2014.4.1. HU Az Európai Unió Hivatalos Lapja C 96/1

II

(Közlemények)

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

EURÓPAI PARLAMENT

AZ EURÓPAI PARLAMENT ELNÖKSÉGÉNEK HATÁROZATA

(2013. április 15.)

a bizalmas adatok Európai Parlament általi kezelésére vonatkozó szabályokról

(2014/C 96/01)

AZ EURÓPAI PARLAMENT ELNÖKSÉGE,

tekintettel az Európai Parlament eljárási szabályzata 23. cikkének (12) bekezdésére,

mivel:

(1) Az Európai Parlament és az Európai Bizottság közötti kapcsolatokról szóló, 2010. október 20-án aláírt keretmegállapodásra ([1]) (keretmegállapodás), illetve az Európai Parlament és a Tanács közötti, a közös kül- és biztonságpolitikától eltérő kérdésekkel kapcsolatos tanácsi minősített adatoknak az Európai Parlament részére történő továbbításáról és ezen adatoknak az Európai Parlament általi kezeléséről szóló, 2014. március 12-én aláírt intézményközi megállapodásra ([2]) (intézményközi megállapodás) tekintettel különleges szabályokat kell megállapítani a bizalmas adatok Európai Parlament általi kezelésére vonatkozóan.

(2) A Lisszaboni Szerződés új feladatokat ró az Európai Parlamentre, és a Parlament tevékenységének a bizonyos fokú titoktartást igénylő területeken történő továbbfejlesztése érdekében szükség van az alapelvek, a biztonsági minimumszabályok és a bizalmas, köztük minősített adatok Európai Parlament általi kezelésére vonatkozó megfelelő eljárások meghatározására.

(3) Az ebben a határozatban lefektetett szabályok célja, hogy az európai uniós döntéshozatali folyamat zökkenőmentes működésének előmozdítása érdekében biztosítsák a védelem közös szabályainak egyenértékűségét és összeegyeztethetőségét a Szerződések által vagy alapján létrehozott többi intézmény, szerv, hivatal és ügynökség, illetve a tagállamok által elfogadott szabályokkal.

(4) E határozat rendelkezései nem érintik a dokumentumokhoz való hozzáférésről szóló jelenlegi és jövőbeli, az Európai Unió működéséről szóló szerződés (EUMSZ) 15. cikkével összhangban elfogadott szabályokat.

([1]) HL L 304., 2010.11.20., 47. o.
([2]) HL C 95., 2014.4.1., 1. o.

(5) E határozat rendelkezései nem érintik a személyes adatok védelméről szóló jelenlegi és jövőbeli, az EUMSZ 16. cikkével összhangban elfogadott szabályokat,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Cél

E határozat a bizalmas adatok Európai Parlament általi igazgatását és kezelését szabályozza, beleértve az ilyen adatok létrehozását, fogadását, továbbítását és tárolását az adatok bizalmas jellegének megfelelő védelme céljából. A határozat az intézményközi megállapodás és a keretmegállapodás – különösen annak II. melléklete – végrehajtását szolgálja.

2. cikk

Fogalommeghatározások

E határozat alkalmazásában:

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

b) „bizalmas adat”: a „minősített adat” és a nem minősített „egyéb bizalmas adat”;

c) „minősített adat”: az „EU-minősített adat” és az „egyenértékű minősített adat”;

d) „EU-minősített adat”: olyan információ és anyag, amelyet TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL vagy RESTREINT UE/EU RESTRICTED minősítéssel láttak el, és amelynek engedély nélküli kiszolgáltatása különböző mértékben sértheti az Uniónak, illetve egy vagy több tagállamának az érdekeit, függetlenül attól, hogy az ilyen adat a szerződések által vagy alapján létrehozott intézményeken, szerveken, hivatalokon vagy ügynökségeken belül keletkezett. E vonatkozásban:

   – TRÈS SECRET UE/EU TOP SECRET („EU SZIGORÚAN TITKOS”) minősítésűek az olyan információk és anyagok, amelyek engedély nélküli kiszolgáltatása rendkívül súlyosan sérthetné az Unió, illetve egy vagy több tagállama alapvető érdekeit,

   – SECRET UE/EU SECRET („EU TITKOS”) minősítésűek az olyan információk és anyagok, amelyek engedély nélküli kiszolgáltatása súlyosan sérthetné az Unió, illetve egy vagy több tagállama alapvető érdekeit,

   – CONFIDENTIEL UE/EU CONFIDENTIAL („EU BIZALMAS”) minősítésűek az olyan információk és anyagok, amelyek engedély nélküli kiszolgáltatása sérthetné az Unió, illetve egy vagy több tagállama alapvető érdekeit;

   – RESTREINT UE/EU RESTRICTED („EU KORLÁTOZOTT TERJESZTÉSŰ”) minősítésűek az olyan információk és anyagok, amelyek engedély nélküli kiszolgáltatása hátrányosan érinthetné az Unió, illetve egy vagy több tagállama érdekeit;

e) „egyenértékű minősítésű adat”: a tagállamok, harmadik államok vagy nemzetközi szervezetek által rendelkezésre bocsátott minősített adat, amelynek biztonsági minősítési jelölése megfelel az EU-minősített adatok esetében használt biztonsági minősítési jelölések valamelyikének, és amelyet a Tanács vagy a Bizottság továbbított az Európai Parlament részére;

f) „egyéb bizalmas adat”: az Európai Parlamentben létrehozott vagy a Szerződések által vagy alapján létrehozott többi intézmény, szerv, hivatal és ügynökség, illetve a tagállamok által az Európai Parlamentnek továbbított minden egyéb nem minősített bizalmas adat, beleértve az adatvédelmi szabályok vagy a szakmai titoktartási kötelezettség hatálya alá tartozó adatokat is;

g) „dokumentum”: minden rögzített információ, fizikai formájától vagy jellemzőitől függetlenül;

h) „anyag”: bármilyen dokumentum, illetve készre gyártott vagy gyártás alatt álló gép vagy berendezés;

i) „szükséges ismeret”: egy adott személy valamely hivatali funkció ellátása vagy feladat elvégzése érdekében szükséges hozzáférése a bizalmas adathoz;

j) „felhatalmazás”: az Európai Parlament képviselői esetében az elnök, az Európai Parlament tisztviselői és a képviselőcsoportok alkalmazásában álló egyéb európai parlamenti alkalmazottak esetében a főtitkár által elfogadott határozat, amely egy meghatározott szintig hozzáférést engedélyez valamely személynek a minősített adatokhoz a nemzeti jogszabályok szerinti nemzeti hatóság által az I. melléklet 2. részében foglalt rendelkezéseknek megfelelően elvégzett biztonsági ellenőrzés (átvilágítás) kedvező eredménye alapján;

k) „visszaminősítés”: a minősítési szint leszállítása;

l) „minősítés megszüntetése”: mindenféle minősítés megszüntetése;

m) „jelölés”: az „egyéb bizalmas adat” mellé illesztett jelölés előre meghatározott konkrét utasítások azonosítására a kezelésére vagy az adott dokumentum által lefedett területre vonatkozóan. A jelölés minősített adat mellé is illeszthető a kezelésére vonatkozó további követelmények támasztása céljából;

n) „jelölés megszüntetése”: mindenféle jelölés megszüntetése;

o) „kibocsátó”: a bizalmas adat megfelelő felhatalmazással rendelkező szerzője;

p) „biztonsági közlemény”: a II. mellékletben foglaltak szerinti végrehajtási intézkedések;

q) „kezelési utasítások”: technikai jellegű utasítások az Európai Parlament szolgálatai részére a bizalmas adatok kezeléséről.

3. cikk

Alapelvek és minimumszabályok

(1) A bizalmas adatok kezelése során az Európai Parlament az I. melléklet 1. részében foglalt alapelveket és minimumszabályokat követi.

(2) Az Európai Parlament ezen alapelveknek és minimumszabályoknak megfelelő információbiztonsági irányítórendszert (ISMS) hoz létre. Az ISMS a biztonsági közleményből, a kezelési utasításokból és a vonatkozó eljárási szabályzatból áll. Az ISMS célja a parlamenti és adminisztrációs munka megkönnyítése, egyúttal biztosítva az Európai Parlament által feldolgozott valamennyi bizalmas adat védelmét, teljes mértékben tiszteletben tartva ezen adat kibocsátója által a biztonsági közleményben meghatározott szabályokat.

A bizalmas adatoknak az Európai Parlament automatizált kommunikációs és információs rendszereivel történő, a 3. számú biztonsági közleményben lefektetett feldolgozása az információvédelmi koncepciónak megfelelően történik.

(3) Az Európai Parlament képviselői a RESTREINT UE/EU RESTRICTED szintig (ezt a szintet is beleértve) biztonsági tanúsítvány nélkül betekinthetnek a minősített adatokba.

(4) A CONFIDENTIEL UE/EU CONFIDENTIAL vagy azzal egyenértékű minősítésű adatokhoz azon európai parlamenti képviselők kaphatnak hozzáférést, akiket erre az elnök az 5. cikk alapján felhatalmazott, vagy miután hivatalos, aláírásukkal hitelesített nyilatkozatot tesznek arról, hogy ezen adatok tartalmát nem közlik harmadik személyekkel, hogy tiszteletben tartják a CONFIDENTIEL UE/EU CONFIDENTIAL szinten minősített adatok védelmének kötelezettségét, illetve hogy vállalják ezen kötelezettség megsértésének következményeit.

(5) A SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET vagy azzal egyenértékű minősítésű adatokhoz azon európai parlamenti képviselők kaphatnak hozzáférést, akiket erre az elnök felhatalmazott, miután:

a) e határozat I. mellékletének 2. részével összhangban átestek a biztonsági ellenőrzésen, vagy

b) valamely illetékes nemzeti hatóságtól értesítés érkezett arról, hogy az érintett képviselők a nemzeti jogszabályokkal összhangban, feladatkörüknél fogva e hozzáférésre megfelelő felhatalmazást kaptak.

(6) A minősített adatokhoz való hozzáférés azt követően adható meg, hogy az európai parlamenti képviselőket röviden tájékoztatták az ilyen adatoknak az I. melléklettel összhangban történő védelmével kapcsolatos kötelezettségeikről, és a képviselőknek tudomásul kell venniük e kötelezettségeiket. A képviselőket emellett röviden tájékoztatni kell e védelmet biztosító eszközökről.

(7) Az Európai Parlament tisztviselői és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak bizalmas adatokba akkor tekinthetnek be, ha a „szükséges ismeret” esetükben igazolt, a RESTREINT UE/EU RESTRICTED szint feletti minősítésű adatokba pedig csak akkor, ha megfelelő szintű biztonsági tanúsítvánnyal rendelkeznek. A minősített adatokhoz csak akkor kapnak hozzáférést, ha tájékoztatást és írásbeli útmutatást kaptak az ilyen adatok védelmével kapcsolatos kötelezettségeikről és e védelmet biztosító eszközökről, továbbá ha nyilatkozatot írtak alá, amelyben elismerik a szóban forgó útmutatás kézhezvételét, és vállalják, hogy a jelen szabályokkal összhangban ezen útmutatás szerint járnak el.

4. cikk

Bizalmas adat létrehozása és adminisztratív kezelése az Európai Parlament által

(1) Bizalmas adat kibocsátására és/vagy adat minősítésére a biztonsági közleményben rögzített módon az Európai Parlament elnöke, az érintett parlamenti bizottságok elnökei, a főtitkár és/vagy az általa írásban megfelelően felhatalmazott személy jogosult.

(2) A minősített adat létrehozásakor a kibocsátó – az ezen elnökségi határozat I. mellékletében foglalt nemzetközi szabályokkal és fogalommeghatározásokkal összhangban – a megfelelő minősítési szintet alkalmazza. A kibocsátó általános szabályként ezen kívül meghatározza az adat megtekintésére a minősítési szintnek megfelelően felhatalmazandó címzetteket. Erről a dokumentumnak a Minősített Adatok Osztályán való elhelyezésekor tájékoztatni kell a Minősített Adatok Osztályát.

(3) A szakmai titoktartás alá tartozó „egyéb bizalmas adat” kezelése során az I. és a II. mellékleteknek, illetve a kezelési utasításoknak megfelelően kell eljárni.

5. cikk

Bizalmas adat Európai Parlament általi fogadása

(1) Az Európai Parlamenthez beérkező bizalmas adatot a következőképpen kell továbbítani:

a) a RESTREINT UE/EU RESTRICTED vagy azzal egyenértékű minősítésű adatot és az „egyéb bizalmas adatot” a továbbítás iránti kérelmet benyújtó parlamenti szerv/tisztségviselő titkárságára vagy közvetlenül a Minősített Adatok Osztályának;

b) a CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET, vagy azzal egyenértékű minősítésű adatot a Minősített Adatok Osztályának.

(2) A bizalmas adatok nyilvántartásáról, tárolásáról és nyomon követhetőségéről az ügy jellegének megfelelően vagy az adatot megkapó parlamenti szerv/tisztségviselő titkársága, vagy a Minősített Adatok Osztálya gondoskodik.

(3) A Bizottság által a keretmegállapodás II. melléklete 3.2. pontjának alapján továbbított bizalmas adat, vagy a Tanács által az intézményközi megállapodás 5. cikke (4) bekezdésének alapján továbbított minősített adat esetében a közös megegyezéssel meghatározandó, az adat bizalmas jellegének megőrzését szolgáló, megállapodás szerinti intézkedéseket a bizalmas adattal együtt az adott parlamenti szerv/tisztségviselő titkárságán vagy a Minősített Adatok Osztályán kell elhelyezni, az ügy jellegének megfelelően.

(4) A 3. bekezdésben említett intézkedések értelemszerűen alkalmazhatók a bizalmas adatok Szerződések által vagy alapján létrehozott többi intézmény, szerv, hivatal és ügynökség, illetve tagállamok általi továbbítása esetében is.

(5) A TRÈS SECRET UE/EU TOP SECRET vagy azzal egyenértékű minősítésnek megfelelő szintű védelem biztosítása érdekében az Elnökök Értekezlete felügyeleti bizottságot hoz létre. A TRÈS SECRET UE/EU TOP SECRET vagy azzal egyenértékű szinten minősített adatokat az Európai Parlament számára további szabályoknak megfelelően kell továbbítani, amelyeket az Európai Parlament az átadó uniós intézménnyel közösen állapít meg.

6. cikk

A minősített adat Európai Parlament általi továbbítása harmadik feleknek

Az Európai Parlament azzal a feltétellel továbbíthat – az ügy jellegének megfelelően a kibocsátó vagy a minősített adatot az Európai Parlament felé továbbító uniós intézmény előzetes írásbeli hozzájárulásával – ilyen minősített adatot harmadik feleknek, ha utóbbiak gondoskodnak arról, hogy az ilyen adatok kezelése során a szolgálataikon és épületeiken belül az e határozatban meghatározott szabályokkal egyenértékű szabályok érvényesülnek.

7. cikk

Biztonságos helyiségek

(1) A bizalmas adatok kezelése céljából az Európai Parlament biztonságos területet és biztonságos olvasótermeket hoz létre.

(2) A biztonságos terület lehetőséget ad a minősített adatok nyilvántartásba vételére, megtekintésére, archiválására, továbbítására és kezelésére. A biztonságos terület többek között egy olvasóteremből és egy ülésteremből áll, amelyek a minősített adatok megtekintését szolgálják, és azokat a Minősített Adatok Osztálya működteti.

(3) A biztonságos területen kívül is lehet biztonságos olvasótermet létesíteni a legfeljebb „RESTREINT UE/EU RESTRICTED” vagy azzal egyenértékű minősítésű szintű adatok, valamint az „egyéb bizalmas adatok” megtekintésének biztosítására. Ezeket a biztonságos olvasótermeket az illetékes parlamenti szerv/tisztségviselő titkársága vagy a Minősített Adatok Osztálya működteti, az ügy jellegének megfelelően. Ezekben a biztonságos olvasótermekben nem helyezhető el fénymásoló, telefon, fax, szkenner, vagy bármely más, dokumentumok másolására vagy továbbítására alkalmas műszaki berendezés.

8. cikk

A bizalmas adatok nyilvántartásba vétele, kezelése és tárolása

(1) A „RESTREINT UE/EU RESTRICTED” vagy azzal egyenértékű minősítésű adatot és az „egyéb bizalmas adatot” az illetékes parlamenti szerv/tisztségviselő titkársága vagy a Minősített Adatok Osztálya veszi nyilvántartásba és tárolja attól függően, hogy ki kapta meg az adatot.

(2) A „RESTREINT UE/EU RESTRICTED" vagy azzal egyenértékű minősítésű adat és az „egyéb bizalmas adat"kezelésére az alábbi feltételek alkalmazandók:

a) a dokumentumokat személyesen kell átadni a titkárság vezetőjének, aki köteles azokat nyilvántartásba venni, és átvételi elismervényt kiállítani róluk;

b) ezeket a dokumentumokat tényleges használatuk idején kívül zárt helyen kell őrizni, a titkárság felelőssége mellett;

c) semmilyen körülmények között nem lehet az adatot más eszközre menteni vagy bárkinek átadni; ezeket a dokumentumokat a biztonsági közleményben meghatározott, megfelelően akkreditált eszközzel lehet csak másolni;

d) az ilyen adathoz csak azok a személyek férhetnek hozzá, akiket a kibocsátó vagy az adatot az Európai Parlament felé továbbító uniós intézmény jelölt meg, a 4. cikk (2) bekezdésében vagy az 5. cikk (3), (4) vagy (5) bekezdésében említett szabályoknak megfelelően;

e) a parlamenti szerv/tisztségviselő titkársága nyilvántartást vezet az adatokat megtekintő személyekről, valamint a megtekintés napjáról és időpontjáról, és azonnal továbbítja a nyilvántartást a Minősített Adatok Osztályára azzal egyidőben, hogy az adatot elhelyezik a Minősített Adatok Osztályán.

(3) A „CONFIDENTIEL UE/EU CONFIDENTIAL", a „SECRET UE/EU SECRET" vagy a „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű minősítésű szintű adatot a Minősített Adatok Osztálya veszi nyilvántartásba, kezeli és tárolja a biztonságos területen, az adott minősítési szintnek megfelelően és a biztonsági közleményben meghatározottak szerint.

(4) Az (1)-(3) bekezdésben foglal szabályok megsértése esetén – az ügy jellegének megfelelően – a parlamenti szerv/tisztségviselő titkárságának vagy a Minősített Adatok Osztályának illetékes tisztviselője tájékoztatja a főtitkárt, aki az ügyet az elnök elé terjeszti, amennyiben abban az Európai Parlament valamely képviselője érintett.

9. cikk

A biztonságos helyiségekhez való hozzáférés

(2) A biztonságos területre csak a következők léphetnek be:

a) azok a személyek, akik a 3. cikk (4)-(7) bekezdése alapján betekinthetnek az ott tárolt adatokba, és akik a 10. cikk (1) bekezdése alapján kérelmet nyújtottak be;

b) azok a személyek, akik a 4. cikk (1) bekezdése alapján minősített adatokat hozhatnak létre, és a 10. cikk (1) bekezdése alapján kérelmet nyújtottak be;

c) az Európai Parlament Minősített Adatok Osztályán dolgozó tisztviselők;

d) a kommunikációs és információs rendszer irányításáért felelős európai parlamenti tisztviselők;

e) szükség esetén az Európai Parlamentnek a biztonságért és tűzvédelemért felelős tisztviselői,

f) a takarító személyzet csak a Minősített Adatok Osztályának tisztviselője jelenlétében és szigorú felügyelete mellett.

(2) A Minősített Adatok Osztálya megtagadhatja a biztonságos területre való belépést minden olyan személy esetében, aki nem jogosult a belépésre. A belépés megtagadása elleni kifogást az Európai Parlament képviselője általi belépés iránti kérelem esetén az elnöknek, más személyek esetében a főtitkárnak kell benyújtani.

(3) A főtitkár engedélyezheti korlátozott számú személyek találkozóját az a biztonságos területen belül található ülésteremben.

(4) A biztonságos olvasóterembe csak a következők léphetnek be:

a) a bizalmas adatok megtekintése vagy létrehozása céljából megfelelően azonosított európai parlamenti képviselők, európai parlamenti tisztviselők és a képviselőcsoportok alkalmazásában álló egyéb európai parlamenti alkalmazottak;

b) az Európai Parlamentnek a kommunikációs és információs rendszer irányításáért felelős tisztviselői, az adatot megkapó parlamenti szerv/tisztségviselő titkárságának tisztviselői és a Minősített Adatok Osztálya tisztviselői;

c) szükség esetén az Európai Parlamentnek a biztonságért és tűzvédelemért felelős tisztviselői;

d) a takarító személyzet csak – az ügy jellegének megfelelően – a parlamenti szerv/tisztségviselő titkárságán vagy a Minősített Adatok Osztályán dolgozó tisztviselő jelenlétében és szigorú felügyelete mellett.

