A BIZOTTSÁG (EU, Euratom) 2015/444 HATÁROZATA

(2015. március 13.)

az EU-minősített adatok védelmét szolgáló biztonsági szabályokról

AZ EURÓPAI BIZOTTSÁG,

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

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

tekintettel a Szerződésekhez mellékelt, az Európai Unió kiváltságairól és mentességeiről szóló 7. jegyzőkönyvre és különösen annak 18. cikkére,

mivel:

(1) Az Európai Unió minősített adatainak védelmére vonatkozó bizottsági biztonsági rendelkezéseket felül kell vizsgálni és naprakésszé kell tenni, figyelembe véve az intézményi, szervezeti, üzemeltetési és technológiai fejlesztéseket.

(2) Az Európai Bizottság fő telephelyeinek biztonsági kérdéseivel kapcsolatban megállapodásokat kötött a belga, a luxemburgi és az olasz kormánnyal. ([1])

(3) A Bizottság, a Tanács és az Európai Külügyi Szolgálat elkötelezett az egyenértékű biztonsági szabványok alkalmazása iránt az EU-minősített adatok védelmére vonatkozóan.

(4) Adott esetben fontos, hogy az Európai Parlamentet és más uniós intézményeket, ügynökségeket, szerveket és hivatalokat is bevonjanak az Unió és tagállamai érdekeinek védelméhez szükséges, a minősített adatok védelmére vonatkozó elvek, előírások és szabályok alkalmazásába.

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

(6) A Bizottságon belül a minősített adatok védelmét szolgáló fizikai biztonság az EU-minősített adatokhoz való illetéktelen hozzáférés megakadályozását célzó fizikai és technikai védelmi intézkedések alkalmazása.

(7) Az EU-minősített adatok kezelése az EU-minősített adatok teljes életciklusán keresztüli ellenőrzésére szolgáló adminisztratív intézkedések alkalmazása e határozat 2., 3. és 5. fejezetében meghatározott intézkedések kiegészítéseként, és ezáltal az ilyen adatoknak szándékosan vagy véletlenszerűen illetéktelen tudomására jutásától vagy elvesztésétől való elrettentéshez, annak észleléséhez és a kár helyreállításához való hozzájárulásként. Az ilyen intézkedések különösen az EU-minősített adatok előállítására, tárolására, nyilvántartásba vételére, másolására, fordítására, visszaminősítésére, minősítése megszüntetésére, szállítására és megsemmisítésére vonatkoznak, valamint kiegészítik a dokumentumok kezelésére vonatkozó általános bizottsági szabályokat (2002/47/EK ([2]), ESZAK, Euratom és 2004/563/EK, Euratom ([3]) határozatok).

([1]) Vö. a 2004. december 31-i „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité", a 2007. január 20-i „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" és az 1959. július 22-i „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale" című megállapodásokkal.

([2]) A Bizottság 2002. január 23-i 2002/47/EK, ESZAK, Euratom határozata eljárási szabályzatának módosításáról (HL L 21., 2002.1.24., 23. o.).

([3]) A Bizottság 2004. július 7-i 2004/563/EK, Euratom határozata eljárási szabályzatának módosításáról (HL L 251., 2004.7.27., 9. o.).

(8) E határozat rendelkezései nem érintik az alábbi rendeleteket:

a) 3. rendelet (Euratom) ([1]);

b) az Európai Parlament és Tanács 1049/2001/EK rendelete ([2]);

c) az Európai Parlament és a Tanács 45/2001/EU rendelete ([3]);

d) a Tanács 354/83/EK, Euratom rendelete ([4]),

ELFOGADTA A KÖVETKEZŐ HATÁROZATOT:

1. FEJEZET

ALAPELVEK ÉS MINIMUMSZABÁLYOK

1. cikk

Fogalommeghatározások

E határozat alkalmazásában a következő fogalommeghatározásokat kell alkalmazni:

1. „a Bizottság szervezeti egysége”: bármely bizottsági főigazgatóság vagy szolgálat vagy a Bizottság bármely tagjának kabinetje;

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

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

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

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

6. „visszaminősítés”: a minősítési szint leszállítása;

7. EU-minősített adat „kezelése”: minden olyan lehetséges tevékenység, amelynek az EU-minősített adat életciklusa során ki lehet téve. Beletartozik az adat előállítása, nyilvántartásba vétele, feldolgozása, szállítása, visszaminősítése, a rá vonatkozó minősítés feloldása és az adat megsemmisítése. A kommunikációs és információs rendszerrel (CIS) összefüggésben ezen felül az adat gyűjtését, megjelenítését, átadását és tárolását is tartalmazza;

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

9. „végrehajtási szabályok”: a Bizottság (EU, Euratom) 2015/443 határozat 5. fejezetével összhangban elfogadott bármely szabály vagy biztonsági közlemény ([5]);

10. „anyag”: bármely közvetítő eszköz, adathordozó, vagy bármely készre gyártott vagy gyártás alatt álló gép vagy berendezés;

11. „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;

12. „létesítmények”: a Bizottság bármely ingatlana vagy azzal összefüggő vagyontárgya és tulajdona;

([1]) Az 1958. július 31-i 3. Euratom-tanácsi rendelet az Európai Atomenergia-közösséget létrehozó szerződés 24. cikkének végrehajtásáról (HL 17., 1958.10.6., 406/58. o.).
([2]) Az Európai Parlament és a Tanács 2001. május 30-i 1049/2001/EK rendelete a nyilvánosságnak az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz történő hozzáféréséről (HL L 145., 2001.5.31., 43. o.).
([3]) Az Európai Parlament és a Tanács 2000. december 18-i 45/2001/EK rendelete 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.).
([4]) A Tanács 1983. február 1-i 354/83/EGK, Euratom rendelete az Európai Gazdasági Közösség és az Európai Atomenergia-közösség levéltárainak a nyilvánosság számára történő megnyitásáról (HL L 43., 1983.2.15., 1. o.).
([5]) A Bizottság 2015. március 13-i (EU, Euratom) 2015/443 határozata a Bizottság biztonságáról (Lásd e Hivatalos Lap 41. oldalát).

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

14. „személyzeti szabályzat”: a 259/68/EGK, Euratom, ESZAK tanácsi rendeletben ([1]) meghatározott, az Európai Unió tisztviselőinek személyzeti szabályzata és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételek;

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

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

2. cikk

Tárgy és hatály

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

(2) Ezen határozat valamennyi bizottsági szervezeti egységre vonatkozik és a Bizottság valamennyi létesítményében alkalmazni kell.

(3) A személyzet egyes csoportjaira vonatkozó konkrét utalások ellenére, ezen határozat a Bizottság tagjaira, a személyzeti szabályzat és az Európai Közösségek egyéb alkalmazottainak alkalmazási feltételeinek hatálya alá tartozó bizottsági személyzetre, a Bizottsághoz kirendelt nemzeti szakértőkre, a szolgáltatókra és azok személyzetére, a gyakornokokra és a Bizottság épületeihez vagy egyéb eszközeihez hozzáféréssel rendelkező bármely személyre vagy a Bizottság által kezelt adatokra vonatkozik.

(4) Ennek a határozatnak a rendelkezései nem érintik a 2002/47/EK, ESZAK, Euratom határozatot és a 2004/563/EK, Euratom határozatot.

3. cikk

Az EU-minősített adat fogalmának meghatározása, a biztonsági szintek és jelölések

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

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

a) TRES SECRET UE/EU TOP SECRET: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele rendkívül súlyosan sértheti az Európai Unió illetve egy vagy több tagállam alapvető érdekeit;

b) SECRET UE/EU SECRET: olyan adatok és anyagok, amelyeknek engedély nélküli hozzáférhetővé tétele súlyosan sértheti az Európai Unió vagy egy vagy több tagállam alapvető érdekeit;

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

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

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

([1]) A Tanács 1968. február 29-i 259/68/EGK, Euratom, ESZAK rendelete az Európai Közösségek tisztviselőinek személyzeti szabályzatáról és az Európai Közösségek egyéb alkalmazottainak alkalmazási feltételeiről, valamint a Bizottság tisztviselőire ideiglenesen alkalmazandó különleges intézkedések bevezetéséről (az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételek) (HL L 56., 1968.3.4., 1. o.).

4. cikk

A minősítés szabályai

(1) A Bizottság vagy bizottsági szervezeti egység valamennyi tagja biztosítja az általa létrehozott EU-minősített adatok megfelelő minősítését, minősített adatokként való egyértelmű azonosíthatóságát és azt, hogy minősítési szintjüket csak a szükséges ideig őrizzék meg.

(2) Az alábbi 26. cikk sérelme nélkül az EU-minősített adatokat kizárólag a kibocsátó előzetes írásbeli hozzájárulásával lehet visszaminősíteni vagy a minősítés alól feloldani, továbbá nem lehet azok 3. cikk (2) bekezdésében említett biztonsági jelöléseit módosítani vagy eltávolítani.

(3) Adott esetben az EU-minősített adatok kezelésére vonatkozó, gyakorlati minősítési útmutatót is tartalmazó végrehajtási szabályokat kell az alábbi 60. cikkel összhangban elfogadni.

5. cikk

A minősített adatok védelme

(1) Az EU-minősített adatokat e határozattal és annak végrehajtási szabályaival összhangban kell védeni.

(2) Az alábbi 4. fejezetben megállapított szabályok szerint az EU-minősített adatok birtokosai felelősek az adatok e határozat és annak végrehajtási szabályai szerinti védelméért.

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

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

6. cikk

Biztonsági kockázatkezelés

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

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

(3) A szolgálatok üzletmenet-folytonossági terveinek a súlyos mulasztások vagy incidensek által az EU-minősített adatok kezelésére és tárolására gyakorolt hatások csökkentését szolgáló megelőző és helyreállító intézkedéseket kell tartalmazniuk.

7. cikk

E határozat végrehajtása

(1) Szükség esetén ezen határozat kiegészítésére vagy támogatására szolgáló végrehajtási szabályokat kell az alábbi 60. cikkel összhangban elfogadni.

(2) A bizottsági szervezeti egységek a felelősségi körükbe tartozó minden szükséges intézkedést megtesznek azért, hogy az EU-minősített adatok és minden más minősített adat kezelésekor vagy tárolásakor ezen határozat és a vonatkozó végrehajtási szabályok alkalmazásra kerüljenek.

(3) Az ezen határozat végrehajtása érdekében hozott biztonsági intézkedéseknek meg kell felelniük a Bizottság (EU, Euratom) 2015/443 határozatának 3. cikkében foglalt, a Bizottság biztonságára vonatkozó elveknek.

(4) A humánerőforrásügyi és biztonsági főigazgató állítja fel a Bizottság Biztonsági Hatóságát a Humánerőforrásügyi és Biztonsági Főigazgatóságon belül. A Bizottság Biztonsági Hatósága az ezen határozatban és annak végrehajtási szabályaiban meghatározott feladatkörökkel rendelkezik.

(5) A Bizottság (EU, Euratom) 2015/443 határozatának 20. cikkében említett helyi biztonsági tisztviselő valamennyi bizottsági szervezeti egységnél az EU-minősített adatok védelmével kapcsolatos alábbi alapvető feladatokat látja el ezen határozattal összhangban, a Humánerőforrásügyi és Biztonsági Főigazgatósággal szoros együttműködésben:

a) a személyzet biztonsági engedélyeire vonatkozó kérelmek kezelése;

b) biztonsági képzésekhez és biztonság-tudatossági tájékoztatókhoz való hozzájárulás;

c) a szervezeti egység nyilvántartó hivatalt ellenőrző tisztviselőjének felügyelete;

d) a biztonsági szabályok megsértésének és az EU-minősített adatok illetéktelen tudomására jutásának bejelentése;

e) a tartalékkulcsok és valamennyi kombinációról írásos jegyzék őrzése;

f) az EU-minősített adatok védelmével összefüggő vagy a végrehajtási szabályokban meghatározott egyéb feladatok ellátása.

8. cikk

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

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

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

(3) A biztonsági szabályok megsértését vagy azok feltételezett megsértését minden esetben haladéktalanul jelenteni kell a Bizottság Biztonsági Hatóságának.

(4) Amennyiben ismert, vagy alapos okkal gyanítható, hogy EU-minősített adatok illetéktelen személy tudomására jutottak vagy elvesztek, a Bizottság (EU, Euratom) 2015/443 határozatának 13. cikkével összhangban biztonsági vizsgálatot kell lefolytatni.

(5) Valamennyi megfelelő intézkedést meg kell tenni az alábbiak érdekében:

a) a kibocsátó tájékoztatására;

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

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

d) az ismételt előfordulás megelőzése érdekében; és

e) értesíti a megfelelő hatóságokat a megtett lépésekről.

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

2. FEJEZET

SZEMÉLYI BIZTONSÁG

9. cikk

Fogalommeghatározások

E fejezet alkalmazásában az alábbi meghatározásokat kell alkalmazni:

1. „engedély EU-minősített adatokhoz való hozzáférésre”: a Bizottság Biztonsági Hatósága által valamely tagállam illetékes hatósága általi azon megállapítás alapján hozott határozat, hogy a Bizottság tisztviselője, egyéb alkalmazott vagy kirendelt nemzeti szakértő – feltéve, hogy az esetében meghatározták a „szükséges ismeretet”, és megfelelő tájékoztatást kapott az ezzel kapcsolatos felelősségéről – meghatározott minősítési szintig (CONFIDENTIEL UE/EU CONFIDENTIAL vagy e fölött) és meghatározott időpontig hozzáférést kaphat EU-minősített adatokhoz; a fentieknek megfelelő személy megjelölése „biztonsági engedéllyel rendelkező” személy.

2. „személyi biztonsági engedély”: olyan intézkedések alkalmazását jelenti, amelyek biztosítják, hogy csak azon személyek kapjanak hozzáférést az EU-minősített adatokhoz:

   a) akiknek esetében a „szükséges ismeret” feltétele teljesül,

   b) akik adott esetben megfelelő szintű biztonsági engedéllyel rendelkeznek, és

   c) akiket tájékoztattak felelősségükről.

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

4. „személyi biztonsági tanúsítványról szóló igazolás”: valamely illetékes hatóság által kiadott igazolás, amely tartalmazza, hogy az adott személy érvényes biztonsági tanúsítvánnyal vagy a Bizottság Biztonsági Hatósága által kibocsátott biztonsági engedéllyel rendelkezik, amely megmutatja, hogy milyen szintű EU-minősített adatokhoz férhet hozzá (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint a vonatkozó biztonsági tanúsítvány vagy engedély érvényességi idejét és az igazolás lejártának időpontját;

5. „biztonsági ellenőrzés”: valamely tagállam illetékes hatósága által a nemzeti törvényekkel és rendeletekkel 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 biztonsági tanúsítványt kapjon.

10. cikk

Alapvető elvek

(1) Egy adott személy csak azt követően kaphat hozzáférést EU-minősített adatokhoz, hogy

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

2. tájékoztatást kapott az EU-minősített adatok védelmére szolgáló biztonsági szabályokról és a vonatkozó biztonsági szabványokról és útmutatókról, és tudomásul vette az ilyen adatok védelmével kapcsolatos felelősségét;

3. a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz megfelelő szintű biztonsági engedéllyel rendelkezik, vagy a nemzeti törvényekkel és rendeletekkel összhangban más módon, feladatkörénél fogva megfelelő felhatalmazást kapott.

