

IV

(Tájékoztatások)

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

EURÓPAI PARLAMENT

AZ EURÓPAI PARLAMENT ELNÖKSÉGÉNEK HATÁROZATA

(2011. június 6.)

a bizalmas információk Európai Parlament általi kezelésére vonatkozó szabályokról

(2011/C 190/02)

AZ EURÓPAI PARLAMENT ELNÖKSÉGE,

egyeztethetőségét a Szerződések által vagy alapján létrehozott többi intézmény, szerv, hivatal és ügynökség, illetve a tagállamok által elfogadott szabályokkal.

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

mivel:

(4) E határozat rendelkezései nem érintik az Európai Unió működéséről szóló szerződés (EUMSZ) 15. cikkét és az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet ⁽²⁾.

(1) Az Európai Parlament és az Európai Bizottság közötti kapcsolatokról szóló, 2010. október 20-án aláírt keretmegállapodásra ⁽¹⁾ (keretmegállapodás) tekintettel szükséges a bizalmas dokumentumok adminisztratív feldolgozására vonatkozó szabályokról szóló, 2006. november 13-i elnökségi határozat felülvizsgálata.

(5) E határozat rendelkezései nem érintik az EUMSZ 16. cikkét és a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletet ⁽³⁾,

(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 információk Európai Parlament általi kezelésére vonatkozó megfelelő eljárások meghatározására.

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Cél

(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 össze-

Ez a határozat a bizalmas információk Európai Parlament általi létrehozását, fogadását, továbbítását és tárolását szabályozza az információk bizalmas jellegüknek megfelelő védelme céljából. A határozat különösen a keretmegállapodás 2. mellékletének végrehajtását szolgálja.

⁽¹⁾ HL L 304., 2010.11.20., 47. o.

⁽²⁾ HL L 145., 2001.5.31., 43. o.

⁽³⁾ HL L 8., 2001.1.12., 1. o.

2. cikk

Fogalommeghatározások

E határozat alkalmazásában:

- a) „információ”: minden szóban vagy írásban tett tájékoztatás, adathordozótól és megfogalmazótól függetlenül;
- b) „bizalmas információ”: az „EU-minősített adat” és a nem minősített „egyéb bizalmas információ”;
- c) „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 Európai Uniónak, illetve egy vagy több tagállamának az érdekeit, függetlenül attól, hogy az ilyen információ a szerződések által vagy alapján létrehozott intézményeken, szerveken, hivatalokon és ügynökségeken belül keletkezett, vagy a tagállamoktól, harmadik államoktól vagy nemzetközi szervezetektől származik. 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;

- d) „egyéb bizalmas információ”: 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 információ, beleértve az adatvédelmi szabályok vagy a szakmai titoktartási kötelezettség hatálya alá tartozó információkat is;

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

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

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

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

- i) „visszaminősítés”: a minősítési szint leszállítása;

- j) „minősítés megszüntetése”: mindenféle minősítés megszüntetése;

- k) „kibocsátó”: az EU-minősített adat vagy egyéb bizalmas információ megfelelő felhatalmazással rendelkező szerzője;

- l) „biztonsági közlemény”: a II. mellékletben ⁽¹⁾ foglaltak szerinti technikai jellegű végrehajtási intézkedések.

3. cikk

Alapelvek és minimumszabályok

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

- (2) Az Európai Parlament ezekkel az alapelvekkel és minimumszabályokkal összhangban információbiztonsági irányítórendszert (ISMS) hoz létre, amelynek célja a parlamenti és adminisztrációs munka megkönnyítése, egyúttal biztosítva az Európai Parlament által feldolgozott valamennyi bizalmas információ védelmét és teljes mértékben tiszteletben tartva az ezen információ kibocsátója által meghatározott és a biztonsági közleményben lefektetett szabályokat.

A bizalmas információknak az Európai Parlament automatizált informatikai rendszerével történő feldolgozása az információvédelmi koncepciónak megfelelően történik, és le van fektetve a biztonsági közleményekben.

⁽¹⁾ Később elfogadandó melléklet.

(3) Az Európai Parlament képviselői a CONFIDENTIEL UE/EU CONFIDENTIAL szintig (ezt a szintet is beleértve) biztonsági tanúsítvány nélkül betekintheznek a minősített információkba. A CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű információk tekintetében nyilatkozatot kell aláírniuk arról, hogy az információ tartalmát nem adják át harmadik személyeknek. A CONFIDENTIEL UE/EU CONFIDENTIAL szint feletti minősítésű információkhoz csak a megfelelő szintű biztonsági tanúsítvánnyal rendelkező képviselők számára adható hozzáférés.