(5) A parlamenti szerv/tisztségviselő illetékes titkársága vagy a Minősített Adatok Osztálya megtagadhatja a biztonságos olvasóterembe való belépést minden olyan személy esetében, aki nem jogosult a belépésre. A belépés megtagadása elleni kifogást az Európai Parlament képviselője általi belépés iránti kérelem esetén az elnöknek, más személyek esetében a főtitkárnak kell benyújtani.

10. cikk

Bizalmas adatok megtekintése vagy létrehozása a biztonságos helyiségekben

(1) A bizalmas adatot a biztonságos helyen megtekinteni vagy létrehozni kívánó személy előzetesen közli a Minősített Adatok Osztályával a nevét. A Minősített Adatok Osztálya ellenőrzi az adott személy személyazonosságát, és meggyőződik arról, hogy az adott személy a 3. cikk (3-(7)) bekezdésében, a 4. cikk (1) bekezdésében vagy az 5. cikk (3), (4) és (5) bekezdésében foglaltakkal összhangban jogosult-e engedéllyel az adat megtekintésére vagy létrehozására.

(2) A „RESTREINT UE/EU RESTRICTED” szinten vagy azzal egyenértékű szinten minősített adatokat és az „egyéb bizalmas adatokat” a 3. cikk (3) és (7) bekezdésének megfelelően a biztonságos olvasóteremben megtekinteni kívánó személy előzetesen közli az illetékes parlamenti szerv/tisztségviselő titkárságával vagy a Minősített Adatok Osztályával a nevét.

(3) Kivételes körülményektől (például ha rövid időn belül számos betekintési kérelmet nyújtanak be) eltekintve egyszerre csak egy személy számára engedélyezhető a bizalmas adat biztonságos helyiségben való, a parlamenti szerv/tisztségviselő titkárságának vagy a Minősített Adatok Osztálya egy tisztviselőjének jelenlétében történő megtekintése.

(4) A megtekintés ideje alatt tilos a külvilággal való kapcsolatfelvétel (beleértve a telefon vagy egyéb technológiai eszközök használatát is), a jegyzetkészítés és a megtekintett bizalmas adat fénymásolása vagy fényképezése.

(5) Mielőtt a betekintő személy engedélyt kapna a biztonságos helyiség elhagyására, a parlamenti szerv/tisztségviselő titkárságának vagy a Minősített Adatok Osztályának tisztviselője ellenőrzi a megtekintett bizalmas adatok meglétét, sértetlenségét és teljességét.

(6) A fenti szabályok megsértése esetén a parlamenti szerv/tisztségviselő titkárságának vagy a Minősített Adatok Osztályának tisztviselője tájékoztatja a főtitkárt, aki az ügyet az elnök elé terjeszti, amennyiben abban az Európai Parlament egy képviselője érintett.

11. cikk

A bizalmas adatoknak a biztonságos helyiségeken kívül, zárt ülésen történő megtekintésére vonatkozó minimumszabályok

(1) A „RESTREINT UE/EU RESTRICTED” szinten vagy azzal egyenértékű szinten minősített adatokat és az „egyéb bizalmas adatokat” a biztonságos helyiségeken kívül, zárt ülésen is megtekinthetik az Európai Parlament parlamenti bizottságainak vagy más politikai és adminisztratív szerveinek tagjai.

(2) Az (1) bekezdésben megfogalmazott körülmények fennállása esetén az ülésért felelős parlamenti szerv/tisztségviselő titkársága köteles gondoskodni az alábbi feltételek teljesüléséről:

a) csak az illetékes bizottság vagy szerv elnöke által az ülésen való részvételre kijelölt személyek léphetnek be az üléstermbe;

b) valamennyi dokumentumot besorszámozzák, az ülés kezdetén kiosztják és az ülés végén újra beszedik őket, továbbá ezekről a dokumentumokról jegyzetek, fénymásolatok és fényképek nem készülhetnek;

c) az ülés jegyzőkönyve nem tehet említést a szóban forgó adat megvitatásának tartalmáról. Kizárólag az esetlegesen e tárgyban hozott határozatokat lehet feljegyezni;

d) az Európai Parlamenten belüli címzettekkel szóban közölt bizalmas adatokra az írásbeli bizalmas adatokkal azonos szintű védelem vonatkozik;

e) nem lehet egyéb dokumentumokat tárolni az üléstermekben;

f) csak a szükséges számban lehet a dokumentumokat kiosztani a résztvevőknek és a tolmácsoknak az ülés kezdetén;

g) a dokumentumok minősítési/jelölési szintjét a levezető elnök az ülés kezdetén egyértelművé teszi;

h) a résztvevők nem vihetik ki a dokumentumokat az üléstermből;

i) a parlamenti szerv/tisztségviselő titkárság az ülés végén összegyűjti és leltárba veszi a dokumentumok minden példányát; és

j) semmilyen elektronikus kommunikációs eszköz vagy egyéb elektronikus eszköz nem vihető be abba az üléstermbe, ahol a kérdéses bizalmas adatokat megtekintik vagy megtárgyalják.

(3) Amikor a keretmegállapodás II. mellékletének 3.2.2 pontjában és az intézményközi megállapodás 6. cikke (5) bekezdésében meghatározott kivételeknek megfelelően a „CONFIDENTIEL UE/EU CONFIDENTIAL” szinten vagy azzal egyenértékű szinten minősített adatokat zárt ülésen tárgyalják, az ülésért felelős parlamenti szerv/tisztségviselő titkársága a (2) bekezdésben foglaltak teljesülése mellett köteles gondoskodni arról is, hogy az ülésen való részvételre kijelölt személyek eleget tegyenek a 3. cikk (4) és (7) bekezdésében foglalt követelményeknek.

(4) A (3) bekezdésben megfogalmazott esetben a Minősített Adatok Osztálya a zárt ülésért felelős parlamenti szerv/tisztségviselő titkársága rendelkezésére bocsátja a tárgyalásra kerülő dokumentumokat a szükséges példányszámban, amelyeket az ülés után vissza kell juttatni a Minősített Adatok Osztálya részére.

12. cikk

A bizalmas adat archiválása

(1) Gondoskodni kell biztonságos archiválási rendszer rendelkezésre állásáról a biztonságos területen belül. A biztonságos irattár kezelése a szabványos archiválási kritériumoknak megfelelően a Minősített Adatok Osztályának feladata.

(2) A Minősített Adatok Osztályán véglegesen elhelyezett minősített adatokat és a parlamenti szerv/tisztségviselő titkárságánál elhelyezett „RESTREINT UE/EU RESTRICTED” szinten vagy azzal egyenértékű szinten minősített adatokat hat hónappal az utolsó megtekintésük után, de legkésőbb elhelyezésük után egy évvel át kell helyezni a biztonságos területen belül található irattárba. Az „egyéb bizalmas adatokat” – kivéve, ha azokat a Minősített Adatok Osztályán helyezték el – az érintett parlamenti szerv/tisztségviselő titkárságai archiválják, a dokumentumkezelés általános szabályainak megfelelően.

(3) A biztonságos irattárban tárolt bizalmas adat az alábbi feltételek teljesülése esetén tekinthető meg:

a) csak a bizalmas adat elhelyezésekor kitöltött kísérőlapon szereplő, név, beosztás vagy tisztség szerint azonosított személyek kaphatnak engedélyt az adott adat megtekintésére;

b) a betekintési kérelmet a Minősített Adatok Osztályának kell benyújtani, amely biztosítja a kérdéses dokumentum átszállítását az irattárból a biztonságos olvasóterembe;

c) a 10. cikkben megállapított, a bizalmas adatok megtekintésére vonatkozó eljárások és feltételek alkalmazandók.

13. cikk

A bizalmas adat visszaminősítése, illetve a minősítés és a jelölés megszüntetése

(1) Bizalmas adatot csak a kibocsátó előzetes engedélyével lehet visszaminősíteni, vagy azok minősítését vagy jelölését megszüntetni, szükség esetén az egyéb érdekelt felekkel történt egyeztetés után.

(2) A visszaminősítést, illetve a minősítés megszüntetését írásban kell megerősíteni. A kibocsátó feladata tájékoztatni a címzetteket a változásról, akiknek viszont azokat a további címzetteket kell tájékoztatniuk a változásról, akiknek ők a dokumentumot megküldték vagy lemásolták. Ha lehetséges, a kibocsátók a minősített dokumentumokon meghatározzák azt az időpontot, időtartamot vagy eseményt, amikortól vagy amelynek lejártát, illetve bekövetkezését követően a tartalom visszaminősíthető vagy minősítése megszüntethető. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálniuk annak megállapítása érdekében, hogy az eredeti minősítés továbbra is szükséges-e.

(3) A biztonságos irattárban tárolt bizalmas adatokat kellő időben, de legkésőbb a dokumentum létrehozását követő 25. évben meg kell vizsgálni annak eldöntésére, hogy szükség van-e azok visszaminősítésére, illetve a minősítés vagy a jelölés megszüntetésére. Ezen adatok vizsgálatára és közzétételére az Európai Gazdasági Közösség és az Európai Atomenergia-közösség levéltárainak a nyilvánosság számára történő megnyitásáról szóló, 1983. február 1-jei 354/83/EGK, Euratom tanácsi rendelet ([1]) rendelkezéseinek megfelelően kerül sor. A minősítés megszüntetését a minősített adat kibocsátója vagy az adott időben illetékes szolgálat hajtja végre az I. melléklet 1. részének 10. szakaszával összhangban.

(4) A minősítés megszüntetését követően a biztonságos irattárban tárolt, korábban minősített adatot át kell helyezni az Európai Parlament levéltárába állandó megőrzésre és további kezelésre az alkalmazandó szabályok szerint.

(5) A jelölés megszüntetését követően a korábbi „egyéb bizalmas adat” az Európai Parlament adatkezelési szabályainak hatálya alá esik.

14. cikk

A biztonsági szabályok megsértése, bizalmas adatok elvesztése vagy illetéktelen tudomására jutása

(1) Általában az adat bizalmas jellegének, vagy kifejezetten e határozatnak a megsértése az Európai Parlament képviselői esetén az Európai Parlament eljárási szabályzatában meghatározott szankciókkal kapcsolatos, vonatkozó rendelkezések alkalmazását vonja maga után.

(2) Az Európai Parlament képviselője vagy személyzete által elkövetett szabálysértés a 259/68/EGK, Euratom, ESZAK rendeletben meghatározott, az Európai Unió tisztviselőinek személyzeti szabályzatában és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben ([2]) (személyzeti szabályzat) foglalt eljárások és szankciók alkalmazását vonja maga után.

([1]) HL L 43., 1983.2.15., 1. o.
([2]) HL L 56., 1968.3.4., 1. o.

(3) A szükséges vizsgálatokat – az ügy jellegének megfelelően – az elnök és/vagy a főtitkár szervezi meg a 6. számú biztonsági közleményben meghatározott szabálysértés esetén.

(4) Amennyiben a bizalmas adatot egy uniós intézmény vagy tagállam továbbította az Európai Parlament felé, az elnök és/vagy a főtitkár – az ügy jellegének megfelelően – tájékoztatja az érintett uniós intézményt vagy tagállamot a minősített adat beigazolódott vagy feltételezett elvesztéséről vagy illetéktelen tudomására jutásáról, a vizsgálat eredményeiről és az ismételt előfordulás megakadályozására tett intézkedésekről.

15. cikk

E határozat és végrehajtási szabályainak kiigazítása, valamint évenkénti jelentéstétel e határozat alkalmazásáról

(1) E határozat és az azt végrehajtó mellékletek szükséges kiigazítására vonatkozóan a főtitkár tesz javaslatot, és e javaslatokat döntéshozatal céljából továbbítja az Elnökségnek.

(2) A főtitkár felelős azért, hogy e határozatot az Európai Parlament szolgálatai végrehajtsák, emellett ő adja ki az ISMS által szabályozott kérdések kezelési utasításait is, az e határozatban foglalt elvekkel összhangban.

(3) A főtitkár éves jelentést nyújt be az Elnökségnek e határozat alkalmazásáról.

16. cikk

Átmeneti és záró rendelkezések

(1) A Minősített Adatok Osztályán vagy az Európai Parlament bármely más archívumában tárolt, bizalmasnak minősülő és 2014. április 1-je előtti keltezésű nem minősített adatokat e határozat alkalmazásában „egyéb bizalmas adatnak" kell tekinteni. A kibocsátó bármikor megváltoztathatja az adat bizalmas jellegének szintjét.

(2) E határozat 5. cikke (1) bekezdésének a) pontjától és 8. cikkének (1) bekezdésétől eltérve, 2014. április 1-jétől számított tizenkét hónapig a Tanács részéről az intézményközi megállapodásnak megfelelően rendelkezésre bocsátott, „RESTREINT UE/EU RESTRICTED" szinten vagy azzal egyenértékű szinten minősített adatokat a Minősített Adatok Osztályán kell elhelyezni, nyilvántartásba venni és tárolni. Az ilyen adatokat az intézményközi megállapodás 4. cikke (2) bekezdésének a) és c) pontjának, illetve 5. cikke (4) bekezdésének megfelelően lehet megtekinteni.

(3) Az Elnökség 2011. június 6-i, a bizalmas információk Európai Parlament általi kezelésére vonatkozó szabályokról szóló határozata hatályát veszti.

17. cikk

Hatálybalépés

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

I. MELLÉKLET

I. rész

A BIZALMAS ADATOK VÉDELMÉRE VONATKOZÓ ALAPELVEK ÉS BIZTONSÁGI MINIMUMSZABÁLYOK

1. **BEVEZETÉS**

Ezek a rendelkezések állapítják meg azokat a bizalmas adatok védelmét szolgáló azon alapelveket és biztonsági minimumszabályokat, amelyeket az Európai Parlamentnek valamennyi munkahelyén, valamint a minősített adatok és „egyéb bizalmas adatok" valamennyi címzettjének tiszteletben kell tartania és/vagy be kell tartania a biztonság fenntartása és annak érdekében, hogy minden érintett személy biztos lehessen afelől, hogy a védelem közös szintje megvalósul. Ezeket a rendelkezéseket a II. mellékletben foglalt biztonsági közlemények és egyéb, a bizalmas adatok parlamenti bizottságok, valamint egyéb parlamenti szervek és tisztségviselők általi kezelésére vonatkozó egyéb rendelkezések egészítik ki.

2. **ALAPELVEK**

Az Európai Parlament biztonsági politikája az általános belső igazgatási politikájának szerves részét képezi, és így alapjául az erre az általános politikára irányadó elvek szolgálnak. Ezek az elvek a törvényességet, az átláthatóságot, az elszámoltathatóságot, a szubszidiaritást és az arányosságot foglalják magukban.

A törvényesség annak szükségességét jelenti, hogy a biztonsági feladatok ellátása során szigorúan a törvényes keretek között kell maradni, és meg kell felelni a vonatkozó jogi követelményeknek. Emellett a biztonság terén a hatásköröket megfelelő jogi rendelkezésekre kell alapozni. A személyzeti szabályzat rendelkezései, különösen a személyzetnek a feladataik ellátása során tudomásukra jutott információk jogosulatlan nyilvánosságra hozatalától való tartózkodására irányuló kötelezettségéről szóló 17. cikk, valamint a fegyelmi intézkedésekről szóló VI. cím maradéktalanul alkalmazandók. Végezetül, a biztonságnak az Európai Parlament felelősségi körén belül történő megsértésével úgy kell foglalkozni, hogy az megfeleljen eljárási szabályzatának és fegyelmi intézkedésekkel kapcsolatos politikájának.

Az átláthatóság annak szükségességét jelenti, hogy valamennyi biztonsági szabálynak és rendelkezésnek világosnak kell lennie, hogy a különböző szolgálatok és a különböző területek között egyensúlynak kell lennie (fizikai biztonság az információk védelmével összehasonlítva stb.), továbbá hogy következetes és strukturált biztonságtudatossági politikát kell folytatni. Emellett a biztonsági intézkedések végrehajtásához világos írásos iránymutatásokra van szükség.

Az elszámolási kötelezettség azt jelenti, hogy a biztonság terén a hatáskörök világosan meghatározásra kerülnek. Emellett azt is jelenti, hogy rendszeresen figyelemmel kell kísérni, hogy ezeket a hatásköröket megfelelően hajtották-e végre.

A szubszidiaritás azt jelenti, hogy a biztonságot a lehető legalacsonyabb szinten és az Európai Parlament Főigazgatóságaihoz és szolgálataihoz a lehető legközelebb szervezik meg.

Az arányosság elve azt jelenti, hogy a biztonsági tevékenységeket szigorúan csak arra korlátozzák, ami feltétlenül szükséges, valamint hogy a biztonsági intézkedéseknek arányosaknak kell lenniük a védeni kívánt érdekekkel, valamint az ezeket az érdekeket fenyegető tényleges vagy lehetséges veszéllyel, annak érdekében, hogy olyan védelemben részesülhessenek, amely a lehető legkisebb zavart okozza.

3. **AZ INFORMÁCIÓBIZTONSÁG ALAPJAI**

A stabil információbiztonság alapjai a következők:

a) megfelelő kommunikációs és információs rendszerek. Ezek az Európai Parlament biztonsági hatóságának hatáskörébe tartoznak (az 1. biztonsági közleményben meghatározottak szerint).

b) az Európai Parlamenten belül az Információvédelmi hatóság (az 1. biztonsági közleményben meghatározottak szerint), amelynek hatáskörébe tartozik, hogy a biztonsági hatósággal együttműködve (az 1. biztonsági közleményben meghatározottak szerint) tájékoztasson és tanácsot adjon a kommunikációs és információs rendszerekre irányuló technikai fenyegetésekről és az e fenyegetésekkel szemben alkalmazandó védelmi eszközökről.

c) az Európai Parlament illetékes szolgálatai és más uniós intézmények biztonsági szolgálatai közötti szoros együttműködés.

4. **AZ INFORMÁCIÓBIZTONSÁG ELVEI**

4.1. ***Célkitűzések***

Az információbiztonság elsődleges céljai a következők:

a) a bizalmas adatok védelme a kémkedés, ezen adatok illetéktelenek tudomására jutása vagy az engedély nélküli kiszolgáltatás ellen;

b) a kommunikációs és információs rendszerekben és hálózatokban kezelt minősített adatok védelme a titkosságukat, integritásukat és rendelkezésre állásukat fenyegető veszélyekkel szemben;

c) a minősített adatoknak helyet adó európai parlamenti helyiségek védelme a szabotázzsal és a szándékos rosszindulatú rongálással szemben;

d) a biztonsági intézkedések kudarca esetén az okozott kár felmérése, a következmények korlátozása, a biztonsági vizsgálatok lefolytatása és a szükséges korrekciós intézkedések elfogadása.

4.2. ***Minősítés***

4.2.1. A titkosság terén körültekintés és tapasztalat szükséges a védendő információk és anyagok kiválasztása és a védelem szükséges fokának megítélése során. Alapvető, hogy a védelem foka megfeleljen az egyes védendő információ vagy anyag biztonsági szempontú érzékenységének. A zökkenőmentes információáramlás biztosítása érdekében el kell kerülni mind a túlzottan magas, mind pedig a túlzottan alacsony minősítést.

4.2.2. A minősítési rendszer az ebben a szakaszban meghatározott elvek gyakorlatba való átültetésének eszköze. Hasonló minősítési rendszer alkalmazandó a kémkedés, a szabotázs, a terrorizmus és az egyéb fenyegetések elleni intézkedések megtervezése és megszervezése során, hogy a minősített adatoknak helyet adó legfontosabb helyiségek és azokon belül a legérzékenyebb pontok a legmagasabb szintű védelemben részesüljenek.

4.2.3. Az információ minősítése kizárólag az adott információ kibocsátójának a feladata.

4.2.4. A minősítés szintje kizárólag az adott információ tartalmán alapulhat.

4.2.5. Több adattétel egy csoportba sorolása esetén az egész anyag tekintetében alkalmazandó minősítési szintnek legalább olyan magasnak kell lennie, mint a legmagasabb minősítésű alkotórész minősítése. Az információk gyűjteménye azonban magasabb minősítést is kaphat, mint az alkotórészei külön-külön.

4.2.6 Minősítés csak akkor és annyi időre adható, amikor és ameddig az szükséges.

4.3. ***A biztonsági intézkedések céljai***

A biztonsági intézkedéseknek:

a) ki kell terjedniük mindazon személyekre, akik minősített adatokhoz férnek hozzá, a minősített adatokat hordozó eszközökre és minden „egyéb bizalmas adatra”, az ilyen adatoknak helyet adó valamennyi helyiségre és a fontos berendezésekre;

b) azonosítani kell tudniuk azokat a személyeket, akiknek a pozíciója (hozzáférés, kapcsolatok vagy egyéb tényezők tekintetében) veszélyeztetheti az ilyen adatok és az ilyen adatoknak helyet adó fontos berendezések biztonságát, és rendelkezniük kell ezen személyek kizárásáról vagy eltávolításáról;

c) meg kell akadályozniuk, hogy illetéktelen személyek az ilyen információkhoz vagy az azokat tartalmazó berendezésekhez hozzáférhessenek;

d) biztosítaniuk kell, hogy az ilyen információk terjesztése kizárólag a „szükséges ismeret” elve alapján történjék, ami a biztonság valamennyi vonatkozása szempontjából alapvető;

e) biztosítaniuk kell az – különösen az elektromágneses formában tárolt, feldolgozott vagy továbbított – bizalmas adatok integritását (azáltal, hogy meg akadályozzák azok megrongálódását, illetéktelen módosítását vagy illetéktelen törlését) és rendelkezésre állását (azok számára, akiknek szükségük van rá és a hozzáféréshez felhatalmazással rendelkeznek).