(2) Valamennyi olyan személy, akinek feladatai szükségessé teszik a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítésű EU-minősített adatokhoz való hozzáférést, az ilyen EU-minősített adatokhoz való hozzáférés engedélyezését megelőzően megfelelő szintű biztonsági engedéllyel kell rendelkeznie. Az érintett személynek írásban hozzá kell járulnia a személyi biztonsági tanúsítvánnyal kapcsolatos eljárásban való részvételéhez. Amennyiben ezt elmulasztja, az érintett személy nem nevezhető ki olyan beosztásba, funkcióba vagy feladatra, amely CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáférést igényel.

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

(4) Az adott személy lojalitásának, szavahihetőségének és megbízhatóságának a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáférést engedélyező biztonsági tanúsítvány megadása céljából történő értékelése valamely tagállam illetékes hatósága által a nemzeti törvényekkel és rendeletekkel összhangban lefolytatott biztonsági ellenőrzés keretében történik.

(5) A Bizottság Biztonsági Hatósága kizárólagos felelősséget vállal valamennyi biztonsági tanúsítvánnyal kapcsolatos kérdés terén a nemzeti biztonsági hatóságokkal és egyéb illetékes nemzeti hatóságokkal való kapcsolattartásért. A Bizottság szolgálatai és azok személyzete, valamint a nemzeti biztonsági hatóságok és egyéb illetékes hatóságok közötti kapcsolattartást a Bizottság Biztonsági Hatóságán keresztül kell irányítani.

11. cikk

Biztonsági engedélyezési eljárás

(1) A Bizottság minden főigazgatója vagy szolgálati vezetője köteles szervezeti egységén belül azonosítani azokat a beosztásokat, amelyek birtokosának feladatai ellátásához CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáféréssel és ezért biztonsági engedéllyel kell rendelkeznie.

(2) Amint ismertté válik, hogy adott személyt olyan beosztásba neveznek ki, amely CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adathoz való hozzáférést tesz szükségessé, a Bizottság érintett szervezeti egységének helyi biztonsági tisztviselője értesíti a Bizottság Biztonsági Hatóságát, amely továbbítja az adott személy számára a személyi biztonsági tanúsítvánnyal kapcsolatos kérdőívet, amelyet azon tagállam nemzeti biztonsági felügyelete bocsátott ki, amelynek állampolgáraként adott személyt az európai intézmény alkalmazottjának kinevezték. Adott személynek írásban hozzá kell járulnia a biztonsági tanúsítvánnyal kapcsolatos eljárásban való részvételéhez és a kitöltött kérdőívet a legrövidebb határidőn belül vissza kell küldenie a Bizottság Biztonsági Hatóságához.

(3) A Bizottság Biztonsági Hatósága továbbítja a kitöltött biztonsági tanúsítvánnyal kapcsolatos kérdőívet azon tagállam nemzeti biztonsági felügyeletének, amelynek állampolgáraként adott személyt az európai intézmény alkalmazottjának kinevezték és kéri, hogy végezzenek olyan minősítési szintű biztonsági ellenőrzést, amilyen szintű EU-minősített adatokhoz az érintett személynek hozzá kell férnie.

(4) Amennyiben olyan személy biztonsági ellenőrzésével kapcsolatos releváns információ jut a Bizottság Biztonsági Hatósága tudomására, aki biztonsági tanúsítványért folyamodott, a Bizottság Biztonsági Hatósága a vonatkozó szabályokkal és rendeletekkel összhangban értesíti erről az illetékes nemzeti biztonsági felügyeletet.

(5) A biztonsági ellenőrzés elvégzését követően, és az érintett nemzeti biztonsági hatóság biztonsági ellenőrzés eredményeire vonatkozó általános értékelésével kapcsolatos értesítését követő lehető legrövidebb időn belül a Bizottság Biztonsági Hatósága:

a) az érintett személy számára megadhatja az engedélyt az EU-minősített adatokhoz való hozzáféréshez és az általa meghatározott időpontig, de legfeljebb 5 évig, és meghatározott szintig engedélyezheti számára az EU-minősített adatokhoz való hozzáférést, amennyiben a biztonsági ellenőrzés során megállapítást nyer, hogy az adott személy lojalitását, szavahihetőségét és megbízhatóságát semmilyen ismert kedvezőtlen tény nem kérdőjelezi meg;

b) amennyiben a biztonsági ellenőrzés kedvezőtlen eredménnyel jár, a vonatkozó szabályokkal és rendeletekkel összhangban értesíti az érintett személyt, aki meghallgatását kérheti a Bizottság Biztonsági Hatóságától, amely viszont felkérheti az illetékes nemzeti biztonsági felügyeletet, hogy ha a nemzeti törvények és rendeletek alapján módjában áll, adjon további felvilágosítást. Ha a biztonsági ellenőrzés eredménye megerősítést nyer, az EU-minősített adatokhoz való hozzáférést nem lehet engedélyezni.

(6) A biztonsági ellenőrzésre és a kapott eredményekre az érintett tagállamban hatályos megfelelő törvények és rendeletek vonatkoznak, beleértve az esetleges jogorvoslattal kapcsolatos törvényeket és rendeleteket is. A Bizottság Biztonsági Hatóságának határozata ellen a személyzeti szabályzattal összhangban lehet fellebbezni.

(7) A Bizottság elfogadja a más uniós intézmény, szerv vagy ügynökség által adott, EU-minősített adatokhoz való hozzáférést lehetővé tevő engedélyt, feltéve ha az továbbra is érvényes. Az engedély az érintett 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.

(8) Amennyiben az adott személy szolgálati jogviszonya a biztonsági ellenőrzés eredményéről a Bizottság Biztonsági Hatóságának részére küldött értesítés dátumától számított 12 hónapon belül nem kezdődik meg, vagy amennyiben a szolgálati jogviszony 12 hónapig szünetel, és ez idő alatt a személy nem áll alkalmazásban a Bizottságnál, más uniós intézménynél, szervnél vagy ügynökségnél vagy valamely tagállam nemzeti közigazgatási szerveinél, a Bizottság Biztonsági Hatóságának az érintett nemzeti biztonsági felügyelettől kell kérnie annak megerősítését, hogy a biztonsági tanúsítvány továbbra is érvényes és megfelelő.

(9) Amennyiben egy érvényes biztonsági engedéllyel rendelkező személy által jelentett biztonsági kockázattal kapcsolatos információ jut a Bizottság Biztonsági Hatósága tudomására, a Biztonsági Hatóság a vonatkozó szabályokkal és rendeletekkel összhangban értesíti erről az illetékes nemzeti biztonsági felügyeletet.

(10) Ha valamely nemzeti biztonsági felügyelet egy EU-minősített adatokhoz való hozzáféréshez érvényes engedéllyel rendelkező személyre vonatkozó, az 5. pont a) alpontjával összhangban tett megállapítás visszavonásáról értesíti a Bizottság Biztonsági Hatóságát, a Bizottság Biztonsági Hatósága felkérheti az illetékes nemzeti biztonsági hatóságot, hogyha a nemzeti törvények és rendeletek alapján módjában áll, adjon további felvilágosítást. Ha a kizáró tényezőket az illetékes nemzeti biztonsági felügyelet megerősíti, a biztonsági engedélyt vissza kell vonni, és a személyt ki kell zárni az EU-minősített adatokhoz való hozzáférésből, valamint azokból a beosztásokból, amelyekben az ilyen hozzáférés lehetséges, vagy amelyekben a személy a biztonságot veszélyeztetheti.

(11) Az EU-minősített adatokhoz való hozzáférésre vonatkozó engedélynek ezen határozat hatálya alá tartozó személytől való visszavonásáról vagy felfüggesztéséről szóló határozatot és adott esetben annak indokait közölni kell az érintett személlyel, aki kérheti a Bizottság Biztonsági Hatósága általi meghallgatását. A nemzeti biztonsági felügyeletek által rendelkezésre bocsátott információkra az érintett tagállamban hatályos megfelelő törvények és rendeletek vonatkoznak. A Bizottság Biztonsági Hatóságának ebben az összefüggésben hozott határozata ellen a személyzeti szabályzattal összhangban lehet fellebbezni.

(12) A Bizottság szervezeti egységeinek gondoskodniuk kell arról, hogy az EU-minősített adatokhoz való hozzáféréshez biztonsági engedélyt igénylő beosztásba a szervezeti egységhez kirendelt nemzeti szakértőknek a feladatuk megkezdését megelőzően érvényes személyi biztonsági tanúsítványt vagy személyi biztonsági tanúsítványról szóló igazolást kell a nemzeti jogszabályok és rendeletek szerint a Bizottság Biztonsági Hatóságának bemutatnia, amely alapján a Hatóság az érintett személy számára az EU-minősített adatokhoz való hozzáféréshez biztonsági engedélyt ad a nemzeti biztonsági tanúsítványban említett szintnek megfelelő szintig, amely legfeljebb a feladatuk idejére érvényes.

A feladatkörüknél fogva megfelelően felhatalmazott személyek EU-minősített adatokhoz való hozzáférése

(13) A feladatkörüknél fogva, a Szerződés alapján EU-minősített adatokhoz való hozzáférésre megfelelően felhatalmazott bizottsági tagokat tájékoztatni kell az EU-minősített adatok védelmével kapcsolatos biztonsági kötelezettségeikről.

A biztonsági tanúsítványok és engedélyek nyilvántartása

(14) Az EU-minősített adatokhoz való hozzáférést lehetővé tevő biztonsági tanúsítványok és engedélyek nyilvántartását ezen határozat szerint a Bizottság Biztonsági Hatósága vezeti. E nyilvántartásnak tartalmaznia kell legalább az EU-minősített adatok minősítési szintjét, amelyhez az adott személy részére hozzáférés biztosítható, a biztonsági tanúsítvány kibocsátásának dátumát és érvényességének időtartamát.

(15) A Bizottság Biztonsági Hatósága személyi biztonsági tanúsítványról szóló igazolást adhat ki, amely tartalmazza, hogy az adott személy milyen szintű EU-minősített adatokhoz rendelkezik hozzáférési engedéllyel (CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb), valamint tartalmazza a vonatkozó engedély érvényességi idejét és az igazolás lejártának időpontját.

A biztonsági engedély megújítása

(16) A biztonsági engedély első megadását követően, valamint feltéve, hogy az adott személy a Bizottságnál vagy más uniós intézménynél, szervnél vagy ügynökségnél folyamatos szolgálati jogviszonyban áll és folyamatosan szükséges van az EU-minősített adatokhoz való hozzáférésre, az EU-minősített adatokhoz való hozzáférést lehetővé tevő biztonsági engedélyt megújítás céljából, általános szabályként, az engedély alapjául szolgáló biztonsági ellenőrzés eredményéről szóló értesítés időpontjától számítva ötévenként felül kell vizsgálni.

(17) A Bizottság Biztonsági Hatósága legfeljebb 12 hónapos időtartamra meghosszabbíthatja a meglévő biztonsági engedély érvényességét, amennyiben az illetékes nemzeti biztonsági hatóság vagy más illetékes nemzeti hatóság nem szolgáltat kizáró tényezőket a megújításra vonatkozó kérelem és a megfelelő biztonsági tanúsítvánnyal kapcsolatos kérdőív továbbításának időpontjától számított két hónapon belül. Amennyiben a 12 hónapos időszak végén az illetékes nemzeti biztonsági hálózat vagy más illetékes nemzeti hatóság nem értesíti a Bizottság Biztonsági Hatóságát véleményéről, az érintett személyt olyan feladatokkal kell megbízni, amelyekhez nem szükséges biztonsági engedély.

12. cikk

Biztonsági engedélyezésre vonatkozó tájékoztató

(1) A biztonsági engedéllyel rendelkező valamennyi személynek írásban nyilatkoznia kell a Bizottság Biztonsági Hatósága által szervezett biztonsági engedélyezésre vonatkozó tájékoztatón való részvételét követően arról, hogy megértette az EU-minősített adatok védelmével kapcsolatos kötelezettségeit, valamint az EU-minősített adatok illetéktelen személy tudomására jutásának következményeit. Az ilyen írásbeli nyilatkozatokról a Bizottság Biztonsági Hatóságának nyilvántartást kell vezetnie.

(2) Mindazon személyekben, akik engedéllyel rendelkeznek EU-minősített adatokhoz való hozzáférésre, vagy akiknek ilyen adatokat kell kezelniük, kezdetben, majd később rendszeres időközönként tudatosítani kell a biztonságot fenyegető veszélyeket, és e személyeknek haladéktalanul jelenteniük kell a Bizottság Biztonsági Hatóságának az általuk gyanúsnak vagy szokatlannak ítélt közeledést vagy tevékenységet.

(3) Bármely személyben, akit nem alkalmaznak tovább az EU-minősített adatokhoz való hozzáférést megkövetelő feladatok ellátására, tudatosítani kell az EU-minősített adatok folyamatos védelmével kapcsolatos kötelezettségét, és adott esetben az érintett személyeknek erről írásbeli nyilatkozatot kell tenniük.

13. cikk

Ideiglenes biztonsági engedélyek

(1) A Bizottság Biztonsági Hatósága – kivételes körülmények között, amennyiben azt a szervezeti egység érdekei kellően indokolják, és a teljes biztonsági ellenőrzés lezárulásáig az érintett állampolgársága szerinti tagállam nemzeti biztonsági felügyeletével folytatott konzultációt követően, valamint a lényeges kizáró tényezők hiányát kereső első vizsgálatok eredményére is figyelemmel – meghatározott feladat tekintetében ideiglenes engedélyt adhat adott személy számára EU-minősített adatokhoz való hozzáférésre, a biztonsági tanúsítványok megújítására vonatkozó rendelkezések sérelme nélkül. Az EU-minősített adatokhoz való hozzáférést lehetővé tevő ideiglenes engedély érvényességének időtartama legfeljebb hat hónap lehet, és nem teheti lehetővé a TRES SECRET UE/EU TOP SECRET minősítésű adatokhoz való hozzáférést.

(2) A 12. cikk (1) bekezdése szerinti tájékoztatót követően minden ideiglenes engedéllyel rendelkező személynek írásban nyilatkoznia kell arról, hogy megértette az EU-minősített adatok védelmével kapcsolatos kötelezettségeit, valamint az EU-minősített adatok illetéktelen tudomására jutásának következményeit. Az ilyen írásbeli nyilatkozatokról a Bizottság Biztonsági Hatóságának nyilvántartást kell vezetnie.

14. cikk

A Bizottság által szervezett minősített üléseken való részvétel

(1) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat tárgyaló ülések szervezéséért felelős bizottsági szervezeti egységek a helyi biztonsági tisztviselőjükön vagy az ülés szervezőjén keresztül jóval előre értesítik a Bizottság Biztonsági Hatóságát ezen ülések napjáról, időpontjáról, helyszínéről és résztvevőiről.

(2) A 11. cikk (13) bekezdése rendelkezéseinek megfelelően a Bizottság által szervezett, CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat tárgyaló üléseken a részvétellel megbízott személyek kizárólag biztonsági tanúsítványuk vagy biztonsági engedélyük státusának megerősítését követően vehetnek részt. A Bizottság Biztonsági Hatósága számára személyi biztonsági tanúsítványról szóló igazolást vagy a biztonsági tanúsítvány egyéb bizonyítékát be nem mutató személyek vagy a biztonsági engedéllyel nem rendelkező bizottsági tagok ezen minősített üléseken való részvételét el kell utasítani.