(4) Az Európai Parlament tisztviselői és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak bizalmas információkba akkor tekinthetnek be, ha a „szükséges ismeret” esetükben igazolt, a RESTREINT UE/EU RESTRICTED szint feletti minősítésű információkba pedig csak akkor, ha megfelelő szintű biztonsági tanúsítvánnyal rendelkeznek.

4. cikk

Bizalmas információ létrehozása és adminisztratív kezelés az Európai Parlament által

(1) Bizalmas információ kibocsátására és/vagy információ 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 információ létrehozásakor a kibocsátó – az ezen elnökségi határozat I. mellékletében foglalt nemzetközi szabályokkal és fogalommeghatározásokkal összhangban – a megfelelő minősítési szintet alkalmazza. A kibocsátó általános szabályként ezenkívül meghatározza az információ megtekintésére a minősítési szintnek megfelelően felhatalmazandó címzeteket. Erről a dokumentumnak a bizalmas információk kezeléséért felelős szolgálatnál való elhelyezésekor tájékoztatni kell a bizalmas információk kezeléséért felelős szolgálatot.

(3) A szakmai titoktartás alá tartozó bizalmas információ kezelése során a biztonsági közleményben meghatározott kezelési utasításoknak megfelelően kell eljárni.

5. cikk

Bizalmas információ Európai Parlament általi fogadása

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

— a RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatot és az egyéb bizalmas információt a továbbítás iránti kérelmet benyújtó parlamenti szerv/tisztségviselő titkárságára,

— a CONFIDENTIEL UE/EU CONFIDENTIAL vagy a fölötti minősítésű EU-minősített adatot a bizalmas információk kezeléséért felelős szolgálatnak.

(2) A bizalmas információk nyilvántartását, tárolását és nyomon követhetőségét vagy az információt megkapó parlamenti szerv/tisztségviselő titkársága, vagy a bizalmas információk kezeléséért felelős szolgálat biztosítja.

(3) A Bizottság által a keretmegállapodás alapján továbbított bizalmas információ esetében a keretmegállapodás 2. melléklete 3.2. pontjának megfelelő, az információ bizalmas jellegének megőrzésére irányuló, megállapodás szerinti intézkedéseket (amelyeket közös megegyezéssel határoztak meg és amelyek a címzettekéről, a biztonságos olvasóteremben és zárt ülésen történő betekintéssel kapcsolatos eljárásról vagy egyebekről szólnak) a bizalmas információval együtt az adott parlamenti szerv/tisztségviselő titkárságán vagy a bizalmas információk kezeléséért felelős szolgálatnál kell elhelyezni, amennyiben az információ CONFIDENTIEL UE/EU CONFIDENTIAL vagy e fölötti minősítésű.

(4) A 3. bekezdésben említett intézkedések értelemszerűen alkalmazhatók a bizalmas információk 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 minősítésű EU-minősített adatokat az Európai Parlament számára kell továbbítani az információ iránti kérelmet benyújtó parlamenti szerv/tisztségviselő és az átadó uniós intézmény vagy tagállam által megállapodással meghatározandó további intézkedéseknek megfelelően. Az Elnökök Értekezlete felügyeleti bizottságot hoz létre. E bizottság feladata a minősítésnek megfelelő szintű védelem biztosítása.

6. cikk

Az EU-minősített adat Európai Parlament általi továbbítása harmadik feleknek

Az Európai Parlament azzal a feltétellel továbbíthat – a kibocsátó hozzájárulása esetén – EU-minősített adatot a Szerződések által vagy alapján létrehozott többi intézménynek, szervnek, hivatalnak és ügynökségnek, illetve a tagállamoknak, ha ezek gondoskodnak arról, hogy az EU-minősített adatok kezelése során a szolgálataikon és épületeiken belül az e határozatban meghatározott szabályokkal egyenértékű szabályok érvényesülnek.

7. cikk

A bizalmas információ tárolása és megtekintése biztosított helyszíneken (biztonságos olvasótermek)

(1) A biztonságos olvasótermek biztosítják a biztonságos tárolást, és nem tartalmaznak fénymásolót, telefont, faxot, szkennert, vagy bármely más, dokumentumok másolására vagy továbbítására alkalmas műszaki berendezést.