5. KÖZÖS MINIMUMSZABÁLYOK

Az Európai Parlament biztosítja, hogy a biztonság közös minimumszabályait a minősített adatok valamennyi, mind az intézményen belüli, mind annak hatáskörébe tartozó címzettje – azaz az összes szolgálata és szerződéses megbízottja – betartsa, hogy az ilyen adatokat annak tudatában lehessen továbbítani, hogy azokat mindenhol ugyanolyan gondossággal kezelik. Ezek a minimumszabályok tartalmazzák az Európai Parlament tisztviselői és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak biztonsági tanúsítványának kritériumait és a bizalmas információk védelmére irányuló eljárásokat.

Az Európai Parlament az ilyen adatokhoz való hozzáférést harmadik felek számára csak azzal a feltétellel engedélyezi, ha azok biztosítják, hogy az adatok kezelése során olyan rendelkezések betartásával járnak el, amelyek ezekkel a közös minimumszabályokkal legalább szigorúan egyenértékűek.

Az ilyen közös minimumszabályok vonatkoznak azokra az esetekre is, amikor az Európai Parlament szerződés vagy támogatási megállapodás alapján ipari vagy más szervezeteket bíz meg bizalmas információkat érintő feladatokkal.

6. A BIZTONSÁG AZ EURÓPAI PARLAMENT TISZTVISELŐI ÉS A KÉPVISELŐCSOPORTOK ALKALMAZÁSÁBAN ÁLLÓ EGYÉB PARLAMENTI ALKALMAZOTTAK VONATKOZÁSÁBAN

6.1. *Az Európai Parlament tisztviselőire és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottakra vonatkozó biztonsági előírások*

Az Európai Parlament azon tisztviselői és a képviselőcsoportok alkalmazásában álló azon egyéb parlamenti alkalmazottak, akik olyan beosztásban dolgoznak, amelyben minősített adatokhoz férhetnének hozzá, hivatalba lépésükkor, majd ezt követően rendszeres időközönként alapos oktatásban részesülnek a biztonság szükségessége és az ezzel kapcsolatos eljárások tekintetében. E személyek számára előírás, hogy írásban erősítsék meg, hogy az alkalmazandó biztonsági rendelkezéseket elolvasták és teljes mértékben megértették.

6.2. *A vezetők felelőssége*

A vezetők kötelezettségeinek részét kell képezze annak ismerete, hogy beosztottjaik közül kik vesznek részt minősített adatokkal kapcsolatos munkában, illetve kik rendelkeznek hozzáféréssel biztonságos kommunikációs vagy információs rendszerekhez, továbbá hogy feljegyezzék és jelentsék azokat az eseményeket vagy nyilvánvalóan gyenge pontokat, amelyek kihatással lehetnek a biztonságra.

6.3. *Az Európai Parlament tisztviselői és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak biztonsági státusza*

Eljárások kialakítására kerül sor annak biztosítására, hogy – amikor az Európai Parlament tisztviselőjével vagy valamely képviselőcsoport alkalmazásában álló egyéb parlamenti alkalmazottal kapcsolatosan kedvezőtlen információk válnak ismertté – lépéseket tegyenek annak meghatározása érdekében, hogy az illető személy munkája során kapcsolatba kerüle minősített adatokkal vagy rendelkezik-e hozzáféréssel biztonságos kommunikációs vagy információs rendszerekhez, és hogy erről tájékoztassák az Európai Parlament illetékes szolgálatát. Ha az illetékes nemzeti biztonsági hatóság jelzi, hogy a kérdéses személy biztonsági kockázatot jelent, az illetőt azon feladatokból, amelyek ellátása során a biztonságot veszélyeztetheti, ki kell zárni vagy beosztásából el kell távolítani.

7. FIZIKAI BIZTONSÁG

A „fizikai biztonság” a minősített adatokhoz való illetéktelen hozzáférés megakadályozását célzó fizikai és technikai védelmi intézkedések alkalmazását jelenti.

7.1. ***A védelem szükségessége***

A minősített adatok védelmének biztosítása érdekében alkalmazandó fizikai biztonsági intézkedések mértékének arányosnak kell lennie a birtokolt információk és anyagok minősítésével és mennyiségével, valamint az azokat fenyegető veszéllyel. A minősített adatok valamennyi birtokosa egységes gyakorlatot köteles követni az ilyen információk minősítése tekintetében, és közös védelmi szabályoknak köteles eleget tenni a védelmet igénylő információk és anyagok megőrzése, továbbítása és megsemmisítése tekintetében.

7.2. ***Ellenőrzés***

A minősített adatok elhelyezésére szolgáló területek elhagyása előtt a minősített adatok biztonságos megőrzéséért felelős személyeknek meg kell győződniük arról, hogy az adatok tárolása kellően biztonságos-e és hogy az összes biztonsági berendezést (zárakat, riasztókat stb.) működésbe hozták-e. Munkaidő után további, független ellenőrzéseket kell végezni.

7.3. ***Az épületek biztonsága***

A minősített adatok vagy a biztonságos kommunikációs és információs rendszerek elhelyezésére szolgáló épületeket védeni kell az illetéktelen behatolás ellen.

A minősített adatok számára nyújtott védelem természete – például ablakrácsok, ajtózárak, őrök a bejáratnál, automatikus hozzáférés-ellenőrző rendszerek, biztonsági ellenőrzések és őrjáratok, riasztórendszerek, behatolásjelző rendszerek és őrkutyák – a következőktől függ:

a) a védendő információ és anyag minősítése, mennyisége és elhelyezkedése az épületen belül;

b) az érintett információkat és anyagokat tartalmazó biztonsági tárolóeszközök minősége; továbbá

c) az épület fizikai jellemzői és elhelyezkedése.

A kommunikációs és információs rendszerek számára nyújtott védelem jellege attól függ, hogy a felmérések szerint milyen eszközérték forog kockán és mekkora a lehetséges kár a biztonság veszélyeztetése esetén, továbbá hogy milyenek a rendszer elhelyezésére szolgáló épület fizikai jellemzői és milyen az elhelyezkedése, valamint attól, hogy a rendszer miként van elhelyezve az épületen belül.

7.4. ***Vészhelyzeti tervek***

Előzetesen részletes terveket kell kidolgozni a minősített adatok védelmére vészhelyzet esetén.

8. **BIZTONSÁGI AZONOSÍTÓK, JELÖLÉSEK, FELTÜNTETÉS ÉS A MINŐSÍTÉS SZABÁLYAI**

8.1. ***Biztonsági azonosítók***

Csak az ezen határozat 2. cikkének d) pontjában meghatározott minősítések alkalmazhatók.

Egyezményes biztonsági azonosító használható a minősítés érvényességi idejének behatárolására (azaz a minősített adatok automatikus visszaminősítése vagy a minősítésük automatikus megszüntetése időpontjának maghatározására).

Biztonsági azonosítókat csak minősítéssel együtt lehet használni.

A 2. biztonsági közlemény további szabályozást tartalmaz a biztonsági azonosítók tekintetében, amelyek meghatározását a kezelési utasítások tartalmazzák.

8.2. ***Jelölések***

A jelöléseket a bizalmas adatok kezelésére vonatkozó, előre meghatározott, konkrét utasítások részletezésére használják. A jelölések továbbá jelölhetnek egy adott dokumentum által érintett területet vagy egy adott, a „szükséges ismeret" elve alapján történő elosztást, illetve (nem minősített adatok esetében) a tilalom végét.

A jelölés nem minősítés, és helyette nem használható.

A 2. biztonsági közlemény további szabályozást tartalmaz a jelölések tekintetében, amelyek meghatározását a kezelési utasítások tartalmazzák.

8.3. ***A minősítések és a biztonsági azonosítók feltüntetése***

A minősítéseket, a biztonsági azonosítókat és a jelöléseket a 2. biztonsági közlemény E. pontjával és a kezelési utasításokkal összhangban kell feltüntetni.

8.4. ***A minősítés szabályai***

8.4.1 *Általános követelmények*

Az adatok csak akkor kapnak minősítést, ha ez szükséges. A minősítést világosan és szabályosan kell jelölni és a minősítés csak addig tartható fenn, amíg az adatok védelemre szorulnak.

Az adatok minősítése és későbbi visszaminősítése vagy a minősítés megszüntetése kizárólag a kibocsátó feladata.

Az Európai Parlament tisztviselői csak a főtitkár utasítására vagy megbízásából végzik el az adatok minősítését, illetve minősítik azokat vissza vagy szüntetik meg minősítésüket.

A minősített dokumentumok kezelésére vonatkozó részletes eljárásokat úgy kell kialakítani, hogy a bennük foglalt információknak megfelelő védelmük biztosítva legyen.

A „TRÈS SECRET UE/EU TOP SECRET" szinten minősített adatok kibocsátására felhatalmazott személyek számát a lehető legkisebbre kell korlátozni és nevüket egy a Minősített Adatok Osztálya (CIU) által összeállított listán kell feljegyezni.

8.4.2 *Minősítések alkalmazása*

Egy dokumentum minősítését az határozza meg, hogy tartalma a 2. cikk d) pontjában foglalt fogalommeghatározásoknak megfelelően mennyire érzékeny. Fontos, hogy a minősítést szabályosan határozzák meg és csak akkor alkalmazzák, ha valóban szükséges.

A csatolmányokat tartalmazó levél vagy feljegyzés legalább ugyanolyan magas minősítést kap, mint a legmagasabb minősítésű csatolmánya. A kibocsátónak világosan jeleznie kell, hogy a levél vagy feljegyzés milyen szintű minősítést kapjon, ha a csatolmányaitól elválasztják.

A minősítendő dokumentum kibocsátójának követnie kell a fenti szabályokat és el kell kerülnie mind a felülminősítést, mind az alulminősítést.

Egy adott dokumentum egyes oldalai, bekezdései, szakaszai, mellékletei, függelékei, toldalékai és csatolmányai eltérő minősítést igényelhetnek és ennek megfelelő jelölést kell kapniuk. A dokumentum egésze a legmagasabb minősítésű rész minősítését kapja.

9. **ELLENŐRZÉSEK**

Az Európai Parlament Biztonsági és Kockázatértékelési Igazgatósága – amely segítséget kérhet a Bizottság vagy a Tanács biztonsági hatóságaitól – rendszeres időközönként belső ellenőrzést végez a minősített adatok védelmét szolgáló biztonsági intézkedések tekintetében.

A biztonsági hatóságok és az uniós intézmények illetékes szolgálatai a valamennyi fél által kezdeményezett, megállapodáson alapuló folyamat részeként elvégezhetik a vonatkozó intézményközi megállapodásoknak megfelelően kicserélt minősített adatok védelmét célzó biztonsági intézkedések szakértői értékelését.

10. **A MINŐSÍTÉS FELOLDÁSÁT ÉS A JELÖLÉS MEGSZÜNTETÉSÉT CÉLZÓ ELJÁRÁSOK**

10.1. A Minősített Adatok Osztálya megvizsgálja a nyilvántartásában szereplő bizalmas adatokat, és a dokumentum kibocsátójának hozzájárulását kéri a minősítés vagy a jelölés legkésőbb a dokumentum létrehozásának 25. évfordulóján történő megszüntetéséhez. Azokat a dokumentumokat, amelyek minősítését vagy jelölését az első vizsgálatkor nem szüntetik meg, rendszeresen, de legalább ötévenként felül kell vizsgálni. A ténylegesen a biztonságos helyen a biztonságos irattárban lévő és megfelelően minősített dokumentumokon kívül a jelölés megszüntetésére irányuló eljárás az akár a Parlament szervénél/hivatalánál, vagy a Parlament levéltáráért felelő szolgálatnál található egyéb bizalmas adatokra is kiterjedhet.

10.2 A dokumentum minősítésének feloldására vagy jelölésének megszüntetésére irányuló döntést főszabályként kizárólag a dokumentum kibocsátója hozhatja meg, vagy, kivételes esetben, az ilyen adatokat birtokoló parlamenti szervvel/hivatallal együttműködésben, mielőtt a dokumentumban szereplő adatok továbbításra kerülnének a Parlament levéltáráért felelős szolgálathoz. A minősített adatok minősítésének feloldására vagy jelölésének megszüntetésére csak a kibocsátó előzetes írásbeli hozzájárulásával kerülhet sor. „Egyéb bizalmas adatok" esetén az ilyen adatok felett rendelkező parlamenti szerv/tisztségviselő titkársága a kibocsátóval együttműködve dönt arról, hogy a dokumentum minősítése feloldható-e.

10.3. A Minősített Adatok Osztályának feladata, hogy a kibocsátó nevében tájékoztassa a dokumentumok címzettjeit a minősítés vagy jelölés megváltozásáról, akiknek viszont azokat a további címzetteket kell tájékoztatniuk a változásról, akiknek ők a dokumentumot megküldték vagy lemásolták.

10.4. A minősítés megszüntetése nem vonatkozik a dokumentumon esetlegesen megjelenő biztonsági azonosítókra vagy jelölésekre.

10.5. A minősítés feloldása esetén a dokumentum minden oldalán alul és felül feltüntetett eredeti minősítést át kell húzni. A dokumentum első oldalát (a borítólapját) le kell pecsételni, és fel kell tüntetni rajta a Minősített Adatok Osztályára való hivatkozást. A jelölés megszüntetése esetén a dokumentum minden oldalán felül feltüntetett eredeti jelölést át kell húzni.

10.6. A dokumentum szövegét, amelynek a minősítését feloldották vagy jelölését megszüntették, hozzá kell csatolni ahhoz az elektronikus mappához vagy az ezzel egyenértékű rendszerhez, amelyben azt regisztrálták.

10.7. A magánszférára és az egyén sérthetetlenségére vagy a természetes vagy jogi személy kereskedelmi érdekeire vonatkozó kivételek hatálya alá eső dokumentumok és a minősített dokumentumok esetében a 354/83/EGK, Euratom rendelet 2. cikke alkalmazandó.

10.8. A 10.1-10.7 pontok rendelkezésein kívül az alábbi szabályok alkalmazandók:

a) harmadik felek dokumentumai tekintetében a Minősített Adatok Osztálya a minősítés feloldása vagy a jelölés megszüntetése előtt konzultál az érintett harmadik féllel;

b) a magánszférára és az egyén sérthetetlenségére vonatkozó kivétel tekintetében a minősítés feloldásakor vagy a jelölés megszüntetésekor figyelembe veszik különösen az érintett személy hozzájárulását, vagy adott esetben az érintett azonosíthatatlanságát;

c) a természetes vagy jogi személy kereskedelmi érdekeire vonatkozó kivétel tekintetében az érintett személy tájékoztatása történhet az *Európai Unió Hivatalos Lapjában* való közzététel révén, a megjegyzések előterjesztésére vonatkozó határidő pedig 4 hét lehet.

2. rész

BIZTONSÁGI ELLENŐRZÉSI ELJÁRÁS

11. **AZ EURÓPAI PARLAMENT KÉPVISELŐIRE VONATKOZÓ BIZTONSÁGI ELLENŐRZÉSI ELJÁRÁS**

11.1. A „CONFIDENTIEL UE/EU CONFIDENTIAL” szinten vagy azzal egyenértékű szinten minősítésett adatokhoz való hozzáférés érdekében az európai parlamenti képviselők felhatalmazást kell hogy kapjanak akár az e melléklet 11.3 és 11.4 pontjában említett eljárásnak megfelelően, akár az e határozat 3. cikkének (4) bekezdése szerinti hivatalos nyilatkozatuk alapján, amelyben vállalják, hogy ezeket az adatokat nem közlik másokkal.

11.2 Ahhoz, hogy az Európai Parlament képviselői hozzáférhessenek a „SECRET UE/EU SECRET” vagy „TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatokhoz, a 11.3 és 11.14 pontban említett eljárásnak megfelelő felhatalmazással kell rendelkezniük.

11.3. Felhatalmazást csak az Európai Parlament azon képviselői kapnak, akiket a tagállamok illetékes nemzeti hatóságai a 11.9-11.14 pontban említett eljárásnak megfelelően biztonsági ellenőrzésnek vetettek alá. A képviselők felhatalmazása tekintetében az elnök az illetékes.

11.4 Az elnök azt követően adhatja meg az írásos felhatalmazást, hogy megkapta a tagállamok illetékes nemzeti hatóságainak véleményét a 11.8-11.13 pontnak megfelelően lefolytatott biztonsági ellenőrzés alapján.

11.5. Az Európai Parlament Biztonsági és Kockázatértékelési Igazgatósága naprakész listát vezet az Európai Parlament azon képviselőiről, akik felhatalmazást kaptak, beleértve a 11.15 pont értelmében vett ideiglenes felhatalmazást is.

11.6. A felhatalmazás ötéves időtartamra vagy azon feladatok időtartamára érvényes, amelyekre tekintettel a felhatalmazást megadták, attól függően, hogy melyik a rövidebb. A felhatalmazás a 11.4 pontban meghatározott eljárásnak megfelelően megújítható.

11.7. Az elnök visszavonja a felhatalmazást, ha úgy ítéli meg, hogy a visszavonásra megfelelő oka van. A felhatalmazás visszavonásáról szóló határozatról értesíteni kell az érintett európai parlamenti képviselőt, aki még a visszavonásról szóló határozat érvénybe lépése előtt meghallgatást kérhet az elnöktől, valamint az illetékes nemzeti hatóságot.

11.8. A biztonsági ellenőrzést az Európai Parlament érintett képviselője közreműködésével és az elnök kérésére folytatják le. Az ellenőrzés tekintetében az érintett képviselő állampolgársága szerinti tagállam nemzeti hatósága az illetékes.

11.9. Az ellenőrzési eljárás részeként az Európai Parlament érintett képviselőjének kérdőívet kell kitöltenie.

11.10. Az elnök az illetékes nemzeti hatósághoz intézett megkeresésében meghatározza az Európai Parlament érintett képviselője rendelkezésére bocsátandó minősített adatok szintjét, hogy az ellenőrzési eljárást lefolytathassa.

11.11 Az illetékes nemzeti hatóság által lefolytatott teljes biztonsági ellenőrzési eljárásra és a kapott eredményekre az érintett tagállamban hatályos megfelelő szabályok és rendelkezések vonatkoznak, beleértve a jogorvoslattal kapcsolatos rendelkezéseket is.

11.12. Ha az illetékes nemzeti hatóság kedvező véleményt ad, az elnök megadhatja a felhatalmazást az Európai Parlament érintett képviselőjének.

11.13. Az illetékes nemzeti hatóság elutasító véleményéről értesíteni kell az Európai Parlament érintett képviselőjét, aki meghallgatást kérhet az elnöktől. Ha az elnök szükségesnek tartja, az illetékes nemzeti hatóságtól további tájékoztatást kérhet. Ha az elutasító véleményt a hatóság megerősítik, akkor a felhatalmazást nem lehet megadni.

11.14. Az Európai Parlament mindazon képviselői, akik a 11.3 pont értelmében felhatalmazást kaptak, a felhatalmazás megadásának időpontjában, majd azt követően rendszeres időközönként minden szükséges utasítást megkapnak a minősített adatok védelmével és a védelem biztosításának módjával kapcsolatosan. E képviselőknek nyilatkozatot kell aláírniuk, amelyben igazolják, hogy megkapták ezeket az iránymutatásokat.

11.15. Kivételes esetben az elnök, miután az illetékes nemzeti hatóságot értesítette és az erre egy hónapon belül nem reagált, legfeljebb hat hónapos időtartamra ideiglenes felhatalmazást adhat az Európai Parlament valamely képviselőjének, amíg a 11.11 pontban említett ellenőrzés eredményét meg nem kapja. Az így megadott ideiglenes felhatalmazások nem biztosítanak hozzáférést a „TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatokhoz.

12. AZ EURÓPAI PARLAMENT TISZTVISELŐIRE ÉS A KÉPVISELŐCSOPORTOK ALKALMAZÁSÁBAN ÁLLÓ EGYÉB PARLAMENTI ALKALMAZOTTAKRA VONATKOZÓ BIZTONSÁGI ELLENŐRZÉSI ELJÁRÁS

12.1. A minősített adatokhoz az Európai Parlamentnek csak azok a tisztviselői és csak azok a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak férhetnek hozzá, akiknek feladataik alapján és a szolgálat követelményei miatt ismerniük vagy használniuk szükséges azokat.

12.2. Ahhoz, hogy az Európai Parlament tisztviselői és az érintett képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak hozzáférhessenek a „CONFIDENTIEL UE/EU CONFIDENTIAL”, „TRÈS SECRET UE/EU TOP SECRET” vagy „SECRET UE/EU SECRET” szinten, illetve az azzal egyenértékű szinten minősített adatokhoz, a 12.3 és 12.4 pontban meghatározott eljárásnak megfelelő felhatalmazással kell rendelkezniük.