(3) A minősített ülés szervezését megelőzően az ülés szervezéséért felelős személy vagy az ülést szervező bizottsági szervezeti egység helyi biztonsági tisztviselője felkéri a külső résztvevőket, hogy a Bizottság Biztonsági Hatósága számára nyújtsák be a személyi biztonsági tanúsítványról szóló igazolást vagy a biztonsági tanúsítvány egyéb bizonyítékát. A Bizottság Biztonsági Hatósága a benyújtott személyi biztonsági tanúsítványról szóló igazolásról vagy a személyi biztonsági tanúsítvány egyéb bizonyítékáról értesíti a helyi biztonsági tisztviselőt vagy az ülés szervezőjét. Adott esetben összesített névjegyzék használható, amely a biztonsági tanúsítvány meglétét bizonyítja.

(4) Amennyiben az illetékes hatóságok arról tájékoztatják a Bizottság Biztonsági Hatóságát, hogy a személyi biztonsági tanúsítványt visszavonták egy olyan személytől, akinek feladatai megkövetelik a Bizottság által szervezett üléseken való részvételt, a Bizottság Biztonsági Hatósága értesíti az ülés szervezéséért felelős bizottsági szervezeti egység helyi biztonsági tisztviselőjét.

15. cikk

Az EU-minősített adatokhoz való potenciális hozzáférés

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

3. FEJEZET

A MINŐSÍTETT ADATOK VÉDELMÉT SZOLGÁLÓ FIZIKAI BIZTONSÁG

16. cikk

Alapelvek

(1) 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. Ezen intézkedések e határozattal és annak végrehajtási szabályaival összhangban kockázatkezelési eljáráson alapulnak.

(2) Különösen a fizikai biztonsági intézkedések célja az EU-minősített adatokhoz való jogosulatlan hozzáférés megakadályozása az alábbiak révén:

a) az EU-minősített adatok megfelelő módon való kezelésének és tárolásának a biztosítása;

b) a személyzet tagjainak szigorúan a szükséges ismeret elve, és szükség szerint biztonsági engedélyük alapján történő megkülönböztetése az EU-minősített adatokhoz való hozzáférés tekintetében;

c) a jogosulatlan cselekményektől való elrettentés, azok megakadályozása és észlelése; valamint

d) behatolók titokban történő vagy erőszakos behatolásának megakadályozása vagy késleltetése.

(3) Fizikai biztonsági intézkedéseket kell bevezetni valamennyi helyiségben, épületekben, irodában, teremben és egyéb területen, ahol EU-minősített adatokat kezelnek vagy tárolnak, ideértve azon területeket is, ahol az 5. fejezetben említett kommunikációs és információs rendszereket tárolják.

(4) Ezen fejezetnek megfelelően biztonsági területként kell meghatározni és a Bizottság Biztonsági Akkreditációs Hatóságának akkreditálnia kell azokat a területeket, ahol CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb minősítéssel rendelkező EU-minősített adatot tárolnak.

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

17. cikk

Fizikai biztonsági követelmények és intézkedések

(1) A fizikai biztonsági intézkedéseket a Bizottság Biztonsági Hatósága által elvégzett fenyegetésértékelés alapján kell megválasztani, szükség szerint más bizottsági szervezeti egységekkel, más uniós intézményekkel, ügynökségekkel vagy szervekkel és/vagy a tagállamok illetékes hatóságaival konzultálva. A Bizottság kockázatkezelési eljárást alkalmaz az EU-minősített adatoknak a saját területén történő védelmére, a felmért kockázattal arányos mértékű fizikai védelem biztosítása érdekében. A kockázatkezelési folyamat figyelembe veszi az összes vonatkozó tényezőt, különösen az alábbiakat:

a) az EU-minősített adatok minősítési szintje;

b) az EU-minősített adatok megjelenési formája és mennyisége, szem előtt tartva, hogy nagy mennyiségű EU-minősített adat vagy ilyen adatok gyűjteménye szigorúbb védelmi intézkedések alkalmazását teheti szükségessé;

c) azon épületek vagy területek közvetlen környezete és kialakítása, ahol EU-minősített adatok adatokat kezelnek, illetve tárolnak; valamint

d) az Unió, annak intézményei, szervei vagy ügynökségei vagy a tagállamok ellen tevékenykedő hírszerző szolgálatok tevékenységéből eredő fenyegetések, valamint a szabotázs, terrorizmus, felforgató tevékenységek vagy más bűncselekmények miatt fenyegető veszélyek.

(2) A Bizottság Biztonsági Hatósága a zónaszerű védelem elvének alkalmazásával meghatározza a végrehajtandó fizikai biztonsági intézkedések megfelelő kombinációját. E célból a Bizottság Biztonsági Hatósága a végrehajtási szabályokban meghatározott minimumszabályokat, normákat és követelményeket dolgoz ki.

(3) A Bizottság Biztonsági Hatósága jogosult lehet a be- és kiléptetésnél átvizsgálást végezni a nem engedélyezett anyagok bevitelétől vagy EU-minősített adatoknak a helyiségből vagy épületből történő engedély nélküli kivitelétől való elrettentés céljából.

(4) Amennyiben EU-minősített adatokat – akár véletlenszerűen is – rálátás veszélye fenyeget, a Bizottság érintett szervezeti egységeinek a Bizottság Biztonsági Hatósága által meghatározott megfelelő intézkedéseket kell hozni e veszély kivédésére.

(5) Az új létesítmények esetében a fizikai biztonsági követelményeket és azok funkcionális jellemzőit a Bizottság Biztonsági Hatóságának hozzájárulásával, a létesítmények tervezése során meg kell határozni. A már meglevő létesítmény esetében a fizikai biztonsági követelményeket a minimumszabályokkal, normákkal és követelményekkel összhangban kell megvalósítani.

18. cikk

Az EU-minősített adatok fizikai védelmére szolgáló berendezések

(1) Az EU-minősített adatok fizikai védelmére két típusú, fizikai védelemben részesülő terület kerül megállapításra:

a) adminisztratív zónák; valamint

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

(2) A Bizottság Biztonsági Hatósága megállapítja, hogy az adott terület megfelel-e az adminisztratív zónaként, biztonsági területként vagy technikailag biztosított biztonsági területként való kijelölés követelményeinek.

(3) Az adminisztratív zónák esetében:

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

b) a kíséret nélküli belépést csak a Bizottság Biztonsági Hatósága vagy más illetékes hatóság megfelelő engedélyével rendelkező személyek számára lehet megadni; valamint

c) minden más személy mellé folyamatos kíséretet kell adni vagy ezzel egyenértékű ellenőrzésnek kell alávetni.

(4) A biztonsági területek esetében:

a) láthatóan elhatárolt és védett körzetet kell meghatározni, amelyen minden be- és kilépést beléptető vagy személyazonosító rendszerrel ellenőriznek;

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

c) minden más személy mellé folyamatos kíséretet kell adni vagy ezzel egyenértékű ellenőrzésnek kell alávetni.

(5) Amennyiben a biztonsági területre való belépés az ott található minősített adatokhoz való közvetlen – bármilyen gyakorlati célt szolgáló – hozzáférést tesz lehetővé, az alábbi kiegészítő követelményeket kell alkalmazni:

a) az adott területen általában tárolt adatok legmagasabb minősítési szintjét egyértelműen fel kell tüntetni,

b) minden látogatónak különleges engedéllyel kell rendelkeznie a területre való belépéshez, minden látogató mellé folyamatos kíséretet kell rendelni és valamennyi látogatónak megfelelő biztonsági ellenőrzésen kell átesnie, kivéve, ha intézkedéseket tettek annak biztosítására, hogy EU-minősített adatokhoz ne legyen lehetséges a hozzáférés.

(6) 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. Valamennyi kulcsot a 20. cikkel összhangban kell kezelni;

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

c) e területeket a Bizottság Biztonsági Hatóságának rendszeres fizikai és/vagy technikai ellenőrzéseknek kell alávetnie. Ezeket az ellenőrzéseket illetéktelen behatolás vagy annak gyanúja esetén is el kell végezni; valamint

d) az ilyen területeken nem lehetnek engedély nélküli kommunikációs vonalak, engedély nélküli telefonvonalak és más engedély nélküli eszközök és elektromos vagy elektronikus berendezések.

(7) A (6) bekezdés d) pontja ellenére minden kommunikációs, elektromos vagy elektronikus berendezést – mielőtt olyan területen használnák őket, ahol SECRET UE/EU SECRET vagy magasabb szintű minősített adatokat érintő üléseket tartanak vagy munkát végeznek, valamint az EU-minősített adatot fenyegető, nagy kockázatúnak értékelt veszély esetén – először a Bizottság Biztonsági Hatóságának kell megvizsgálnia annak biztosítása érdekében, hogy ilyen berendezés révén véletlenül vagy tiltott módon ne közvetíthessenek értelmezhető adatokat az adott biztonsági területen kívülre.

(8) Azokat a biztonsági területeket, ahol nem tartózkodik napi 24 órán át munkavégző személyzet, adott esetben a rendes munkaidő végén ellenőrizni, valamint a rendes munkaidőn kívül szúrópróbaszerűen ellenőrizni kell, amennyiben az említett területeken nem működik behatolásjelző rendszer.

(9) Biztonsági területeket és technikailag biztosított biztonsági területeket ideiglenesen is fel lehet állítani egy adminisztratív zónán belül, minősített üléshez vagy más hasonló célból.

(10) A Bizottság érintett szervezeti egységének helyi biztonsági tisztviselője biztonsági üzemeltetési eljárásokat dolgoz ki a felelőssége alá tartozó valamennyi biztonsági területre, amelyek ezen határozat és annak végrehajtási szabályai szerint az alábbiakat határozzák meg:

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

b) a fenntartandó ellenőrzési és védelmi intézkedések;

c) a szükséges ismeret elve és biztonsági engedély alapján a területre kíséret nélkül való belépésre engedéllyel rendelkező személyek;

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

e) minden más vonatkozó intézkedés és eljárás.

(11) A biztonsági területeken megerősített helyiségeket kell kialakítani. A Bizottság Biztonsági Hatóságának ellenőriznie kell a falakat, padlókat, plafonokat, ablakokat és zárható ajtókat, amelyek az ugyanilyen minősítési szintű EU-minősített adat tárolásához jóváhagyott tárolóeszköz által nyújtottal egyenértékű védelmet kell biztosítaniuk.

19. cikk

Az EU-minősített adat kezelésére és tárolására vonatkozó fizikai védelmi intézkedések

(1) Az olyan EU-minősített adatot, amely RESTREINT UE/EU RESTRICTED minősítésű, az alábbi helyeken lehet kezelni:

a) biztonsági területen;

b) adminisztratív zónában, amennyiben az EU-minősített adat védelemben részesül az engedéllyel nem rendelkező egyének hozzáférésével szemben; vagy

c) biztonsági területen vagy adminisztratív zónán kívül, amennyiben az adat birtokosa a 31. cikkel összhangban szállítja az EU-minősített adatot, és vállalta, hogy eleget tesz az EU-minősített adatok engedéllyel nem rendelkező személyek általi hozzáféréssel szembeni védelme céljából a végrehajtási szabályokban meghatározott kiegészítő intézkedéseknek.

(2) Az olyan EU-minősített adatot, amely RESTREINT UE/EU RESTRICTED minősítésű, megfelelően zárható irodabútorokban kell tárolni az adminisztratív zónában vagy biztonsági területen. Ideiglenesen adminisztratív zónában vagy biztonsági területen kívül is lehet tárolni, amennyiben az adat birtokosa vállalja, hogy eleget tesz a végrehajtási szabályokban meghatározott kiegészítő intézkedéseknek.

(3) Az olyan EU-minősített adatot, amely CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű, az alábbi helyeken lehet kezelni:

a) biztonsági területen;

b) a, amennyiben az EU-minősített adat védve van az engedéllyel nem rendelkező egyének hozzáférésétől; vagy

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

i. vállalta, hogy eleget tesz az EU-minősített adatok engedéllyel nem rendelkező személyek általi hozzáféréssel szembeni védelme céljából a végrehajtási szabályokban meghatározott kiegészítő intézkedéseknek;

ii. az EU-minősített adatot mindenkor személyes felügyelete alatt tartja; valamint

iii. papíralapú dokumentumok esetében értesítette erről az érintett nyilvántartót.

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

(5) A TRES SECRET UE/EU TOP SECRET minősítésű adatokat a Bizottság Biztonsági Hatósága által felállított és fenntartott, a Bizottság biztonsági akkreditációs hatósága által ezen a szinten akkreditált biztonsági területen kell kezelni.

(6) A TRES SECRET UE/EU TOP SECRET minősítésű adatokat a Bizottság biztonsági akkreditációs hatósága által ezen a szinten akkreditált biztonsági területen az alábbi módok valamelyike szerint kell tárolni:

a) a 18. cikk rendelkezései szerinti biztonsági tárolóeszközben, az alábbiak közül egy vagy több kiegészítő ellenőrzés kíséretében:

1. ellenőrzött biztonsági vagy munkavégző személyzet általi folyamatos védelem vagy ellenőrzés;

2. jóváhagyott behatolásjelző rendszer, a biztonságért felelős elhárító személyzettel együttesen;

vagy

b) behatolásjelző rendszerrel ellátott megerősített helyiségben, a biztonságért felelős elhárító személyzettel együttesen.

20. cikk

Az EU-minősített adatok védelmére szolgáló kulcsok és kombinációk kezelése

(1) Az irodák, termek, megerősített helyiségek és biztonsági tárolóeszközök kulcsainak és kombinációinak kezelésére vonatkozó eljárásokat a végrehajtási szabályokban, az alábbi 60. cikkel összhangban határozzák meg. Ezen eljárások célja a jogosulatlan hozzáféréssel szembeni védelem.

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

a) új tárolóeszköz átvételekor;

b) a kombinációt ismerő személyzet minden változásakor;

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

d) amikor a záron javítást vagy karbantartást végeztek; valamint

e) legalább 12 havonta.

4. FEJEZET

AZ EU-MINŐSÍTETT ADATOK KEZELÉSE

21. cikk

Alapelvek

(1) Valamennyi EU-minősített adatot a dokumentumok kezelésére vonatkozó bizottsági politikának megfelelően kell kezelni és ennélfogva az Európai Bizottság aktáinak közös megőrzési listájával összhangban szükséges azokat nyilvántartásba venni, iktatni, megőrizni és végül megsemmisíteni, mintavételezni vagy a levéltárba szállítani.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű minősített adatokat továbbítás előtt és kézhezvételkor biztonsági célokból nyilvántartásba kell venni. A TRES SECRET UE/EU TOP SECRET minősítésű adatokat erre kijelölt nyilvántartásokban kell kezelni.

(3) A Bizottságon belül a 27. cikk rendelkezéseivel összhangban létre kell hozni az EU-minősített adatok nyilvántartási rendszerét.

(4) A Bizottság Biztonsági Hatóságának rendszeresen ellenőriznie kell azokat a bizottsági szervezeti egységeket és létesítményeket, ahol EU-minősített adatokat kezelnek vagy tárolnak.

