ([1]) az Európai Unió Bírósága vonatkozó ítélkezési gyakorlatával összefüggésben értelmezett 4. cikke alapján védelemben részesített érdekek körébe tartozó adatok, vagy a 45/2001/EK rendelet hatálya alá tartozó személyes adatok.

„rendszerspecifikus biztonsági követelmények” (SSRS): egy sor kötelezően betartandó biztonsági elv és végrehajtandó részletes biztonsági követelmény, amely a számítógépes információs rendszer tanúsítási és akkreditációs eljárásának alapját képezi;

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

„fenyegetés”: egy adott szervezet vagy az általa használt bármely rendszer számára esetlegesen károsodást eredményező, nem kívánt esemény lehetséges oka; a fenyegetések lehetnek véletlenszerűek vagy szándékosak (rosszindulatúak), és azokat fenyegető elemek, potenciális célpontok és támadási módszerek jellemzik;

„sebezhetőség”: bármilyen jellegű gyenge pont, amelyet egy vagy több fenyegetés kihasználhat. A sebezhetőség oka lehet mulasztás, vagy az összefügghet az ellenőrzés gyengeségével, hiányosságával vagy következetlenségével, továbbá lehet technikai, eljárási, fizikai, szervezeti vagy üzemeltetési jellegű.

([1]) Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről (HL L 145., 2001.5.31., 43. o.).

B. függelék

Biztonsági minősítések egyenértékűsége

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgium	Très Secret (Loi 1998.12.11.) Zeer 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 a lenti lábjegyzetet ([1])
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 lenti lábjegyzetet ([3])
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-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Hollandia	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Ausztria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lengyelország	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugália	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
România	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 ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Egyesült Királyság	UK TOP SECRET	UK SECRET	Nincs megfelelője ([5])	UK OFFICIAL – SENSITIVE

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

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

([5]) Az Egyesült Királyság a CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű EU-minősített adatokat a UK SECRET minősítésű adatokra alkalmazandó védelmi biztonsági követelményeknek megfelelően kezeli és védi.

ISSN 1977-0979 (elektronikus kiadás)
ISSN 1725-518X (nyomtatott kiadás)

Az Európai Unió Kiadóhivatala
2985 Luxembourg
LUXEMBURG

HU