12.3. Felhatalmazást a 12.1 pontban említett személyek közül csak azok kapnak, akiket a tagállamok illetékes nemzeti hatóságai a 12.9-12.14 pontban említett eljárásnak megfelelően biztonsági ellenőrzésnek vetettek alá. Az Európai Parlament tisztviselőinek és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak felhatalmazása tekintetében a főtitkár az illetékes.

12.4. A főtitkár azt követően adhatja meg az írásos felhatalmazást, hogy megkapta a tagállamok illetékes nemzeti hatóságainak véleményét a 12.8-12.13 pontoknak megfelelően lefolytatott biztonsági ellenőrzés alapján.

12.5. Az Európai Parlament Biztonsági és Kockázatértékelési Igazgatósága naprakész listát vezet az Európai Parlament megfelelő szolgálatai által megadott valamennyi, biztonsági ellenőrzéshez kötött beosztásról, valamint mindazokról a személyekről, akik felhatalmazást kaptak, beleértve a 12.15 pont értelmében vett ideiglenes felhatalmazást is.

12.6. A felhatalmazás ötéves időtartamra vagy azon feladatok időtartamára érvényes, amelyekre tekintettel a felhatalmazást megadták, attól függően, hogy melyik a rövidebb. A felhatalmazás a 12.4 pontban említett eljárásnak megfelelően megújítható.

12.7. Az elnök visszavonja a felhatalmazást, ha úgy ítéli meg, hogy a visszavonásra megfelelő oka van. A felhatalmazás visszavonásáról szóló határozatról értesíteni kell az Európai Parlament érintett tisztviselőjét vagy valamely képviselőcsoport alkalmazásában álló egyéb érintett parlamenti alkalmazottat, akik még a visszavonás hatályba lépése előtt meghallgatást kérhetnek a főtitkártól, valamint az illetékes nemzeti hatóságot.

12.8. A biztonsági ellenőrzést az Európai Parlament érintett képviselője vagy valamely képviselőcsoport alkalmazásában álló egyéb érintett parlamenti alkalmazott közreműködésével, és a főtitkár kérésére folytatják le. Az ellenőrzés tekintetében az érintett személy állampolgársága szerinti tagállam nemzeti hatósága az illetékes. Amennyiben a nemzeti jogszabályok és rendelkezések ezt lehetővé teszik, az illetékes nemzeti hatóságok vizsgálatot folytathatnak az ország állampolgárságával nem rendelkező azon személyekkel kapcsolatban, akik hozzáférést kérnek „CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET" szinten minősített adatokhoz.

12.9. Az ellenőrzési eljárás részeként az Európai Parlament érintett tisztviselőjének vagy valamely képviselőcsoport alkalmazásában álló egyéb érintett parlamenti alkalmazottnak kérdőívet kell kitöltenie.

12.10. A főtitkár az illetékes nemzeti hatósághoz intézett megkeresésében meghatározza az Európai Parlament érintett tisztviselője vagy valamely képviselőcsoport alkalmazásában álló egyéb érintett parlamenti alkalmazott rendelkezésére bocsátandó minősített adatok szintjét, hogy az az ellenőrzési eljárást lefolytathassa, és véleményt adhasson arról, hogy milyen szintű felhatalmazást lenne helyénvaló adni az adott személynek.

12.11. Az illetékes nemzeti hatóság által lefolytatott teljes biztonsági ellenőrzési eljárásra és a kapott eredményekre az érintett tagállamban hatályos megfelelő szabályok és rendelkezések vonatkoznak, beleértve a jogorvoslattal kapcsolatos rendelkezéseket is.

12.12. Ha az illetékes nemzeti hatóság kedvező véleményt ad, a főtitkár megadhatja a felhatalmazást az Európai Parlament képviselőjének vagy a valamely képviselőcsoport alkalmazásában álló egyéb érintett parlamenti alkalmazottnak.

12.13. Az illetékes nemzeti hatóság elutasító véleményéről értesíteni kell az Európai Parlament érintett tisztviselőjét vagy valamely képviselőcsoport alkalmazásában álló egyéb érintett parlamenti alkalmazottat, akik meghallgatást kérhetnek a főtitkártól. Ha a főtitkár szükségesnek tartja, az illetékes nemzeti hatóságtól további tájékoztatást kérhet. Ha az elutasító véleményt a hatóság megerősíti, akkor a felhatalmazást nem lehet megadni.

12.14. Az Európai Parlament mindazon tisztviselői és a képviselőcsoportok alkalmazásában álló mindazon egyéb parlamenti alkalmazottak, akik a 12.4 és 12.5 pont értelmében felhatalmazást kaptak, a felhatalmazás megadásának időpontjában, majd azt követően rendszeres időközönként minden szükséges utasítást megkapnak a minősített adatok védelmével és a védelem biztosításának módjával kapcsolatosan. E tisztviselők és alkalmazottak nyilatkozatot írnak alá, amelyben igazolják, hogy megkapták ezeket az utasításokat és vállalják azok betartását.

12.15. Kivételes esetben a főtitkár, miután az illetékes nemzeti hatóságot értesítette és az erre egy hónapon belül nem reagált, legfeljebb hat hónapos időtartamra ideiglenes felhatalmazást adhat az Európai Parlament tisztviselőjének vagy valamely képviselőcsoport alkalmazásában álló egyéb parlamenti alkalmazottnak, amíg a 12.11 pontban említett ellenőrzés eredményét meg nem kapja. Az így megadott ideiglenes felhatalmazások nem biztosítanak hozzáférést a „TRÈS SECRET UE/EU TOP SECRET" szinten vagy ezzel egyenértékű szinten minősített adatokhoz.

II. MELLÉKLET

BEVEZETÉS

Ezek a rendelkezések megállapítják a bizalmas adatok Európai Parlament általi biztonságos kezelésére és igazgatására vonatkozó, illetve ezt biztosító biztonsági közleményeket. Ezek a biztonsági közlemények és a kezelési utasítások együttesen képezik az Európai Parlament e határozat 3. cikkének (2) bekezdésében említett információbiztonsági irányítórendszerét (ISMS):

1. BIZTONSÁGI KÖZLEMÉNY

A bizalmas adatok védelmét célzó biztonság kialakítása az Európai Parlamentben

2. BIZTONSÁGI KÖZLEMÉNY

A bizalmas adatok kezelése

3. BIZTONSÁGI KÖZLEMÉNY

A bizalmas adatok kezelése automatizált kommunikációs és információs rendszerekkel

4. BIZTONSÁGI KÖZLEMÉNY

Fizikai biztonság

5. BIZTONSÁGI KÖZLEMÉNY

Ipari biztonság

6. BIZTONSÁGI KÖZLEMÉNY

A biztonsági szabályok megsértése, bizalmas adatok elvesztése vagy illetéktelen tudomására jutása

1. BIZTONSÁGI KÖZLEMÉNY

A BIZALMAS ADATOK VÉDELMÉT CÉLZÓ BIZTONSÁG KIALAKÍTÁSA AZ EURÓPAI PARLAMENTBEN

1. A főtitkár felel e határozat átfogó és következetes végrehajtásáért.

A főtitkár minden szükséges intézkedést meghoz annak biztosítása érdekében, hogy a bizalmas adatok kezelése és tárolása céljából ezt a határozatot az Európai Parlament képviselői, tisztviselői, a képviselőcsoportoknak dolgozó egyéb alkalmazottai és az alvállalkozók az Európai Parlament épületeiben alkalmazzák.

2. A főtitkár a biztonsági hatóság (SA). E minőségében az alábbiakért felel:

2.1. a Parlament bizalmas adatok védelmét érintő tevékenységeivel kapcsolatos biztonsági kérdések összehangolása;

2.2. biztonságos hely, biztonságos olvasótermek kialakításának, illetve ezek biztonságos felszerelésekkel való ellátásának jóváhagyása;

2.3. minősített adatoknak az Európai Parlament által harmadik felek részére történő továbbítását engedélyező határozatok az e határozat 6. cikke szerint történő végrehajtása;

2.4. bizalmas adatok látszólag a Parlamentben történő kiszivárogtatásának kivizsgálása, illetve ilyen vizsgálat elrendelése az Európai Parlament elnökével együttműködve, európai parlamenti képviselő érintettsége esetén;

2.5. szoros kapcsolattartás az egyéb uniós intézmények biztonsági hatóságaival, valamint a tagállamok nemzeti biztonsági hatóságaival a minősített adatokkal kapcsolatos biztonsági politikák lehető legjobb összehangolásának biztosítása érdekében;

2.6. a Parlament biztonságpolitikájának folyamatos felügyelete és ennek alapján ajánlások közzététele;

2.7. jelentés a nemzeti biztonsági hatóságnak, amely végrehajtja a biztonsági ellenőrzési eljárást az I. melléklet 2. rész 11.3 pontjának megfelelően, a hatóságot esetleg érintő kedvezőtlen információkat is magukban foglaló esetekben.

3. Európai parlamenti képviselő érintettsége esetén a főtitkár az Európai Parlament elnökével együtt látja el feladatát.

4. A főtitkárt a (2) és (3) bekezdés szerinti feladatainak ellátásában a főtitkárhelyettes, a Biztonsági és Kockázatértékelési Igazgatóság, az Informatikai Igazgatóság (DIT) és a Minősített Adatok Osztálya (CIU) segíti.

4.1. A Biztonsági és Kockázatértékelési Igazgatóság felel a személyi védelmi intézkedésekért és különösen a biztonsági ellenőrzési eljárásért, az I. melléklet 2. részében megállapítottaknak megfelelően. A Biztonsági és Kockázatértékelési Igazgatóság emellett:

a) az egyéb uniós intézmények biztonsági hatóságai és a nemzeti biztonsági hatóságok kapcsolattartója az európai parlamenti képviselőket, az Európai Parlament tisztviselőit és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottakat érintő biztonsági ellenőrzési eljárások tekintetében;

b) általános biztonsági tájékoztatást ad a minősített adatok védelmére vonatkozó kötelezettséggel és e kötelezettség teljesítésének elmulasztásával kapcsolatban;

c) nyomon követi a biztonságos hely és a biztonságos olvasótermek a Parlament helyiségeiben való működtetését adott esetben együttműködve az egyéb uniós intézmények és tagállamok biztonsági hatóságaival;

d) az egyéb uniós intézmények és tagállamok biztonsági hatóságaival együttműködve ellenőrzi a minősített adatok kezelésére és tárolására vonatkozó eljárásokat, valamint a Parlament helyiségeiben található biztonságos helyet és biztonságos olvasótermeket, ahol minősített adatok kezelésére kerül sor;

e) javaslatot tesz a megfelelő kezelési utasításokra a főtitkár számára.

4.2. A DIT felel azért, hogy az Európai Parlament a bizalmas adatokat biztonságos informatikai rendszerek segítségével kezelje.

4.3. A Minősített Adatok Osztálya felel a következőkért:

a) a bizalmas adatok hatékony védelméhez szükséges biztonsági követelmények azonosítása szoros együttműködésben a Biztonsági és Kockázatértékelési Igazgatósággal és a DIT-vel, valamint az egyéb uniós intézmények biztonsági hatóságaival;

b) a bizalmas adatok Parlamenten belüli kezelése és tárolása valamennyi aspektusának azonosítása a kezelési utasításoknak megfelelően;

c) a biztonságos hely működtetése;

d) a bizalmas adatok kezelése és az azokba való betekintés a biztonságos helyen vagy a Minősített Adatok Osztálya biztonságos olvasótermében az e határozat 7. cikke (2) és (3) bekezdésének megfelelően;

e) a Minősített Adatok Osztálya nyilvántartásának kezelése;

f) jelentés a biztonsági hatóságnak (SA) minden olyan esetről, amikor bizonyítottan sérültek a biztonsági szabályok, a Minősített Adatok Osztályánál elhelyezett és a biztonságos helyen vagy a Minősített Adatok Osztálya biztonságos olvasótermében tárolt bizalmas adatok vesztek el vagy jutottak illetéktelenek tudomására, illetve ha felmerül a gyanú, hogy ilyen események történtek.

5. Ezenfelül a főtitkár biztonsági hatóságként kijelöli az alábbi hatóságokat:

a) Biztonsági akkreditációs hatóság (SAA);

b) Információvédelmi üzemeltetési hatóság (IAOA);

c) Kriptográfiai terjesztési hatóság (CDA);

d) TEMPEST-hatóság (TA);

e) Információvédelmi hatóság (IAA).

E feladatkörök nem igényelnek külön szervezeti egységeket. E hatóságoknak külön megbízatással kell rendelkezniük. Ugyanakkor a szóban forgó funkciók és az azokkal járó feladatkörök kombinálhatók egyazon szervezeti egységen belül, illetve integrálhatók abba, vagy pedig különböző szervezeti egységekké választhatók szét, feltéve, hogy elkerülik az összeférhetetlenségeket és a feladatok megkettőződését.

6. Az SAA tanácsadást biztosít valamennyi, az egyes információtechnológiai rendszerek és a Parlamenten belüli hálózatok akkreditációjával kapcsolatos biztonsági kérdés vonatkozásában az alábbiak révén:

6.1. annak biztosítása, hogy a kommunikációs és információs rendszer megfeleljen a vonatkozó biztonsági politikáknak és biztonsági iránymutatásoknak, jóváhagyási tanúsítvány kiadása arról, hogy a kommunikációs és információs rendszer működési környezetében meghatározott minősítési szintig minősített adatokat kezelhet, valamint az akkreditáció feltételeinek és azon kritériumoknak a meghatározása, amelyek esetében ismételt jóváhagyás szükséges;

6.2. biztonsági akkreditációs folyamat létrehozása a vonatkozó politikákkal összhangban, egyértelműen megállapítva a jóváhagyási feltételeket a felelőssége alá tartozó kommunikációs és információs rendszer tekintetében;

6.3. biztonsági akkreditációs stratégia kialakítása, amely a megkövetelt biztonsági szinttel arányosan meghatározza az akkreditációs eljárás részletességének mértékét;

6.4. a biztonsággal kapcsolatos dokumentáció, többek között a kockázatkezelés és a fennmaradó kockázat megállapítása, a biztonsági végrehajtás ellenőrzési dokumentációja és a biztonsági üzemeltetési eljárások megvizsgálása és jóváhagyása, valamint annak biztosítása, hogy az összhangban álljon a Parlament biztonsági szabályaival és politikájával;

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

6.6. biztonsági követelmények azonosítása (pl. személyi biztonsági felhatalmazások szintjei) a kommunikációs és információs rendszer tekintetében betöltött szenzitív beosztások tekintetében;

6.7. kommunikációs és információs rendszer másik kommunikációs és információs rendszerrel való összekapcsolódásának jóváhagyása, vagy adott esetben a közös engedélyezésben való részvétel;

6.8. a minősített adatok biztonságos kezelését és védelmét célzó technikai berendezésekre vonatkozó biztonsági előírások jóváhagyása;

6.9. annak biztosítása, hogy az Európai Parlament által használt kriptográfiai termékek szerepeljenek az EU által jóváhagyott termékek listáján; továbbá

6.10. a rendszerszolgáltatóval, a biztonsági szereplőkkel és a felhasználók képviselőivel való konzultálás a biztonsági kockázatkezelés tekintetében – különös tekintettel a fennmaradó kockázatra –, valamint a jóváhagyási tanúsítvány kiadási feltételei tekintetében.

7. Az IAOA az alábbiakért felel:

7.1. biztonsági dokumentáció kidolgozása a biztonsági politikákkal és biztonsági iránymutatásokkal összhangban, különösen ideértve a fennmaradó kockázat megállapítását, a biztonsági üzemeltetési eljárásokat és a kommunikációs és információs rendszer akkreditálása folyamatának részét képező kriptográfiai tervet;

7.2. részvétel a rendszerspecifikus technikai biztonsági intézkedések, eszközök és szoftverek kiválasztásában és tesztelésében, végrehajtásuk felügyelete és annak biztosítása érdekében, hogy azokat a vonatkozó biztonsági dokumentációnak megfelelően, biztonságosan telepítsék, konfigurálják és tartsák karban;

7.3. a biztonsági üzemeltetési eljárások végrehajtásának és alkalmazásának ellenőrzése és szükség esetén a működési biztonsággal kapcsolatos felelősségnek a rendszertulajdonosra, a Minősített Adatok Osztályára ruházása;

7.4. a kriptográfiai termékek kezelése, biztosítva a kriptográfiai és ellenőrzött elemek megőrzését és – adott esetben – biztosítva a kriptográfiai változók generálását;

7.5. biztonsági elemzések felülvizsgálatának és tesztelésének a kivitelezése, különösen a vonatkozó kockázati jelentéseknek a biztonsági akkreditációs hatóság (SAA) előírásai szerinti elkészítése céljából;

7.6. a kommunikációs és információs rendszerre vonatkozó specifikus információvédelmi képzés nyújtása;

7.7. A kommunikációs és információs rendszerre vonatkozó specifikusbiztonsági intézkedések végrehajtása és működtetése.

8. A kriptográfiai terjesztési hatóság (CDA) az alábbiakért felel:

8.1. az EU kriptográfiai anyag kezelése és könyvelése;

8.2. az SAA-val való szoros együttműködésben annak biztosítása, hogy a megfelelő eljárásokat alkalmazzák, valamint hogy valamennyi uniós kriptográfiai anyag könyvelése, biztonságos kezelése, tárolása és terjesztése tekintetében tervek készüljenek; továbbá

8.3. az EU kriptográfiai anyag az azt felhasználó egyének vagy szolgálatok felé, illetve az ilyen egyénektől vagy szolgálatoktól való továbbításának biztosítása.

9. A TA felelős azért, hogy a kommunikációs és információs rendszer megfeleljen a TEMPEST-politikáknak és kezelési utasításoknak. Megadja a jóváhagyást a működési környezetükben meghatározott minősítési szintig minősített adatok védelmét szolgáló berendezésekre és termékekre vonatkozó TEMPEST-ellenintézkedésekre.

10. Az IAA felel a Parlamenten belüli bizalmas adatok kezelésének valamennyi aspektusa, és különösen az alábbiak tekintetében:

10.1 információvédelmi biztonsági politikák és ezek biztonsági iránymutatásainak kidolgozása, valamint ezek hatékonyságának és helyénvalóságának nyomon követése;

10.2. a kriptográfiai termékekkel kapcsolatos technikai információk védelme és igazgatása;

10.3. annak biztosítása, hogy a minősített adatok védelmére kiválasztott információvédelmi intézkedések megfeleljenek a jogosultságot és kiválasztást szabályozó, vonatkozó politikáknak;

10.4. annak biztosítása, hogy a kriptográfiai termékek kiválasztása a jogosultságot és kiválasztást szabályozó politikáknak megfelelően történjen;

10.5. konzultáció a rendszerszolgáltatóval, a biztonsági szereplőkkel és a felhasználók képviselőivel az információvédelmi biztonsági politikák tekintetében;

2. BIZTONSÁGI KÖZLEMÉNY

A BIZALMAS ADATOK KEZELÉSE

A. **BEVEZETÉS**

1. E biztonsági közlemény megállapítja a bizalmas adatok Parlament általi kezelésére vonatkozó rendelkezéseket.

2. Bizalmas adat létrehozásakor a kibocsátó értékeli a bizalmas jelleg fokát és az e biztonsági közleményben rögzített elvek alapján meghatározza az adat minősítését vagy jelölését.

B. **AZ EU-MINŐSÍTETT ADATOK BESOROLÁSA**

3. A dokumentum besorolásáról létrehozása előtt kell határozni. Ennek megfelelően az adat EU-minősített adatként történő besorolása szükségessé teszi, hogy a kibocsátó megállapítsa az adat bizalmas jellegének szintjét és annak eldöntését, hogy az adat felhatalmazás nélkül történő kiadása az Európai Unió vagy tagállamai vagy egyes személyek érdekeinek különböző fokú sérelmét okozná-e.

4. Az adat besorolására vonatkozó döntés meghozatala után második lépésben meg kell állapítani a besorolás megfelelő szintjét. A dokumentum besorolása attól függ, hogy tartalmának érzékenysége milyen fokú.

5. Az adat besorolásáért kizárólag a kibocsátó felel. A Parlament tisztviselői az adatok besorolását a főtitkár utasítására vagy felhatalmazásából végzik.

6. A besorolást megfelelő módon és mértékkel kell alkalmazni. A besorolandó dokumentum kibocsátójának ügyelnie kell arra, hogy a dokumentumnak ne adjon a kelleténél se magasabb, se alacsonyabb szintű minősítést.

7. A dokumentum minősítésének szintje meghatározza védettségének szintjét a személyi biztonság, a fizikai biztonság, az eljárás biztonsága és az adatbiztonság szempontjából.