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

a) az EU-minősített adatokat – főszabályként – az 5. fejezettel összhangban jóváhagyott, kriptográfiai termékekkel védett elektronikus úton továbbítják;

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

   i. vagy a 5. fejezettel összhangban jóváhagyott kriptográfiai termékekkel védett elektronikus eszközökön (pl. USB-kulcsokon, CD-ken, merevlemezeken); vagy

   ii. bármely egyéb esetben a végrehajtási szabályokban előírt módon.

22. cikk

Minősítések és jelölések

(1) Az adatokat akkor kell minősíteni, ha a titkosságuk biztosításához védelemre van szükség, a 3. cikk (1) bekezdésével összhangban.

(2) Az EU-minősített adatok minősítési szintjének a vonatkozó végrehajtási szabályok, szabványok és a minősítési útmutató szerinti meghatározásáért és a címzettekhez történő kezdeti továbbításáért az adat kibocsátója felel.

(3) Az EU-minősített adatok minősítési szintjét a 3. cikk (2) bekezdésével, valamint a vonatkozó végrehajtási szabályokkal összhangban kell meghatározni.

(4) A minősítést és jelölést egyértelműen és helyesen fel kell tüntetni, tekintet nélkül arra, hogy az EU-minősített adat papír, szóbeli, elektronikus vagy egyéb formájú.

(5) Egy adott dokumentum egyes részei (például oldalai, bekezdései, szakaszai, mellékletei, függelékei, toldalékai és csatolmányai) eltérő minősítést igényelhetnek, és ennek megfelelő jelölést kell kapniuk, többek között az elektronikus formában történő tárolásuk alkalmával.

(6) A dokumentum vagy a fájl egésze a legmagasabb minősítési szintű rész minősítését kapja. Ha egy dokumentumot különböző forrásokból származó adatokból állítanak össze, a kész anyagot a minősítési szint meghatározása céljából át kell nézni, mivel összességében magasabb szintű minősítést igényelhet, mint külön-külön egyes részei külön-külön.

(7) A különböző minősítési szintű részeket tartalmazó dokumentumokat lehetőség szerint úgy kell szerkeszteni, hogy az eltérő minősítésű részek könnyen felismerhetők és szükség esetén leválaszthatók legyenek.

(8) A mellékleteket kísérő levél vagy feljegyzés ugyanolyan minősítést kap, mint legmagasabb minősítési szintű melléklete. A kibocsátónak megfelelő jelöléssel egyértelműen jeleznie kell, hogy a kísérő levél vagy feljegyzés milyen szintű minősítést kap, ha a mellékleteitől elválasztják, például a következő formában:

CONFIDENTIEL UE/EU CONFIDENTIAL

melléklet(ek) nélkül RESTREINT UE/EU RESTRICTED

23. cikk

Jelölések

A 3. cikk (2) bekezdésében meghatározott minősítési jelölések mellett az EU-minősített adatok további jelölésekkel láthatók el, úgymint:

a) kibocsátójelölő-azonosító;

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

c) a kiadhatóságra vonatkozó jelölések;

d) adott esetben azon időpont vagy konkrét esemény, amelyet követően a minősített adat visszaminősíthető vagy a minősítés megszüntethető.

24. cikk

Rövidített minősítési jelölések

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

(2) 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

25. cikk

EU-minősített dokumentumok létrehozása

(1) EU-minősített dokumentum létrehozásakor:

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

b) minden egyes oldalt számozni kell;

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

d) a dokumentumot dátummal kell ellátni;

e) a SECRET UE/EU SECRET és magasabb minősítési szintű dokumentumok minden egyes oldalán fel kell feltüntetni a példány sorszámát, ha azokat több példányban továbbítják.

(2) Amennyiben az EU-minősített adatokra az (1) bekezdés nem alkalmazható, a végrehajtási szabályoknak megfelelő egyéb intézkedéseket kell hozni.

26. cikk

EU-minősített adatok visszaminősítése és a minősítés megszüntetése

(1) Az adat létrehozásakor – amennyiben lehetséges – a kibocsátó jelöli, hogy adott időpontban vagy konkrét eseményt követően az EU-minősített adat visszaminősíthető-e vagy minősítése megszüntethető-e.

(2) Valamennyi bizottsági szervezeti egység rendszeresen felülvizsgálja az általa kibocsátott EU-minősített adatokat annak megállapítására, hogy minősítésük még érvényes-e. A végrehajtási szabályok kialakítanak egy rendszert a Bizottság által kibocsátott, nyilvántartásban lévő EU-minősített adatok minősítési szintjének legalább ötévenkénti felülvizsgálatára. Nincs szükség ilyen felülvizsgálatra akkor, ha a kibocsátó már kezdetben jelezte, hogy az adatot automatikusan vissza fogják minősíteni vagy a minősítését meg fogják szüntetni, és az adatot ennek megfelelően jelölték.

(3) A Bizottság által kibocsátott, RESTREINT UE/EU RESTRICTED minősítésű adatok minősítése harminc év után automatikusan megszüntetettnek tekintendő a Tanács 1700/2003/EK, Euratom rendelet által módosított 354/83/EGK, Euratom rendelettel ([1]) összhangban.

27. cikk

Az EU-minősített adatok bizottsági nyilvántartási rendszere

(1) Az alábbi 52. cikk (5) bekezdése sérelme nélkül a Bizottság minden szervezeti egységénél, amely EU-minősített adatokat CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szinten kezel vagy tárol, az EU-minősített adatok nyilvántartásáért felelős helyi hivatalokat kell kialakítani, amelyek biztosítják, hogy az EU-minősített adatok kezelése e határozattal összhangban történjen.

(2) A Főtitkárság által irányított EU-minősített adatokat nyilvántartó hivatal a Bizottság EU-minősített adatokat nyilvántartó központi hivatala. Az alábbi szerepeket tölti be:

— a Bizottság Főtitkárságának EU-minősített adatokat nyilvántartó helyi hivatala;

— a bizottsági tagok kabinetjének EU-minősített adatokat nyilvántartó hivatala, amennyiben nincs EU-minősített adatokat nyilvántartó kijelölt helyi hivatala;

— azon Főigazgatóságok vagy szolgálatok EU-minősített adatokat nyilvántartó hivatala, amelyek nem rendelkeznek EU-minősített adatokat nyilvántartó helyi hivatallal;

— a Bizottság és szolgálatai, valamint harmadik államok és nemzetközi szervezetek, és amennyiben különös rendelkezések úgy rendelkeznek, egyéb uniós intézmények, ügynökségek és szervek között kicserélt RESTREINT UE/EU RESTRICTED minősítésű adatok – ideértve legfeljebb a SECRET UE/EU SECRET minősítésű adatokat is – fő beérkezési és kiküldési helye.

(3) A Bizottságon belül a Bizottság Biztonsági Hatóságának ki kell jelölnie a TRES SECRET UE/EU TOP SECRET minősítésű adatok központosított kézhez vételével és elosztásával megbízott nyilvántartót. Szükség esetén ennek alárendelt nyilvántartók is kijelölhetők ezen adatok nyilvántartására és kezelésére.

(4) Az alárendelt nyilvántartók nem továbbíthatnak közvetlenül TRES SECRET UE/EU TOP SECRET dokumentumokat az ugyanazon TRES SECRET UE/EU TOP SECRET minősítéssel rendelkező, központi nyilvántartóhoz tartozó többi alárendelt nyilvántartó számára vagy kifelé e központi nyilvántartó kifejezett írásbeli jóváhagyása nélkül.

(5) Az EU-minősített adatokat nyilvántartó hivatalokat a 3. fejezetnek megfelelően biztonsági területként kell kialakítani, és azokat a Bizottság Biztonsági Akkreditációs Hatóságának akkreditálnia kell.

28. cikk

Nyilvántartó hivatalt ellenőrző tisztviselő

(1) Az EU-minősített adatokat nyilvántartó minden egyes hivatalt a nyilvántartó hivatalt ellenőrző tisztviselő irányítja.

(2) A nyilvántartó hivatalt ellenőrző tisztviselő megfelelő biztonsági ellenőrzésen esik át.

(3) A nyilvántartó hivatalt ellenőrző tisztviselő az EU minősített dokumentumok kezelésére vonatkozó rendelkezések alkalmazását és a megfelelő biztonsági intézkedések betartását illetően a Bizottság szervezeti egységének helyi biztonsági tisztviselőjének felügyelete alá tartozik.

(4) A nyilvántartó hivatalt ellenőrző tisztviselő a rábízott EU-minősített adatokat nyilvántartó hivatal irányítását illető felelősségi körén belül ezen határozat és a vonatkozó végrehajtási szabályok, szabványok és útmutató szerint a következő alapvető feladatokat látja el:

— az adatok nyilvántartásba vételével, megőrzésével, sokszorosításával, fordításával, továbbításával, elküldésével és megsemmisítésével vagy az EU-minősített adatok levéltári szolgálatának való átadásával kapcsolatos igazgatási feladatok ellátása;

— az adatok minősítésének további fenntartására vonatkozó szükségesség időközönkénti ellenőrzése;

— az EU-minősített adatok védelmével összefüggő vagy a végrehajtási szabályokban meghatározott egyéb feladatok ellátása.

29. cikk

Az EU-minősített adatok biztonsági célú nyilvántartásba vétele

(1) E határozat alkalmazásában a biztonsági célú nyilvántartásba vétel (a továbbiakban: nyilvántartásba vétel) olyan eljárások alkalmazása, amelyek során rögzítésre kerül az EU-minősített adatok életciklusa, beleértve a terjesztését is.

([1]) A Tanács 2003. szeptember 22-i 1700/2003/EK, EURATOM rendelete az Európai Gazdasági Közösség és az Európai Atomenergia-közösség levéltárainak a nyilvánosság számára történő megnyitásáról szóló 354/83/EGK, Euratom rendelet módosításáról (HL L 243., 2003.9.27., 1. o.).

(2) Valamennyi CONFIDENTIEL UE/EU CONFIDENTIAL és annál magasabb minősítésű adatot és anyagot a szervezeti egységhez való beérkezés vagy onnan történő elküldés alkalmával külön erre a célra szolgáló nyilvántartásokban kell kezelni.

(3) Ha az EU-minősített adatokat a kommunikációs és információs rendszer segítségével kezelik vagy tárolják, a nyilvántartási eljárások a kommunikációs és információs rendszerbeli folyamatok keretében is elvégezhetők.

(4) Az EU-minősített adatok biztonsági célú nyilvántartásba vételével kapcsolatos részletesebb rendelkezéseket a végrehajtási szabályokban határozzák meg.

30. cikk

Az EU-minősített dokumentumok másolása és fordítása

(1) TRES SECRET EU/EU TOP SECRET minősítésű dokumentumok kizárólag a kibocsátó előzetes írásbeli hozzájárulásával másolhatók vagy fordíthatók le.

(2) Amennyiben a SECRET UE/EU SECRET és ennél alacsonyabb minősítésű dokumentumok kibocsátója a másolásra vagy fordításra vonatkozóan nem szab korlátozásokat, e dokumentumok a titokbirtokos utasítására másolhatók vagy fordíthatók.

(3) Az eredeti dokumentumra vonatkozó biztonsági intézkedéseket a másolatokra és a fordításokra is alkalmazni kell.

31. cikk

Az EU-minősített adatok szállítása

(1) Az EU-minősített adatokat úgy kell szállítani, hogy azok a szállítás közben védve legyenek az illetéktelen hozzáféréstől.

(2) Az EU-minősített adatok szállítására a védelmi intézkedések vonatkoznak, amelyek:

— a szállított EU-minősített adatok minősítési szintjével arányosak; és

— a szállítmány egyedi feltételeihez igazodnak, különösen annak függvényében, hogy szállítanak-e EU-minősített adatokat:

  — bizottsági épületen vagy zárt épületcsoporton belül;

  — azonos tagállamban található bizottsági épületek között;

  — az Unión belül;

  — az Unióból valamely harmadik állam területére; és

  — az EU-minősített adatok jellegéhez és formájához igazodnak.

(3) Ezen védelmi intézkedéseket a végrehajtási szabályokban vagy, a 42. cikkben említett projektek és programok esetén, a vonatkozó program vagy projektbiztonsági utasítások szerves részeként részletesen meghatározzák.

(4) A végrehajtási szabályok vagy program vagy projektbiztonsági utasítások az EU-minősített adatok szintjével arányos rendelkezéseket tartalmaznak az alábbiak tekintetében:

— szállítási típus, például kézi szállítás, katonai vagy diplomáciai futár útján történő szállítás, postaszolgálatok vagy kereskedelmi futárszolgálatok útján történő szállítás;

— az EU-minősített adatok csomagolása;

— elektronikus eszközökön szállított EU-minősített adatok számára kialakított technikai ellenintézkedések;

— bármely más eljárási, fizikai vagy elektronikus intézkedés;

— nyilvántartásba vételi eljárások;

— biztonsági engedéllyel rendelkező személyzet használata.

(5) Az EU-minősített adatok elektronikus eszközökön történő szállítása során – a 21. cikk (5) bekezdésétől eltérően – a vonatkozó végrehajtási szabályokban meghatározott védelmi intézkedéseket – az elvesztés vagy az illetéktelen tudomására jutás kockázatának minimalizálása érdekében – kiegészíthetik a Bizottság Biztonsági Hatósága által elfogadott, megfelelő technikai ellenintézkedések.

32. cikk

Az EU-minősített adatok megsemmisítése

(1) A már nem szükséges EU-minősített dokumentumok a levéltárakra vonatkozó rendeletek, valamint a dokumentumok kezelésére és archiválására vonatkozó bizottsági szabályok és rendeletek, különösen a közös megőrzési lista figyelembevételével megsemmisíthetők.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb szintű EU-minősített adatokat az EU-minősített adatok nyilvántartásáért felelős hivatal ellenőrző tisztviselője semmisíti meg az adat birtokosa vagy az illetékes hatóság utasítására. A nyilvántartó hivatalt ellenőrző tisztviselő ennek megfelelően aktualizálja az iktatókönyveket és egyéb nyilvántartásokat.

(3) A SECRET UE/EU SECRET vagy TRES SECRET UE/EU TOP SECRET minősítésű dokumentumok esetében a nyilvántartó hivatalt ellenőrző tisztviselő által végrehajtott ezen megsemmisítést olyan tanú jelenlétében kell végrehajtani, aki a megsemmisítendő dokumentum minősítési szintjével legalább megegyező minősítési szintű adatok megismerésére jogosító személyi biztonsági tanúsítvánnyal rendelkezik.

(4) Az ügykezelő és – amennyiben annak jelenléte kötelező – a tanú aláírja a megsemmisítési jegyzőkönyvet, amelyet a nyilvántartóban kell iktatni. Az EU-minősített adatok nyilvántartásáért felelős hivatal ellenőrző tisztviselője a megsemmisítési jegyzőkönyveket TRES SECRET UE/EU TOP SECRET minősítésű dokumentumok esetében legalább tíz évig, a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű dokumentumok esetében pedig legalább öt évig őrzi meg.

(5) A minősített dokumentumokat – ideértve a RESTREINT UE/EU RESTRICTED minősítéssel rendelkezőket is – a végrehajtási szabályokban meghatározott és a vonatkozó uniós vagy az ezzel egyenértékű szabványoknak megfelelő módszerekkel kell megsemmisíteni.

(6) Az EU-minősített adatok tárolására szolgáló számítógépes adathordozókat a végrehajtási szabályokban meghatározott eljárásokkal összhangban kell megsemmisíteni.