(2) A biztonságos olvasóterembe való belépés feltételei:

a) csak a következő személyek léphetnek be:

- a 4. cikk (2) bekezdésében vagy az 5. cikk (3) és (4) bekezdésében említett intézkedésekkel összhangban megfelelően azonosított európai parlamenti képviselők, európai parlamenti tisztviselők és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottak,
- az Európai Parlamentnek a bizalmas információk kezeléséért felelős szolgálat irányításáért felelős tisztviselői,
- szükség szerint az Európai Parlamentnek a biztonságért és tűzvédelemért felelős tisztviselői.

A biztosított helyszínek takarítására csak egy a bizalmas információk kezeléséért felelős szolgálatnál dolgozó tisztviselő jelenlétében és szoros felügyelete mellett kerülhet sor;

b) a bizalmas információhoz hozzáférni kívánó személy előzetesen közli a bizalmas információk kezeléséért felelős szolgálattal a nevét. A bizalmas információk kezeléséért felelős szolgálat ellenőrzi minden egyes olyan személy személyazonosságát, aki bizalmas információ megtekintését kérvényezi, és adott esetben meggyőződik arról, hogy az adott személy rendelkezik-e a szükséges szintű biztonsági tanúsítvánnyal, valamint hogy a 4. cikk (2) bekezdésében vagy az 5. cikk (3) és (4) bekezdésében említett intézkedésekkel összhangban rendelkezik-e az információ megtekintésére felhatalmazással;

c) a bizalmas információk kezeléséért felelős szolgálat megtagadhatja a terembe való belépést minden olyan személy esetében, aki az a) és b) pont értelmében nem jogosult a belépésre. A bizalmas információk kezeléséért felelős szolgálat döntése elleni fellebbezést az Európai Parlament képviselői esetén az elnöknek, más személyek esetében a főtitkárnak kell benyújtani.

(3) A bizalmas információk biztonságos olvasóteremben való megtekintésének feltételei:

a) az információ megtekintésére jogosult és a 2. bekezdés b) pontjában említett kérelmet benyújtó személyeknek személyesen kell megjelenniük a bizalmas információk kezeléséért felelős szolgálatnál.

Kivételes körülményektől (például ha rövid időn belül számos betekintési kérelmet nyújtanak be) eltekintve egyszerre csak egy személy számára engedélyezhető a bizalmas információ biztonságos olvasóteremben való, a bizalmas információk kezeléséért felelős szolgálat egy tisztviselője jelenlétében történő megtekintése.

Ez a tisztviselő tájékoztatja a betekintésre ekként jogosult személyt kötelezettségeiről, és aláírta vele egy nyilatkozatot,

amelyben a betekintő kötelezettséget vállal arra, hogy az információ tartalmát nem adja tovább harmadik személynek;

b) a megtekintés ideje alatt nem engedélyezett a külvilággal való kapcsolat (beleértve telefon vagy egyéb technológia használatát is), a jegyzetkészítés és a megtekintett bizalmas információ fénymásolása vagy fényképezése;

c) mielőtt a betekintő személy engedélyt kapna a biztonságos olvasóterem elhagyására, a bizalmas információk kezeléséért felelős szolgálat a) pontban említett tisztviselője ellenőrzi a megtekintett bizalmas információ/információk meglétét, sértetlenségét és teljességét.

(4) A fenti szabályok megsértése esetén a bizalmas információk kezeléséért felelős szolgálat illetékes tisztviselője tájékoztatja a főtitkárt, aki az ügyet az elnök elé terjeszti, amennyiben a szabályokat az Európai Parlament egy képviselője szegi meg.

8. cikk

A bizalmas információ más módon való megtekintésére vonatkozó minimumszabályok

(1) A bizalmas információk zárt ülésen történő adminisztratív feldolgozása tekintetében az ülést felelős parlamenti szerv/tisztviselő titkársága köteles gondoskodni az alábbiakról:

— csak az ülésen való részvételre kijelölt és a szükséges szintű biztonsági tanúsítvánnyal rendelkező személyek léphetnek be az ülésterembe,

— valamennyi dokumentumot besorszámozzák, az ülés kezdetén kiosztják és az ülés végén újra beszedik őket, továbbá ezekről a dokumentumokról jegyzetek, fénymások és fényképek nem készülhetnek,

— az ülés jegyzőkönyve nem tehet említést a bizalmas eljárás alá tartozó információ megvitatásának tartalmáról,

— az Európai Parlamenten belüli címzettekkel szóban közölt bizalmas információkra az írásbeli bizalmas információkkal azonos szintű védelem vonatkozik. Ebbe beletartozhat egy olyan nyilatkozat az információ címzettjei részéről, hogy az információ tartalmát nem hozzák harmadik személy tudomására.

(2) A bizalmas információk parlamenti szerv/tisztviselő titkársága általi, zárt ülésen kívüli adminisztratív feldolgozására az alábbi szabályok vonatkoznak:

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

- ezeket a dokumentumokat tényleges használatuk idején kívül zárt helyen kell őrizni, a titkárság felelőssége mellett,
- a bizalmas információk zárt ülésen történő, az első bekezdésben szabályozott adminisztratív feldolgozásának sérelme nélkül a dokumentumok semmilyen esetben nem sokszorozhatók, nem menthetők másik adathordozóra, és nem továbbíthatók senkinek,
- az ilyen dokumentumokhoz való hozzáférés a címzettekre korlátozódik, és a 4. cikk (2) bekezdésében vagy az 5. cikk (3) vagy (4) bekezdésében említett intézkedéseknek megfelelően, a titkárság felügyelete alatt történik,
- a titkárság nyilvántartást vezet a dokumentumokat megtekinthető személyekről, valamint a megtekintés napjáról és időpontjáról. Ezt a nyilvántartást a 12. cikkben említett éves jelentés elkészítésére tekintettel továbbítani kell a bizalmas információk kezeléséért felelős szolgálatnak.

9. cikk

A bizalmas információ archiválása

- (1) Gondoskodni kell biztonságos archiválási rendszer rendelkezésre állásáról az Európai Parlament épületeiben.

A bizalmas információk kezeléséért felelős szolgálatnál vagy a parlamenti szerv/tisztségviselő titkárságánál véglegesen elhelyezett bizalmas információkat hat hónappal az utolsó megtekintésük után, de legkésőbb elhelyezésük után egy évvel át kell helyezni a bizalmas információk kezeléséért felelős szolgálatnál található biztonságos irattárba.

- (2) A biztonságos irattár kezelése a szabványos archiválási kritériumoknak megfelelően a bizalmas információk kezeléséért felelős szolgálat feladata.

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

- csak a bizalmas információ elhelyezésekor kitöltött kísérő-lapon szereplő, név vagy tisztség szerint azonosított személyek kaphatnak engedélyt az adott információ megtekintésére,
- a bizalmas információ megtekintése iránti kérelmet a bizalmas információk kezeléséért felelős szolgálatnak kell benyújtani, majd a bizalmas információk kezeléséért felelős szolgálat biztosítja az adott dokumentum átszállítását a biztonságos olvasóterembe,
- a 7. cikkben megállapított, a bizalmas információk megtekintésére vonatkozó eljárások és feltételek alkalmazandók.

10. cikk

Az EU-minősített adat visszaminősítése és minősítésének megszüntetése

- (1) EU-minősített adatot csak a kibocsátó engedélyével lehet visszaminősíteni, vagy azok minősítését megszüntetni, szükség

esetén az egyéb érdekelt felekkel történt egyeztetés után. A visszaminősítést, illetve a minősítés megszüntetését írásban kell megerősíteni. A kibocsátó feladata tájékoztatni a címzeteket a változásról, akiknek viszont azokat a további címzettek 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 öt évente felül kell vizsgálniuk annak megállapítása érdekében, hogy az eredeti minősítés továbbra is szükséges-e.

- (2) A biztonságos irattárban tárolt dokumentumok minősítésének megszüntetésére 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 legkésőbb 30 év után kerül sor. A minősítés megszüntetését a minősített információ kibocsátója vagy az adott időben illetékes szolgálat hajtja végre az I. melléklet 1. részének 10. szakaszával összhangban.

11. cikk

Az információ bizalmas jellegének megsértése

- (1) Általában az információ 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 maguk után.

- (2) A személyzet által elkövetett szabálysértések a 259/68/EGK, Euratom, ESZAK rendeletben⁽²⁾ meghatározott, az Európai Unió tisztviselőinek személyzeti szabályzatában és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben (személyzeti szabályzat) foglalt eljárások és szankciók alkalmazását vonják maguk után.

- (3) A szükséges vizsgálatokat az elnök és a főtitkár szervezi meg.

12. 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 éves jelentést nyújt be az Elnökségnek e határozat alkalmazásáról.

⁽¹⁾ HL L 43., 1983.2.15., 1. o.

⁽²⁾ HL L 56., 1968.3.4., 1. o.

13. cikk

Átmeneti és záró rendelkezések

(1) Az e határozat alkalmazását megelőzően a bizalmas információk kezeléséért felelős szolgálatnál vagy az irattárakban meglévő bizalmas információk RESTREINT UE/EU RESTRICTED minősítésűnek tekintendők, kivéve, ha azok kibocsátója e határozat hatálybalépésétől számított egy éven belül a minősítés mellőzése vagy magasabb minősítési kategóriába sorolás vagy jelöléssel való ellátás mellett dönt.

(2) Ha az ilyen bizalmas információ kibocsátója magasabb minősítési kategóriába sorolás mellett dönt, azt a kibocsátónak vagy megbízottjainak a lehető legalacsonyabb szintű minősítéssel kell ellátnia, a bizalmas információk kezeléséért felelős szolgálattal konzultálva és az I. mellékletben meghatározott kritériumokkal összhangban.

(3) Az Elnökség 2006. november 13-i, a bizalmas dokumentumok adminisztratív feldolgozására vonatkozó szabályokról szóló határozata hatályát veszti.

(4) Az Elnökség 2005. október 24-i határozata, amelyben megbízza a főtitkárt, hogy állítson fel a dokumentumok minősítésének megszüntetésével foglalkozó bizottságot, és fogadjon el határozatokat a dokumentumok minősítésének megszüntetésére vonatkozóan, hatályát veszti.

14. cikk

Hatálybalépés

(1) Ez a határozat az Európai Unió Hivatalos Lapjában való kihirdetése napján lép hatályba.

(2) A határozat 2011. július 1-jétől alkalmazandó.

I. MELLÉKLET

1. RÉSZ

A BIZALMAS INFORMÁCIÓK VÉDELMERE VONATKOZÓ ALAPELVEK ÉS BIZTONSÁGI MINIMUMSZABÁLYOK**1. Bevezetés**

Ezek a rendelkezések állapítják meg azokat az alapelveket és biztonsági minimumszabályokat, amelyeket az Európai Parlamentnek valamennyi munkahelyén, valamint az EU-minősített adatok és egyéb minősített információk valamennyi címzettjének be kell tartania a biztonság fenntartása és annak érdekében, hogy minden érintett személy biztos lehessen afelől, hogy a védelem közös szintje megvalósul. Ezeket a bizalmas információk parlamenti bizottságok, valamint egyéb parlamenti szervek és tisztségviselők általi kezelésére vonatkozó szabályok egészítik ki.

2. Általános elvek

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, valamint a szubszidiaritást és az arányosságot foglalják magukban.

A törvényesség elve annak szükségességét jelenti, hogy a biztonsági feladatok ellátása során szigorúan a törvényes keretek között kell maradni, és meg kell felelni a vonatkozó jogi követelményeknek. Azt is jelenti, hogy 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. A törvényesség végezetül azt jelenti, hogy a biztonságnak az Európai Parlament felelősségi körén belül történő megsértésével úgy kell foglalkozni, hogy az megfeleljen az Európai Parlament fegyelmi intézkedésekkel kapcsolatos politikájának.

Az átláthatóság elve 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. Az átláthatóság azt is jelenti, hogy a biztonsági intézkedések végrehajtásához világos írásos iránymutatásokra van szükség.

Az elszámoltathatóság elve azt jelenti, hogy a biztonság területén a hatásköröket világosan meghatározzák. Emellett azt is jelenti, hogy rendszeresen figyelemmel kell kísérni, hogy ezeket a hatásköröket megfelelően hajtották-e végre.

A szubszidiaritás elve 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, és hogy a biztonsági intézkedéseknek arányosnak 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) Az Európai Parlamenten belül egy INFOSEC (információbiztonság) védelmi szolgálat, amelynek hatáskörébe tartozik, hogy az érintett biztonsági hatósággal együttműködve tájékoztasson, és tanácsot adjon a biztonságot fenyegető technikai veszélyekről és a velük szemben alkalmazandó védelmi intézkedésekről.
- b) 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) az EU-minősített adatok és egyéb bizalmas információk védelme a kémkedés, az illetéktelenek tudomására jutás vagy az engedély nélküli kiszolgáltatás ellen;

- b) a kommunikációs és információs rendszerekben és hálózatokban kezelt EU-minősített adatok védelme a bizalmas jellegüket, integritásukat és rendelkezésre állásukat fenyegető veszélyekkel szemben;
- c) az EU-minősített adatoknak helyet adó európai parlamenti helyiségek védelme a szabotázzsal és a szándékos 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 körütekintés 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 érzékenységeinek. 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 fenyegető veszélyek elleni intézkedések megtervezése és megszervezése során, hogy az EU-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. Ha különböző információk kerülnek egy anyagba, akkor az egész anyag tekintetében alkalmazandó minősítési szintnek legalább olyan magasnak kell lennie, mint a legmagasabb minősítésű elem 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 EU-minősített adatokhoz férnek hozzá, az EU-minősített adatokat hordozó eszközökre és egyéb bizalmas információra, valamint az ilyen információknak és fontos berendezéseknek helyet adó valamennyi helyiségre;
- b) ki kell tudniuk szűrni azokat a személyeket, akiknek a helyzete veszélyeztetheti az ilyen információk és az ilyen információknak 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 összes – akár minősített, akár nem minősített, és különösen az elektromágneses formában tárolt, feldolgozott vagy továbbított – bizalmas információ integritását (vagyis meg kell akadályozniuk 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 az EU-minősített adatok valamennyi, mind az intézményen belüli, mind annak hatáskörébe tartozó címzettje – azaz az összes szolgálata és szerződéses megbízottja – betartsa, hogy az ilyen információkat 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 információkhoz való hozzáférést külső szervek számára csak azzal a feltétellel engedélyezi, ha azok biztosítják, hogy azok 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, akiket olyan beosztásban dolgoznak, amelyben EU-minősített adatokhoz férhetnek hozzá, hivatalba lépésükkor, majd rendszeres időközönként valamennyien alapos oktatásban részesülnek a biztonság szükségessége és az ezek megvalósítására irányuló eljárások tekintetében. E személyek számára előírás, hogy írásban igazolják, hogy az alkalmazandó biztonsági rendelkezéseket elolvasták, és teljes mértékben megértették.

6.2. A vezetők felelőssége

A vezetők kötelezettsége, hogy ismerjék a minősített információkkal dolgozó vagy a biztonságos kommunikációs vagy információs rendszerekhez hozzáféréssel rendelkező beosztottjaikat, továbbá hogy feljegyezzék és jelentsek 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 státusa

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 kerül-e minősített információkkal, vagy rendelkezik-e hozzáféréssel biztonságos kommunikációs vagy információs rendszerekhez, és hogy erről tájékoztassák az Európai Parlament illetékes szolgálatát. Ha azt állapítják meg, 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 az EU-minősített adatokhoz való illetéktelen hozzáférés megakadályozását célzó fizikai és technikai védelmi intézkedések alkalmazását jelenti

7.1. A védelem szükségessége

Az EU-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. Az EU-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

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

7.3. Az épületek biztonsága

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

Az EU-minősített adatok számára nyújtott védelem természete – például ablakrácsok, ajtózárok, őrkök a bejáratnál, automatikus hozzáférés-ellenőrző rendszerek, biztonsági ellenőrzések és őrkutatok, riasztórendszerek, behatolás-jelző 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 tervekkel kell kidolgozni a minősített információk védelmére vészhelyzet esetében.

8. Biztonsági azonosítók, jelölések, feltüntetés és a minősítés szabályai

8.1. Biztonsági azonosítók

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

Egyezményes biztonsági azonosító használható a minősítés érvényességi idejének behatárolására (azaz a minősített információk automatikus visszaminősítése vagy a minősítésük automatikus megszüntetése időpontjának meghatározására). Ez az azonosító a „(dátum/időpont) ... -IG” vagy az „(esemény) ... -IG” lehet.

Olyan kiegészítő biztonsági azonosítók, mint a CRYPTO vagy egyéb, az EU által elismert biztonsági azonosító akkor alkalmazandó, ha a biztonsági minősítés által meghatározott kezelés mellett korlátozott elosztásra és különleges kezelésre van szükség.

Biztonsági azonosítókat csak minősítéssel együtt lehet használni.

8.2. Jelölések

Jelölést lehet használni egy adott dokumentum által érintett terület vagy egy adott, a „szükséges ismeret” elve alapján történő elosztás meghatározására, illetve (nem minősített információk esetében) a tilalom végének jelzése.

A jelölés nem minősítés, ezért helyette nem használható.

8.3. A minősítések és a biztonsági azonosítók feltüntetése

A minősítéseket a következők szerint tüntetik fel:

- a) a RESTREINT UE/EU RESTRICTED minősítésű dokumentumokon mechanikus vagy elektronikus eszközökkel;
- b) a CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű dokumentumokon mechanikus eszközökkel vagy kézzel vagy előre lebélyegzett, regisztrált papíron nyomtatással;
- c) a SECRET UE/EU SECRET és a TRÈS SECRET UE/EU TOP SECRET minősítésű dokumentumokon mechanikus eszközökkel vagy kézzel.

A biztonsági azonosítókat közvetlenül a minősítés alatt tüntetik fel ugyanazokkal az eszközökkel, mint amelyeket a minősítések feltüntetéséhez használnak.

8.4. A minősítés szabályai

8.4.1. Általános követelmények

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

Az információ 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 információk 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 minősítésű dokumentumok kibocsátására felhatalmazott személyek számát a lehető legkisebbre kell korlátozni, és nevükről listát kell vezetni, amelyet a bizalmas információk kezeléséért felelős szolgálat állít össze.

8.4.2. Minősítések alkalmazása

Egy dokumentum minősítését az határozza meg, hogy tartalma a 2. cikk c) pontjában foglalt fogalommeghatározásoknak megfelelően mennyire érzékeny. Fontos, hogy a minősítést szabályosan és csak akkor használják, ha valóban szükséges, különösen a TRÈS SECRET UE/EU TOP SECRET minősítés esetében.

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.

A minősítendő dokumentum kibocsátójának szem előtt kell tartania a fenti szabályokat, és el kell kerülnie mind a felülminősítés, mind az alulminősítés irányába történő elmozdulást.

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 Biztonságért Felelős Igazgatósága – amelyet a feladat elvégzésében a bizalmas információk kezeléséért felelős szolgálat segíthet – rendszeres időközönként ellenőrzi az EU-minősített adatok védelmét szolgáló biztonsági intézkedéseket.

Az Európai Parlament Biztonságért Felelős Igazgatósága és az EU-minősített adatokat birtokló, a Szerződések által vagy alapján létrehozott többi intézmény, szerv, hivatal és ügynökség biztonsági szolgálatai szintén megállapodhatnak az EU-minősített adatok védelmét szolgáló biztonsági intézkedések szakértői értékelésének elvégzésében.

10. A minősítés megszüntetésére irányuló eljárás

- 10.1. A bizalmas információk kezeléséért felelős szolgálat megvizsgálja az EU-minősített adatokat, és javaslatot tesz a dokumentum kibocsátójának a minősítés megszüntetésére, legkésőbb a dokumentum létrehozását követő 25. évben. Azokat a dokumentumokat, amelyek minősítését az első vizsgálatkor nem szüntetik meg, rendszeresen, de legalább ötvenként felül kell vizsgálni.
- 10.2. A ténylegesen a biztonságos irattárban lévő és megfelelően minősített dokumentumokon kívül a minősítés megszüntetésére irányuló eljárás a biztonságos irattárban vagy az Európai Parlament Irattár és Dokumentációs Központjában (CARDOC) lévő egyéb bizalmas információkra is kiterjedhet.
- 10.3. A bizalmas információk kezeléséért felelős szolgálat feladata, hogy a kibocsátó nevében tájékoztassa a dokumentumok címzettjeit a minősítés 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 jelzésekre.
- 10.5. 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 bizalmas információk kezeléséért felelős szolgálatra való hivatkozást.
- 10.6. A dokumentum szövegét, amelynek a minősítését megszüntették, hozzá kell csatolni ahhoz az elektronikus mappához vagy az ezzel egyenértékű rendszerhez, amelyben azt regisztrálták.
- 10.7. A magánszférára és az egyén sérthetlenségére 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 bizalmas információk kezeléséért felelős szolgálat a minősítés megszüntetése előtt konzultál az érintett harmadik féllel. A harmadik félnek 8 hét áll rendelkezésére megjegyzései benyújtására;
- b) a magánszférára és az egyén sérthetetlenségére vonatkozó kivétel tekintetében a minősítés megszüntetésekor figyelembe veszik különösen az érintett személy hozzájárulását, az érintett személy felismerhetetlenségét, és/vagy a tényt, hogy az érintett személy már nem él;
- 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. Az Európai Parlament előjogaira és hatásköreire tekintettel a képviselői biztonsági tanúsítvány nélkül kaphatnak hozzáférést az EU-minősített adatokhoz a CONFIDENTIEL UE/EU CONFIDENTIAL szintig (ezt a szintet is beleértve). A CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű információkhoz való hozzáféréshez nyilatkozat aláírására van szükség, amelyben kötelezettséget vállalnak arra, hogy az információ tartalmát harmadik fél előtt nem fedik fel.
- 11.2. Ahhoz, hogy az Európai Parlament képviselői hozzáférhessenek a TRÈS SECRET UE/EU TOP SECRET vagy SECRET UE/EU SECRET minősítésű információkhoz, a 11.3 és 11.4 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 a felhatalmazást, hogy megkapta a tagállamok illetékes nemzeti hatóságainak véleményét a 11.8–11.13 pontban említett eljárásnak megfelelően lefolytatott biztonsági ellenőrzés alapján.
- 11.5. Az Európai Parlament Biztonságért Felelős 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 öt éves 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 arra megfelelő oka van. A felhatalmazás visszavonásáról szóló határozatról értesíteni kell az Európai Parlament érintett képviselőjét, aki még a visszavonás hatályba 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 hatóságokhoz intézett megkeresésében meghatározza az Európai Parlament érintett képviselője rendelkezésére bocsátandó minősített információk szintjét, hogy az ellenőrzési eljárást lefolytathassák.

- 11.11. Az illetékes nemzeti hatóságok 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 a tagállam illetékes nemzeti hatóságai kedvező véleményt adnak, az elnök megadhatja a felhatalmazást az Európai Parlament érintett képviselőjének.
- 11.13. Az illetékes nemzeti hatóságok elutasító véleményéről értesítik 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 hatóságok 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 információk védelmével és a védelem biztosításának módjával kapcsolatosan. Ezen képviselőknek nyilatkozatot kell aláírniuk, amelyben igazolják, hogy ezeket az utasításokat megkapták.
- 11.15. Kivételes esetben az elnök, miután az illetékes nemzeti hatóságokat értesítette, és azok erre egy hónapon belül nem reagáltak, 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 minősítésű információkhoz.
- 12. Az Európai Parlament tisztviselőire és a képviselőcsoportok alkalmazásában álló egyéb parlamenti alkalmazottakra vonatkozó biztonsági ellenőrzési eljárás**
- 12.1. A minősített információkhoz 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 a 12.1 pontban említett személyek hozzáférhessenek a TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, valamint a CONFIDENTIEL UE/EU CONFIDENTIAL minősítésű információkhoz, 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 a felhatalmazást, hogy megkapta a tagállamok illetékes nemzeti hatóságainak véleményét a 12.8–12.13 pontban említett eljárásnak megfelelően lefolytatott biztonsági ellenőrzés alapján.
- 12.5. Az Európai Parlament Biztonságért Felelős Igazgatósága naprakész listát vezet az Európai Parlament megfelelő szolgálatait 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 öt éves 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. A főtitkár visszavonja a felhatalmazást, ha úgy ítéli meg, hogy arra 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 érintett személy 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 vagy efölötti minősítésű információkhoz.

- 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 hatóságokhoz intézett megkeresésében meghatározza az érintett személy rendelkezésre bocsátandó minősített információk szintjét, hogy az ellenőrzési eljárást lefolytathassák, és véleményt adhassanak arról, milyen szintű felhatalmazást lenne helyénvaló adni az adott személynek.
- 12.11. Az illetékes nemzeti hatóságok 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 a tagállam illetékes nemzeti hatóságai kedvező véleményt adnak, a főtitkár megadhatja a felhatalmazást az érintett személynek.
- 12.13. Az illetékes nemzeti hatóságok elutasító véleményéről értesítik 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 hatóságok megerősítik, 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 információk védelmével és a védelem biztosításának módjával kapcsolatosan. Ezen tisztviselőknak és alkalmazottnak nyilatkozatot kell aláírniuk, amelyben igazolják, hogy ezeket az utasításokat megkapták, és vállalják azok betartását.
- 12.15. Kivételes esetben a főtitkár, miután az illetékes nemzeti hatóságokat értesítette, és azok erre egy hónapon belül nem reagáltak, 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 minősítésű információkhoz.
-