8. A minősített adatot fizikai formájától függetlenül ilyenként kell megjelölni és kezelni. A minősítésről egyértelműen tájékoztatni kell a címzetteket, akár a biztonsági besorolásra utaló jelölés (írásos formában – papíralapon vagy a kommunikációs és információs rendszerben – történő továbbítás esetén), akár bármiféle közlés révén (szóbeli – beszélgetés közben vagy zárt ülés keretében történő – továbbítás esetén). A minősített dokumentumon a minősítés tényét a könnyű azonosítást szolgáló biztonsági besorolhatóság érdekében fel kell tüntetni.

9. EU-minősített adat elektronikus formában csak az akkreditált kommunikációs és információs rendszeren belül hozható létre. A minősített adaton, valamint a fájl nevében és a tárolóeszközön (amennyiben ez külső egység, pl. CD-ROM vagy pendrive) fel kell tüntetni a besorolásra vonatkozó megfelelő jelölést.

10. A megformázott adatot azonnal minősíteni kell. Például a minősítést igénylő adatot tartalmazó személyes feljegyzéseket, vázlatokat vagy elektronikus üzeneteket már keletkezésükkor „EU-minősített" jelzéssel kell ellátni, előállításukat és kezelésüket pedig fizikai és technikai értelemben e határozattal és a vonatkozó kezelési utasításokkal összhangban kell végezni. Az ilyen adat a későbbiekben hivatalos dokumentummá alakulhat, amelyet szintén megfelelő módon kell megjelölni és kezelni. Az előállítás során elfordulhat, hogy a hivatalos dokumentum minősítését felül kell vizsgálni és a folyamat eredményeképpen magasabb vagy alacsonyabb minősítéssel kell ellátni.

11. A kibocsátó dönthet úgy, hogy sztenderd minősítési szintet jelöl meg az általa rendszeresen létrehozott adattípusok számára. A kibocsátónak azonban meg kell győződnie arról, hogy ennek során nem minősíti rendszerszerűen felül vagy alul az egyes adatokat.

12. Az EU-minősített adaton mindig fel kell tüntetni a biztonsági besorolásának megfelelő biztonsági besorolási jelzést.

B.1. ***Minősítési szintek***

13. Az EU-minősített adatot a következő szintek egyikére kell besorolni:

– „TRÈS SECRET UE/EU TOP SECRET", e határozat 2. cikkének d) pontja szerint, amennyiben napvilágra kerülése várhatóan:

a) közvetlen fenyegetést jelent az Unió vagy egy vagy több uniós tagállam vagy harmadik államok vagy nemzetközi szervezetek belső stabilitása számára,

b) kivételesen nagy kárt okoz harmadik államokkal vagy nemzetközi szervezetekkel fenntartott kapcsolatok szempontjából,

c) közvetlenül számos emberéletet követelhet,

d) kivételesen nagy kárral jár a tagállamok operatív hatékonysága vagy biztonsága vagy más közreműködők személyi állománya, illetve rendkívüli értékkel bíró biztonsági és hírszerzési műveletek folyamatos hatékonysága számára,

e) súlyos és hosszú távú károkat eredményez az Unió vagy a tagállamok gazdasága számára;

– „SECRET UE/EU SECRET", e határozat 2. cikkének d) pontja szerint, amennyiben napvilágra kerülése várhatóan:

a) jelentős nemzetközi feszültséget kelt,

b) súlyos károkkal jár a harmadik államokkal és nemzetközi szervezetekkel fenntartott kapcsolatok szempontjából,

c) közvetlen életveszélyt okoz, vagy a közrend vagy a személyi biztonság vagy szabadság súlyos sérelmével jár,

d) fontos kereskedelmi vagy politikai tárgyalásokat veszélyeztet, jelentősen hátráltatja az Unió vagy a tagállamok működését,

e) súlyos károkkal jár a tagállamok működésének biztonsága számára, vagy magas értékű biztonsági vagy hírszerzési műveletek hatékonysága szempontjából,

f) súlyos anyagi károkozással jár az Unió vagy a tagállamok pénzügyi, monetáris, gazdasági és kereskedelmi érdekei szempontjából,

g) alapvetően veszélyezteti a legfontosabb szervezetek vagy szereplők pénzügyi életképességét, vagy

h) súlyosan akadályozza a fontos gazdasági, kereskedelmi vagy pénzügyi következményekkel járó uniós politikák végrehajtását vagy működését;

– „CONFIDENTIEL UE/EU CONFIDENTIAL", e határozat 2. cikkének d) pontja szerint, amennyiben napvilágra kerülése várhatóan:

a) jelentős kárt okoz a diplomáciai kapcsolatoknak, például hivatalos tiltakozást vagy más szankciókat válthat ki,

b) veszélyezteti a személyi biztonságot vagy szabadságot,

c) súlyosan veszélyezteti kereskedelmi vagy politikai tárgyalások eredményét, hátráltatja az EU vagy a tagállamok működését,

d) károkkal jár a tagállamok működésének biztonsága számára, vagy biztonsági vagy hírszerzési műveletek hatékonysága szempontjából,

e) alapvetően veszélyezteti a fontosabb szervezetek vagy szereplők pénzügyi életképességét,

f) akadályozza bűncselekmények vagy terrorista cselekmények felderítését vagy megkönnyíti ezek elkövetését,

g) alapvetően ellentétes az Unió vagy a tagállamok pénzügyi, monetáris, gazdasági és kereskedelmi érdekeivel,

h) súlyosan akadályozza a fontos gazdasági, kereskedelmi vagy pénzügyi következményekkel járó uniós politikák végrehajtását vagy működését;

– „RESTREINT UE/EU RESTRICTED”, e határozat 2. cikkének d) pontja szerint, amennyiben napvilágra kerülése várhatóan:

a) előnytelen az Unió általános érdekei szempontjából,

b) hátrányosan hat a diplomáciai kapcsolatokra,

c) lényeges károkozással jár személyek vagy vállalatok számára,

d) hátrányos az Unió vagy a tagállamok által folytatott kereskedelmi vagy politikai tárgyalások szempontjából,

e) megnehezíti az Unió vagy a tagállamok hatékony belső biztonságának fenntartását,

f) akadályozza az uniós politikák hatékony végrehajtását vagy működését,

g) hátráltatja az Unió hatékony irányítását és az Unió műveleteit,

h) sérti a Parlament harmadik felek által szolgáltatott adatok minősített státuszának fenntartására irányuló kötelezettségvállalásait,

i) sérti az adatok terjesztésére vonatkozó szabályozási korlátozásokat, vagy

j) pénzügyi veszteséget okoz vagy elősegíti jogtalan nyereség vagy előny képződését személyek vagy vállalatok számára,

k) bűncselekmények felderítésének sérelmével jár vagy megkönnyíti ezek elkövetését.

B.2. ***Összeállítások, fedőlapok és kivonatok minősítése***

14. A csatolmányokat tartalmazó levél vagy feljegyzés ugyanolyan magas minősítést kap, mint a legmagasabb minősítésű csatolmánya. A kibocsátónak világosan jeleznie kell, hogy a levél vagy feljegyzés milyen szintű minősítést kapjon, ha a csatolmányaitól elválasztják. Amennyiben a kísérő feljegyzést vagy levelet nem kell minősíteni, tartalmaznia kell a következő záró megjegyzést: „Csatolmányai nélkül e feljegyzés/levél nem minősített dokumentum.”

15. A különböző minősítésű részekből álló dokumentumokat vagy fájlokat lehetőleg oly módon kell összeállítani, hogy az megkönnyítse a különböző minősítésű részek azonosítását és szükség esetén leválasztását. A dokumentum vagy fájl általános minősítési szintje legalább olyan magas legyen, mint a legmagasabb szinten minősített összetevője.

16. Egy adott dokumentum egyes oldalai, bekezdései, szakaszai, mellékletei, függelékei, toldalékai és csatolmányai eltérő minősítést igényelhetnek, és ennek megfelelő jelölést kell kapniuk. Az EU-minősített adatokat tartalmazó dokumentumokban a szakaszok vagy egy oldalnál rövidebb szövegrészek minősítési szintjének jelölésére használhatók a sztenderd rövidítések.

17. Több forrásból származó adatok esetében a végtermék általános biztonsági besorolásának megállapítása céljából el kell végezni annak felülvizsgálatát, mivel a végtermék magasabb szintű biztonsági besorolást igényelhet, mint összetevői.

C. **EGYÉB BIZALMAS ADAT**

18. Az „egyéb bizalmas adat” megjelölést e biztonsági közlemény E. pontjával és a kezelési utasításokkal összhangban kell feltüntetni.

D. **BIZALMAS ADAT LÉTREHOZÁSA**

19. Bizalmas adatot csak az e határozatban felhatalmazott vagy a biztonsági hatóság által feljogosított személyek hozhatnak létre.

20. Bizalmas adatot tilos az interneten vagy a belső hálózat dokumentumkezelő rendszereiben megjeleníteni.

D.1. ***EU-minősített adat létrehozása***

21. „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" és e feletti szinten minősített adatot az a személy hozhat létre, akit erre e határozat feljogosít, vagy aki már rendelkezik a határozat 4. cikkének (1) bekezdésében meghatározott felhatalmazással.

22. „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" és e feletti szinten minősített adat csak biztonságos területen hozható létre.

23. Az EU-minősített adatok létrehozására a következő szabályok vonatkoznak:

a) minden egyes oldalon szerepelnie kell a megfelelő besorolási szint egyértelmű jelölésének;

b) minden egyes oldalt számozással kell ellátni és jelölni kell az összoldalszámot is;

c) a dokumentum első oldalán fel kell tüntetni a hivatkozási számot és a dokumentum tárgyát, amely önmagában nem minősített adat, kivéve ha ilyenként jelölték meg;

d) a dokumentum első oldalán szerepelnie kell a dátumnak;

e) minden „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" és e fölötti szinten minősített dokumentum első oldalán szerepelnie kell a mellékletek és csatolmányok felsorolásának;

f) amennyiben több másolat készül, a „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" és e fölötti szinten minősített dokumentumok minden egyes oldalán fel kell tüntetni a másolat sorszámát. Minden egyes másolati példány első oldalán fel kell tüntetni a másolatok és az oldalak össz-számát, továbbá

g) ha a dokumentum más, egyéb uniós intézménytől származó minősített adatokat tartalmazó dokumentumokra hivatkozik, vagy ha ilyen dokumentumokból átvett minősített adatokat tartalmaz, akkor a dokumentum minősítési szintjének meg kell egyeznie az említett dokumentumok minősítési szintjével, és azok kibocsátójának írásos hozzájárulása nélkül nem továbbíthatók az eredeti dokumentum vagy a minősített adatot tartalmazó dokumentumok terjesztési listáján megnevezetteken kívül más személyeknek.

24. A kibocsátó rendelkezik az általa létrehozott EU-minősítésű adatok feletti ellenőrzés jogával. Tőle származó írásos engedélye szükséges ahhoz, hogy az EU-minősítésű adat

a) alacsonyabb szintű besorolást kapjon vagy minősített besorolása megszűnjön;

b) a kibocsátó által meghatározott céltól eltérő célra felhasználható legyen;

c) bármely harmadik államhoz vagy nemzetközi szervezethez továbbítható legyen;

d) a kibocsátó által az adat megismerésére eredetileg felhatalmazottakon kívül bármely személynek, intézménynek, országnak vagy nemzetközi szervezetnek eljuttatható legyen;

e) harmadik országban letelepedett szerződő félhez vagy lehetséges szerződő félhez eljuttatható legyen;

f) másolható vagy lefordítható legyen, amennyiben minősítése „TRES SECRET UE/EU TOP SECRET" szintű;

g) megsemmisítésre kerüljön.

D.2. ***Egyéb bizalmas adat létrehozása***

25. A főtitkár mint biztonsági hatóság dönthet arról, hogy egy adott beosztás, szervezeti egység és/vagy adott személy számára engedélyezi-e, hogy „egyéb bizalmas adatot" hozzon létre.

26. Az „egyéb bizalmas adaton" fel kell tüntetni a kezelési utasításokban meghatározott valamely jelölést.

27. Az „egyéb bizalmas adat" létrehozására a következő szabályok vonatkoznak:

a) a jelölésnek a dokumentum első oldalának felső szélén kell szerepelnie;

b) minden egyes oldalt számozással kell ellátni, és jelölni kell az összoldalszámot is;

c) a dokumentumon fel kell tüntetni a hivatkozási számot és a dokumentum tárgyát;

d) a dokumentum első oldalán szerepelnie kell a dátumnak, továbbá

e) a dokumentum utolsó oldalán fel kell sorolni valamennyi mellékletet és csatolmányt.

28. „Egyéb bizalmas adat" létrehozására a kezelési utasításokban meghatározott külön szabályok és eljárások vonatkoznak.

E. **BIZTONSÁGI AZONOSÍTÓK ÉS JELÖLÉSEK**

29. A dokumentumon szereplő biztonsági azonosítók és jelölések célja az információáramlás ellenőrzés alatt tartása és a bizalmas adatokhoz való hozzáférésnek a „szükséges ismeret" elv szellemében történő korlátozása.

30. Amennyiben biztonsági azonosítók és/vagy jelölések használatára kerül sor, illetve ezeket feltüntetik, ügyelni kell az EU-minősített adatok esetében használt következő biztonsági besorolásokkal való keveredés veszélyére: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

31. A biztonsági azonosítók és jelölések használatára vonatkozó külön szabályokat, valamint az Európai Parlament jóváhagyott biztonsági jelöléseit a kezelési utasításokban meg kell határozni.

E.1. ***Biztonsági azonosítók***

32. Biztonsági azonosítókat csak biztonsági besorolással együtt lehet alkalmazni, illetve tilos őket a dokumentumokra külön-külön alkalmazni. Biztonsági azonosító EU-minősített adat esetében az alábbi célokból alkalmazható:

a) a besorolás érvényességének jelölésére (a minősített adat automatikus lejjebb sorolásának vagy a besorolás megszűnésének jelölésére);

b) az EU-minősített adat terjesztési körének korlátozására;

c) a biztonsági besorolás szintjének megfelelő kezelési utasításokhoz járuló egyedi utasítások meghatározására.

33. Az EU-minősített adatokat tartalmazó dokumentumok kezelésére és tárolására vonatkozó külön ellenőrzések további feladatokat jelentenek valamennyi érintett számára. Az ezzel járó munkateher csökkentése céljából helyes eljárás a dokumentum létrehozásakor egy olyan határidő vagy esemény meghatározása, amely után a besorolási szint automatikusan megszűnik és a dokumentumban található adat alacsonyabb szintű besorolást kap, vagy besorolása megszűnik.

34. Amennyiben a dokumentum jól körülhatárolt kérdéssel foglalkozik, és terjesztését korlátozni szükséges, és/vagy egyedi kezelési utasításokat kell alkalmazni, az erre vonatkozó jelölés a célközönség meghatározásának elősegítése céljából csatolható a besoroláshoz.

E.2. ***Jelölések***

35. A jelölések nem jelentenek biztonsági besorolást. Céljuk csupán az, hogy konkrét utasításokat adjanak a dokumentum kezelésével kapcsolatban, és nem alkalmazhatók a dokumentumok tartalmának ismertetésére sem.

36. A jelölések a dokumentumokra külön-külön is alkalmazhatók, és használhatók a biztonsági besorolással együtt is.

37. Általános szabályként a jelöléseket az EUMSZ 339. cikkében és a személyzeti szabályzat 17. cikkében említett szakmai titoktartás hatálya alá tartozó adatokra, vagy olyan adatokra kell alkalmazni, amelyeket a Parlamentnek jogi indokból védenie kell, de amelyeket nem szükséges vagy nem lehet minősíteni.

E.3. ***Jelölések alkalmazása a kommunikációs és információs rendszerben***

38. A jelölések használatára vonatkozó szabályok az akkreditált kommunikációs és információs rendszerben is alkalmazandók.

39. A biztonsági hatóság a jelöléseknek az akkreditált kommunikációs és információs rendszerben való használatára vonatkozó egyedi szabályokat állapít meg.

F. **A BIZALMAS ADATOK FOGADÁSA**

40. A Parlament részéről a harmadik felektől érkező „CONFIDENTIEL UE/EU CONFIDENTIAL" „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" és e feletti minősítésű vagy ezzel egyenértékű adatokat csak a Minősített Adatok Osztálya fogadhatja.

41. A harmadik felektől érkező „RESTREINT UE/EU RESTRICTED" szinten vagy azzal egyenértékű szinten minősített adatokat és az „egyéb bizalmas adatokat" mind a Minősített Adatok Osztálya, mind az illetékes parlamenti szerv/tisztségviselő fogadhatja, illetve felel az e biztonsági közleményben foglalt elvek alkalmazásáért.

G. **NYILVÁNTARTÁSBA VÉTEL**

42. A nyilvántartásba vétel azon eljárások alkalmazása, amelyek során rögzítésre kerül a bizalmas adatok életciklusa, beleértve terjesztésüket, tartalmuk megismerését és megsemmisítésüket.

43. E biztonsági közlemény alkalmazásában az „iktatókönyv" az a nyilvántartás, amelyben rögzítésre kerülnek különösen azok a dátumok és időpontok, amikor

a) a bizalmas adat megérkezik az illetékes parlamenti szerv/tisztségviselő titkárságára vagy adott esetben a Minősített Adatok Osztályához, illetve elhagyja azt;

b) a bizalmas adatba betekintenek vagy a megfelelő szintű biztonsági ellenőrzésen átesett személynek továbbítják; továbbá

c) a bizalmas adat megsemmisítésre kerül.

44. A minősített adat kibocsátója felel az ilyen adatokat tartalmazó dokumentum létrehozásakor feltüntetendő eredeti nyilatkozat megjelöléséért. Ez a nyilatkozat a dokumentum létrehozásakor továbbításra kerül a Minősített Adatok Osztályához.

45. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatokat biztonsági okokból csak a Minősített Adatok Osztálya vehet nyilvántartásba. A harmadik felektől érkező „RESTREINT UE/EU RESTRICTED" szinten vagy azzal egyenértékű szinten minősített adatokat és az „egyéb bizalmas adatokat" a dokumentum hivatalos érkeztetéséért felelős osztály veszi nyilvántartásba, amely lehet a Minősített Adatok Osztálya vagy – adminisztrációs célból – a parlamenti szerv/tisztségviselő titkársága. A parlamentben keletkező „egyéb bizalmas adatokat" – adminisztrációs célból – a kibocsátó veszi nyilvántartásba.

46. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatot nyilvántartásba kell venni, különösen az alább meghatározott esetekben:

a) keletkezésekor;

b) a Minősített Adatok Osztályára érkezésekor vagy amikor elhagyja azt; továbbá

c) a kommunikációs és információs rendszerbe érkezésekor vagy amikor elhagyja azt.

47. A „RESTREINT UE/EU RESTRICTED" szinten vagy azzal egyenértékű szinten minősített adatot nyilvántartásba kell venni különösen az alább meghatározott esetekben:

a) keletkezésekor;

b) a parlamenti szerv/tisztségviselő titkárságára vagy a Minősített Adatok Osztályra érkezésekor, vagy amikor elhagyja azt; továbbá

c) a kommunikációs és információs rendszerbe érkezésekor vagy amikor elhagyja azt.

48. A bizalmas adat nyilvántartásba vételéhez papíralapú vagy elektronikus iktatókönyv használható a kommunikációs és információs rendszerben.

49. A „RESTREINT UE/EU RESTRICTED" szinten vagy azzal egyenértékű szinten minősített adatok és „egyéb bizalmas adatok" esetében legalább a következők veendők nyilvántartásba:

a) az a dátum és időpont, amikor a bizalmas adat megérkezik az illetékes parlamenti szerv/tisztségviselő titkárságára vagy adott esetben a Minősített Adatok Osztályára, illetve elhagyja azt;

b) a dokumentum címe, a besorolási szint vagy a jelölés, a besorolás/jelölés lejáratának dátuma, továbbá a dokumentum hivatkozási száma.

50. A „RESTREINT UE/EU RESTRICTED", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatok esetében legalább a következők veendők nyilvántartásba:

a) az a dátum és időpont, amikor az adat megérkezik a Minősített Adatok Osztályára, illetve elhagyja azt;

b) a dokumentum címe, a besorolási szint vagy a jelölés, a dokumentum hivatkozási száma és a besorolás/jelölés lejáratának dátuma.

c) a kibocsátó adatai;

d) nyilvántartás a dokumentumhoz hozzáféréssel rendelkező személyek személyazonosságáról és a dokumentum adott személy általi megtekintésének időpontjairól;

e) nyilvántartás a dokumentumról készült másolatokról és fordításokról;

f) az a dátum és időpont, amikor a dokumentumról készült másolatok vagy fordítások elhagyják a Minősített Adatok Osztályát, vagy amikor azokat visszaküldik, továbbá részletes adatok arról, hogy hová küldték el azokat, és ki küldte őket vissza;

g) az a dátum és időpont, amikor a dokumentumot a Parlament megsemmisítésre vonatkozó biztonsági szabályaival összhangban megsemmisítik, valamint a megsemmisítést végző személy neve; továbbá

h) a dokumentum minősítésének megszüntetése vagy visszaminősítése.

51. Az iktatókönyveket szükség szerint minősítéssel vagy jelöléssel kell ellátni. A „TRES SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatokat tartalmazó iktatókönyveket ugyanezen a szinten kell nyilvántartásba venni.