33. cikk

Az EU-minősített adatok vészhelyzetben történő megsemmisítése

(1) Az EU-minősített adatok birtokában levő bizottsági szervezeti egységek a helyi feltételek alapján terveket dolgoznak ki az EU minősített anyagok válsághelyzetben történő védelmére, beleértve adott esetben a vészhelyzeti megsemmisítési és kiürítési terveket is. Kiadják az annak megakadályozására szükségesnek ítélt utasításokat, hogy az EU-minősített információk illetéktelen személyek kezébe kerülhessenek.

(2) A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET anyagok válsághelyzetben történő védelmére és/vagy megsemmisítésére irányuló intézkedések semmilyen körülmények között sem akadályozhatják az olyan TRES SECRET UE/EU TOP SECRET anyagok – a kriptográfiai berendezéseket is beleértve – védelmét vagy megsemmisítését, amelyek ellátása minden más feladattal szemben elsőbbséget élvez.

(3) Vészhelyzet esetén, ha illetéktelen hozzáférés közvetlen kockázata áll fenn, a tulajdonosnak meg kell semmisítenie az EU-minősített adatokat úgy, hogy azokat sem részben, sem egészben ne lehessen helyreállítani. A nyilvántartásba vett EU-minősített adatok vészhelyzeti megsemmisítéséről tájékoztatni kell az adatok kibocsátóját és a származási nyilvántartót.

(4) Az EU-minősített adatok megsemmisítésével kapcsolatos részletesebb rendelkezéseket a végrehajtási szabályokban kell meghatározni.

5. FEJEZET

AZ EU-MINŐSÍTETT ADATOK VÉDELME A KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZERBEN

34. cikk

Információvédelmi alapelvek

(1) Az információvédelem a kommunikációs és információs rendszerek tekintetében azt jelenti, hogy az ilyen rendszerek megvédik az általuk kezelt adatot, továbbá a szükséges módon, a szükséges időben, a jogszerű felhasználók ellenőrzése alatt működnek.

(2) A hatékony információvédelem az alábbi tényezők megfelelő szintjét biztosítja:

Hitelesség: annak garanciája, hogy az információ valódi és *jóhiszemű* forrásokból származik;

Elérhetőség: 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 eszközök és információ hitelességének és teljességének védelme;

Letagadhatatlanság: egy cselekmény vagy esemény megtörténtének bizonyíthatósága annak érdekében, hogy ezt a cselekedetet vagy eseményt később ne lehessen letagadni.

(3) Az információvédelem kockázatkezelési eljáráson alapul.

35. cikk

Fogalommeghatározások

E fejezet alkalmazásában az alábbi meghatározásokat kell alkalmazni:

a) „akkreditáció": az a hivatalos engedély és jóváhagyás, amelyet a Biztonsági Akkreditációs Hatóság egy kommunikációs és információs rendszer számára kiad, hogy működési környezetében EU minősített információkat kezelhessen a biztonsági terv hivatalos jóváhagyását és annak helyes végrehajtását követően;

b) „akkreditációs eljárás": a Biztonsági Akkreditációs Hatóság akkreditálását megelőzően szükséges lépések és feladatok. Ezen lépéseket és feladatokat az akkreditációs eljárás szabványában határozzák meg;

c) „kommunikációs és információs rendszer": 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 információs forrásokat;

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

e) „kockázat": annak valószínűsége, hogy egy adott fenyegetés kihasználja valamely szervezet vagy az általa használt rendszerek bármelyikének belső, illetve külső sebezhetőségét, és ezáltal kárt okoz az adott szervezetnek, illetve kárt tesz annak tárgyi eszközeiben vagy immateriális javaiban. Mérése a fenyegetések bekövetkezése valószínűségének és hatásának kombinációjával történik.

f) „kockázatelfogadás": a kockázatkezelést követően fennmaradó kockázat további meglétéhez való hozzájárulásra vonatkozó határozat;

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

h) „kockázatkommunikáció": a kommunikációs és információs rendszer felhasználói közösségei körében a kockázatokkal kapcsolatos tudatosság növelése, a jóváhagyó hatóságok tájékoztatása a kockázatokról és jelentéstétel azokról a működtető hatóságok részére;

i) „kockázatkezelés": a kockázat (megfelelő technikai, fizikai, szervezeti vagy eljárási intézkedések kombinálásával történő) enyhítése, megszüntetése, csökkentése, illetve annak átruházása vagy figyelemmel kísérése.

36. cikk

Az EU-minősített adatokat kezelő kommunikációs és információs rendszer

(1) A kommunikációs és információs rendszer az információvédelem koncepciójával összhangban kezeli az EU-minősített adatokat.

(2) Az EU-minősített adatokat kezelő kommunikációs és információs rendszer tekintetében C(2006) 3602 bizottsági határozatban ([1]) említett, az információs rendszerek biztonságával kapcsolatos bizottsági politikának való megfelelés az alábbiakat vonja maga után:

a) Tervezés-Megvalósítás-Ellenőrzés-Intézkedés szemléletet az információs rendszerek biztonságával kapcsolatos politika végrehajtásakor, az információs rendszer teljes életciklusa alatt alkalmazni kell;

b) a biztonsági igényeket üzleti hatásvizsgálat által kell azonosítani;

c) az információs rendszert és az abban foglalt adatokat hivatalos adatvagyon-minősítésnek kell alávetni;

([1]) Az Európai Bizottság 2006. augusztus 16-i C(2006) 3602 határozata az Európai Bizottság informatikai rendszereinek biztonságára vonatkozó szabályokról.

d) az információs rendszerek biztonságával kapcsolatos politika alapján meghatározott valamennyi kötelező biztonsági intézkedést végre kell hajtani;

e) kockázatkezelési eljárást kell alkalmazni, amely a következő lépésekből áll: a fenyegetések és sebezhetőségek azonosítása, kockázatértékelés, kockázatkezelés, kockázatelfogadás és kockázatkommunikáció;

f) biztonsági politikát és biztonsági üzemeltetési eljárásokat tartalmazó biztonsági terv meghatározása, végrehajtása, ellenőrzése és felülvizsgálata.

(3) Az EU-minősített adatokat kezelő kommunikációs és információs rendszer tervezésében, fejlesztésében, vizsgálatában, üzemeltetésében, irányításában vagy használatában részt vevő minden munkatárs valamennyi lehetséges biztonsági hiányosságról, incidensről, a biztonság megsértéséről illetve az adatok illetéktelen tudomására jutásáról értesíti a Biztonsági Akkreditációs Hatóságot, amely a kommunikációs és információs rendszer és/vagy az abban foglalt EU-minősített adatok védelmére hatással lehet.

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

a) előnyben kell részesíteni azon termékeket, amelyeket a Tanács vagy a Tanács Főigazgatósága a Tanács kriptográfiai jóváhagyó hatóságának minőségében, a Bizottság biztonsági szakértői csoportjának ajánlására jóváhagyott;

b) A kriptográfiai jóváhagyó hatóság – konkrét működési indokok alapján – a Bizottság biztonsági szakértői csoportjának ajánlására figyelmen kívül hagyhatja az a) pontban említett követelményeket és meghatározott időtartamra ideiglenes jóváhagyást biztosíthat.

(5) EU-minősített adatok elektronikus eszközökkel történő továbbítása, feldolgozása és tárolása során jóváhagyott kriptográfiai termékeket kell használni. E követelmény ellenére szükséghelyzet vagy a kriptográfiai jóváhagyó hatóság által történő jóváhagyást követő speciális technikai konfigurációk esetén különleges eljárások alkalmazhatók.

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

(7) A Bizottság Biztonsági Hatósága az alábbi szerepeket tölti be:

— információvédelmi hatóság;

— Biztonsági akkreditációs hatóság;

— TEMPEST-hatóság;

— Kriptográfiai jóváhagyó hatóság;

— Kriptográfiai terjesztési hatóság.

(8) A Bizottság Biztonsági Hatósága minden rendszer esetén kijelöli az információvédelmi üzemeltetési hatóságot.

(9) A (7) és (8) bekezdésben ismertetett szerepek kötelezettségeit a végrehajtási szabályokban határozzák meg.

37. cikk

Az EU-minősített adatokat kezelő kommunikációs és információs rendszer akkreditálása

(1) Az EU-minősített adatokat kezelő valamennyi kommunikációs és információs rendszer az információvédelmi elvek alapján akkreditálási eljáráson megy keresztül, amelynek részletessége a szükséges védelmi szinttel arányos.

(2) Az akkreditálási eljárás magában foglalja a kommunikációs és információs rendszer vonatkozó biztonsági tervének a Bizottság Biztonsági Akkreditációs Hatósága általi hivatalos jóváhagyását az alábbiak biztosítása érdekében:

a) a 36. cikk (2) bekezdésében említett kockázatkezelési eljárást megfelelő módon teljesítették;

b) a rendszertulajdonos tudatosan elfogadta a fennmaradó kockázatot; és

c) ezen határozattal összhangban elérték a kommunikációs és információs rendszer, valamint a benne kezelt EU-minősített adatok megfelelő védelmi szintjét.

(3) A Bizottság Biztonsági Akkreditációs Hatósága akkreditációs nyilatkozatot ad ki, amely meghatározza az EU-minősített adatoknak azt a megengedett legmagasabb minősítési szintjét, amelyet a kommunikációs és információs rendszer kezelhet, valamint az üzemeltetéshez kapcsolódó feltételeket. Ez nem érinti az 512/2014/EU európai parlamenti és tanácsi rendelet ([1]) 11. cikkében meghatározott, a Biztonsági Akkreditációs Tanácsra ruházott feladatokat.

(4) Egy közös Biztonsági Akkreditációs Tanács felel a Bizottság számos felet magában foglaló kommunikációs és információs rendszerének akkreditálásáért. A Biztonsági Akkreditációs Tanács a részt vevő összes tagállam biztonsági akkreditációs hatóságának képviselőiből áll, és ülésein részt vesz a Bizottság biztonsági akkreditációs hatóságának egy képviselője.

(5) Az akkreditálási eljárás az érintett felek által ellátandó feladatok egész sorából áll. Az akkreditálási iratok és dokumentáció elkészítésének felelőssége teljes mértékben a kommunikációs és információs rendszer tulajdonosát terheli.

(6) Az akkreditálásért a Bizottság Biztonsági Akkreditációs Hatósága felel, amelynek a kommunikációs és információs rendszer életciklusának bármely pillanatában joga van az alábbiakhoz:

a) akkreditálási eljárás alkalmazásának előírása;

b) a kommunikációs és információs rendszer ellenőrzése vagy kivizsgálása;

c) ha az üzemeltetési feltételek többé nem teljesülnek, egy biztonsági fejlesztési terv meghatározásának és világosan meghatározott időn belül történő hatékony végrehajtásának előírása, a kommunikációs és információs rendszer üzemeltetési engedélyének az üzemeltetési feltételek újbóli teljesüléséig történő esetleges visszavonása mellett.

(7) Az akkreditálási eljárást az EU-minősített adatokat kezelő kommunikációs és információs rendszer akkreditálási eljárásának szabványában kell létrehozni, amelyet a C(2006) 3602 határozat 10. cikkének (3) bekezdésével összhangban kell jóváhagyni.

38. cikk

Szükséghelyzet

(1) Az e fejezetben foglalt rendelkezések ellenére, szükséghelyzetben – például fenyegető vagy ténylegesen fennálló válság-, konfliktus- vagy háborús helyzetben – vagy rendkívüli üzemeltetési körülmények között az alábbiakban leírt különös eljárások alkalmazhatók.

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

a) a küldő, illetve a címzett nem rendelkezik az előírt rejtjelezési lehetőséggel; valamint

b) a minősített anyag más eszközökkel nem továbbítható időben.

(3) A 1. pontban meghatározott körülmények esetén továbbított minősített adat nem látható el olyan jelöléssel vagy jelzéssel, amely azt a nem minősített adatoktól vagy elérhető kriptográfiai eszköz által védhető adattól megkülönbözteti. A címzetteket késedelem nélkül, egyéb módon értesíteni kell a minősítési szintről.

(4) Ezt követően jelentést kell tenni az illetékes hatóságnak és a Bizottság biztonsági szakértői csoportjának.

6. FEJEZET

IPARI BIZTONSÁG

39. cikk

Alapelvek

(1) Az iparbiztonság az EU-minősített adatok védelmét biztosító intézkedések alkalmazása

a) minősített szerződések keretén belül

   i. a részvételre jelentkezők vagy ajánlattevők által, a pályázati és szerződéskötési eljárás során;

   ii. a vállalkozók vagy alvállalkozók által, a minősített szerződések életciklusa során;

([1]) Az Európai Parlament és a Tanács 2014. április 16-i 512/2014/EU rendelete az Európai GNSS Ügynökség létrehozásáról szóló 912/2010/EU rendelet módosításáról (HL L 150., 2014.5.20., 72. o.).

b) minősített támogatási megállapodások keretén belül,

i. a pályázók által, a támogatás-odaítélési eljárások során;

ii. a kedvezményezettek által, a minősített támogatási megállapodások életciklusa során.

(2) Az ilyen szerződések vagy támogatási megállapodások nem foglalhatnak magukban TRES SECRET UE/EU TOP SECRET szintű minősített adatot.

(3) Eltérő rendelkezés hiányában ezen fejezet minősített szerződésekre vagy vállalkozókra vonatkozó rendelkezéseit a minősített alvállalkozói szerződésekre vagy alvállalkozókra is alkalmazni kell.

40. cikk

Fogalommeghatározások

E fejezet alkalmazásában a következő fogalom-meghatározások alkalmazandóak:

a) „minősített szerződés": az 1605/2002/EK, Euratom tanácsi rendeletben ([1]) említett, a Bizottság vagy egyik szervezeti egysége által egy vállalkozóval ingó vagy ingatlan eszközök szállítása, munkák kivitelezése vagy szolgáltatások nyújtása céljából kötött keretszerződés vagy szerződés, amelynek teljesítése EU-minősített adatok létrehozását, kezelését vagy tárolását teszi szükségessé vagy foglalja magában.

b) „minősített alvállalkozói szerződés": a Bizottság vagy egyik szervezeti egysége által egy másik vállalkozóval (azaz alvállalkozóval) ingó vagy ingatlan eszközök szállítása, munkálatok elvégzése vagy szolgáltatások nyújtása céljából kötött szerződés, amelynek teljesítése EU-minősített adatok létrehozását, kezelését vagy tárolását teszi szükségessé vagy foglalja magában;

c) „minősített támogatási megállapodás": egy megállapodás, amelynek keretében az 1605/2002/EK, Euratom tanácsi rendelet I. részének VI. címében említettek szerint a Bizottság támogatást ítél oda, amelynek teljesítése EU-minősített adatok létrehozását, kezelését vagy tárolását teszi szükségessé vagy foglalja magában;

d) „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 elvégezheti.

41. cikk

A minősített szerződésekre vagy támogatási megállapodásokra vonatkozó eljárás

(1) A Bizottság minden egyes szervezeti egysége – mint ajánlatkérő – a minősített szerződések vagy támogatási megállapodások odaítélésekor gondoskodik arról, hogy az iparbiztonság e fejezetben meghatározott minimumszabályait a szerződésbe belefoglalják vagy abban azokra utalás történjen, valamint, hogy e szabályokat betartsák.