52. Minősített adatok az alábbiak szerint vehetők nyilvántartásba:

a) egyetlen iktatókönyvben, vagy

b) különböző iktatókönyvekben, a minősítési szintnek, az adat beérkező vagy kimenő státuszának, valamint a forrásának és a címzettjének megfelelően.

53. A kommunikációs és információs rendszeren belüli elektronikus adatkezelés esetén a nyilvántartásba vételi eljárás a kommunikációs és információs rendszeren belüli eszközökkel is végrehajtható, amennyiben a rendszer megfelel a fentebb leírt követelményeknek. Minden esetben, amikor az EU-minősített adatok elhagyják a kommunikációs és információs rendszert, a fenti nyilvántartásba vételi eljárást kell alkalmazni.

54. A Minősített Adatok Osztálya nyilvántartást vezet a Parlament által harmadik feleknek átadott valamennyi minősített adatról és a harmadik felek által a Parlamentnek átadott minősített adatokról.

55. A „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” vagy „TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatok nyilvántartásba vételének befejezését követően a Minősített Adatok Osztálya ellenőrzi, hogy a címzett rendelkezik-e érvényes biztonsági felhatalmazással. Ebben az esetben a Minősített Adatok Osztálya értesíti a címzettet. A minősített adat megtekintésére csak az azt tartalmazó dokumentum nyilvántartásba vétele után kerülhet sor.

H. **TERJESZTÉS**

56. A kibocsátó összeállítja az általa létrehozott EU-minősített adat első terjesztési listáját.

57. A Parlament által készített, „RESTREINT UE/EU RESTRICTED, SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatok és egyéb bizalmas adatok Parlamenten belüli terjesztését a vonatkozó kezelési utasításoknak megfelelően és a „szükséges ismeret” elve alapján a kibocsátó végzi. A Parlament által a biztonságos területen belül létrehozott „CONFIDENTIEL UE/EU CONFIDENTIAL” vagy efölötti minősítésű adat esetében a terjesztési listát (és a terjesztést érintő valamennyi további utasítást) át kell adni a Minősített Adatok Osztályának, amely annak kezeléséért felelős.

58. A Parlament által készített EU-minősített adatot csak a Minősített Adatok Osztálya adhat át harmadik feleknek, a „szükséges ismeret” elve alapján.

59. A Minősített Adatok Osztálya vagy a továbbítás iránti kérelmet benyújtó más parlamenti szerv/tisztségviselő által kapott bizalmas adatot a kibocsátótól kapott utasításokkal összhangban kell terjeszteni.

I. **KEZELÉS, TÁROLÁS ÉS MEGTEKINTÉS**

60. A bizalmas adatok kezelése, tárolása és megtekintése a 4. biztonsági közleménnyel és a kezelési utasításokkal összhangban történik.

J. **BIZALMAS ADATOK MÁSOLÁSA/FORDÍTÁSA/TOLMÁCSOLÁSA**

61. A „TRES SECRET EU/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatot tartalmazó dokumentumok a kibocsátó előzetes írásbeli hozzájárulása nélkül nem másolhatók vagy fordíthatók le. A „SECRET UE/EU SECRET" vagy azzal egyenértékű minősítésű vagy a „CONFIDENTIEL UE/EU CONFIDENTIAL" vagy azzal egyenértékű minősítésű adat a titokbirtokos utasítására lemásolható vagy lefordítható, feltéve, hogy a kibocsátó ezt nem tiltotta meg.

62. A „TRES SECRET UE/EU TOP SECRET", „SECRET UE/EU SECRET EU" vagy „CONFIDENTIEL UE/EU CONFIDENTIAL" szinten vagy azzal egyenértékű szinten minősített adatot tartalmazó dokumentumok minden egyes másolatát biztonsági okokból nyilvántartásba kell venni.

63. A minősített adatot tartalmazó eredeti dokumentumra vonatkozó biztonsági intézkedések a másolatokra és a fordításokra is alkalmazandók.

64. A Tanácstól kapott dokumentumok általában az összes hivatalos nyelven beérkeznek.

65. A kibocsátó vagy a másolati birtokos másolatot és/vagy fordítást kérhet a minősített adatot tartalmazó dokumentumokról. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatot tartalmazó dokumentumokról csak a biztonságos területen, megfelelő hitelesítéssel rendelkező kommunikációs és információs rendszer részét képező másolókon lehet másolatot készíteni. A „RESTREINT UE/EU RESTRICTED" vagy azzal egyenértékű minősítésű adatot vagy egyéb bizalmas adatot tartalmazó dokumentumok másolatait csak a Parlament épületein belül található, megfelelő hitelesítéssel rendelkező másolóeszközön lehet elkészíteni.

66. A bizalmas adatot tartalmazó valamennyi dokumentum összes másolatát és fordítását vagy az ilyen dokumentumok másolatainak bizalmas adatot tartalmazó részét megfelelő jelzéssel és számozással kell ellátni, valamint nyilvántartásba kell venni.

67. Nem készíthető a feltétlenül szükségesnél több másolat. A megtekintési időszak végén minden másolatot a kezelési utasításoknak megfelelően meg kell semmisíteni.

68. A minősített adatokhoz hozzáférő tolmácsoknak és fordítóknak a Parlament tisztviselőinek kell lenniük.

69. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatot tartalmazó dokumentumokhoz hozzáférő tolmácsoknak és fordítóknak rendelkezniük kell a megfelelő biztonsági tanúsítvánnyal.

70. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatot tartalmazó dokumentumokon folytatott munkájukat a tolmácsoknak és a fordítóknak a biztonságos területen kell végezniük.

K. **A BIZALMAS ADAT VISSZAMINŐSÍTÉSE, ILLETVE A MINŐSÍTÉS ÉS A JELÖLÉS MEGSZÜNTETÉSE**

K.1. ***Általános elvek***

71. Amennyiben a védelemre vagy annak eredeti szinten történő biztosítására már nincs szükség, a bizalmas adat minősítését vagy jelölését meg kell szüntetni, illetve az adatot vissza kell minősíteni.

72. A Parlamenten belül készült dokumentumokban található adatok visszaminősítésére, illetve minősítésének vagy jelölésének megszüntetésére vonatkozó határozat meghozatala eseti alapon is szükségessé válhat, például a nyilvánosság vagy egy másik uniós intézmény kérésére, illetve a Minősített Adatok Osztálya vagy valamely parlamenti szerv/tisztségviselő kezdeményezésére.

73. Az EU-minősített adat létrehozásakor – amennyiben lehetséges – a kibocsátó jelöli, hogy egy adott időpontban vagy valamely konkrét eseményt követően a szóban forgó EU-minősített adat visszaminősíthető-e vagy minősítése feloldható-e. Amennyiben gyakorlati okokból ilyen tájékoztatás nem adható, a kibocsátó, a Minősített Adatok Osztálya vagy az adatot birtokló parlamenti szerv/tisztségviselő legalább ötévente felülvizsgálja az EU-minősített adat minősítési szintjét. Az EU-minősített adat visszaminősítésére vagy minősítésének megszüntetésére minden esetben kizárólag a kibocsátó előzetes írásbeli hozzájárulásával kerülhet sor.

74. Abban az esetben, ha valamely Parlamenten belül készült dokumentum tekintetében az EU-minősített adat kibocsátójának kiléte nem állapítható meg vagy nem követhető vissza, a biztonsági hatóság vizsgálja felül az adott EU-minősített adat minősítésének szintjét az adatot birtokló parlamenti szerv/tisztségviselő javaslatára, és tekintetben konzultálhat a Minősített Adatok Osztályával.

75. A Minősített Adatok Osztálya vagy az adatot birtokló parlamenti szerv/tisztségviselő feladata, hogy értesítse a címzett(ek)et az adat visszaminősítéséről vagy minősítésének megszüntetéséről, és e címzett(ek) feladata, hogy értesítse azokat a további címzett(ek)et, akiknek ők a dokumentumot megküldték vagy lemásolták.

76. A dokumentumokban található adatok visszaminősítését, minősítésének vagy jelölésének megszüntetését rögzíteni kell a nyilvántartásban.

K.2. ***A minősítés megszüntetése***

77. EU-minősített adat minősítése teljes mértékben vagy részlegesen szüntethető meg. EU-minősített adat minősítésének részleges megszüntetésére abban az esetben kerülhet sor, ha az azt tartalmazó dokumentum meghatározott része esetében a védelem fenntartása nem tekinthető szükségesnek, a dokumentum többi része esetében azonban továbbra is indokolt fenntartani a védelmet.

78. Ha a Parlamenten belül készült dokumentumban található EU-minősített adat felülvizsgálata az adat minősítésének megszüntetését eredményezi, meg kell vizsgálni, hogy a dokumentumot nyilvánosságra lehet-e hozni, vagy terjesztési jelöléssel kell-e ellátni (azaz nem hozható nyilvánosságra).

79. EU-minősített adat minősítésének megszüntetése esetén a minősítés feloldását rögzíteni kell az iktatókönyvben a következő adatokkal együtt: a minősítés megszüntetésének dátuma, a minősítés megszüntetését kérelmező és engedélyező személyek neve, az érintett dokumentum referenciaszáma és végső rendeltetési helye.

80. A megszüntetett minősítésű dokumentum és minden másolata régi minősítési jelöléseit át kell húzni. A dokumentumokat és azok valamennyi másolatát ennek megfelelően kell tárolni.

81. Minősített adat minősítésének részleges megszüntetése esetén a megszüntetett minősítésű részről kivonatot kell készíteni, és azt a megfelelő módon kell tárolni. Az illetékes szervezeti egység rögzíti:

a) a minősítés részleges megszüntetésének dátumát;

b) a minősítés megszüntetését kérelmező és engedélyező személyek nevét; továbbá

c) a megszüntetett minősítésű kivonat referenciaszámát.

K.3. ***Visszaminősítés***

82. Minősített adat visszaminősítését követően az iktatókönyvekben az érintett dokumentumot a régi és az új minősítési szintje szerinti nyilvántartásba is fel kell venni. A visszaminősítés dátumát és a visszaminősítést engedélyező személy nevét rögzíteni kell.

83. A visszaminősített adatot tartalmazó dokumentumon és annak minden másolatán fel kell tüntetni az új minősítési szintet, és ennek megfelelően kell azt tárolni.

L. **BIZALMAS ADAT MEGSEMMISÍTÉSE**

84. A szükségtelenné vált bizalmas adatot (papíralapú és elektronikus formában egyaránt) a kezelési utasításokkal és az archiválásra vonatkozó szabályokkal összhangban meg kell semmisíteni vagy törölni kell.

85. A „TRES SECRET UE/EU TOP SECRET" vagy ezzel egyenértékű, illetve a „SECRET UE/EU SECRET" szinten vagy azzal egyenértékű szinten minősített adatok megsemmisítését a Minősített Adatok Osztálya hajtja végre. A megsemmisítést egy olyan tanú jelenlétében kell elvégezni, aki legalább a megsemmisítendő adat minősítési szintjével megegyező biztonsági tanúsítvánnyal rendelkezik.

86. „TRES SECRET EU/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adat a kibocsátó előzetes írásbeli hozzájárulása nélkül nem semmisíthető meg.

87. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatok megsemmisítését és ártalmatlanítását a kibocsátó vagy valamely illetékes hatóság utasítására a Minősített Adatok Osztálya végzi. Az iktatókönyveket és egyéb nyilvántartásokat ennek megfelelő módon frissíteni kell. A „RESTREINT UE/EU RESTRICTED" vagy ezzel egyenértékű minősítésű adatok megsemmisítését és ártalmatlanítását vagy a Minősített Adatok Osztálya, vagy a megfelelő parlamenti szerv/tisztségviselő végzi.

88. A megsemmisítésért felelős tisztviselő és a megsemmisítést tanúsító személy megsemmisítési jegyzőkönyvet ír alá, amelyet a Minősített Adatok Osztálya vezet és archivál. A Minősített Adatok Osztálya a „TRES SECRET UE/EU TOP SECRET" vagy ezzel egyenértékű minősítésű adatok esetében legalább tíz évig, a „SECRET UE/EU SECRET" vagy ezzel egyenértékű és a „CONFIDENTIEL UE/EU CONFIDENTIAL" vagy ezzel egyenértékű minősítésű adatok esetében pedig legalább öt évig megőrzi a megsemmisítési jegyzőkönyvet a terjesztési listákkal együtt.

89. A minősített adatot tartalmazó dokumentumokat a vonatkozó uniós szabványoknak vagy ezzel egyenértékű szabványoknak megfelelően kell megsemmisíteni, megakadályozandó a dokumentum egészének vagy egy részének helyreállítását.

90. A minősített adathoz használt számítógépes adathordozók megsemmisítését a vonatkozó kezelési utasításokkal összhangban kell végrehajtani.

91. A minősített adat megsemmisítését az alábbi adatokkal együtt rögzíteni kell a megfelelő iktatókönyvben:

a) a megsemmisítés dátuma és időpontja;

b) a megsemmisítésért felelős tisztviselő;

c) a megsemmisített dokumentum vagy másolatok azonosítója;

d) a megsemmisített EU-minősített adat eredeti fizikai formája;

e) a megsemmisítés eszköze; továbbá

f) a megsemmisítés helye.

M. **ARCHIVÁLÁS**

92. A minősített adatot – a kísérő feljegyzést/levelet, mellékleteket, az elhelyezést igazoló szelvényt és az akta egyéb részeit is beleértve – utolsó megtekintése után hat hónappal, de legkésőbb elhelyezése után egy évvel át kell helyezni a biztonságos helyre. A minősített adatok archiválásának részletes szabályait a kezelési utasítások határozzák meg.

93. Az „egyéb bizalmas adatok" esetében – a kezelésükre vonatkozó bármely más egyedi rendelkezés sérelme nélkül – a dokumentumkezelés általános szabályai alkalmazandók.

3. BIZTONSÁGI KÖZLEMÉNY

A BIZALMAS ADATOK KEZELÉSE AUTOMATIZÁLT KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZEREKKEL

A. **AZ INFORMÁCIÓS RENDSZEREKBEN KEZELT MINŐSÍTETT ADATOK INFORMÁCIÓVÉDELME**

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

2. A minősített adatok kezelésére szolgáló „kommunikációs és információs rendszer" az adatok elektronikus formában történő kezelését lehetővé tevő rendszer. Ez az információs rendszer magában foglalja a működéséhez szükséges valamennyi eszközt, beleértve az infrastruktúrát, a szervezetet, a személyzetet és az információforrásokat.

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

4. A kommunikációs és információs rendszert akkreditálni kell. Az akkreditáció célja, hogy bizonyosságot nyújtson az összes megfelelő biztonsági intézkedés végrehajtásáról, valamint a minősített adatok és a kommunikációs és információs rendszer megfelelő szintű védelmének biztosításáról e biztonsági közleménnyel összhangban. Az akkreditációs nyilatkozat meghatározza a kommunikációs és információs rendszerben kezelhető adatok legmagasabb minősítési szintjét, valamint a megfelelő feltételeket.

5. A kommunikációs és információs rendszerben végzett műveletek biztonsága és helyes működése szempontjából az információvédelem következő jellemzői és szempontjai tekintendők alapvető fontosságúnak:

a) hitelesség: annak garanciája, hogy az adat valódi és jóhiszemű forrásokból származik;

b) rendelkezésre állás: az engedéllyel rendelkező szervezet kérelemére megvalósuló hozzáférhetőség és felhasználhatóság;

c) bizalmas jelleg: az adatot illetéktelen személyek, szervezetek vagy folyamatok részére nem szolgáltatják ki;

d) sértetlenség: az adatok és eszközök pontosságának és teljességének védelme;

e) letagadhatatlanság: egy cselekedet vagy esemény megtörténtének bizonyíthatósága annak érdekében, hogy ezt a cselekedetet vagy eseményt később ne lehessen letagadni.

B. **INFORMÁCIÓVÉDELMI ELVEK**

6. Az alábbiakban foglalt rendelkezések képezik a minősített adatokat kezelő kommunikációs és információs rendszerek biztonságosságának alapját. E rendelkezések végrehajtásának részletes követelményeit az információvédelmi biztonsági politikák és technikai biztonsági iránymutatások határozzák meg.

B.1. ***Biztonsági kockázatkezelés***

7. A biztonsági kockázatkezelés a kommunikációs és információs rendszer meghatározásának, kialakításának, működtetésének és fenntartásának szerves részét képezi. A kockázatkezelést (értékelést, kezelést, elfogadást, kommunikációt) az 1. biztonsági közleményben meghatározott rendszertulajdonosok, projekthatóságok, működtető hatóságok és biztonsági jóváhagyó hatóságok képviselői együttesen végzik el ismétlődő folyamatként egy kipróbált, átlátható és érthető kockázatértékelési folyamat alkalmazásával. A kommunikációs és információs rendszer hatókörét és eszközeit a kockázatkezelési folyamat kezdetekor egyértelműen meg kell határozni.

8. Az 1. biztonsági közleményben meghatározott illetékes hatóságoknak át kell tekinteniük a kommunikációs és információs rendszert fenyegető potenciális veszélyeket, valamint naprakész és pontos, az aktuális működési környezetet tükröző fenyegetésértékeléssel kell rendelkezniük. A változó információtechnológiai környezettel való lépéstartás érdekében folyamatosan frissíteniük kell a sebezhetőségi kérdésekkel kapcsolatos ismereteiket, és rendszeresen felül kell vizsgálniuk a sebezhetőségi értékeléseket.

9. A biztonsági kockázatkezelés célja olyan biztonsági intézkedések alkalmazása, melyek eredményeképpen kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a fennmaradó biztonsági kockázatok között.

10. A kommunikációs és információs rendszer akkreditációja magában foglalja a fennmaradó kockázat hivatalos megállapítását és a fennmaradó kockázatnak a felelős hatóság általi elfogadását. Egy adott kommunikációs és információs rendszer akkreditálásának vonatkozásában a megfelelő biztonsági akkreditációs hatóság által meghatározott különös követelményeknek, nagyságrendnek és részletességnek arányban kell állnia a valamennyi vonatkozó tényező figyelembe vételével – a kommunikációs és információs rendszerben kezelt minősített adatok minősítési szintjét is beleértve – megállapított kockázattal.

B.2. ***Biztonság a kommunikációs és információs rendszer teljes életciklusán keresztül***

11. Követelmény a biztonság garantálása a kommunikációs és információs rendszer teljes életciklusa alatt, a beüzemeléstől kezdve egészen a működésből való kivonásig.

12. Az életciklus minden szakaszára meg kell állapítani a kommunikációs és információs rendszerben részt vevő minden egyes szereplő biztonsági szerepét és a biztonság tekintetében a többi résztvevővel folytatott interakcióját.

13. A kommunikációs és információs rendszert – a technikai és nem technikai biztonsági intézkedéseket is beleértve – az akkreditációs folyamat során biztonsági tesztelésnek kell alávetni a kellő biztonsági szintről való meggyőződés érdekében, valamint annak ellenőrzése céljából, hogy a kommunikációs és információs rendszert – a technikai és nem technikai biztonsági intézkedéseket is beleértve – helyesen telepítették, integrálták és konfigurálták.

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

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

16. A kommunikációs és információs rendszer által végrehajtott nyilvántartási eljárásokat – szükség esetén – az akkreditációs folyamat részeként ellenőrizni kell.

B.3. ***Legjobb gyakorlat***

17. Az információvédelmi hatóságnak (IAA) ki kell alakítania a kommunikációs és információs rendszerben kezelt minősített adatok védelmére szolgáló legjobb gyakorlatot. A legjobb gyakorlatra vonatkozó iránymutatások tartalmazzák a kommunikációs és információs rendszerrel kapcsolatos, az adott fenyegetésekkel és sebezhetőségekkel szemben bizonyítottan hatékony technikai, fizikai, szervezeti és eljárási biztonsági intézkedéseket.

18. A kommunikációs és információs rendszer által kezelt minősített adatok védelme az információvédelemben részt vevő szervezetek által levont tanulságokra épül.

19. A legjobb gyakorlat terjesztése és azt követő végrehajtása hozzájárul ahhoz, hogy a minősített adatokat kezelő parlamenti titkárság által működtetett kommunikációs és információs rendszer egyenértékű védelmi szintet érjen el.

B.4. ***Alapos védelem***

20. A kommunikációs és információs rendszer kockázatainak enyhítése érdekében technikai és nem technikai biztonsági intézkedéseket kell végrehajtani, melyek többrétegű védelmi réteget alkotnak. E rétegek az alábbiak:

a) elrettentés: a kommunikációs és információs rendszer megtámadását tervező bármilyen ellenség elrettentését célzó biztonsági intézkedések;

b) megelőzés: a kommunikációs és információs rendszer megtámadásának megakadályozását célzó biztonsági intézkedések;

c) észlelés: a kommunikációs és információs rendszer megtámadásának észlelését célzó biztonsági intézkedések;

d) ellenállóképesség: a támadás hatásának az adatok vagy a kommunikációs és információs rendszer eszközei minimumára való korlátozását és a további kár megelőzését célzó biztonsági intézkedések; továbbá

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

E biztonsági intézkedések szigorúságának mértékét kockázatértékelés alapján kell meghatározni.

21. Az 1. biztonsági közleményben meghatározott illetékes hatóságok biztosítják, hogy képesek legyenek a szervezeti vagy nemzeti határokon esetlegesen átnyúló eseményekre való reagálásra a reagálások összehangolása, valamint az ilyen eseményekről és a kapcsolódó kockázatokról való információcsere érdekében (számítógépes szükséghelyzeti válaszadási képességek).

B.5. ***A minimalitás és a legkisebb kiváltság elve***

22. A szükségtelen kockázat elkerülése érdekében kizárólag a működési követelmények teljesítéséhez alapvetően szükséges funkciókat, eszközöket és szolgáltatásokat kell alkalmazni és végrehajtani.

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

B.6. ***Információvédelmi tudatosság***

24. A kommunikációs és információs rendszerek biztonsága védelmének első vonalát a kockázatok és a rendelkezésre álló biztonsági intézkedések ismerete képezi. A kommunikációs és információs rendszerek életciklusában érintett valamennyi személynek tudatában kell lennie különösen annak, hogy:

a) a biztonsági hiányosságok jelentősen károsíthatják a minősített adatokat kezelő kommunikációs és információs rendszereket;

b) az összekapcsolódásból és egymásra utaltságból adódóan másokat milyen károk érhetnek; továbbá

c) a rendszerben és folyamatokban betöltött szerepeik szerint személyesen felelősek és elszámoltathatók a kommunikációs és információs rendszerek biztonságáért.

25. A biztonsággal kapcsolatos felelősség ismeretének biztosítása érdekében valamennyi érintett személy – beleértve a vezető tisztviselőket, az európai parlamenti képviselőket és a kommunikációs és információs rendszerek felhasználóit is – számára kötelező információvédelmi oktatást és tudatosságnövelő képzést kell szervezni.

B.7. ***Az információtechnológiai biztonsági termékek értékelése és jóváhagyása***

26. A „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatokat kezelő kommunikációs és információs rendszereket olyan módon kell védeni, hogy az adatok nem szándékos elektromágneses kisugárzás révén ne legyenek veszélyeztethetők („TEMPEST biztonsági intézkedések").

27. Amennyiben a minősített adatok védelmét kriptográfiai termékek biztosítják, e termékekről az SAA-nak igazolnia kell, hogy szerepelnek az EU által jóváhagyott kriptográfiai termékek között.

28. A minősített adatok elektronikus eszközökkel történő továbbítása során az EU által jóváhagyott kriptográfiai terméket kell használni. E követelmény ellenére a 41–44. pontban meghatározott szükséghelyzet esetén egyedi technikai konfigurációk vagy különleges eljárások alkalmazhatók.

29. A biztonsági intézkedések – védelmi szintként meghatározott – szükséges megbízhatósági szintjét a kockázatkezelési eljárás eredménye alapján és a vonatkozó biztonsági politikákkal és technikai biztonsági iránymutatásokkal összhangban kell meghatározni.

30. A védelmi szintet nemzetközileg elismert vagy nemzeti szinten jóváhagyott folyamatok és módszerek alkalmazásával kell ellenőrizni. Ez elsősorban értékelés, ellenőrzés és auditálás lehet.

31. Az SAA biztonsági iránymutatásokat hagy jóvá a nem kriptografikus információtechnológiai biztonsági termékek minősítésére és jóváhagyására vonatkozóan.

B.8. ***Továbbítás a biztonságos területen belül***

32. Amennyiben a minősített adatok továbbítása a biztonságos területre korlátozódik, kódolatlan továbbítás vagy alacsonyabb szintű adattitkosítás alkalmazható a kockázatkezelési folyamat eredményére alapozva és az SAA jóváhagyásával.

B.9. ***A kommunikációs és információs rendszerek biztonságos összekapcsolása***

33. A rendszerek összekapcsolása két vagy több információtechnológiai rendszer adatok és egyéb információforrások megosztása céljából történő, egyirányú vagy többirányú, közvetlen összekapcsolását jelenti.

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

35. A kommunikációs és információs rendszer más információtechnológiai rendszerrel való minden összekapcsolása tekintetében a következő alapkövetelményeknek kell eleget tenni:

a) az ilyen összekapcsolások üzleti vagy üzemeltetési követelményeit az illetékes hatóságok határozzák meg és hagyják jóvá;

b) az adott összekapcsolást kockázatkezelési és akkreditációs eljárásnak kell alávetni, és ahhoz az illetékes SAA jóváhagyása szükséges;

c) a kommunikációs és információs rendszer körzethatárán védelmi szolgáltatásokat kell létesíteni.

36. Akkreditált kommunikációs és információs rendszer nem kapcsolható össze nem védett vagy nyilvános hálózattal, kivéve, ha a kommunikációs és információs rendszer jóváhagyott, a kommunikációs és információs rendszer és a nyilvános hálózat között e célból telepített védelmi szolgáltatással rendelkezik. Az ilyen összekapcsolásra vonatkozó biztonsági intézkedéseket az illetékes információvédelmi hatóságnak (IAA) felül kell vizsgálnia, és az illetékes SAA-nak jóvá kell hagynia.

37. Amennyiben a nem védett vagy nyilvános hálózatot kizárólag adatközvetítésre használják, és az adatokat a 27. cikknek megfelelően az EU által jóváhagyott kriptográfiai termékkel kódolták, az ilyen kapcsolat nem tekintendő összekapcsolásnak.

38. Tilos a „TRES SECRET UE/EU TOP SECRET” vagy ezzel egyenértékű, illetve a „SECRET UE/EU SECRET” vagy ezzel egyenértékű szinten minősített adatok kezelésére akkreditált kommunikációs és információs rendszer közvetlen vagy kaszkád módon való összekapcsolása nem védett vagy nyilvános hálózattal.

B.10. ***Számítógépes adathordozók***

39. A számítógépes adathordozókat az illetékes biztonsági hatóság által jóváhagyott eljárással összhangban kell semmisíteni.

40. A számítógépes adathordozókat a kezelési utasításoknak megfelelően kell újrahasznosítani, illetve minősített besorolásukat alacsonyabb szintűvé tenni vagy megszüntetni.

B.11. ***Szükséghelyzet***

41. Szükséghelyzetben – például fenyegető vagy ténylegesen fennálló válság-, konfliktus- vagy háborús helyzetben – vagy rendkívüli üzemeltetési körülmények között az alábbiakban leírt különös eljárások alkalmazhatók.

42. Minősített adatok az illetékes hatóság beleegyezésével továbbíthatók alacsonyabb minősítési szintre jóváhagyott kriptográfiai termékek felhasználásával vagy kódolás nélkül, amennyiben a késedelem által okozott kár egyértelműen meghaladná a minősített adatok illetéktelen kezekbe jutása által esetlegesen okozott kárt, és ha:

a) a küldő, illetve a címzett nem rendelkezik az előírt kódolási lehetőséggel vagy egyáltalán kódolási lehetőséggel, továbbá

b) a minősített anyag más eszközökkel nem továbbítható kellő időben.

43. A 41. pontban meghatározott körülmények esetén továbbított minősített adat nem látható el olyan jelöléssel vagy jelzéssel, amely azt a nem minősített adattól vagy a rendelkezésre álló kódolási lehetőséggel védhető adattól megkülönbözteti. A címzetteket késedelem nélkül, egyéb módon értesíteni kell a minősítés szintjéről.

44. Amennyiben a 41. vagy 42. pontban említett eljárás alkalmazására kerül sor, jelentést kell tenni az illetékes hatóságnak.

4. BIZTONSÁGI KÖZLEMÉNY

FIZIKAI BIZTONSÁG

A. **BEVEZETÉS**

E biztonsági közlemény megállapítja a bizalmas adatok Európai Parlament általi helyes kezelése biztonságos környezetének létrehozásához szükséges elveket. Ezeket az elveket – köztük a technikai biztonság elveit – a kezelési utasítások egészítik ki.

B. **BIZTONSÁGI KOCKÁZATKEZELÉS**

1. A 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 biztonsági közleményben rögzített alapelvekkel és minimumszabályokkal összhangban, és ezen intézkedések alkalmazása a 3. biztonsági közleményben rögzített „alapos védelem" elvének megfelelően. A fenti intézkedések hatékonyságát folyamatosan értékelni kell.

2. A minősített adatok teljes életciklusuk alatti védelmét szolgáló biztonsági intézkedések arányban állnak különösen az adatok biztonsági minősítésével, az érintett adat vagy anyag fizikai formájával és mennyiségével, a minősített adatok tárolására használt helyiségek elhelyezkedésével és felépítésével, valamint a rosszindulatú cselekményekből és/vagy bűncselekményekből – a hírszerzést, szabotázst és a terrorizmust is ideértve – eredően helyi szinten fennálló fenyegetéssel.

3. Az engedély nélküli hozzáférés és kiszolgáltatás, valamint az információk és anyagok megsérülésének és a rendelkezésre állás megszűnésének a megelőzése érdekében a szükséghelyzeti terveknek figyelembe kell venniük a minősített adatok veszélyhelyzet esetén való védelmének a szükségességét.

4. Az üzletmenetfolytonossági-terveknek a súlyos mulasztások vagy események által a minősített adatok kezelésére és tárolására gyakorolt hatások csökkentését szolgáló megelőző és helyreállító intézkedéseket kell tartalmazniuk.

C. **ÁLTALÁNOS ELVEK**

5. Az adat minősítése vagy jelölési szintje meghatározza a tárolás védelmi szintjét a fizikai biztonság területein.

6. A minősített adatot fizikai formájától függetlenül ilyenként kell megjelölni és kezelni. A minősítésről egyértelműen tájékoztatni kell a címzetteket, akár a biztonsági besorolásra utaló jelölés (írásos formában – papíralapon vagy a kommunikációs és információs rendszerben – történő továbbítás esetén), akár bármiféle közlés révén (szóbeli – beszélgetés közben vagy zárt ülés keretében történő – továbbítás esetén). A minősített dokumentumon a minősítés tényét a könnyű azonosítást szolgáló biztonsági besorolhatóság érdekében fel kell tüntetni.

7. A bizalmas adat semmilyen körülmények között nem olvasható nyilvános helyen (pl. vonaton, repülőgépen, kávéházban, bárban stb.), ahol bárki megláthatja, anélkül, hogy a szükséges ismerettel rendelkezne. Bizalmas adatot nem szabad szállaodai szobában vagy széfben elhelyezni és nem szabad felügyelet nélkül nyilvános helyen hagyni.

D. **FELELŐSSÉGI KÖRÖK**

8. A Minősített Adatok Osztálya felel a biztonságos helyiségeiben elhelyezett bizalmas adatok kezelésének fizikai biztonságáért. A Minősített Adatok Osztálya felel saját biztonságos helyiségeinek irányításáért is.

9. A „RESTREINT UE/EU RESTRICTED" vagy azzal egyenértékű minősítésű adat és az „egyéb bizalmas adat" fizikai biztonságáért az illetékes parlamenti szerv/tisztviselő felel.

10. Európai Parlament Biztonsági és Kockázatértékelési Igazgatósága biztosítja a Parlamenten belüli bizalmas adatok biztonságos kezeléséhez szükséges a személyi biztonságot és a biztonsági tanúsítványt.

11. Az Informatikai Igazgatóság (DIT) feladata a tanácsadás és annak biztosítása, hogy valamennyi létrehozott vagy használt kommunikációs és információs rendszer maradéktalanul megfeleljen a 3. biztonsági közleménynek és a megfelelő kezelési utasításoknak.

E. **BIZTONSÁGOS HELYISÉGEK**

12. Biztonságos helyiségeket lehet létrehozni a technikai biztonsági előírásokkal és a 7. cikkben meghatározott minősített adat besorolási szintjével összhangban.

13. A biztonságos helyiségeket az SAA-nak tanúsítja és a biztonsági hatóság hagyja jóvá.

F. **BETEKINTÉS A BIZALMAS ADATOKBA**

14. Amennyiben „RESTREINT UE/EU RESTRICTED" vagy ezzel egyenértékű minősített adatot, illetve „egyéb bizalmas adatot" helyeznek el a Minősített Adatok Osztályán és ezekbe az adatokba a biztonságos területen kívül kell betekinteni, a Minősített Adatok Osztálya eljuttatja az adatok másolatát a megfelelő felhatalmazott szervezeti egységnek, amelynek biztosítania kell, hogy az adott adatok megtekintése és kezelése megfeleljen e határozat 8. cikke (2) bekezdésének és 10. cikkének, valamint a vonatkozó kezelési utasításoknak.

15. Amennyiben „RESTREINT UE/EU RESTRICTED" vagy szinten vagy azzal egyenértékű szinten minősített adatot, illetve „egyéb bizalmas adatot" helyeznek el a Minősített Adatok Osztályától eltérő parlamenti szervnél/tisztségviselőnél, az adott parlamenti szerv/tisztségviselő titkárságának biztosítania kell, hogy az adatok megtekintése és kezelése megfeleljen e határozat 7. cikke (3) bekezdésének, 8. cikke (1), (2) és (4) bekezdésének, 9. cikke (3), (4) és (5) bekezdésének, és 10. cikke (2)–(6) bekezdésének és 11. cikkének, valamint a vonatkozó kezelési utasításoknak.

16. Amennyiben „RESTREINT UE/EU RESTRICTED, SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET" vagy ezzel egyenértékű, illetve ennél magasabb fokú minősített adatokban a biztonságos területen belül kell betekinteni, a Minősített Adatok Osztálya biztosítja, hogy az adatok megtekintése és kezelése megfeleljen e határozat 9. és 10. cikkének, valamint a vonatkozó kezelési utasításoknak.

G. **TECHNIKAI BIZTONSÁG**

17. A technikai biztonsággal kapcsolatos intézkedések a biztonsági akkreditációs hatóság felelősségi körébe tartoznak, ennek kell meghatároznia a vonatkozó kezelési utasításokban az alkalmazandó konkrét technikai biztonsági intézkedéseket.

18. Az e határozat értelmében „RESTREINT UE/EU RESTRICTED" vagy azzal egyenértékű minősítésű szintű adatok megtekintésére szolgáló biztonságos olvasótermeknek meg kell felelniük a kezelési utasításokban rögzített vonatkozó technikai intézkedéseknek.

19. A biztonságos helynek az alábbi helyiségekkel kell rendelkeznie:

a) biztonsági beléptető helyiség (Security Access Screening Room, „SAS"), amelyet a kezelési utasításokban rögzített technikai intézkedéseknek megfelelően kell kialakítani. A helyiségbe való belépésekről nyilvántartást kell vezetni. A biztonsági beléptető helyiségnek magas szintű normáknak kell megfelelnie a belépésre jogosult személyek azonosítása tekintetében, videofelvétellel, valamint a biztonsági termekben nem engedélyezett személyes holmik (telefonok, tollak stb.) tárolására alkalmas biztonságos tárolókkal;

b) a minősített adatok, többek között kódolt minősített adatok továbbítására és érkeztetésére szolgáló kommunikációs terem, a 3. biztonsági közleménynek és a vonatkozó kezelési utasításoknak megfelelően;

c) biztonságos irattár, ahol jóváhagyott és tanúsítvánnyal rendelkező tárolókat kell használni külön a „RESTREINT UE/EU RESTRICTED", „CONFIDENTIEL UE/EU CONFIDENTIAL". illetve „SECRET UE/EU SECRET" szinten vagy azzal egyenértékű szinten adatok tárolására. A „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatokat külön helyiségben, erre a célra szolgáló, tanúsítvánnyal rendelkező tárolóban kell elhelyezni. Ebben a helyiségben ezen kívül csakis egy asztalt lehet elhelyezni, amelyen a Minősített Adatok Osztálya az irattár tartalmát kezeli.

d) nyilvántartó helyiség, amelyben megtalálhatók a nyilvántartás vezetéséhez szükséges papíralapú vagy elektronikus eszközök, vagyis kommunikációs és információs rendszerek kialakításához szükséges biztonságos eszközök. Csakis a nyilvántartó helyiségben lehetnek jóváhagyott és akkreditált másolóeszközök (papíralapú vagy elektronikus másolatok készítéséhez). A kezelés utasítások rögzítik, hogy mely másolóeszközöket hagyják jóvá és akkreditálják. A nyilvántartó helyiségben kell biztosítani a minősített adatok fizikai formában történő jelöléséhez, másolásához és elosztásához szükséges eszközök tárolását és kezelését, minősítési szintenkét. Valamennyi akkreditált eszközt a Minősített Adatok Osztályának kell meghatároznia, és a biztonsági akkreditációs hatóságnak kell akkreditálnia azokat az IAOA szakvéleménye alapján. Ezt a helyiséget fel kell szerelni továbbá a legmagasabb minősítési szintnek megfelelően akkreditált iratmegsemmisítő eszközzel, a kezelési utasításoknak megfelelően. A legalább „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" vagy „TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatok fordítását a nyilvántartó helyiségben kell végezni, az erre szolgáló és akkreditált rendszer segítségével. A nyilvántartó helyiségben legfeljebb két fordító számára lehet egyidőben ugyanazon dokumentum fordítása céljából munkaállomást biztosítani. A Minősített Adatok Osztálya egy alkalmazottjának jelen kell lennie.

e) olvasóterem, a minősített adatok megfelelő felhatalmazással rendelkezők általi egyéni megtekintéséhez. Az olvasóterem kellő teret biztosít két személy számára, beleértve a Minősített Adatok Osztálya egy alkalmazottját is, akinek valamennyi megtekintés alkalmával mindvégig jelen kell lennie. E terem biztonsági szintje megfelelő kell, hogy legyen a „CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vagy TRÈS SECRET UE/EU TOP SECRET" szinten vagy azzal egyenértékű szinten minősített adatok megtekintéséhez. Az olvasóterem felszerelhető TEMPEST eszközökkel az elektronikus formában történő megtekintés céljából, a szóban forgó adat minősítési szintjének megfelelően.

f) egy ülésterem, amelyben akár 25 fő is meg tudja vitatni a „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" és azzal egyenértékű minősítésű adatokat. Az ülésterem biztosítja a szükséges, technikai szempontból biztonságos és tanúsítvánnyal rendelkező eszközöket, valamint a tolmácsolási lehetőséget akár két nyelvre is. Amikor a teremben nem tartanak ülést, további olvasóteremként használható dokumentumok egyedi megtekintésére. Rendkívüli esetekben a Minősített Adatok Osztálya engedélyezheti, hogy egynél több felhatalmazott személy tekintsen meg minősített adatokat, amennyiben a helyiségben tartózkodó személyek biztonsági tanúsítványa és szükséges ismerete megegyezik. Ugyanakkor egyidőben négynél több személy nem tekinthet meg minősített adatokat. A Minősített Adatok Osztálya tisztviselőinek jelenlétét meg kell erősíteni.

g) biztonságos technikai helyiségek a biztonságos terület és a biztonságos IT-szerverek biztonságához kapcsolódó valamennyi technikai felszerelés elhelyezése céljából.

20. A biztonságos területnek meg kell felelnie az alkalmazandó nemzetközi biztonsági normáknak, valamint rendelkeznie kell a Biztonsági és Kockázatértékelési Igazgatóság által adott tanúsítvánnyal. A biztonságos területnek legalább az alábbi biztonságtechnikai felszereléssel kell rendelkeznie:

a) riasztórendszer és biztonsági kamerarendszer;

b) biztonsági felszerelés és vészhelyzeti rendszerek (kétirányú figyelmeztető rendszer);

c) CCTV-rendszer;

d) behatolásjelző rendszer;

e) beléptető rendszer (beleértve a biometrikus biztonsági rendszert is);

f) tárolók;

g) zárható szekrények;

h) elektromágnesesség elleni védelem.

21. Amennyiben további biztonságtechnikai intézkedésekre van szükség, ezeket a biztonsági akkreditációs hatóság írhatja elő, szorosan együttműködve a Minősített Adatok Osztályával, illetve a biztonsági hatóság jóváhagyását követően.

22. Az infrastrukturális eszközök csatlakoztathatók a biztonságos területnek otthont adó épület általános rendszereihez. A beléptetésre szolgáló biztonsági eszközöknek és a kommunikációs és információs rendszereknek azonban függetlennek kell lenniük az Európai Parlament valamennyi egyéb ilyen létező rendszerétől.

H. **A BIZTONSÁGOS TERÜLET ELLENŐRZÉSE**

23. A biztonsági akkreditációs hatóság rendszeresen ellenőrzi a biztonságos területet, a Minősített Adatok Osztálya kérésére pedig külön ellenőrzéseket is tart.

24. A biztonsági akkreditációs hatóság összeállítja és naprakészen tartja a biztonsági ellenőrzés ellenőrző listáját, amely tartalmazza a kezelési utasítások alapján az ellenőrzések alkalmával megszemlélendő elemeket.

I. **A BIZALMAS ADATOK SZÁLLÍTÁSA**

25. A bizalmas adatokat a kezelési utasításoknak megfelelően a tartalom bizalmas jellegére való utalás nélkül, oly módon kell szállítani, hogy ne lehessenek láthatók.

26. A legalább „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” vagy „TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatokat csakis megfelelő biztonsági felhatalmazással rendelkező futárok vagy tisztviselők szállíthatják.

27. A bizalmas adatokat külső posta vagy az épületen kívüli személyes szállítás útján csak a kezelési utasítások szerinti feltételek mellett lehet továbbítani.

28. A legalább „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” vagy „TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatok semmilyen körülmények között sem küldhetők emailben vagy faxon, még „biztonságos” email-rendszer vagy kódolt faxgép esetén sem. A „RESTREINT UE/EU RESTRICTED” szinten vagy azzal egyenértékű szinten minősített adatok és egyéb bizalmas adatok akkreditált kódolási rendszer alkalmazásával küldhetők emailben.

J. **A BIZALMAS ADATOK TÁROLÁSA**

29. A bizalmas adatok minősítése vagy jelölési szintje meghatározza a tárolás védelmi szintjét. A bizalmas adatokat a kezelési utasítás értelmében e célra tanúsított eszközökben kell tárolni.

30. A „RESTREINT UE/EU RESTRICTED” szinten vagy azzal egyenértékű szinten minősített adatokat és az „egyéb bizalmas adatokat”:

a) használaton kívül általános szabályként zárt acélszekrényben kell tartani, amely egy irodában vagy valamilyen munkaterületen található;

b) csak megfelelően elzárva és tárolva szabad felügyelet nélkül hagyni;

c) nem szabad oly módon az íróasztalon, asztalon, stb. hagyni, hogy felhatalmazással nem rendelkező személyek, például látogatók, takarítószemélyzet, karbantartók, stb. elolvashassák vagy magukkal vigyék;

d) nem mutathatók meg felhatalmazással nem rendelkező személyeknek és ilyenekkel nem vitathatók meg.

31. A „RESTREINT UE/EU RESTRICTED”, „SECRET UE/EU SECRET” vagy „TRÈS SECRET UE/EU TOP SECRET” szinten vagy azzal egyenértékű szinten minősített adatokat és az „egyéb bizalmas adatokat” a parlamenti szerv/tisztségviselő titkárságán vagy a Minősített Adatok Osztályán szabad tárolni, a kezelési utasításoknak megfelelően.

32. A „CONFIDENTIEL UE/EU CONFIDENTIAL” és e fölötti minősítésű vagy ezzel egyenértékű adatokat:

a) a biztonságos területen belül, biztonsági tárolóban vagy páncélteremben kell tárolni; ám kivételes jelleggel, például ha a Minősített Adatok Osztálya zárva van, a biztonsági szolgálaton belüli, jóváhagyott és tanúsítással rendelkező széfben is lehet tárolni;

b) a biztonságos területen belül sem szabad felügyelet nélkül hagyni (még rövid távollétek esetére sem) anélkül, hogy előzőleg el ne zárták volna egy jóváhagyott széfben;

c) nem szabad oly módon az íróasztalon, asztalon, stb. hagyni, hogy felhatalmazással nem rendelkező személyek elolvashassák vagy magukkal vigyék, még abban ez esetben sem, ha a Minősített Adatok Osztályának tisztviselője a teremben marad.

Amennyiben minősített adatot tartalmazó dokumentum készül elektronikus formában a biztonságos területen belül, a számítógépet le kell zárni, a képernyőt pedig olvashatatlanná kell tenni minden olyan esetben, amikor a dokumentum készítője vagy a Minősített Adatok Osztályának tisztviselője (akár rövid időre) elhagyja az irodát. A néhány perc után működésbe lépő automatikus biztonsági zárak nem minősülnek kielégítő megoldásnak e tekintetben.

5. BIZTONSÁGI KÖZLEMÉNY

IPARI BIZTONSÁG

A. **BEVEZETÉS**

1. Ez a biztonsági közlemény csak a minősített adatokra vonatkozik.

2. Rendelkezéseket tartalmaz a határozat I. mellékletének 1. részében említett közös minimumszabályok végrehajtását illetően.

3. Ipari biztonság alatt értendő annak biztosítása, hogy a szerződő felek és alvállalkozóik is megvédjék a minősített adatokat a szerződéskötést megelőző tárgyalások során és a minősített szerződések teljes életciklusa folyamán. Az ilyen szerződések nem biztosíthatnak hozzáférést a „TRÈS SECRET UE/EU TOP SECRET” minősítésű adatokhoz.

4. Az Európai Parlament szerződő hatóságként köteles biztosítani az e határozatban az ipari biztonságra vonatkozóan rögzített, és a szerződésben említett minimumszabályok tiszteletben tartását a minősített szerződések ipari vagy egyéb szereplők számára történő odaítélésekor.

B. **BIZTONSÁGI ELEMEK A MINŐSÍTETT SZERZŐDÉSEKBEN**

B.1. ***Biztonsági minősítési útmutató (SCG)***

5. Az Európai Parlament szerződő hatóságként az ajánlattételi felhívás közzétételét vagy a minősített szerződés odaítélését megelőzően meghatározza a pályázók és a szerződő felek tudomására hozandó, illetve a szerződő fél által rendelkezésre bocsátandó adatok biztonsági besorolását. Az Európai Parlament e célból elkészíti a szerződés teljesítéséhez felhasználandó biztonsági minősítési útmutatót.

6. A minősített szerződések különféle elemeire vonatkozó biztonsági besorolás szintjének meghatározásakor az alábbi elveket kell alkalmazni:

a) az SCG elkészítése során az Európai Parlamentnek figyelembe kell vennie valamennyi vonatkozó biztonsági szempontot, köztük az adat kibocsátója által a szerződéshez való használat céljából rendelkezésre bocsátott és jóváhagyott adathoz rendelt biztonsági minősítést;

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

B.2. ***Biztonsági vonatkozások záradéka (SAL)***

7. A szerződésspecifikus biztonsági követelményeket biztonsági vonatkozások záradékban (SAL) kell leírni. Adott esetben a SAL tartalmazza az SCG-t, és a minősített vállalkozói vagy alvállalkozói szerződésnek szerves részét képezi.

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

B.3. ***A programra/projektre vonatkozó biztonsági utasítások (PSI)***

9. Az EU-minősített adatokhoz való hozzáférést, vagy azok kezelését vagy tárolását magában foglaló program vagy projekt hatályának függvényében a program vagy projekt irányítására kijelölt szerződő hatóság az adott programra/projektre vonatkozó biztonsági utasításokat (PSI) dolgozhat ki.

C. **TELEPHELY-BIZTONSÁGI TANÚSÍTVÁNY (FSC)**

10. Az FSC-t a tagállam nemzeti biztonsági hatósága vagy bármely más illetékes biztonsági hatósága bocsátja ki annak jelzésére, hogy – a nemzeti jogszabályokkal és rendeletekkel összhangban – egy ipari vagy más szervezet képes az EU-minősített adatoknak a létesítményeiben, megfelelő minősítési szinten („CONFIDENTIEL UE/EU CONFIDENTIAL” vagy „SECRET UE/EU SECRET”) való védelmére. Az FSC megadásáról szóló igazolást be kell mutatni az Európai Parlamentnek mint a szerződő hatóságnak, mielőtt egy vállalkozó, alvállalkozó, illetve potenciális vállalkozó vagy alvállalkozó számára az EU-minősített adatokhoz való hozzáférést biztosítanának vagy engedélyeznének.

11. Az FSC

a) értékeli az ipari vagy egyéb szervezet integritását;

b) értékeli a biztonsági kockázatnak tekinthető tulajdonlást, ellenőrzést vagy esetleges indokolatlan befolyást;

c) ellenőrzi, hogy az ipari vagy egyéb szervezet olyan helyszíni biztonsági rendszert létesített, amely a „CONFIDENTIEL UE/EU CONFIDENTIAL" vagy „SECRET UE/EU SECRET" minősítésű adatok vagy anyagok – az e határozatban foglalt előírások szerinti – védelméhez szükséges minden megfelelő biztonsági intézkedésre kiterjed;

d) ellenőrzi, hogy azon vezetők, tulajdonosok és alkalmazottak személyi biztonsági státusát, akiknek „CONFIDENTIEL UE/EU CONFIDENTIAL" vagy „SECRET UE/EU SECRET" minősítésű adatokhoz hozzáféréssel kell rendelkezniük, az e határozatban megállapított rendelkezéseknek megfelelően határozták meg; és

e) ellenőrzi, hogy az ipari vagy egyéb szervezet létesítménybiztonsági tisztviselőt (FSO) nevezett ki, aki felelősséggel tartozik a vezetőinek a biztonsági kötelezettségeknek a szervezeten belül történő érvényesítéséért.

12. Adott esetben az Európai Parlament szerződő hatóságként értesíti a megfelelő nemzeti biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot, hogy a szerződést megelőző szakaszban vagy a szerződés teljesítéséhez FSC-re van szükség. Már a szerződéskötést megelőző szakaszban FSC-t vagy PSC-t kell előírni abban az esetben, ha az ajánlattételi eljárás során „CONFIDENTIEL UE/EU CONFIDENTIAL" vagy „SECRET UE/EU SECRET" minősítésű adatokat kell rendelkezésre bocsátani.

13. A szerződő hatóság nem köthet minősített szerződést a megfelelőnek tartott pályázóval azt megelőzően, hogy kézhez kapná az azon tagállam nemzeti biztonsági hatósága által kiállított megerősítést, amelyben az érintett vállalkozót vagy alvállalkozót bejegyezték, arról hogy szükség esetén megfelelő FSC-vel rendelkeznek.

14. Az FSC-t kibocsátó illetékes biztonsági hatóságok az FSC-t érintő bármely változásról értesítik az Európai Parlamentet mint szerződő hatóságot. Alvállalkozói szerződés esetén az illetékes biztonsági hatóságot ennek megfelelően tájékoztatni kell

15. Az FSC-nek az adott nemzeti biztonsági hatóság vagy bármely más illetékes biztonsági hatóság általi visszavonása kellően feljogosítja az Európai Parlamentet mint szerződő hatóságot a minősített szerződés megszűntetésére vagy a pályázónak a versenyből való kizárására.

D. **MINŐSÍTETT SZERZŐDÉSEK ÉS ALVÁLLALKOZÓI SZERZŐDÉSEK**

16. Amikor egy esetleges pályázó részére a szerződést megelőző szakaszban minősített adatot adnak át, a pályázati felhívásnak tartalmaznia kell egy olyan kitételt, amely azt a pályázót, aki végül nem nyújtja be pályázatát, vagy akit nem választanak ki, arra kötelezi, hogy adott időn belül valamennyi minősített dokumentumot szolgáltassa vissza.

17. Amint sor kerül egy minősített vállalkozói vagy alvállalkozói szerződés odaítélésére, az Európai Parlament szerződő hatóságként értesíti a vállalkozó vagy alvállalkozó nemzeti biztonsági hatóságát és/vagy bármely más illetékes biztonsági hatóságát a minősített szerződés biztonsági előírásairól.

18. Amennyiben egy ilyen szerződést megszüntetnek, az Európai Parlament szerződő hatóságként (és/vagy a nemzeti biztonsági hatóság vagy alvállalkozói szerződés esetén bármely más illetékes biztonsági hatóság) késedelem nélkül értesíti azon tagállam nemzeti biztonsági hatóságát, amelyben a vállalkozót vagy alvállalkozót bejegyezték.

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

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

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

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

23. Mielőtt a vállalkozó a minősített szerződés bármely részére alvállalkozókat szerződtetne, ehhez engedélyt kér az Európai Parlamenttől mint szerződő hatóságtól. Nem ítélhető oda szerződés vagy alvállalkozói szerződés olyan harmadik államokban bejegyzett ipari vagy más szervezetek számára, amelyek nem kötöttek adatbiztonsági megállapodást az Unióval.

24. A vállalkozó felelős 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 engedélye nélkül.

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

E. MINŐSÍTETT SZERZŐDÉSEKHEZ KAPCSOLÓDÓ LÁTOGATÁSOK

26. Amennyiben egy minősített szerződés teljesítése érdekében az Európai Parlament, a szerződő fél vagy az alvállalkozó „CONFIDENTIEL UE/EU CONFIDENTIAL” vagy „SECRET UE/EU SECRET” szinten vagy azzal egyenértékű szinten minősített adathoz kér helyszíni hozzáférést a másik fél épületében, a látogatást a nemzeti biztonsági hatóságokkal vagy bármely más érintett illetékes biztonsági hatósággal együttműködésben kell megszervezni. Konkrét projektekkel összefüggésben azonban a nemzeti biztonsági hatóságok hozzájárulhatnak a látogatás közvetlen megszervezéséhez is.

27. Minden látogatónak megfelelő PSC-vel kell rendelkeznie, és teljesítenie kell a „szükséges ismeret” feltételét az Európai Parlament szerződésével kapcsolatos minősített adatokhoz való hozzáféréshez.

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

F. MINŐSÍTETT ADATOK TOVÁBBÍTÁSA ÉS SZÁLLÍTÁSA

29. A minősített adatok elektronikus úton történő továbbítása tekintetében a 3. biztonsági közlemény vonatkozó rendelkezéseit kell alkalmazni.

30. A minősített adatok szállítása tekintetében a 4. biztonsági közlemény és a vonatkozó kezelési utasítások idevágó rendelkezéseit kell alkalmazni.

31. A 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 úticélig;

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

c) a szállítást végző vállalatok megfelelő szintű FSC-vel rendelkeznek. Ilyen esetekben a szállítmányt kezelő személyzetnek biztonsági felhatalmazással kell rendelkeznie az I. melléklettel összhangban;

d) a „CONFIDENTIEL UE/EU CONFIDENTIAL" és „SECRET UE/EU SECRET" vagy azzal egyenértékű minősítésű adatok bármilyen, határokon átnyúló szállítását megelőzően a feladó szállítási tervet készít, amelyet a főtitkár hagy jóvá;

e) az utakat lehetőség szerint egy adott kiindulási ponttól egy adott rendeltetési pontra kell megtenni, és a szállítást a körülmények engedte lehető leggyorsabban kell végrehajtani;

f) az útvonalnak lehetőség szerint a tagállamok területén kell keresztülhaladnia.

G. MINŐSÍTETT ADATOK HARMADIK ORSZÁGOKBAN TALÁLHATÓ SZERZŐDŐ FELEKNEK TÖRTÉNŐ ÁTADÁSA

32. A minősített adatok harmadik államokban működő vállalkozók vagy alvállalkozók részére való átadása az Európai Parlament mint szerződő hatóság és azon érintett harmadik állam nemzeti biztonsági hatósága vagy más illetékes biztonsági hatósága által elfogadott biztonsági intézkedésekkel összhangban történik, ahol a vállalkozót bejegyezték.

H. A „RESTREINT UE/EU RESTRICTED" MINŐSÍTÉSŰ ADATOK KEZELÉSE ÉS TÁROLÁSA

33. Az Európai Parlament mint szerződő hatóság a tagállam nemzeti biztonsági hatóságával összeköttetésben a szerződéses rendelkezések alapján látogatásokat tehet a vállalkozók/alvállalkozók létesítményeibe annak ellenőrzése céljából, hogy a „RESTREINT UE/EU RESTRICTED" szintű minősítéssel rendelkező adatok védelméhez szükséges, a szerződésben előírt biztonsági intézkedéseket megvalósították.

34. Az Európai Parlamentnek mint szerződő hatóságnak a nemzeti törvények és jogszabályok által előírt mértékig értesítenie kell a nemzeti biztonsági hatóságokat vagy bármely más illetékes biztonsági hatóságot a „RESTREINT UE/EU RESTRICTED" minősítésű adatokat tartalmazó szerződésekről és alvállalkozói szerződésekről.

35. A „RESTREINT UE/EU RESTRICTED" minősítésű adatot magukban foglaló, az Európai Parlament által odaítélt szerződések esetén az FSC vagy a PSC nem kötelező a vállalkozók, alvállalkozók és alkalmazottaik számára.

36. Az Európai Parlament mint szerződő hatóság megvizsgálja azon szerződésekre kiírt pályázati felhívásokra érkezett válaszokat, amelyek „RESTREINT UE/EU RESTRICTED" minősítésű adatokhoz való hozzáférést igényelnek, a nemzeti jogszabályok és rendeletek értelmében az FSC-vel és a PSC-vel kapcsolatban esetleg meglévő bármely követelmény sérelme nélkül.

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

38. Amennyiben egy adott szerződés „RESTREINT UE/EU RESTRICTED" minősítésű adatok vállalkozó által működtetett kommunikációs és információs rendszerekben való kezelésére is kiterjed, az Európai Parlament mint szerződő hatóság biztosítja, hogy a szerződésben vagy alvállalkozói szerződésben a kommunikációs és információs rendszerek akkreditálásának tekintetében meghatározzák a szükséges technikai és igazgatási követelményeket, melyek arányban állnak a valamennyi vonatkozó tényező figyelembevételével megállapított kockázattal. Az ilyen kommunikációs és információs rendszerek akkreditálásának hatáskörét illetően a szerződő hatóságnak és az érintett nemzeti vagy kijelölt biztonsági hatóságnak kell megállapodnia.

6. BIZTONSÁGI KÖZLEMÉNY

A BIZTONSÁGI SZABÁLYOK MEGSÉRTÉSE, BIZALMAS ADATOK ELVESZTÉSE VAGY ILLETÉKTELEN TUDOMÁSÁRA JUTÁSA

1. A biztonság megsértése az e határozatban foglalt biztonsági szabályokkal ellentétes cselekedet vagy mulasztás eredményeként következik be.

2. Bizalmas adat illetéktelen tudomására jutásáról van szó abban az esetben, ha a bizalmas adat részben vagy egészben arra fel nem hatalmazott, vagyis megfelelő biztonsági tanúsítvánnyal vagy a szükséges ismerettel nem rendelkező személyek kezébe kerül, illetve amennyiben feltételezhető, hogy ez megtörtént.

3. Bizalmas adat illetéktelenek tudomására juthat gondatlanság, hanyagság vagy indiszkrét magatartás miatt, valamint az Unióval szemben fellépő szolgálatok vagy felforgató szervezetek tevékenysége következtében.

4. Amennyiben a főtitkár megállapítja vagy megtudja, hogy sérültek a biztonsági szabályok, bizalmas adatok illetéktelenek tudomására jutottak vagy elvesztek, illetve ha felmerül a gyanú, hogy ilyen események történtek:

a) megállapítja a tényeket;

b) értékeli és minimalizálja a károkat;

c) intézkedéseket hoz az ilyen esetek újbóli előfordulásának megelőzése érdekében;

d) értesíti a bizalmas adatot rendelkezésre bocsátó harmadik fél vagy tagállam illetékes hatóságát.

Amennyiben az ügy európai parlamenti képviselőt érint, a Parlament főtitkára a Parlament elnökével együtt jár el.

Amennyiben az adatot más uniós intézmény bocsátotta rendelkezésre, a főtitkár a minősített adatokra vonatkozó megfelelő biztonsági intézkedésekkel, valamint a Bizottsággal kötött keretmegállapodás és a Tanáccsal kötött intézményközi megállapodás útján rögzített előírásoknak megfelelően jár el.

5. A bizalmas adatok kezelésével megbízott valamennyi személyt alaposan tájékoztatni kell a biztonsági eljárásokról, az indiszkrét magatartás és a médiával ápolt kapcsolatok veszélyeiről, valamint szükség esetén valamennyi ilyen személynek nyilatkozatot kell aláírnia arról, hogy nem hozza harmadik személyek tudomására a bizalmas adatok tartalmát, eleget tesz a minősített adatok védelmével kapcsolatos kötelezettségeinek, és tudatában van a vonatkozó előírások megsértéséből eredő következményeknek. A biztonsági szabályok megsértésének minősül minden olyan eset, amikor megfelelő tájékoztatásban nem részesült és az említett nyilatkozatot korábban alá nem író személy ismer meg vagy használ fel minősített adatot.

6. Az Európai Parlament képviselői, tisztviselői és a képviselőcsoportoknak vagy szerződő feleknek dolgozó egyéb alkalmazottai azonnal kötelesek értesíteni a főtitkárt abban az esetben, ha tudomásukra jut, hogy sérültek a biztonsági szabályok, illetve ha bizalmas adat veszett el vagy jutott illetéktelen tudomására.

7. A bizalmas adatot illetéktelenek tudomására hozó személyek ellen fegyelmi eljárást kell indítani a vonatkozó szabályoknak és előírásoknak megfelelően. A fegyelmi eljárás nem zárja ki az alkalmazandó jog szerinti esetleges jogi lépéseket.

8. A Parlament tisztviselői és a képviselőcsoportoknak dolgozó egyéb alkalmazottak által elkövetett szabálysértések a személyzeti szabályzat IV. címében foglalt eljárások és szankciók alkalmazását vonják maga után, ám ezek nem zárják ki a további jogi lépéseket.

9. A biztonsági szabályok európai parlamenti képviselők által elkövetett megsértése esetén az eljárási szabályzat 9. cikkének (2) bekezdése, valamint 152., 153. és 154. cikke szerint kell eljárni, fenntartva a jogot további jogi lépések megtételére.