(2) Az (1) bekezdés alkalmazásában a Bizottság illetékes szolgálatai kikérik a Humánerőforrásügyi és Biztonsági Főigazgatóság és különösen annak Biztonsági Igazgatóságának véleményét, és biztosítják, hogy a vállalkozói és alvállalkozói mintaszerződések és támogatási mintamegállapodások a vállalkozók és alvállalkozók, illetve a támogatási megállapodások kedvezményezettjei által betartandó, az EU-minősített adatok védelmére vonatkozó alapelveket és minimumszabályokat tükröző rendelkezéseket tartalmaznak.

(3) A Bizottság szorosan együttműködik a nemzeti biztonsági hatósággal, a kijelölt biztonsági hatósággal és az érintett tagállamok más illetékes hatóságával.

(4) Amennyiben egy ajánlatkérő egy minősített szerződés vagy támogatási megállapodás megkötésére irányuló eljárást tervez elindítani, az eljárás minősített jellegével és az eljárás elemeivel kapcsolatban az eljárás valamennyi szakaszában kikéri a Bizottság Biztonsági Hatóságának véleményét.

(5) A minősített vállalkozói és alvállalkozói szerződésekre, minősített támogatási megállapodásokra, szerződési hirdetményekre, telephely-biztonsági tanúsítvány használatát előíró körülményekre vonatkozó iránymutatásra, program vagy projektbiztonsági utasításokra, a biztonsági vonatkozások záradékára, a látogatásokra, az EU-minősített adatok minősített szerződések és minősített támogatási megállapodások alapján történő továbbítására és szállítására vonatkozó sablonokat és mintákat az iparbiztonsággal kapcsolatos végrehajtási szabályokban kell meghatározni, a Bizottság biztonsági szakértői csoportjával folytatott konzultációt követően.

([1]) A Tanács 2002. június 25-i 1605/2002/EK, Euratom rendelete az Európai Közösségek általános költségvetésére alkalmazandó költségvetési rendeletről (HL L 248., 2002.9.16., 1. o.).

(6) A Bizottság minősített szerződést vagy támogatási megállapodást köthet, amely az EU-minősített adatokhoz való hozzáféréssel, vagy azok kezelését vagy tárolását magában foglaló vagy azzal járó feladatokkal bízhat meg egy tagállamban vagy olyan harmadik államban bejegyzett gazdasági szereplőt, amellyel a Bizottság ezen határozat 7. fejezete szerinti megállapodást vagy igazgatási megállapodást fogadott el.

42. cikk

A minősített szerződésben vagy támogatási megállapodásban található biztonsági elemek

(1) A minősített szerződések és támogatási megállapodások az alábbi biztonsági elemeket tartalmazzák:

A programra vagy projektre vonatkozó biztonsági utasítások

a) „A programra vagy projektre vonatkozó biztonsági utasítások": adott programra vagy projektre alkalmazandó biztonsági eljárások felsorolása a biztonsági eljárások egységesítése céljából. A felsorolás a program vagy projekt teljes időtartama alatt felülvizsgálható.

b) A Humánerőforrásügyi és Biztonsági Főigazgatóság programra vagy projektre vonatkozó általános biztonsági utasításokat dolgoz ki, az EU-minősített adatok kezelését vagy tárolását magában foglaló programokért vagy projektekért felelős bizottsági szervezeti egységek adott esetben programra vagy projektre vonatkozó külön biztonsági utasításokat dolgozhat ki, amelyek a programra vagy projektre vonatkozó általános biztonsági utasításokon alapulnak.

c) A programra vagy projektre vonatkozó külön biztonsági utasításokat különösen a jelentős hatókörű, mértékű vagy komplexitású vagy a nagyszámú és/vagy sokféle vállalkozót, kedvezményezettet és más partnert és érdekelt felet magában foglaló programok és projektek esetén kell kidolgozni, például azok jogállására vonatkozóan. A programra vagy projektre vonatkozó külön biztonsági utasításokat a programot vagy projektet irányító bizottsági szervezeti egység(ek) a Humánerőforrásügyi és Biztonsági Főigazgatósággal szoros együttműködésben dolgozzák ki.

d) A Humánerőforrásügyi és Biztonsági Főigazgatóság a programra vagy projektre vonatkozó általános, illetve külön biztonsági utasításokat is benyújtja a Bizottság biztonsági szakértői csoportjának tanácsadás céljából.

Biztonsági vonatkozások záradéka

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

b) A szerződésspecifikus biztonsági követelményeket biztonsági mellékletben (SAL) kell leírni. Adott esetben a biztonsági vonatkozások záradéka tartalmazza az biztonsági minősítési útmutatót, és a minősített vállalkozói vagy alvállalkozói szerződésnek vagy támogatási megállapodásnak szerves részét képezi;

c) A biztonsági vonatkozások záradéka tartalmazza a vállalkozók vagy kedvezményezettek részére az e határozatban foglalt minimumszabályok teljesítését előíró rendelkezéseket. Az ajánlatkérő biztosítja, hogy a biztonsági vonatkozások záradéka jelezze, hogy a minimumszabályok be nem tartása elegendő indokot jelenthet a szerződés vagy a támogatási megállapodás felbontására.

(2) A programra vagy projektre vonatkozó biztonsági utasítások és a biztonsági vonatkozások záradéka is kötelező biztonsági elemként tartalmazza a biztonsági minősítési útmutatót:

a) „Biztonsági minősítési útmutató": olyan dokumentum, amely – az alkalmazandó biztonsági minősítési szinteket meghatározva – leírja egy program, projekt, szerződés vagy támogatási megállapodás minősített elemeit. A biztonsági minősítési útmutató kiterjeszthető a program, projekt, szerződés vagy támogatási megállapodás teljes időtartamára, az egyes információk pedig újraosztályozhatók, illetve alacsonyabb szintbe sorolhatók; amennyiben létezik biztonsági minősítési útmutató, az a biztonsági vonatkozások záradékának része kell, hogy legyen.

b) A pályázati felhívás kiírását vagy a minősített szerződés odaítélését megelőzően a Bizottság szervezeti egysége ajánlatkérőként meghatározza a részvételre jelentkezők és ajánlattevők vagy vállalkozók részére nyújtandó bármely adat biztonsági minősítését, valamint a vállalkozó által létrehozandó bármely adat biztonsági minősítését. E célból a Bizottság szervezeti egysége a szerződés teljesítése során alkalmazandó biztonsági minősítési útmutató készít e határozattal és annak végrehajtási szabályaival összhangban, a Bizottság Biztonsági Hatóságával folytatott konzultációt követően.

c) A minősített szerződés különféle elemeire vonatkozó biztonsági minősítések meghatározása érdekében az alábbi elveket kell alkalmazni:

i. a biztonsági minősítési útmutató elkészítése során a Bizottság szervezeti egységének mint ajánlatkérőnek figyelembe kell vennie valamennyi vonatkozó biztonsági szempontot, ideértve a nyújtott adathoz rendelt és az adat kibocsátója által a szerződéshez való használatra jóváhagyott biztonsági minősítést;

ii. a szerződés minősítésének általános szintje nem lehet alacsonyabb bármely elemének legmagasabb minősítési szintjénél; valamint

iii. adott esetben az ajánlatkérő a Bizottság Biztonsági Hatóságán keresztül kapcsolatba lép a tagállamok nemzeti biztonsági hatóságaival, kijelölt biztonsági hatóságaival vagy más érintett illetékes biztonsági hatósággal, egy szerződés teljesítése során a vállalkozók által létrehozott vagy azok részére nyújtott adat minősítését érintő bármilyen változás esetén és a biztonsági minősítési útmutató bármilyen további változása esetén.

43. cikk

A vállalkozók és kedvezményezettek alkalmazottainak EU-minősített adatokhoz való hozzáférése

Az ajánlatkérő vagy támogatást nyújtó hatóság biztosítja, hogy a minősített szerződés vagy minősített támogatási megállapodás rendelkezéseket tartalmaz, amelyek feltüntetik, hogy egy vállalkozó, alvállalkozó vagy kedvezményezett olyan alkalmazottja számára, akinek a minősített szerződés teljesítéséhez szüksége van az EU-minősített adatokhoz való hozzáférésre, a hozzáférés csak akkor adható meg, ha:

a) a megfelelő szintű biztonsági engedéllyel rendelkezik vagy más módon megfelelő felhatalmazást kapott „szükséges ismereteinek” meghatározásával;

b) tájékoztatást kaptak az EU-minősített adatok védelme esetén alkalmazandó biztonsági szabályokról és eljárásokról, és tudomásul vették az ilyen adatok védelmével kapcsolatos felelősségüket.

c) a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférés érdekében átestek adott nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság megfelelő szintű biztonsági ellenőrzésén.

44. cikk

Telephely-biztonsági tanúsítvány

(1) „Telephely-biztonsági tanúsítvány”: annak a nemzeti biztonsági hatóság vagy kijelölt biztonsági hatóság vagy bármely más illetékes 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.

(2) A tagállam nemzeti biztonsági hatósága vagy kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatósága által kibocsátott telephely-biztonsági tanúsítványt, amely annak jelzésére szolgál, hogy – a nemzeti törvényekkel és rendeletekkel összhangban – egy gazdasági szereplő képes az EU-minősített adatnak a telephelyükön, megfelelő minősítési szinten (CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET) való védelmére, be kell mutatni a Bizottság Biztonsági Hatóságának, amely továbbítja azt az ajánlatkérő vagy támogatást nyújtó hatóságként eljáró bizottsági szervezeti egységének, mielőtt egy részvételre jelentkező, ajánlattevő vagy vállalkozó, illetve támogatást kérelmező vagy kedvezményezett számára az EU-minősített adathoz való hozzáférést biztosítanák vagy engedélyeznék.

(3) Adott esetben az ajánlatkérő a Bizottság Biztonsági Hatóságán keresztül értesíti a megfelelő nemzeti vagy kijelölt biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot, hogy a szerződés teljesítéséhez telephely-biztonsági tanúsítványra van szükség. Telephely-biztonsági tanúsítványra vagy személyi biztonsági tanúsítványra akkor van szükség, ha a közbeszerzés vagy a támogatás-odaítélési eljárás során CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatot kell átadni.

(4) Az ajánlatkérő vagy támogatást nyújtó hatóság nem köthet minősített szerződést vagy támogatási megállapodást a megfelelőnek tartott pályázóval vagy résztvevővel azt megelőzően, hogy kézhez kapná az érintett vállalkozó vagy alvállalkozó bejegyzésének helye szerinti tagállam nemzeti biztonsági hatósága, kijelölt biztonsági hatósága által kiállított megerősítést arról, hogy szükség szerint megfelelő telephely-biztonsági tanúsítvánnyal rendelkeznek.

(5) Ha a telephely-biztonsági tanúsítványt kibocsátó nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság a Bizottság Biztonsági Hatóságát a telephely-biztonsági tanúsítványt érintő bármely változásról értesíti, a Bizottság Biztonsági Hatósága tájékoztatja az ajánlatkérő vagy támogatást nyújtó hatóságként eljáró bizottsági szervezeti egységet. Alvállalkozói szerződés esetén a nemzeti vagy kijelölt biztonsági hatóságot, illetve bármely egyéb illetékes biztonsági hatóságot ennek megfelelően tájékoztatni kell.

(6) A telephely-biztonsági tanúsítványnak az adott nemzeti vagy kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság általi visszavonása elegendő indokot szolgáltat az ajánlatkérőnek a minősített szerződés megszüntetésére vagy a részvételre jelentkezőnek, ajánlattevőnek vagy a pályázónak versenyből való kizárására. Az ilyen értelmű rendelkezést a kidolgozandó mintaszerződések és támogatási megállapodások tartalmazzák.

45. cikk

A minősített szerződésekre és támogatási megállapodásokra vonatkozó rendelkezések

(1) Amikor egy részvételre jelentkező, ajánlattevő vagy pályázó részére a közbeszerzési eljárás során EU-minősített adatot adnak át, a pályázati vagy ajánlattételi felhívásnak tartalmaznia kell egy olyan kitételt, amely azt a részvételre jelentkezőt, ajánlattevőt vagy pályázót, aki végül nem nyújtja be pályázatát vagy ajánlatát, vagy akit nem választanak ki, arra kötelezi, hogy adott időn belül valamennyi minősített dokumentumot szolgáltassa vissza.

(2) Az ajánlatkérő a Bizottság Biztonsági Hatóságán keresztül értesíti a megfelelő nemzeti vagy kijelölt biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot, hogy minősített szerződést vagy támogatási megállapodást kötöttek, valamint közli a vonatkozó adatokat, például a vállalkozó(k) vagy kedvezményezett(ek) nevét, a szerződés időtartamát és a legmagasabb minősítési szintet.

(3) Amennyiben egy ilyen szerződést vagy támogatási megállapodást megszüntetnek, az ajánlatkérő vagy támogatást nyújtó hatóság haladéktalanul értesíti a Bizottság Biztonsági Hatóságán keresztül annak a tagállamnak a nemzeti vagy kijelölt biztonsági hatóságát vagy bármely más illetékes biztonsági hatóságát, amelyben a vállalkozót vagy a támogatás kedvezményezettjét nyilvántartásba vették.

(4) Általános szabály, hogy a vállalkozó vagy a támogatás kedvezményezettje a minősített vállalkozói vagy támogatási megállapodás vagy a támogatási kedvezményezett részvételének lejártát követően köteles valamennyi EU-minősített adatot visszaszolgáltatni az ajánlatkérő vagy támogatást nyújtó hatóságnak.

(5) Az EU-minősített adatoknak a minősített szerződés vagy minősített támogatási megállapodás teljesítése során vagy azok lejártával történő megsemmisítésére vonatkozó egyedi rendelkezéseket a biztonsági vonatkozások záradékában kell lefektetni.

(6) Amennyiben a vállalkozó vagy a támogatás kedvezményezettje engedélyt kap az EU-minősített adatok megtartására a minősített szerződés vagy támogatási megállapodás lejártát követően, továbbra is be kell tartani az e határozatban foglalt minimumszabályokat, és a vállalkozónak vagy a támogatás kedvezményezettjének védenie kell az EU-minősített adatok bizalmasságát.

46. cikk

Minősített szerződésekre vonatkozó egyedi rendelkezések

(1) A pályázati kiírásban és a minősített szerződésben meg kell határozni az EU-minősített adatok védelme szempontjából lényeges feltételeket, amelyek szerint a vállalkozó alvállalkozói szerződést köthet.

(2) Mielőtt a vállalkozó a minősített szerződés bármely részére alvállalkozókat szerződtetne, ehhez engedélyt kér az ajánlatkérőtől. Az EU-minősített adatokhoz való hozzáférést magában foglaló alvállalkozói szerződés nem köthető harmadik országban nyilvántartásba vett alvállalkozóval, kivéve, ha a 7. fejezetben meghatározottak szerint létrehozták az adatok biztonságára vonatkozó keretszabályozást.

(3) A vállalkozó felel annak biztosításáért, hogy minden alvállalkozói tevékenységet az e határozatban foglalt minimumszabályokkal összhangban folytassanak, és az alvállalkozó részére nem ad át EU-minősített adatot vagy anyagot az azt kibocsátó előzetes írásbeli engedélye nélkül.

(4) A vállalkozó által létrehozott vagy kezelt EU-minősített adatok tekintetében a Bizottságot kell kibocsátónak tekinteni, és a kibocsátót megillető jogokat az ajánlatkérő gyakorolja.

47. cikk

A minősített szerződésekkel kapcsolatos látogatások

(1) Amennyiben a Bizottság egyik alkalmazottjának vagy a vállalkozók vagy a támogatás kedvezményezettjei személyzetének valamely minősített szerződés vagy támogatási megállapodás teljesítéséhez egymás telephelyén CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adathoz kell hozzáférnie, a látogatásokat a nemzeti vagy kijelölt biztonsági hatóságokkal vagy bármely más érintett illetékes biztonsági hatósággal összeköttetésben kell megszervezni. A Bizottság Biztonsági Hatóságát tájékoztatják e látogatásokról. Egyes meghatározott programokra vagy projektekre vonatkozóan azonban a nemzeti biztonsági hatóság, a kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság megállapodhat egy olyan eljárásról, amely alapján közvetlenül meg lehet szervezni e látogatásokat.

(2) Minden látogatónak megfelelő biztonsági tanúsítvánnyal kell rendelkeznie, és teljesítenie kell a „szükséges ismeret" feltételét a minősített szerződéssel kapcsolatos EU-minősített adatokhoz való hozzáféréshez.

(3) A látogatók csak a látogatás céljához kapcsolódó EU-minősített adatokhoz kapnak hozzáférést.

(4) A részletesebb rendelkezéseket a végrehajtási szabályokban határozzák meg.

(5) Az e határozatban megállapított és a (4) bekezdésben említett végrehajtási szabályokban említett minősített szerződésekkel kapcsolatos látogatásokra vonatkozó rendelkezéseknek való megfelelés kötelező.

48. cikk

Az EU-minősített adatok minősített szerződésekkel és minősített támogatási megállapodásokkal kapcsolatos továbbítása és szállítása

(1) Az EU-minősített adatok elektronikus úton történő továbbítása tekintetében ezen határozat 5. fejezetének vonatkozó rendelkezéseit kell alkalmazni.

(2) Az EU-minősített adatok szállítására ezen határozat 4. fejezetének és annak végrehajtási szabályainak vonatkozó rendelkezéseit kell alkalmazni, a nemzeti törvényekkel és rendeletekkel összhangban.

(3) Az EU-minősített adatok szállítmányként való szállítása biztonsági előírásainak meghatározása során az alábbi elveket kell alkalmazni:

a) a szállítás valamennyi szakasza alatt garantálni kell a biztonságot, a kiindulási helytől a végső úti célig;

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

c) a SECRET UE/EU SECRET vagy CONFIDENTIEL UE/EU CONFIDENTIEL adatként minősített anyag bármilyen, határokon átnyúló szállítását megelőzően a feladó szállítási tervet készít, amelyet az érintett nemzeti biztonsági hatóságok, kijelölt biztonsági hatóságok vagy más illetékes biztonsági hatóságok jóváhagynak;

d) az útvonalak lehetőség szerint közvetlenek, és a szállítást a körülmények engedte lehető leggyorsabban hajtják végre;

e) az útvonalak lehetőség szerint kizárólag tagállamokon keresztül vezetnek. Nem uniós tagállamokon keresztül vezető útvonalakon kizárólag mind a feladó, mind a címzett államának nemzeti vagy kijelölt biztonsági hatósága vagy más illetékes biztonsági hatósága által kiadott jóváhagyást követően lehet haladni.

49. cikk

Az EU-minősített adatok átadása harmadik államban működő vállalkozók vagy támogatási kedvezményezettek részére

Az EU-minősített adat harmadik államokban működő vállalkozók vagy támogatási kedvezményezettek részére való átadása a Bizottság Biztonsági Hatósága, a Bizottság szervezeti egysége mint ajánlatkérő vagy támogatást nyújtó hatóság, valamint azon érintett harmadik ország nemzeti biztonsági hatósága kijelölt biztonsági hatósága vagy más illetékes biztonsági hatósága által elfogadott biztonsági intézkedésekkel összhangban történik, ahol a vállalkozót vagy a támogatás kedvezményezettjét bejegyezték.

50. cikk

A RESTREINT UE/EU RESTRICTED minősítésű adatok minősített szerződések vagy minősített támogatási megállapodások keretében történő kezelése

(1) A RESTREINT UE/EU RESTRICTED minősítésű adatok minősített szerződések vagy minősített támogatási megállapodások keretében történő védelme az arányosság és költséghatékonyság elvén alapszik.

(2) A RESTREINT UE/EU RESTRICTED minősítésű adatok kezelését magában foglaló minősített szerződések vagy minősített támogatási megállapodások összefüggésében nincs szükség telephely-biztonsági tanúsítványra vagy személyi biztonsági tanúsítványra.

(3) Amennyiben egy adott szerződés vagy támogatási megállapodás RESTREINT UE/EU RESTRICTED minősítési szintű adatok adott vállalkozó vagy a támogatás kedvezményezettje által működtetett kommunikációs és információs rendszerben való kezelésére is kiterjed, az ajánlatkérő vagy támogatási nyújtó hatóság a Bizottság Biztonsági Hatóságával való konzultációt követően biztosítja, hogy a szerződés vagy a támogatási megállapodás meghatározza a kommunikációs és információs rendszer akkreditálásához vagy jóváhagyásához szükséges, valamennyi kockázati tényezőre kiterjedő technikai és adminisztratív követelményeket. Az ilyen kommunikációs és információs rendszer akkreditációjának vagy jóváhagyásának hatályáról a Bizottság Biztonsági Hatósága és az érintett nemzeti biztonsági hatóság vagy kijelölt biztonsági hatóság állapodik meg.

7. FEJEZET

A MINŐSÍTETT ADATOK MÁS UNIÓS INTÉZMÉNYEKKEL, ÜGYNÖKSÉGEKKEL, SZERVEKKEL ÉS HIVATALOKKAL, TAGÁLLAMOKKAL, HARMADIK ÁLLAMOKKAL ÉS NEMZETKÖZI SZERVEZETEKKEL VALÓ CSERÉJE

51. cikk

Alapelvek

(1) Amennyiben a Bizottság vagy egyik szervezeti egysége megállapítja, hogy EU-minősített adatok más uniós intézménnyel, ügynökséggel, szervvel vagy hivatallal, illetve harmadik állammal vagy nemzetközi szervezettel való cseréjére van szüksége, e célból meg kell tenni a megfelelő jogi vagy igazgatási keret létrehozására irányuló szükséges lépéseket, amely keret magában foglalhatja a vonatkozó rendeletekkel összhangban megkötött adatbiztonsági megállapodásokat vagy igazgatási megállapodásokat is.

(2) Az 57. cikk sérelme nélkül az EU-minősített adatok más uniós intézménnyel, ügynökséggel, szervvel vagy hivatallal, illetve harmadik állammal vagy nemzetközi szervezettel történő cseréjére csak abban az esetben van lehetőség, ha megfelelő jogi vagy adminisztratív keretet hoztak létre, és elegendő garancia áll rendelkezésre arra vonatkozóan, hogy az érintett uniós intézmény, ügynökség, szerv vagy hivatal, illetve harmadik állam vagy nemzetközi szervezet egyenértékű alapelveket és minimumszabályokat alkalmaz a minősített adatok védelmére vonatkozóan.

52. cikk

Az EU-minősített adatok más uniós intézményekkel, ügynökségekkel, szervekkel és hivatalokkal való cseréje

(1) Mielőtt más uniós intézménnyel, ügynökséggel, szervvel vagy hivatallal igazgatási megállapodást kötne az EU-minősített adatok cseréjére vonatkozóan, a Bizottság megbizonyosodik arról, hogy az érintett uniós intézmény, ügynökség, szerv vagy hivatal:

a) rendelkezik az EU-minősített adatok védelmére vonatkozó keretszabályozással, amely az e határozatban és annak végrehajtási szabályaiban megállapított alapelvekkel és minimumszabályokkal egyenértékű alapelveket és minimumszabályokat állapít meg;

b) a személyi biztonsággal, fizikai biztonsággal, EU-minősített adatok kezelésével és a kommunikációs és információs rendszerek biztonságával kapcsolatos biztonsági szabványokat és útmutatókat alkalmaz, amelyek az EU-minősített adatok számára a Bizottságban biztosított védelmi szinttel egyenértékű védelmi szintet biztosítanak.

c) az általa létrehozott minősített adatokat EU-minősített adatokként jelöli meg.

(2) Szoros együttműködésben a Bizottság egyéb illetékes szervezeti egységeivel, a Humánerőforrásügyi és Biztonsági Főigazgatóság a Bizottságon belüli illetékes szolgálat a más uniós intézménnyel, ügynökséggel, szervvel vagy hivatallal EU-minősített adatok cseréjére vonatkozóan megkötött igazgatási megállapodások tekintetében.

(3) Az igazgatási megállapodást általában levélváltás formájában kötik, a humánerőforrásügyi és biztonsági főigazgató Bizottság nevében történő aláírásával.

(4) Mielőtt megállapodást kötne az EU-minősített adatok cseréjére vonatkozóan, a Bizottság Biztonsági Hatósága értékelő látogatást tesz az EU-minősített adatok védelmére vonatkozó keretszabályozás értékelése és az EU-minősített adatok védelme érdekében tett intézkedések hatékonyságának megállapítása céljából. Az igazgatási megállapodás csak akkor lép hatályba és az EU-minősített adatok kicserélésére csak akkor kerül sor, hogyha az értékelő látogatás eredménye kielégítő és a látogatás során tett további ajánlásokat betartották. Rendszeres nyomon követő értékelő látogatásokat kell tenni annak megerősítésére, hogy az igazgatási megállapodást betartják-e és a meglevő biztonsági intézkedések továbbra is megfelelnek-e az alapelveknek és az elfogadott minimumszabályoknak.

(5) Általános szabályként a minősített adatok más uniós intézményekkel, ügynökségekkel, szervekkel és hivatalokkal való cseréjének fő beérkezési és kiküldési helye a Bizottságon belül a Főtitkárság által irányított EU-minősített adatokat nyilvántartó hivatal. Ha azonban biztonsági, szervezeti vagy üzemeltetési okokból az EU-minősített adatok védelme szempontjából ez megfelelőbb, az e határozattal és annak végrehajtási szabályaival összhangban a Bizottság szervezeti egységeiben létrehozott EU-minősített adatokat nyilvántartó helyi hivatalok működnek a minősített adatok beérkezési és kiküldési helyeként a Bizottság érintett szervezeti egységeinek hatáskörébe tartozó kérdésekben.

(6) A Bizottság biztonsági szakértői csoportját tájékoztatni kell a (2) bekezdés szerinti igazgatási megállapodások megkötésének folyamatáról.

53. cikk

Az EU-minősített adatok tagállamokkal való cseréje

(1) Az EU-minősített adatokat ki lehet cserélni a tagállamokkal és át lehet adni a tagállamoknak feltéve, hogy azok ezeket az adatokat a nemzeti minősítési jelöléssel ellátott azonos szintű minősített adatokra alkalmazandó előírásoknak megfelelően védik a biztonsági minősítések I. mellékletben szereplő egyenértékűségi táblázatában foglaltak szerint.

(2) Amennyiben a tagállamok nemzeti minősítési jelöléssel ellátott minősített adatokat visznek be az Európai Unió struktúráiba vagy hálózataiba, a Bizottság ezeket az adatokat az azonos szintű EU-minősített adatokra alkalmazandó előírásoknak megfelelően védi a biztonsági minősítések I. mellékletben szereplő egyenértékűségi táblázatában foglaltak szerint.

54. cikk

Az EU-minősített adatok harmadik államokkal és nemzetközi szervezetekkel való cseréje

(1) Abban az esetben, ha a Bizottság a minősített adatok harmadik államokkal és nemzetközi szervezetekkel való cseréjének hosszú távú szükségességét állapítja meg, e célból meg kell tenni a megfelelő jogi vagy igazgatási keret létrehozására irányuló szükséges lépéseket, amely keret magában foglalhatja a vonatkozó rendeletekkel összhangban megkötött adatbiztonsági megállapodásokat vagy igazgatási megállapodásokat is.

(2) A (1) bekezdésben említett ilyen adatbiztonsági vagy igazgatási megállapodások rendelkezéseket tartalmaznak annak biztosítására, hogy amennyiben a harmadik állam vagy a nemzetközi szervezet EU-minősített adatot kap, az ilyen adatot a minősítési szintjének és az e határozatban foglaltakkal egyenértékű minimumszabályoknak megfelelő védelemben részesítsék.

(3) Az általános szabályként legfeljebb RESTREINT UE/EU RESTRICTED minősítési szintű EU-minősített adatok esetén a Bizottság az 56. cikknek megfelelően igazgatási megállapodásokat köthet.

(4) A (3) bekezdésben említett, minősített adatok cseréjére vonatkozó igazgatási megállapodások rendelkezéseket tartalmaznak annak biztosítására, hogy amennyiben a harmadik állam vagy a nemzetközi szervezet EU-minősített adatot kap, az ilyen adatot a minősítési szintjének és az e határozatban foglaltakkal egyenértékű minimumszabályoknak megfelelő védelemben részesítsék. A Bizottság biztonsági szakértői csoportja véleményét kikérik az adatbiztonsági megállapodások vagy igazgatási megállapodások megkötéséről.

(5) A Bizottságtól származó EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére történő átadásáról szóló határozatot csak a Bizottság szervezeti egysége, mint ezen EU-minősített adatok Bizottságon belüli kibocsátója hozhatja meg eseti alapon, az adat jellegétől és tartalmától, a címzett számára szükséges ismeret elvétől, valamint az Unió számára jelentkező előnyök mértékétől függően. Ha az átadni kért minősített adat vagy az abban esetlegesen jelen lévő forrásanyag kibocsátója nem a Bizottság, akkor a Bizottság EU-minősített adatot birtokló szervezeti egységének a kibocsátó előzetes írásbeli beleegyezését kell kérnie az adat átadásához. Ha a kibocsátó nem állapítható meg, feladatkörét a Bizottság minősített adatot birtokló szervezeti egysége látja el, a Bizottság biztonsági szakértői csoportjával folytatott konzultációt követően.

55. cikk

Adatbiztonsági megállapodások

(1) Harmadik államokkal és nemzetközi szervezetekkel az EUMSZ 218. cikkével összhangban kötnek adatbiztonsági megállapodásokat.

(2) Az adatbiztonsági megállapodások:

a) megállapítják a minősített adatoknak az Unió és harmadik államok vagy nemzetközi szervezetek közötti cseréjére irányadó alapelveket és minimumszabályokat;

b) rendelkeznek technikai végrehajtási szabályokról is, amelyeket az érintett uniós intézmények és szervek illetékes biztonsági hatóságai és a szóban forgó harmadik állam vagy nemzetközi szervezet illetékes biztonsági hatósága közösen alakítanak ki. A végrehajtási szabályok figyelembe veszik az érintett harmadik állam vagy nemzetközi szervezet hatályos biztonsági szabályai, struktúrái és eljárásai által biztosított védelmi szintet;

c) előírják, hogy a minősített adatoknak az adott megállapodás szerinti cseréjét megelőzően meg kell állapítani, hogy az átvevő fél képes a neki átadott minősített adatok megfelelő védelmére és megőrzésére.

(3) Amennyiben az 51. cikk (1) bekezdése szerint megállapítást nyer, hogy minősített adatok cseréjére van szükség, a Bizottság konzultál az Európai Külügyi Szolgálattal, a Tanács Főtitkárságával és adott esetben más uniós intézményekkel és szervekkel annak megállapítása céljából, hogy szükség van-e az EUMSZ 218. cikkének (3) bekezdése szerinti ajánlás előterjesztésére.

(4) Az EU-minősített adatok elektronikus eszközökkel történő cseréje nem megengedett, kivéve, ha az adatbiztonsági megállapodás vagy a technikai végrehajtási szabályok erről kifejezetten rendelkeznek.

(5) Általános szabályként a Bizottságon belül a Főtitkárság által irányított EU-minősített adatokat nyilvántartó hivatal a minősített adatok harmadik államokkal és nemzetközi szervezetekkel való cseréjének fő beérkezési és kiküldési helye. Ha azonban biztonsági, szervezeti vagy üzemeltetési okokból az EU-minősített adatok védelme szempontjából ez megfelelőbb, e határozattal és annak végrehajtási szabályaival összhangban a Bizottság szervezeti egységeiben létrehozott EU-minősített adatokat nyilvántartó helyi hivatalok működnek a minősített adatok beérkezési és kiküldési helyeként a Bizottság érintett szervezeti egységeinek hatáskörébe tartozó kérdésekben.

(6) Az érintett harmadik állam vagy nemzetközi szervezet biztonsági szabályai, struktúrái és eljárásai hatékonyságának megállapítása céljából a Bizottság más uniós intézményekkel, ügynökségekkel vagy szervekkel együttműködve értékelő látogatásokon vesz részt az érintett harmadik állammal vagy nemzetközi szervezettel való kölcsönös megállapodás alapján. Az ilyen értékelő látogatások az alábbiak értékelését végzik el:

a) a minősített adatok védelmére alkalmazandó szabályozási keret;

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

c) a ténylegesen hatályos biztonsági intézkedések és eljárások; valamint

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

56. cikk

Igazgatási megállapodások

(1) Amennyiben az Unió szakpolitikai vagy jogi keretével összefüggésben harmadik állammal vagy nemzetközi szervezettel általános szabályként legfeljebb RESTREINT UE/EU RESTRICTED minősítési jelölésű adatok hosszú távú cseréjére van szükség, és amennyiben a Bizottság Biztonsági Hatósága a Bizottság biztonsági szakértői csoportjával folytatott konzultációt követően különösen megállapította, hogy az érintett fél nem rendelkezik kellőképpen fejlett biztonsági rendszerrel ahhoz, hogy lehetséges legyen az adatbiztonsági megállapodás megkötése, a Bizottság igazgatási megállapodást köthet a szóban forgó harmadik állam vagy nemzetközi szervezet megfelelő hatóságaival.

(2) Az ilyen igazgatási megállapodást általában levélváltás formájában kell megkötni.

(3) Az értékelő látogatásra a megállapodás megkötése előtt kerül sor. A Bizottság biztonsági szakértői csoportját tájékoztatják az értékelő látogatás eredményéről. Amennyiben rendkívüli okok indokolják az EU-minősített adatok sürgős cseréjét, az EU-minősített adat átadható azzal a feltétellel, hogy megtesznek mindent annak érdekében, hogy a lehető leghamarabb sor kerüljön az értékelő látogatásra.

(4) Az EU-minősített adatok elektronikus eszközökkel történő cseréje csak akkor megengedett, ha az adminisztratív megállapodás erről kifejezetten rendelkezik.

57. cikk

Az EU-minősített adatok rendkívüli ad hoc átadása

(1) Amennyiben nincs meglévő adatbiztonsági vagy igazgatási megállapodás és amennyiben a Bizottság vagy egyik szervezeti egysége megállapítja, hogy az Unió szakpolitikai vagy jogi keretével összefüggésben rendkívüli igény merül fel EU-minősített adatok harmadik állam vagy nemzetközi szervezet részére való átadására, a Bizottság Biztonsági Hatósága a lehetséges mértékben ellenőrzi, hogy az adott harmadik állam vagy nemzetközi szervezet biztonsági hatóságainak biztonsági szabályai, struktúrái és eljárásai garantálni tudják, hogy a részére átadott EU-minősített adatok az e határozatban foglaltaknál nem kevésbé szigorú szabályoknak megfelelő védelemben részesüljenek.

(2) Az EU-minősített adatok érintett harmadik államnak vagy nemzetközi szervezetnek való átadásáról szóló döntést a Bizottság hozza meg a Bizottság biztonsági kérdésekért felelős egyik tagjának javaslata alapján, a Bizottság biztonsági szakértői csoportjával való konzultációt követően.

(3) A Bizottság EU-minősített adat átadására vonatkozó döntését követően és a kibocsátó előzetes írásbeli hozzájárulásának függvényében, ideértve az esetlegesen jelen lévő forrásanyag kibocsátóit is, a Bizottság illetékes szervezeti egysége továbbítja az érintett adatot, amelyen szerepel az átvevő harmadik államot vagy nemzetközi szervezetet feltüntető átadásra jogosító jelölés is. A tényleges átadást megelőzően vagy annak alkalmával az adott harmadik fél írásban kötelezettséget vállal az átvett EU-minősített adatoknak az e határozatban megállapított alapelvek és minimumszabályok szerinti védelmére.

8. FEJEZET

ZÁRÓ RENDELKEZÉSEK

58. cikk

A korábbi határozat hatályon kívül helyezése

Ez a határozat hatályon kívül helyezi a 2001/844/EK, ESZAK, Euratom bizottsági határozatot ([1]) és annak helyébe lép.

59. cikk

Az e határozat hatálybalépése előtt létrehozott minősített adatok

(1) A 2001/844/EK, ESZAK, Euratom határozat értelmében minősített valamennyi EU-minősített adatot a továbbiakban e határozat vonatkozó rendelkezéseivel összhangban kell védeni.

(2) A 2001/844/EK, ESZAK, Euratom határozat hatálybalépésének napján a Bizottság birtokában levő valamennyi minősített adat, kivéve az Euratom-minősített adatokat:

a) alapértelmezésben – amennyiben azt a Bizottság hozta létre – továbbra is RESTREINT UE körbe átminősítettnek tekintendő, hacsak kibocsátója úgy nem határozott, hogy 2002. január 31-ig az adatot más minősítési fokozatba sorolja és erről az érintett dokumentum valamennyi címzettjét tájékoztatta;

b) eredeti minősítését – amennyiben a Bizottságon kívüli kibocsátó hozta létre – megtartja, és ily módon a vele egyenértékű minősítésű EU-minősített adatként kezelendő, hacsak a kibocsátó bele nem egyezik az információ minősítésének megszüntetésébe vagy visszaminősítésébe.

60. cikk

Végrehajtási szabályok és biztonsági közlemények

(1) E határozat végrehajtási szabályainak elfogadása szükség esetén egy, a Bizottság biztonsági kérdésekért felelős tagjának felhatalmazásáról szóló külön bizottsági határozat tárgya lesz, a belső eljárási szabályzattal teljes összhangban.

(2) A Bizottság fent említett határozata általi felhatalmazást követően a Bizottság biztonsági kérdésekért felelős tagja biztonsági közleményeket dolgozhat ki, amelyek ezen határozat és annak végrehajtási szabályainak alkalmazási körébe tartozó biztonsági útmutatókat és legjobb gyakorlatokat határoznak meg.

(3) A Bizottság egy külön hatáskör-átruházási határozatban az e cikk első és második bekezdésében említett feladatokat a humánerőforrásügyi és biztonsági főigazgatóra ruházhatja, a belső eljárási szabályzattal teljes összhangban.

61. cikk

Hatálybalépés

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

Kelt Brüsszelben, 2015. március 13-án.

a Bizottság részéről

az elnök

Jean-Claude JUNCKER

([1]) A Bizottság 2001. november 29-i határozata eljárási szabályzatának módosításáról (HL L 317., 2001.12.3., 1. o.).

I. MELLÉKLET

A 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 Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (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 Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettország	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litvánia	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Magyarország	„Szigorúan titkos!”	„Titkos!”	„Bizalmas!”	„Korlátozott terjesztésű!”
Málta	L-Oghla Segretezza	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
Románia	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Szlovénia	Strogo tajno	Tajno	Zaupno	Interno
Szlovákia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finnország	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Svédország ([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 egyenértékű minősítés ([5])	UK OFFICIAL – SENSITIVE

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

([2]) Németország: VS = Verschlusssache.

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

([4]) 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 adatot a UK SECRET minősítésű adatokra alkalmazandó védelmi biztonsági követelményeknek megfelelően kezeli és védi.

II. MELLÉKLET

A RÖVIDÍTÉSEK JEGYZÉKE

Mozaikszó	Jelentés
CA	kriptográfiai hatóság
CAA	kriptográfiai jóváhagyó hatóság
CCTV	zárt láncú televízió
CDA	kriptográfiai terjesztési hatóság
CIS	az EU-minősített adatokat kezelő kommunikációs és információs rendszer
DSA	kijelölt biztonsági hatóság
EUCI	EU-minősített adat
FSC	telephely-biztonsági tanúsítvány
IA	információvédelem
IAA	információvédelmi hatóság
IDS	behatolásjelző rendszer
IT	információtechnológia
LSO	helyi biztonsági tisztviselő
NSA	nemzeti biztonsági hatóság
PSC	személyi biztonsági tanúsítvány
PSCC	személyi biztonsági tanúsítványról szóló igazolás
PSI	a programra/a projektre vonatkozó biztonsági utasítások
RCO	Nyilvántartó hivatalt ellenőrző tisztviselő
SAA	biztonsági akkreditációs hatóság
SAL	biztonsági vonatkozások záradéka
SCG	biztonsági minősítési útmutató
SecOPs	biztonsági üzemeltetési eljárások
TA	TEMPEST-hatóság
EUMSZ	Az Európai Unió működéséről szóló szerződés

III. MELLÉKLET

A NEMZETI BIZTONSÁGI HATÓSÁGOK JEGYZÉKE

BELGIUM

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
B-1000 Bruxelles
Titkársági telefonszám: +32 25014542
Telefax: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGÁRIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Telefonszám: +359 29333600
Telefax: +359 29873750
E-mail: dksi@government.bg
Honlap: www.dksi.bg

CSEH KÖZTÁRSASÁG

Národní bezpečnostní úřad
(Nemzeti Biztonsági Hatóság)
Na Popelce 2/16
150 06 Praha 56 Tel.
Telefonszám: +420 257283335
Telefax: +420 257283110
E-mail: czech.nsa@nbu.cz
Honlap: www.nbu.cz

DÁNIA

Politiets Efterretningstjeneste
(dán biztonsági hírszerzési szolgálat)
Klausdalsbrovej 1
2860 Søborg Tel.
Telefonszám: +45 33148888
Telefax: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø Tel.
Telefonszám: +45 33325566
Telefax: +45 33931320

NÉMETORSZÁG

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin Tel.
Telefonszám: +49 30186810
Telefax: +49 30186811441
E-mail: oesIII3@bmi.bund.de

ÉSZTORSZÁG

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn Tel.
Telefonszám: +372 7170113 0019, +372 7170117
Telefax: +372 7170213
E-mail: nsa@mod.gov.ee

GÖRÖGORSZÁG

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα Τηλ.
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Telefonszám: +30 2106572045
+30 2106572009
Telefax: +30 2106536279, +30 2106577612

SPANYOLORSZÁG

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid Tel.
Telefonszám: +34 913725000
Telefax: +34 913725808
E-mail: nsa-sp@areatec.com

FRANCIAORSZÁG

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP Tel.
Telefonszám: +33 171758177
Telefax: + 33 171758200

HORVÁTORSZÁG

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb (Zágráb)
Horvátország
Telefonszám: +385 14681222
Telefax: + 385 14686049
Honlap: www.uvns.hr

ÍRORSZÁG

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
IE-Dublin 2
Telefonszám: +353 14780822
Telefax: +353 14082959

OLASZORSZÁG

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma Tel.
Telefonszám: +39 0661174266
Telefax: +39 064885273

CIPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia Tel.
Telefonszám: +357 22807569, +357 22807643,
+357 22807764
Telefax: +357 22302351
E-mail: cynsa@mod.gov.cy

LETTORSZÁG

National Security Authority
Constitution Protection Bureau of the Republic of Latvia (A Lett Köztársaság Alkotmányvédelmi Hivatalának Nemzeti Biztonsági Hatósága) P.O.
P.O.Box 286
LV-1001 Riga Tel.
Telefonszám: +371 67025418
Telefax: +371 67025454
E-mail: ndi@sab.gov.lv

LITVÁNIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(A Litván Köztársaság Titokvédelmi Koordinációs Bizottsága Nemzeti Biztonsági Hatóság)
Gedimino 40/1
01110 Vilnius
Telefonszám: +370 706 66701; +370 706 66702
Telefax: +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Telefonszám: +352 24782210 central
+ 352 24782253 direct
Telefax: +352 24782243

MAGYARORSZÁG

Nemzeti Biztonsági Felügyelet
1024 Budapest, Szilágyi Erzsébet fasor 11/B
Telefonszám: +36 (1) 7952303
Telefax: +36 (1) 7950344

Postacím:
1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Honlap: www.nbf.hu

MÁLTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta Tel.
Telefonszám: +356 21249844
Telefax: +356 25695321

HOLLANDIA

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag Tel.
Telefonszám: +31 703204400
Telefax: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag Tel.
Telefonszám: +31 703187060
Telefax: +31 703187522

AUSZTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Telefonszám: +43 1531152594
Telefax: +43 1531152615
E-mail: ISK@bka.gv.at

LENGYELORSZÁG

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Belbiztonsági Hivatal)
2A Rakowiecka St.
00-993 Warszawa Tel.
Telefonszám: +48 22 58 57 944
fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Honlap: www.abw.gov.pl

PORTUGÁLIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa Tel.
Telefonszám: +351 213031710
Telefax: +351 213031711

ROMÁNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Román NSA – ORNISS Minősített Adatok Nemzeti Nyilvántartó Hivatala)
4 Mures Street
012275 București Tel.
Telefonszám: +40 212245830
Telefax: +40 212240714
E-mail: nsa.romania@nsa.ro
Honlap: www.orniss.ro

SZLOVÉNIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana Tel.
Telefonszám: +386 14781390
Telefax: +386 14781399
E-mail: gp.uvtp@gov.si

SZLOVÁKIA

Národný bezpečnostný úrad
(Nemzeti Biztonsági Hatóság)
Budatínska 30 P.O.
P.O. Box 16
850 07 Bratislava Tel.
Telefonszám: +421 268692314
Telefax: +421 263824005
Honlap: www.nbusr.sk

FINNORSZÁG

National Security Authority
Ministry for Foreign Affairs P.O.
P.O. Box 453
FI-00023 Government Tel.
Telefonszám: 16055890
Telefax: +358 916055140
E-mail: NSA@formin.fi

SVÉDORSZÁG

Utrikesdepartementet
(Külügyminisztérium)
SSSB
S-103 39 Stockholm
Telefonszám: +46 84051000
Telefax: +46 87231176
E-mail: ud-nsa@foreign.ministry.se

EGYESÜLT KIRÁLYSÁG

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Telefax: +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk