A BIZOTTSÁG (EU, Euratom) 2021/259 HATÁROZATA

(2021. február 10.)

a minősített támogatásokkal kapcsolatos, az iparbiztonságra vonatkozó végrehajtási szabályok megállapításáról

AZ EURÓPAI BIZOTTSÁG,

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

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

tekintettel az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról, az 1296/2013/EU, az 1301/2013/EU, az 1303/2013/EU, az 1304/2013/EU, az 1309/2013/EU, az 1316/2013/EU, a 223/2014/EU és a 283/2014/EU rendelet és az 541/2014/EU határozat módosításáról, valamint a 966/2012/EU, Euratom rendelet hatályon kívül helyezéséről szóló, 2018. július 18-i (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendeletre ([1]),

tekintettel a Bizottságon belüli biztonságról szóló, 2015. március 13-i (EU, Euratom) 2015/443 bizottsági határozatra ([2]),

tekintettel az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2015. március 13-i (EU, Euratom) 2015/444 bizottsági határozatra ([3]),

tekintettel az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról szóló, 2017. január 10-i (EU, Euratom) 2017/46 bizottsági határozatra ([4]),

az (EU, Euratom) 2015/444 határozat 41. cikke (5) bekezdésének megfelelően a Bizottság biztonsági szakértői csoportjával folytatott konzultációt követően,

mivel:

(1) Az (EU, Euratom) 2015/444 határozat 41., 42., 47. és 48. cikke előírja, hogy a határozat 6. fejezetének kiegészítése és támogatása érdekében az iparbiztonsággal kapcsolatos végrehajtási szabályokban részletesebb rendelkezéseket kell meghatározni, kitérve olyan kérdésekre, mint a minősített támogatási megállapodások odaítélése, a telephely-biztonsági tanúsítványok, a személyi biztonsági tanúsítványok, a látogatások, valamint az EU-minősített adatok továbbítása és szállítása.

(2) Az (EU, Euratom) 2015/444 határozat értelmében, a minősített támogatási megállapodásokat a nemzeti biztonsági hatósággal, a kijelölt biztonsági hatósággal vagy az érintett tagállam más illetékes hatóságaival szoros együttműködésben kell végrehajtani. A tagállamok megállapodtak abban, hogy biztosítani kell a joghatóságuk alatt álló, a Bizottságtól származó minősített adatokat fogadó vagy előállító gazdálkodó egységek megfelelő biztonsági ellenőrzését, és azt, hogy azok képesek legyenek olyan megfelelő védelmet biztosítani, amely megegyezik azzal, amelyet az Európai Unió Tanácsának biztonsági szabályai a megfelelő minősítési megjelöléssel ellátott EU-minősített adatok védelme tekintetében az Európai Uniónak a Tanács keretében ülésező tagállamai közötti, az Európai Unió érdekében kicserélt minősített adatok védelméről szóló megállapodásnak (2011/C 202/05) ([5]) megfelelően előírnak.

([1]) HL L 193., 2018.7.30., 1. o.
([2]) HL L 72., 2015.3.17., 41. o.
([3]) HL L 72., 2015.3.17., 53. o.
([4]) HL L 6., 2017.1.11., 40. o.
([5]) HL C 202., 2011.7.8., 13. o.

(3) A Tanács, a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője megállapodott abban, hogy az EU-minősített adatok védelme tekintetében – a konkrét intézményi és szervezeti igények figyelembevételével, az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló 2013/488/EU tanácsi határozatot ([6]) elfogadó tanácsi ülés jegyzőkönyvéhez csatolt nyilatkozatoknak megfelelően – biztosítani kell a biztonsági szabályok lehető legkövetkezetesebb alkalmazását.

(4) A minősített támogatásokkal kapcsolatos, az iparbiztonságra vonatkozó bizottsági végrehajtási szabályoknak ezért biztosítaniuk kell a maximális következetességet, és figyelembe kell venniük az iparbiztonságra vonatkozó, a Tanács Biztonsági Bizottsága által 2016. december 13-án jóváhagyott iránymutatást.

(5) A Bizottság 2016. május 4-én határozatot ([7]) fogadott el, amely felhatalmazza a Bizottság biztonsági kérdésekért felelős tagját arra, hogy a Bizottság nevében és felelősségi körében elfogadja az (EU, Euratom) 2015/444 bizottsági határozat 60. cikkében előírt végrehajtási szabályokat,

ELFOGADTA EZT A HATÁROZATOT:

1. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) Ez a határozat az (EU, Euratom) 2015/444 határozat és különösen annak 6. fejezete értelmében megállapítja a minősített támogatásokkal kapcsolatos, az iparbiztonságra vonatkozó végrehajtási szabályokat.

(2) Ez a határozat egyedi követelményeket állapít meg az EU-minősített adatok védelmének biztosítása érdekében a pályázati felhívások közzétételekor, valamint a támogatások odaítélésekor és az Európai Bizottság által kötött minősített támogatási megállapodások végrehajtásakor.

(3) Ez a határozat a következő szinteken minősített adatokat tartalmazó támogatásokra alkalmazandó:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

(4) Ezt a határozatot az egyéb – például az európai védelmi ipari fejlesztési programra vonatkozó – jogi aktusokban megállapított egyedi szabályok sérelme nélkül kell alkalmazni.

2. cikk

Feladatok a Bizottságon belül

(1) A támogatást nyújtó hatóság engedélyezésre jogosult tisztviselőjének az (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendeletben említett feladatai részeként biztosítja, hogy a minősített támogatás megfeleljen az (EU, Euratom) 2015/444 határozatnak és annak végrehajtási szabályainak.

([6]) A Tanács 2013/488/EU határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 274., 2013.10.15., 1. o.).

([7]) A Bizottság határozata (2016. május 4.) biztonsági tárgyú felhatalmazásról [C(2016) 2797 final].

(2) Az érintett engedélyezésre jogosult tisztviselő ennek érdekében az eljárás minden szakaszában kikéri a Bizottság biztonsági hatóságának tanácsát a minősített támogatási megállapodás, program vagy projekt biztonsági elemeivel kapcsolatos kérdésekben, és tájékoztatja a helyi biztonsági tisztviselőt az aláírt minősített támogatási megállapodásokról. Az egyes témák minősítési szintjére vonatkozó határozatot a támogatást nyújtó szerv hozza meg a biztonsági minősítési útmutató megfelelő figyelembevételével.

(3) Amennyiben az 5. cikk (3) bekezdésében említett program- vagy projektbiztonsági utasításokat alkalmazzák, a támogatást nyújtó hatóság és a Bizottság biztonsági hatósága ellátja az említett utasításokban rájuk ruházott feladatokat.

(4) A Bizottság biztonsági hatósága a végrehajtási szabályok követelményeinek teljesítésében – különösen a telephely-biztonsági tanúsítványok, a személyi biztonsági tanúsítványok, a látogatási eljárások és a szállítási tervek vonatkozásában – szorosan együttműködik az érintett tagállamok nemzeti biztonsági hatóságaival és kijelölt biztonsági hatóságaival.

(5) Amennyiben a támogatásokat uniós végrehajtó ügynökségek vagy más finanszírozó szervek kezelik, és az 1. cikk (4) bekezdésében említett egyéb jogi aktusokban meghatározott különös szabályok nem alkalmazandók:

a) amennyiben a hatáskör-átruházási szabályok úgy rendelkeznek, a Bizottság átruházó szervezeti egysége gyakorolja a támogatásokkal összefüggésben létrehozott EU-minősített adatok kibocsátójára vonatkozó jogokat;

b) a biztonsági minősítés meghatározásáért a Bizottság átruházó szervezeti egysége felel;

c) a biztonsági tanúsítványra vonatkozó adatok iránti megkereséseket és a nemzeti és/vagy kijelölt biztonsági hatóságok értesítéseit a Bizottság biztonsági hatóságán keresztül kell megküldeni.

2. FEJEZET

A MINŐSÍTETT TÁMOGATÁSOK ELNYERÉSÉRE VONATKOZÓ FELHÍVÁSOK KEZELÉSE

3. cikk

Alapelvek

(1) A támogatások minősített részeit csak tagállamban bejegyzett kedvezményezettek és harmadik országban bejegyzett vagy nemzetközi szervezet által létrehozott kedvezményezettek – amennyiben a harmadik ország vagy nemzetközi szervezet adatbiztonsági megállapodást kötött az Unióval vagy igazgatási megállapodást kötött a Bizottsággal ([8]) – vehetik igénybe.

(2) A minősített támogatásra vonatkozó felhívás közzététele előtt a támogatást nyújtó hatóság meghatározza a kérelmezők rendelkezésére bocsátható adatok biztonsági minősítési szintjét. A támogatást nyújtó hatóság emellett meghatározza a szerződés, a program vagy a projekt teljesítése során felhasznált vagy előállított adatok maximális biztonsági minősítési szintjét, vagy legalább az előállítandó vagy kezelendő adatok várható mennyiségét és típusát, valamint a minősített kommunikációs és információs rendszer szükségességét.

(3) A támogatást nyújtó hatóság gondoskodik arról, hogy a minősített támogatásra vonatkozó felhívások tájékoztatást nyújtsanak a minősített adatokkal kapcsolatos speciális biztonsági kötelezettségekről. A pályázati dokumentációban világosan meg kell határozni, hogy a kedvezményezettek mikor szerezhetik be a telephelybiztonsági tanúsítványokat, amennyiben azokra szükség van. Az I. és a II. melléklet mintasablonokat tartalmaz a pályázati feltételekkel kapcsolatos tájékoztatáshoz.

([8]) A Bizottság internetes honlapján megtalálható az EU által kötött azon megállapodások és az Európai Bizottság által kötött azon igazgatási megállapodások jegyzéke, amelyek értelmében sor kerülhet EU-minősített adatok harmadik országokkal és nemzetközi szervezetekkel való cseréjére.

(4) A támogatást nyújtó hatóság gondoskodik arról, hogy a RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok csak azután juthassanak a kérelmezők tudomására, hogy olyan titoktartási megállapodást írtak alá, amely arra kötelezi a kérelmezőket, hogy az EU-minősített adatokat az (EU, Euratom) 2015/444 határozattal, annak végrehajtási szabályaival és az alkalmazandó nemzeti szabályokkal összhangban kezeljék és védjék.

(5) Amennyiben a kérelmezők RESTREINT UE/EU RESTRICTED minősítésű adatokat kapnak, az e határozat 5. cikkének (7) bekezdésében említett minimumkövetelményeket bele kell foglalni a pályázati felhívásba vagy a pályázati szakaszban megkötött titoktartási megállapodásokba.

(6) Minden olyan kérelmezőnek és kedvezményezettnek, akinek CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat kell kezelnie vagy tárolnia létesítményeiben, akár a pályázat szakaszában, akár magának a minősített támogatási megállapodásnak a teljesítése során, a (9) bekezdésben említett esetek kivételével az előírt szintű telephelybiztonsági tanúsítvánnyal kell rendelkeznie. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű EU-minősített adatokat érintő minősített támogatások pályázati szakaszában a következő három eset fordulhat elő:

a) a pályázati szakaszban nincs hozzáférés CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű EU-minősített adatokhoz:

   amennyiben a felhívás olyan támogatásra vonatkozik, amely CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű EU-minősített adatokat érint, de a kérelmezőnek nem kell ilyen adatokat kezelnie a pályázati szakaszban, az előírt szintű telephelybiztonsági tanúsítvánnyal nem rendelkező kérelmező nem zárható ki a pályázati eljárásból azon az alapon, hogy nem rendelkezik telephelybiztonsági tanúsítvánnyal;

b) hozzáférés CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű EU-minősített adatokhoz a támogatást nyújtó hatóság telephelyén a pályázati szakaszban:

   biztosítani kell a hozzáférést a kérelmező előírt szintű személyi biztonsági tanúsítvánnyal rendelkező olyan alkalmazottjai számára, akiknek ismerniük kell ezeket az adatokat;

c) a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű EU-minősített adatok kezelése vagy tárolása a kérelmező telephelyén a pályázati szakaszban:

   amennyiben a felhívás értelmében a kérelmezőnek EU-minősített adatokat kell kezelnie vagy tárolnia a telephelyén, rendelkeznie kell az előírt szintű telephelybiztonsági tanúsítvánnyal. Ebben az esetben a támogatást nyújtó hatóság – a Bizottság biztonsági hatóságán keresztül – megszerzi az érintett nemzeti biztonsági hatóság vagy kijelölt biztonsági hatóság arra vonatkozó megerősítését, hogy a kérelmező megfelelő telephelybiztonsági tanúsítvánnyal rendelkezik, mielőtt bármilyen EU-minősített adatot a kérelmező rendelkezésére bocsátana. Biztosítani kell a hozzáférést a kérelmező előírt szintű személyi biztonsági tanúsítvánnyal rendelkező olyan alkalmazottjai számára, akiknek ismerniük kell ezeket az adatokat.

(7) Főszabály szerint a RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáféréshez sem a pályázati szakaszban, sem a támogatási megállapodás teljesítése során nincs szükség telephelybiztonsági vagy személyi biztonsági tanúsítványra. Amennyiben a tagállamok a nemzeti törvényi és rendeleti rendelkezéseik értelmében – a IV. mellékletnek megfelelően – telephelybiztonsági vagy személyi biztonsági tanúsítványt írnak elő a RESTREINT UE/EU RESTRICTED minősítésű támogatási megállapodások vagy alvállalkozói szerződések esetében, ezek a nemzeti követelmények nem jelentenek további kötelezettségeket más tagállamok számára, és nem zárják ki az olyan tagállamokból származó kérelmezőket, kedvezményezetteket vagy alvállalkozókat, amelyek a kapcsolódó támogatási megállapodások/alvállalkozói szerződések vagy versenyek vonatkozásában nem írják elő a telephelybiztonsági vagy személyi biztonsági tanúsítvány meglétét a RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáférés feltételeként. Ezeket a támogatási megállapodásokat a tagállamokban a nemzeti törvényi és rendeleti rendelkezéseknek megfelelően kell teljesíteni.

(8) Amennyiben egy felhívás kezeléséhez és egy minősített támogatási megállapodás végrehajtásához telephelybiztonsági tanúsítványra van szükség, a támogatást nyújtó hatóság a Bizottság biztonsági hatóságán keresztül kérelmet nyújt be a kedvezményezett nemzeti vagy kijelölt biztonsági hatóságához a telephelybiztonsági tanúsítványra vonatkozó adatlap (FSCIS) vagy bármely más, azzal egyenértékű elektronikus űrlap használatával. A telephelybiztonsági tanúsítványra vonatkozó adatlap ([9]) mintája megtalálható a III. melléklet D. függelékében. A telephelybiztonsági tanúsítványra vonatkozó adatlapra lehetőség szerint a kérelem benyújtásától számított 10 munkanapon belül válaszolni kell.

(9) Amennyiben a tagállamok kormányzati intézményei vagy a kormányaik ellenőrzése alatt álló intézmények olyan minősített támogatásokban vesznek részt, amelyekhez telephelybiztonsági tanúsítványra van szükség, és amennyiben a telephelybiztonsági tanúsítványokat nem a nemzeti jogszabályok alapján adják ki ezen intézmények számára, a támogatást nyújtó hatóság a Bizottság biztonsági hatóságán keresztül ellenőrzi az érintett nemzeti vagy kijelölt biztonsági hatóságnál, hogy az említett kormányzati intézmények képesek-e az EU-minősített adatok megfelelő szintű kezelésére.

([9]) Más felhasznált formanyomtatványok a felépítésükben eltérhetnek az e végrehajtási szabályokban található példától.

(10) Amennyiben a minősített támogatási megállapodás teljesítéséhez személyi biztonsági tanúsítványra van szükség, és amennyiben a nemzeti szabályok szerint telephelybiztonsági tanúsítványra van szükség személyi biztonsági tanúsítvány megadása előtt, a támogatást nyújtó hatóság a Bizottság biztonsági hatóságán keresztül a telephelybiztonsági tanúsítványra vonatkozó adatlap segítségével ellenőrzi a kedvezményezett nemzeti vagy kijelölt biztonsági hatóságánál, hogy a kedvezményezett rendelkezik-e telephelybiztonsági tanúsítvánnyal, vagy hogy a telephelybiztonsági tanúsítvány kiállítása folyamatban van-e. Ebben az esetben a Bizottság nem bocsát ki személyi biztonsági tanúsítvány iránti kérelmeket a személyi biztonsági tanúsítványra vonatkozó adatlap használatával.

4. cikk

Alvállalkozók részvétele a minősített szerződésekben

(1) A pályázati felhívásban és a támogatási megállapodásban meg kell határozni azokat a feltételeket, amelyek mellett a kedvezményezettek az intézkedés EU-minősített adatokat tartalmazó feladatait alvállalkozásba adhatják. E feltételek között szerepel az a követelmény, hogy minden telephelybiztonsági tanúsítványra vonatkozó adatlapot a Bizottság biztonsági hatóságán keresztül kell benyújtani. Az alvállalkozásba adáshoz a támogatást nyújtó hatóság előzetes írásbeli hozzájárulása szükséges. Adott esetben az alvállalkozásba adásnak meg kell felelnie a programot létrehozó alap-jogiaktusnak.

(2) A támogatások minősített részeit alvállalkozóként csak tagállamban bejegyzett szervezetek vehetik igénybe, valamint harmadik országban bejegyzett vagy nemzetközi szervezet által létrehozott kedvezményezettek abban az esetben, ha a harmadik ország vagy nemzetközi szervezet adatbiztonsági megállapodást kötött az Unióval vagy igazgatási megállapodást kötött a Bizottsággal ([10]).

3. FEJEZET

A MINŐSÍTETT TÁMOGATÁSOK KEZELÉSE

5. cikk

Alapelvek

(1) Minősített támogatás odaítélésekor a támogatást nyújtó szerv – a Bizottság biztonsági hatóságával együtt – gondoskodik arról, hogy a támogatási megállapodás szerves részét képezze a kedvezményezett arra vonatkozó kötelezettsége, hogy biztosítsa a támogatási megállapodás teljesítése során felhasznált vagy előállított EU-minősített adatok védelmét. A támogatásspecifikus biztonsági követelményeket biztonsági vonatkozások záradékában kell rögzíteni. A biztonsági vonatkozások záradékának mintája a III. mellékletben található.

(2) A minősített szerződés aláírását megelőzően a támogatást nyújtó hatóság – a Bizottság biztonsági hatóságával folytatott konzultációt követően – szükség szerint biztonsági minősítési útmutatót készít a szerződés teljesítése során, illetve adott esetben program- vagy projektszinten elvégzendő feladatokhoz és előállított adatokhoz. A biztonsági minősítési útmutatót a biztonsági vonatkozások záradékának részeként kell elkészíteni.

(3) A program- vagy projektspecifikus biztonsági követelményeket program- vagy projektbiztonsági utasítások formájában kell meghatározni. A program- vagy projektbiztonsági utasítások megfogalmazhatók a biztonsági vonatkozások záradéka tekintetében a III. mellékletben található mintára vonatkozó rendelkezések alapján. A program- vagy projektbiztonsági utasításokat a programot vagy projektet irányító szervezeti egység dolgozza ki a Bizottság biztonsági hatóságával szoros együttműködésben, majd tanácsadás céljából benyújtja a Bizottság biztonsági szakértői csoportjának. Amennyiben a támogatási megállapodás saját program- vagy projektbiztonsági utasításokkal rendelkező program vagy projekt része, a támogatási megállapodáshoz tartozó biztonsági vonatkozások záradékát egyszerűsített formában kell elkészíteni, és abban hivatkozni kell a program vagy projekt program- vagy projektbiztonsági utasításaiban meghatározott biztonsági rendelkezésekre.

(4) A 3. cikk (9) bekezdésében említett esetek kivételével a minősített támogatási megállapodást nem lehet aláírni mindaddig, amíg a kérelmező nemzeti vagy kijelölt biztonsági hatósága meg nem erősíti a kérelmező telephelybiztonsági tanúsítványát, vagy amennyiben a minősített támogatási megállapodást konzorciumnak ítélik oda, addig, amíg a konzorciumon belül legalább egy – vagy szükség esetén több – kérelmező nemzeti vagy kijelölt biztonsági hatósága meg nem erősíti a kérelmező telephelybiztonsági tanúsítványát.

(5) Elvben, és amennyiben más vonatkozó szabályok másként nem rendelkeznek, a támogatást nyújtó hatóság tekintendő a támogatási megállapodás teljesítése során keletkezett EU-minősített adatok kibocsátójának.

([10]) A Bizottság internetes honlapján megtalálható az EU által kötött azon megállapodások és az Európai Bizottság által kötött azon igazgatási megállapodások jegyzéke, amelyek értelmében sor kerülhet EU-minősített adatok harmadik országokkal és nemzetközi szervezetekkel való cseréjére.

(6) A támogatást nyújtó hatóság – a Bizottság biztonsági hatóságán keresztül – értesíti valamennyi kedvezményezett és alvállalkozó nemzeti biztonsági hatóságát és/vagy kijelölt biztonsági hatóságát a minősített támogatási megállapodások vagy alvállalkozói szerződések megkötéséről, valamint e támogatási megállapodások vagy alvállalkozói szerződések meghosszabbításáról vagy idő előtti megszüntetéséről. Az országspecifikus követelmények felsorolását a IV. melléklet tartalmazza.

(7) A RESTREINT UE/EU RESTRICTED minősítésű adatokat érintő támogatási megállapodásoknak tartalmazniuk kell olyan szerződésbiztonsági kikötést, amely kötelezi a kedvezményezetteket a III. melléklet E. függelékében található rendelkezések követésére. Ezeknek a támogatási megállapodásoknak olyan biztonsági vonatkozások záradékát kell tartalmazniuk, amely meghatározza legalább a RESTREINT UE/EU RESTRICTED minősítésű adatok kezelésére vonatkozó követelményeket, beleértve az adatvédelmi kérdéseket és azokat a konkrét követelményeket is, amelyeket a kedvezményezetteknek a RESTREINT UE/EU RESTRICTED minősítésű adatokat kezelő kommunikációs és információs rendszerének akkreditálása érdekében teljesíteniük kell.

(8) Amennyiben a tagállamok nemzeti törvényi és rendeleti rendelkezései azt előírják, a nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságok gondoskodnak arról, hogy a joghatóságuk alá tartozó kedvezményezettek vagy alvállalkozók megfeleljenek a RESTREINT UE/EU RESTRICTED minősítésű adatok védelmére vonatkozó biztonsági rendelkezéseknek, és ellenőrzési látogatásokat tesznek a kedvezményezetteknek vagy az alvállalkozóknak a területükön található létesítményeiben. Amennyiben nem vonatkoznak ilyen kötelezettségek a nemzeti biztonsági hatóságokra/kijelölt biztonsági hatóságokra, a támogatást nyújtó hatóság gondoskodik arról, hogy a kedvezményezettek végrehajtsák a III. melléklet E. függelékében meghatározott szükséges biztonsági rendelkezéseket.

6. cikk

A kedvezményezettek és az alvállalkozók alkalmazottjainak hozzáférése az EU-minősített adatokhoz

(1) A támogatást nyújtó hatóság gondoskodik arról, hogy a minősített támogatási megállapodások tartalmazzanak olyan rendelkezéseket, amelyek értelmében a kedvezményezettek vagy alvállalkozók azon alkalmazottja számára, akinek a minősített támogatási megállapodás vagy alvállalkozói szerződés teljesítéséhez szüksége van az EU-minősített adatokhoz való hozzáférésre, a hozzáférés csak akkor adható meg, ha:

a) megállapítást nyert, hogy az adott személynek szüksége van ezen adatok ismeretére;

b) CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatok esetében az adott személy részére az érintett nemzeti biztonsági hatóság/kijelölt biztonsági hatóság vagy más illetékes biztonsági hatóság a releváns szinten megfelelő védelmet biztosított;

c) az adott személy tájékoztatást kapott az EU-minősített adatok védelme érdekében alkalmazandó biztonsági szabályokról, és tudomásul vette az ilyen adatok védelmével kapcsolatos felelősségét.

(2) Adott esetben az EU-minősített adatokhoz való hozzáférésnek meg kell felelnie a programot létrehozó alapjogiaktusnak is, és figyelembe kell vennie a biztonsági minősítési útmutatóban meghatározott minden további jelölést.

(3) Ha a kedvezményezett vagy alvállalkozó harmadik ország állampolgárát kívánja alkalmazni olyan pozícióban, amelyhez CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű EU-minősített adatokhoz való hozzáférés szükséges, a kedvezményezett vagy alvállalkozó kezdeményezi az adott személyre vonatkozó biztonsági ellenőrzési eljárás lefolytatását az abban az országban érvényes nemzeti törvényi és rendeleti rendelkezéseknek megfelelően, ahol biztosítani tervezi az EU-minősített adatokhoz való hozzáférést.

7. cikk

Az ellenőrzésben, felülvizsgálatban vagy auditban részt vevő szakértők hozzáférése az EU-minősített adatokhoz

(1) Amennyiben a támogatást nyújtó hatóság által végzett ellenőrzésekben, felülvizsgálatokban vagy auditokban, illetve a kedvezményezettek CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáférést igénylő teljesítményértékelésében külső személyek („szakértők") vesznek részt, ezek csak akkor kaphatnak szerződést, ha átestek az érintett nemzeti vagy kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság által végzett megfelelő szintű biztonsági ellenőrzésen. A támogatást nyújtó hatóság a Bizottság biztonsági hatóságán keresztül ellenőrzi, és szükség esetén felkéri a nemzeti vagy kijelölt biztonsági hatóságot, hogy legalább hat hónappal a vonatkozó szerződések kezdete előtt kezdeményezze a szakértők átvilágítási eljárását.

(2) Szerződésük aláírása előtt a szakértőket tájékoztatni kell az EU-minősített adatok védelme érdekében alkalmazandó biztonsági szabályokról, és azoknak tudomásul kell venniük az ilyen adatok védelmével kapcsolatos felelősségüket.

4. FEJEZET

A MINŐSÍTETT TÁMOGATÁSI MEGÁLLAPODÁSOKKAL KAPCSOLATOS LÁTOGATÁSOK

8. cikk

Alapelvek

(1) Amennyiben a támogatást nyújtó hatóságnak, a szakértőknek, a kedvezményezetteknek vagy az alvállalkozóknak egy minősített támogatási megállapodás végrehajtásához egymás telephelyén CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz kell hozzáférniük, a látogatásokat a nemzeti vagy kijelölt biztonsági hatóságokkal vagy bármely más érintett illetékes biztonsági hatósággal egyeztetve kell megszervezni.

(2) Az (1) bekezdésben említett látogatásokra az alábbi követelmények vonatkoznak:

a) a látogatásnak a minősített támogatással kapcsolatos hivatalos célúnak kell lennie;

b) a minősített támogatás teljesítése során felhasznált vagy előállított EU-minősített adatokhoz való hozzáférés érdekében minden látogatónak előírt szintű személyi biztonsági tanúsítvánnyal kell rendelkeznie, és meg kell ismernie az érintett adatokat.

9. cikk

Látogatási kérelmek

(1) Ha a kedvezményezettek vagy alvállalkozók más kedvezményezettek vagy alvállalkozók telephelyét vagy a támogatást nyújtó hatóság létesítményeit keresik fel, és ennek során CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz férnek hozzá, a látogatást az alábbi eljárásnak megfelelően kell megszervezni:

a) a látogatót küldő telephely biztonsági tisztviselője kitölti a látogatási kérelemre vonatkozó formanyomtatvány releváns részét, és benyújtja a kérelmet a telephely nemzeti biztonsági hatóságának vagy kijelölt biztonsági hatóságának. A látogatási kérelem formanyomtatványa a III. melléklet C. függelékében található;

b) a látogatási kérelemnek a fogadó telephely nemzeti biztonsági hatóságánál vagy kijelölt biztonsági hatóságánál (a támogatást nyújtó hatóság létesítményeiben tett látogatás esetén a Bizottság biztonsági hatóságánál) történő benyújtása előtt a küldő telephely nemzeti biztonsági hatósága vagy kijelölt biztonsági hatósága megerősíti a látogató személyi biztonsági tanúsítványát;

c) a küldő telephely biztonsági tisztviselője a nemzeti biztonsági hatóságától vagy kijelölt biztonsági hatóságától megszerzi a fogadó telephely nemzeti biztonsági hatóságának vagy kijelölt biztonsági hatóságának (vagy a Bizottság biztonsági hatóságának) válaszát, amely jóváhagyja vagy elutasítja a látogatási kérelmet;

d) a látogatási kérelem jóváhagyottnak tekintendő, ha a látogatás időpontját megelőző ötödik munkanapig nem érkezik ellenvetés.

(2) Ha a támogatást nyújtó hatóság tisztviselői vagy a szakértők, illetve az ellenőrök a kedvezményezettek vagy alvállalkozók telephelyeit keresik fel, és ennek során CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz férnek hozzá, a látogatást az alábbi eljárásnak megfelelően kell megszervezni:

a) a látogató kitölti a látogatási kérelem vonatkozó részeit, és benyújtja a látogatási kérelmet a Bizottság biztonsági hatóságának;

b) a látogatási kérelemnek a fogadó telephely nemzeti biztonsági hatóságánál vagy kijelölt biztonsági hatóságánál történő benyújtása előtt a Bizottság biztonsági hatósága megerősíti a látogató személyi biztonsági tanúsítványát;

c) a Bizottság biztonsági hatósága megszerzi a fogadó telephely nemzeti biztonsági hatóságának vagy kijelölt biztonsági hatóságának válaszát, amely jóváhagyja vagy elutasítja a látogatási kérelmet;

d) a látogatási kérelem jóváhagyottnak tekintendő, ha a látogatás időpontját megelőző ötödik munkanapig nem érkezik ellenvetés.

(3) A látogatási kérelem egyszeri vagy ismétlődő látogatásra vonatkozhat. Ismétlődő látogatás esetén a látogatási kérelem érvényessége a kérelem dátumától számított egy évre szólhat.

(4) A látogatási kérelem nem szólhat a látogató személyi biztonsági tanúsítványának érvényességét meghaladó időre.

(5) A látogatási kérelmet a fogadó telephely illetékes biztonsági hatóságánál főszabályként legkésőbb 15 munkanappal a látogatás időpontját megelőzően kell benyújtani.

10. cikk

Látogatási eljárások

(1) Ahhoz, hogy a látogatók számára lehetőséget adhasson az EU-minősített adatokhoz való hozzáférésre, a fogadó telephely biztonsági hivatalának meg kell felelnie a nemzeti biztonsági hatósága vagy kijelölt biztonsági hatósága által a látogatásokkal kapcsolatban megállapított valamennyi biztonsági eljárásnak és szabálynak.

(2) A látogatóknak a fogadó telephelyre való érkezésükkor érvényes személyazonosító igazolvánnyal vagy útlevéllel kell igazolniuk személyazonosságukat. A személyazonosító információknak meg kell felelniük a látogatási kérelemben megadott információknak.

(3) A fogadó telephely valamennyi látogatóról nyilvántartást vezet, és ennek keretében feljegyzi a látogatók nevét, az általuk képviselt szervezetet, a személyi biztonsági tanúsítvány érvényességének lejártát, a látogatás dátumát és a felkeresett személyek nevét. A nyilvántartást legalább öt évig – vagy ha a fogadó telephely országának nemzeti szabályai és jogszabályi rendelkezései előírják, akkor ennél hosszabb ideig – meg kell őrizni.

11. cikk

Közvetlenül szervezett látogatások

(1) Konkrét projektek összefüggésében az érintett nemzeti biztonsági hatóságok vagy kijelölt biztonsági hatóságok és a Bizottság biztonsági hatósága megállapodhatnak olyan eljárásban, amelynek megfelelően egy adott minősített támogatás vonatkozásában a látogató biztonsági tisztviselője és a meglátogatni kívánt telephely biztonsági tisztviselője közvetlenül szervezheti meg a látogatásokat. Az erre a célra használandó formanyomtatvány mintája a III. melléklet C. függelékében található. Az ilyen kivételes eljárásokat a program- vagy projektbiztonsági utasításokban vagy más konkrét megállapodásokban kell meghatározni. Ilyen esetekben a 9. cikkben és a 10. cikk (1) bekezdésében meghatározott eljárások nem alkalmazandók.

(2) A RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáféréssel járó látogatásokat a küldő és a fogadó szervezetnek kell közvetlenül megszerveznie, és e látogatások tekintetében nem kell követni a 9. cikkben és a 10. cikk (1) bekezdésében meghatározott eljárásokat.

5. FEJEZET

AZ EU-MINŐSÍTETT ADATOK TOVÁBBÍTÁSA ÉS SZÁLLÍTÁSA A MINŐSÍTETT TÁMOGATÁSI MEGÁLLAPODÁSOK TELJESÍTÉSE SORÁN

12. cikk

Alapelvek

A támogatást nyújtó hatóság gondoskodik arról, hogy az EU-minősített adatok továbbításával és szállításával kapcsolatos valamennyi döntés megfeleljen az (EU, Euratom) 2015/444 határozatnak és annak végrehajtási szabályainak, továbbá a minősített támogatási megállapodás feltételeinek, beleértve a kibocsátó beleegyezését is.

13. cikk

Elektronikus kezelés

(1) Az EU-minősített adatok elektronikus kezelését és továbbítását az (EU, Euratom) 2015/444 határozat 5. és 6. fejezetének, valamint a határozat végrehajtási szabályainak megfelelően kell végezni.

A kedvezményezett kommunikációs és információs rendszerét, amelyet a kedvezményezett a támogatási megállapodás teljesítésével összefüggésben az EU-minősített adatok kezelésére használ (a továbbiakban: a kedvezményezett kommunikációs és információs rendszere), a felelős biztonsági akkreditációs hatóságnak akkreditálnia kell. Az EU-minősített adatok elektronikus továbbításának védelmét az (EU, Euratom) 2015/444 határozat 36. cikke (4) bekezdésének megfelelően jóváhagyott kriptográfiai termékek útján kell biztosítani. Az említett határozat 36. cikke (6) bekezdésének megfelelően TEMPEST biztonsági intézkedéseket kell végrehajtani.

(2) A kedvezményezett RESTREINT UE/EU RESTRICTED szintű EU-minősített adatokat kezelő kommunikációs és információs rendszere és az összekapcsolás tekintetében a biztonsági akkreditáció elvégzése, amennyiben a nemzeti törvényi és rendeleti rendelkezések azt lehetővé teszik, átruházható a kedvezményezett biztonsági tisztviselőjére. A feladat átruházása esetén a kedvezményezett feladata, hogy akkor, amikor a kommunikációs és információs rendszerében RESTREINT UE/EU RESTRICTED minősítésű adatokat kezel, gondoskodjon a biztonsági vonatkozások záradékában meghatározott biztonsági minimumkövetelmények teljesüléséről. Ugyanakkor továbbra is az érintett nemzeti biztonsági hatóságok vagy kijelölt biztonsági hatóságok és biztonsági akkreditációs hatóságok felelősek a kedvezményezett által kezelt, RESTREINT UE/EU RESTRICTED minősítésű adatok védelméért, és joguk van megvizsgálni a kedvezményezett által hozott biztonsági intézkedéseket. A kedvezményezett emellett bemutatja a támogatást nyújtó hatóságnak – és amennyiben a nemzeti jogszabályok és rendeletek előírják, az illetékes nemzeti biztonsági akkreditációs hatóságnak – a megfelelőségi nyilatkozatot, amely tanúsítja, hogy a kedvezményezett kommunikációs és információs rendszere és az összekapcsolás akkreditációval rendelkezik a RESTREINT UE/EU RESTRICTED szintű EU-minősített adatok kezelésére ([11]).

14. cikk

Szállítás kereskedelmi futárszolgálat igénybevételével

Az EU-minősített adatok kereskedelmi futárok általi szállítása során be kell tartani a RESTREINT UE/EU RESTRICTED minősítésű adatok kezelésére vonatkozó végrehajtási szabályokról szóló (EU, Euratom) 2019/1962 bizottsági határozat ([12]) és a CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok kezelésére vonatkozó végrehajtási szabályokról szóló (EU, Euratom) 2019/1961 bizottsági határozat ([13]) vonatkozó rendelkezéseit.

15. cikk

Kézi szállítás

(1) A minősített adatok kézi szállítása esetén szigorú biztonsági követelményeknek kell megfelelni.

(2) A RESTREINT UE/EU RESTRICTED minősítésű adatokat a kedvezményezett alkalmazottjai az Unión belül akkor szállíthatják kézi úton, ha teljesülnek az alábbi követelmények:

a) a boríték vagy csomag nem átlátszó, és nem szerepel rajta a tartalom minősítése;

b) a szállító nem adja ki a kezéből a minősített adatot;

c) útközben nem kerül sor a boríték vagy csomag felnyitására.

(3) A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatok esetében a küldő és a fogadó szervezet előre megszervezi az uniós tagállamokon belül a kedvezményezett alkalmazottja általi kézi szállítást. A küldő hatóság vagy telephely tájékoztatja a fogadó hatóságot vagy telephelyet a szállítmány részleteiről, beleértve a hivatkozási adatokat, a minősítést, az érkezés várható időpontját és a futár nevét is. Az ilyen kézi szállítás az alábbi követelmények teljesülése esetén megengedett:

a) a minősített adatok szállítására dupla borítékban vagy csomagban kerül sor;

b) a külső boríték vagy csomag zárt, nem szerepel rajta a tartalom minősítése, míg a belső borítékon szerepel a tartalom minősítése;

c) az EU-minősített adat nem kerül ki a szállító kézéből;

d) útközben nem kerül sor a boríték vagy csomag felnyitására;

e) a boríték vagy csomag szállítása olyan zárható aktatáskában vagy olyan méretű és súlyú hasonló jóváhagyott táskában történik, amely mindig a szállítónál maradhat, és nem kerül a poggyásztérbe;

f) a futár olyan, az illetékes biztonsági hatósága által kiállított tanúsítvánnyal rendelkezik, amely felhatalmazza a meghatározott minősített szállítmány szállítására.

([11]) A RESTREINT UE/EU RESTRICTED szintű EU-minősített adatokat kezelő kommunikációs és információs rendszerekre vonatkozó minimumkövetelményeket a III. melléklet E. függeléke tartalmazza.

([12]) A Bizottság (EU, Euratom) 2019/1962 határozata (2019. október 17.) a RESTREINT UE/EU RESTRICTED adatok kezelésére vonatkozó végrehajtási szabályokról (HL L 311., 2019.12.2., 21. o.).

([13]) A Bizottság (EU, Euratom) 2019/1961 határozata (2019. október 17.) a CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatok kezelésére vonatkozó végrehajtási szabályokról (HL L 311., 2019.12.2., 1. o.).

(4) A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatoknak a kedvezményezett alkalmazottja általi, uniós tagállamok közötti kézi szállítására a következő további szabályok vonatkoznak:

a) a futár mindaddig felelős a szállított minősített anyag biztonságáért, amíg azt át nem adja a címzettnek;

b) a biztonsági előírások megszegése esetén a küldő nemzeti biztonsági hatósága vagy kijelölt biztonsági hatósága kérheti, hogy annak az országnak a hatóságai, ahol a biztonsági előírások megszegésére sor került, folytasson vizsgálatot, jelentse a megállapításait, és adott esetben tegyen jogi vagy egyéb lépéseket;

c) a futárt tájékoztatni kell a szállítás során betartandó valamennyi biztonsági kötelezettségről, és a futárnak alá kell írnia a megfelelő, ennek tudomásulvételét tanúsító dokumentumot;

d) a futárnak szóló utasításokat mellékelni kell a futár tanúsítványához;

e) a futár rendelkezésére kell bocsátani a szállítmány és az útvonal leírását;

f) az utazás végén a dokumentumokat vissza kell juttatni a dokumentumokat kiállító nemzeti biztonsági hatósághoz vagy kijelölt biztonsági hatósághoz, vagy az átvevőnek meg kell őriznie azokat ellenőrzési célból;

g) ha a vámhatóság, a bevándorlási hatóság vagy a határrendészet meg kívánja vizsgálni a szállítmányt, azt az annak megállapításához elégséges mértékben felnyithatják és ellenőrizhetik, hogy a szállítmány csak a bejelentett anyagokat tartalmazza;

h) a vámhatóságot fel kell szólítani a szállítási dokumentumok és a futár birtokában lévő felhatalmazási dokumentumok hivatalos jellegének tiszteletben tartására.

Ha a vámhatóság felnyitja a szállítmányt, ezt lehetőség szerint a futár jelenlétében, az arra jogosulatlan személyek jelenlétének kizárásával kell megtenni. A futárnak kérnie kell a szállítmány újbóli becsomagolását, valamint azt, hogy a vizsgálatot végző hatóságok újból zárják le a szállítmányt, és írásban igazolják, hogy ők nyitották azt fel.

(5) A RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatoknak a kedvezményezett alkalmazottja általi, harmadik országba vagy nemzetközi szervezetnek való kézi szállítására az Unió, illetve a Bizottság és az érintett harmadik ország vagy nemzetközi szervezet közötti adatbiztonsági megállapodás, illetve igazgatási megállapodás rendelkezései irányadók.

6. FEJEZET

ÜZLETMENET-FOLYTONOSSÁGI TERVEZÉS

16. cikk

Szükséghelyzeti tervek és helyreállító intézkedések

A támogatást nyújtó hatóság gondoskodik arról, hogy a minősített támogatási megállapodás a minősített támogatás teljesítésével kapcsolatban kezelt EU-minősített adatok szükséghelyzeti tervek védelme érdekében előírja a kedvezményezettek számára az üzletmenet-folytonossági terv kidolgozását, valamint az üzletmenet-folytonossági tervezéssel összefüggő, az EU-minősített adatok kezelésével és tárolásával kapcsolatos események hatásának minimalizálását célzó megelőző és helyreállító intézkedések meghozatalát. A kedvezményezettek megerősítik a támogatást nyújtó hatóságnak üzletmenet-folytonossági terveik bevezetését.

17. cikk

Hatálybalépés

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

Kelt Brüsszelben, 2021. február 10-én.

a Bizottság részéről,
az elnök nevében,
Johannes HAHN
a Bizottság tagja

I. MELLÉKLET

A FELHÍVÁSBAN FOGLALT SZOKVÁNYOS INFORMÁCIÓK

(az alkalmazott felhíváshoz igazítandó)

Biztonság

Az EU-minősített adatokat tartalmazó projekteket a finanszírozás engedélyezéséhez biztonsági ellenőrzésnek kell alávetni, és azok különleges biztonsági szabályok alá vethetők (ezeket a támogatási megállapodáshoz csatolt biztonsági vonatkozások záradéka részletezi).

Ezek a szabályok (amelyeket az (EU, Euratom) 2015/444/EK bizottsági határozat ([1]) és/vagy a nemzeti szabályok szabályoznak) például a következőkről rendelkeznek:

– a TRES SECRET UE/EU TOP SECRET (vagy azzal egyenértékű) minősítésű adatokat tartalmazó projektek **NEM** finanszírozhatók;

– a minősített adatokat a biztonsági vonatkozások záradékában foglalt alkalmazandó biztonsági utasításoknak megfelelően kell megjelölni;

– a CONFIDENTIEL UE/EU CONFIDENTIAL vagy magasabb (és RESTREINT UE/EU RESTRICTED, ha a nemzeti szabályok előírják) minősítési szintű adatok:

  – az adatokat telephelybiztonsági tanúsítvánnyal rendelkező helyiségekben kizárólag az illetékes nemzeti biztonsági hatóság (NSA) – a nemzeti szabályokkal összhangban – hozta létre vagy hozzáféréssel rendelkezik azokhoz;

  – minősített adatok csak az illetékes nemzeti biztonsági hatóság által akkreditált biztonsági területen kezelhetők;

  – csak érvényes személyi biztonsági tanúsítvánnyal (PSC) és a szükséges ismeretekkel rendelkező személyek férhetnek hozzá az adatokhoz és kezelhetik azokat;

– a támogatás lejártakor a minősített adatokat vagy vissza kell küldeni, vagy az alkalmazandó szabályoknak megfelelően továbbra is védelemben kell részesíteni;

– a cselekvéshez kapcsolódó, EU-minősített adatokat érintő feladatok alvállalkozásba adására csak a támogatást nyújtó hatóság előzetes írásbeli jóváhagyásával kerülhet sor, és csak uniós tagállamban vagy az EU-val kötött adatbiztonsági megállapodással (vagy a Bizottsággal kötött igazgatási megállapodással) rendelkező nem uniós országban letelepedett szervezetek részére;

– az EU-minősített adatok harmadik felek részére történő átadásához a támogatást nyújtó hatóság előzetes írásbeli jóváhagyása szükséges.

Kérjük, vegye figyelembe, hogy a tevékenység típusától függően előfordulhat, hogy a telephelybiztonsági tanúsítványt a támogatás aláírása előtt kell beszerezni. A támogatást nyújtó hatóság minden esetben értékeli az átvilágítás szükségességét, és a támogatás előkészítése során meghatározza azok teljesítési határidejét. Kérjük, vegye figyelembe, hogy támogatási megállapodást **semmilyen körülmények** között sem írhatunk alá mindaddig, amíg a konzorcium legalább egy kedvezményezettje nem rendelkezik telephelybiztonsági tanúsítvánnyal.

A támogatási megállapodást biztonsági eredmények formájában további biztonsági ajánlásokkal lehet kiegészíteni (*pl. biztonsági tanácsadó csoport létrehozása, a részletesség szintjének korlátozása, hamis forgatókönyv alkalmazása, a minősített adatok felhasználásának kizárása stb.*).

A kedvezményezetteknek biztosítaniuk kell, hogy projektjeikre ne vonatkozzanak olyan nemzeti/harmadik országbeli biztonsági követelmények, amelyek érinthetik a végrehajtást vagy megkérdőjelezhetik a támogatás odaítélését (*pl. technológiai korlátozások, nemzetbiztonsági minősítés stb.*). A támogatást nyújtó hatóságot haladéktalanul értesíteni kell az esetleges biztonsági problémákról.

[kiegészítő LEHETŐSÉG a partnerségi keretmegállapodások esetében: A partnerségi keretmegállapodások esetében előfordulhat, hogy mind a partnerségi keretpályázatokat, mind a támogatási kérelmeket biztonsági vizsgálatnak kell alávetni.]

([1]) Lásd az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2015. március 13-i (EU, Euratom) 2015/444 bizottsági határozatot (HL L 72., 2015.3.17., 53. o.).

II. MELLÉKLET

A TÁMOGATÁSI MEGÁLLAPODÁS SZOKVÁNYOS ZÁRADÉKAI

(az alkalmazott támogatási megállapodáshoz igazítandó)

13.2. Biztonság – Minősített adatok

A feleknek a(z EU vagy nemzeti) minősített adatokat a minősített adatokra vonatkozó alkalmazandó uniós vagy nemzeti jogszabályokkal (különösen az (EU, Euratom) 2015/444 bizottsági határozattal [1]) és annak végrehajtási szabályaival) összhangban kell kezelniük.

A különleges biztonsági szabályokat (ha vannak ilyenek) az 5. melléklet ismerteti.

5. MELLÉKLET

Biztonság – Az EU-minősített adatok

[LEHETŐSÉG – EU-minősített adatokat tartalmazó intézkedések esetében (standard): Ha az intézkedés EU-minősített adatok használatával vagy előállításával jár, az ilyen adatokat a minősítés feloldásáig a biztonsági minősítési útmutatóval és az I. mellékletben foglalt biztonsági vonatkozások záradékával, valamint az (EU, Euratom) 2015/444 határozattal és annak végrehajtási szabályaival összhangban kell kezelni.

Az EU-minősített adatokat tartalmazó leszállítandó anyagokat a támogatást nyújtó hatósággal egyeztetett speciális eljárásoknak megfelelően kell benyújtani.

A cselekvéshez kapcsolódó, EU-minősített adatokat érintő feladatok alvállalkozásba adására csak a támogatást nyújtó hatóság kifejezett írásbeli jóváhagyásával kerülhet sor, és csak uniós tagállamban vagy az EU-val kötött adatbiztonsági megállapodással (vagy a Bizottsággal kötött igazgatási megállapodással) rendelkező nem uniós országban letelepedett jogalanyok részére.

EU-minősített adatok nem adhatók át harmadik feleknek (beleértve az intézkedés végrehajtásában részt vevő személyeket is) a támogatást nyújtó hatóság kifejezett előzetes írásbeli jóváhagyása nélkül.]

---

[1] A Bizottság (EU, Euratom) 2015/444 határozata (2015. március 13.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 72., 2015.3.17., 53. o.).

III. MELLÉKLET

[IV. melléklet (a(z) ...-hez/-hoz/-höz)]

BIZTONSÁGI VONATKOZÁSOK ZÁRADÉKA (SAL) [1]

[Minta]

[1] A biztonsági vonatkozások záradéka e modelljét akkor kell alkalmazni, ha a Bizottság minősül a támogatási megállapodás végrehajtása céljából létrehozott és kezelt minősített adatok kibocsátójának. Amennyiben a támogatási megállapodás teljesítése céljából létrehozott és kezelt minősített adatok kibocsátója nem a Bizottság, és ha a támogatásban részt vevő tagállamok külön biztonsági keretet hoznak létre, a biztonsági vonatkozások záradékának más modelljei is alkalmazhatók.

A. függelék

BIZTONSÁGI KÖVETELMÉNYEK

A támogatást nyújtó hatóságnak a biztonsági vonatkozások záradékában az alábbi biztonsági követelményeket kell szerepeltetnie. Elképzelhető, hogy néhány kikötés nem alkalmazandó a támogatási megállapodásra. Ezek szögletes zárójelben szerepelnek.

A kikötések felsorolása nem kimerítő jellegű. A felsorolás a minősített támogatás jellegétől függően további kikötésekkel bővíthető.

ÁLTALÁNOS FELTÉTELEK [*N.B.: valamennyi minősített támogatási megállapodásra alkalmazandó*]

1. A biztonsági vonatkozások záradéka a minősített támogatási megállapodás [vagy alvállalkozói szerződés] szerves része, és a támogatási megállapodás specifikus biztonsági követelményeit ismerteti. A követelmények teljesítésének elmulasztása elegendő ok lehet a támogatási megállapodás felmondására.

2. A támogatás kedvezményezettjeinek az (EU, Euratom) 2015/444 bizottsági határozatban ([2]) és annak végrehajtási szabályaiban ([3]) meghatározott valamennyi kötelezettségnek eleget kell tenniük. Ha a támogatás kedvezményezettje valamely tagállamban az alkalmazandó jogi keret alkalmazásával kapcsolatos problémával szembesül, a Bizottság biztonsági hatóságához és a nemzeti biztonsági hatósághoz vagy a kijelölt biztonsági hatósághoz kell fordulnia.

3. A támogatási megállapodás teljesítése során előállított minősített adatokat a biztonsági minősítés szempontjából EU-minősített adatként kell megjelölni a záradék B. függelékében szereplő biztonsági minősítési útmutatónak megfelelően. A biztonsági minősítési útmutató szerinti biztonsági minősítési szinttől csak a támogatást nyújtó hatóság írásos engedélyével lehet eltérni.

4. A minősített támogatási megállapodás teljesítése vonatkozásában előállított és kezelt EU-minősített adatok kibocsátói jogát a Bizottság mint támogatást nyújtó hatóság gyakorolja.

5. A támogatást nyújtó hatóság írásbeli hozzájárulása nélkül a kedvezményezett vagy alvállalkozó csak a támogatási megállapodás teljesítésének céljára használhatja fel a támogatást nyújtó hatóság által biztosított vagy a támogatást nyújtó hatóság nevében előállított adatokat vagy anyagokat.

6. Amennyiben a támogatási megállapodás teljesítéséhez telephelybiztonsági tanúsítványra van szükség, a kedvezményezettnek telephelybiztonsági tanúsítványt kell kérelmeznie a támogatást nyújtó hatóságnál.

7. A kedvezményezettnek ki kell vizsgálnia az EU-minősített adatokkal kapcsolatos biztonsági előírások megszegésének minden esetét, és a lehető leghamarabb jelentenie kell azokat a támogatást nyújtó hatóságnak. A kedvezményezettnek vagy alvállalkozónak haladéktalanul jelentenie kell a felelős nemzeti biztonsági hatóságának vagy kijelölt biztonsági hatóságának – és ahol a nemzeti törvényi és rendeleti rendelkezések lehetővé teszik, a Bizottság biztonsági hatóságának – minden olyan esetet, amelyben ismert vagy okkal feltételezhető, hogy a támogatási megállapodás értelmében biztosított vagy előállított EU-minősített adatok elvesztek vagy illetéktelen személyek tudomására jutottak.

([2]) A Bizottság (EU, Euratom) 2015/444 határozata (2015. március 13.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 72., 2015.3.17., 53. o.).

([3]) A támogatást nyújtó hatóság a végrehajtási szabályok elfogadását követően beilleszti a hivatkozásokat.

8. A támogatási megállapodás lejártával a kedvezményezett vagy alvállalkozó a birtokában lévő EU-minősített adatokat köteles a lehető leghamarabb visszajuttatni a támogatást nyújtó hatósághoz. A kedvezményezett vagy alvállalkozó az EU-minősített adatokat a visszajuttatás helyett meg is semmisítheti (amennyiben kivitelezhető). Ezt a kedvezményezett székhelye szerinti országban érvényes nemzeti törvényi és rendeleti rendelkezéseknek megfelelően kell megtenni a Bizottság biztonsági hatóságának előzetes engedélyével és az utasításainak megfelelően. Az EU-minősített adatokat úgy kell megsemmisíteni, hogy azokat sem részben, sem egészben ne lehessen helyreállítani.

9. Amennyiben a kedvezményezett vagy alvállalkozó a támogatási megállapodás felmondását vagy lejártát követően megtarthatja az EU-minősített adatokat, azokat továbbra is védeni kell az (EU, Euratom) 2015/444 határozatnak és annak végrehajtási szabályainak ([4]) megfelelően.

10. Az EU-minősített adatok elektronikus kezelése, feldolgozása és továbbítása esetében meg kell felelni az (EU, Euratom) 2015/444 bizottsági határozat 5. és 6. fejezetében meghatározott rendelkezéseknek. Idetartozik többek között az a követelmény, hogy a kedvezményezett tulajdonában lévő és a támogatási megállapodás teljesítése céljából az EU-minősített adatok kezelésére használt kommunikációs és információs rendszerek (a továbbiakban: a kedvezményezett kommunikációs és információs rendszere) akkreditáció tárgyát képezik ([5]); elektronikus továbbítás esetén az EU-minősített adatok védelmét az (EU, Euratom) 2015/444 bizottsági határozat 36. cikkének (4) bekezdésével összhangban jóváhagyott kriptográfiai termékekkel kell biztosítani, és az (EU, Euratom) 2015/444 bizottsági határozat 36. cikke (6) bekezdésének megfelelően TEMPEST biztonsági intézkedéseket kell végrehajtani.

11. A kedvezményezettnek vagy alvállalkozónak üzletmenet-folytonossági tervvel kell rendelkeznie a minősített támogatási megállapodás teljesítésével kapcsolatban kezelt EU-minősített adatok szükséghelyzeti védelme érdekében, és megelőző és helyreállító intézkedéseket kell hoznia az EU-minősített adatok kezelésével és tárolásával kapcsolatos események hatásának minimalizálása érdekében. A kedvezményezettnek vagy alvállalkozónak tájékoztatnia kell a támogatást nyújtó hatóságot az üzletmenet-folytonossági tervéről.

A RESTREINT UE/EU RESTRICTED MINŐSÍTÉSŰ ADATOKHOZ VALÓ HOZZÁFÉRÉST IGÉNYLŐ TÁMOGATÁSI MEGÁLLAPODÁSOK

12. A támogatási megállapodás teljesítéséhez elvileg nincs szükség személyi biztonsági tanúsítványra ([6]). Ugyanakkor a RESTREINT UE/EU RESTRICTED minősítésű adatokhoz vagy anyagokhoz csak a kedvezményezett olyan alkalmazottja férhet hozzá, akinek szüksége van az ilyen adatokra a támogatási megállapodás teljesítéséhez (*a szükséges ismeret elve*), akit a kedvezményezett biztonsági tisztviselője tájékoztatott a feladatairól és az ilyen adatok tekintetében a biztonsági szabályok megsértésének következményeiről, és aki írásban tudomásul vette, hogy milyen következményekkel jár az EU-minősített adatok védelmének elmulasztása.

13. A kedvezményezett vagy alvállalkozó csak a támogatást nyújtó hatóság írásbeli hozzájárulásával biztosít hozzáférést a RESTREINT UE/EU RESTRICTED minősítésű adatokhoz vagy anyagokhoz a saját, a szükséges ismeret elvének hatálya alá eső alkalmazottjain kívüli szervezetek vagy személyek számára.

14. A kedvezményezett vagy alvállalkozó nem változtathatja meg a támogatási megállapodás teljesítése során előállított vagy rendelkezésre bocsátott minősített adatok biztonsági minősítési jelölését, és a támogatást nyújtó hatóság írásbeli hozzájárulása nélkül nem szüntetheti meg az adatok minősítését.

15. A használaton kívüli időszakban a RESTREINT UE/EU RESTRICTED minősítésű adatokat vagy anyagokat zárt irodai szekrényben kell tárolni. Szállítás során a dokumentumokat nem átlátszó borítékban kell tartani. A dokumentumok mindvégig a szállítónál maradnak, és útközben nem nyithatók fel.

([4]) A támogatást nyújtó hatóság a végrehajtási szabályok elfogadását követően beilleszti a hivatkozásokat.

([5]) Az akkreditációt végző félnek a támogatást nyújtó hatóság rendelkezésére kell bocsátania a megfelelőségi nyilatkozatot – a Bizottság biztonsági hatóságán keresztül – a releváns nemzeti biztonsági akkreditációs hatóság koordinálásával.

([6]) Amennyiben a kedvezményezettek tagállama a RESTREINT UE/EU RESTRICTED minősítésű támogatásokhoz személyi biztonsági tanúsítványokat és/vagy telephelybiztonsági tanúsítványokat igényel, a támogatást nyújtó hatóság a biztonsági vonatkozások záradékában felsorolja a szóban forgó kedvezményezettekre vonatkozó követelményeket a személyi biztonsági és telephelybiztonsági tanúsítványokat illetően.

16. A kedvezményezett vagy alvállalkozó kereskedelmi futárszolgálat útján, postaszolgálat útján, kézi szállítással vagy elektronikus úton továbbíthatja a támogatást nyújtó hatóságnak a RESTREINT UE/EU RESTRICTED minősítésű dokumentumokat. A kedvezményezett vagy alvállalkozó ennek érdekében követi a Bizottság által kiadott programbiztonsági (vagy projektbiztonsági) utasításokat és/vagy a minősített támogatások tekintetében az iparbiztonságra vonatkozó bizottsági végrehajtási szabályokat ([7]).

17. Amikor már nincs szükség rájuk, a RESTREINT UE/EU RESTRICTED minősítésű dokumentumokat úgy kell megsemmisíteni, hogy ne lehessen őket sem részben, sem egészben helyreállítani.

18. A kedvezményezett RESTREINT UE/EU RESTRICTED szintű EU-minősített adatokat kezelő kommunikációs és információs rendszerének és az összekapcsolásnak a biztonsági akkreditációja – amennyiben a nemzeti törvényi és rendeleti rendelkezések azt lehetővé teszik – átruházható a kedvezményezett biztonsági tisztviselőjére. Az akkreditáció ilyen átruházása esetén továbbra is a nemzeti biztonsági hatóságok, a kijelölt biztonsági hatóságok vagy a biztonsági akkreditációs hatóságok felelősek a kedvezményezett által kezelt, RESTREINT UE/EU RESTRICTED minősítésű adatok védelméért, és joguk van megvizsgálni a kedvezményezett által hozott biztonsági intézkedéseket. A kedvezményezett emellett bemutatja a támogatást nyújtó hatóságnak – és amennyiben a nemzeti törvényi és rendeleti rendelkezések előírják, az illetékes nemzeti biztonsági akkreditációs hatóságnak – a megfelelőségi nyilatkozatot, amely tanúsítja, hogy a kedvezményezett kommunikációs és információs rendszere és az összekapcsolás akkreditációval rendelkezik a RESTREINT UE/EU RESTRICTED szintű EU-minősített adatok kezelésére.

A RESTREINT UE/EU RESTRICTED MINŐSÍTÉSŰ ADATOK KEZELÉSE A KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZEREKBEN

19. A RESTREINT UE/EU RESTRICTED minősítésű adatokat kezelő kommunikációs és információs rendszerekre vonatkozó minimumkövetelményeket e biztonsági vonatkozások záradékának E. függeléke tartalmazza.

MILYEN FELTÉTELEK MELLETT VEHET IGÉNYBE ALVÁLLALKOZÓKAT A KEDVEZMÉNYEZETT?

20. Mielőtt a kedvezményezett a minősített támogatási megállapodás bármely részét alvállalkozásba adná, be kell szereznie a támogatást nyújtó hatóság engedélyét.

21. A nem uniós országban bejegyzett vállalatok és a nemzetközi szervezethez tartozó szervezetek nem vehetők igénybe alvállalkozóként, ha az adott nem uniós tagállam vagy nemzetközi szervezet nem kötött adatbiztonsági megállapodást az EU-val vagy igazgatási megállapodást a Bizottsággal.

22. Amennyiben a kedvezményezett alvállalkozókat vesz igénybe, a támogatási megállapodás biztonsági rendelkezései értelemszerűen az alvállalkozóra és alkalmazottjaira is vonatkoznak. Ebben az esetben a kedvezményezettnek kell biztosítania, hogy valamennyi alvállalkozó alkalmazza ezeket az alapelveket a saját alvállalkozói megállapodásaiban. A megfelelő biztonsági felügyelet biztosítása érdekében a Bizottság biztonsági hatósága értesíti a kedvezményezett és az alvállalkozó nemzeti biztonsági hatóságát és/vagy kijelölt biztonsági hatóságát a CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET szintű minősített alvállalkozói szerződések odaítéléséről. Adott esetben a kedvezményezett és az alvállalkozó nemzeti biztonsági hatósága és/vagy kijelölt biztonsági hatósága rendelkezésére kell bocsátani az alvállalkozói szerződéssel kapcsolatos biztonsági rendelkezések másolatát. A minősített támogatási megállapodások tekintetében az iparbiztonságra vonatkozó bizottsági végrehajtási szabályok melléklete felsorolja azokat a nemzeti biztonsági hatóságokat és kijelölt biztonsági hatóságokat, amelyeket értesíteni kell a RESTREINT UE/EU RESTRICTED szintű minősített támogatási megállapodások biztonsági rendelkezéseiről ([8]).

23. A kedvezményezett a támogatást nyújtó hatóság előzetes írásbeli jóváhagyása nélkül nem bocsáthatja az alvállalkozó rendelkezésére az EU-minősített adatokat. Ha az alvállalkozók gyakran vagy rutinszerűen kapnak EU-minősített adatokat, a támogatást nyújtó hatóság adott időtartamra (például 12 hónapra) vagy az alvállalkozói szerződés érvényességének időtartamára is megadhatja a jóváhagyását.

([7]) A támogatást nyújtó hatóság a végrehajtási szabályok elfogadását követően beilleszti a hivatkozásokat.
([8]) A támogatást nyújtó hatóság a végrehajtási szabályok elfogadását követően beilleszti a hivatkozásokat.

LÁTOGATÁSOK

Ha a szabványos látogatási kérelmi eljárás a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat érintő látogatásokra vonatkozik, a támogatást nyújtó hatóságnak fel kell tüntetnie a 24., a 25. és a 26. pontot, és el kell hagynia a 27. pontot. Ha a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat érintő látogatásokat közvetlenül a küldő és fogadó létesítmény szervezi meg egymás között, a támogatást nyújtó hatóságnak el kell hagynia a 25. és a 26. pontot, és csak a 27. pontot kell feltüntetnie.

24. A RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáféréssel vagy potenciális hozzáféréssel járó látogatásokat a küldő és a fogadó létesítménynek kell közvetlenül megszerveznie, és e látogatások tekintetében nem kell követni a 25–27. pontban leírt eljárásokat.

[25. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáféréssel vagy potenciális hozzáféréssel járó látogatásokat az alábbi eljárásnak megfelelően kell megszervezni:

a) látogatót küldő telephely biztonsági tisztviselője kitölti látogatási kérelemre vonatkozó formanyomtatvány releváns részét (C. függelék), és benyújtjkérelmet telephely nemzeti biztonsági hatóságának vagy kijelölt biztonsági hatóságának;

b) látogatási kérelemnek fogadó telephely nemzeti biztonsági hatóságánál vagy kijelölt biztonsági hatóságánál (vagy támogatást nyújtó hatóság létesítményeiben tett látogatás esetén Bizottság biztonsági hatóságánál) történő benyújtáselőtt küldő telephely nemzeti biztonsági hatóságvagy kijelölt biztonsági hatóságmegerősíti látogató személyi biztonsági tanúsítványát;

c) küldő telephely biztonsági tisztviselője nemzeti biztonsági hatóságától vagy kijelölt biztonsági hatóságától megszerzi fogadó telephely nemzeti biztonsági hatóságának vagy kijelölt biztonsági hatóságának (vagy Bizottság biztonsági hatóságának) válaszát, amely jóváhagyjvagy elutasítjlátogatási kérelmet;

d) látogatási kérelem akkor tekintendő jóváhagyottnak, hlátogatás időpontját megelőző ötödik munkanapig nem érkezik ellenvetés.]

[26. Mielőtt a látogató hozzáférést kap a CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz, a fogadó telephelynek meg kell szereznie a nemzeti biztonsági hatósága vagy kijelölt biztonsági hatósága engedélyét.]

[27. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz való hozzáféréssel vagy potenciális hozzáféréssel járó látogatásokat a küldő és a fogadó létesítménynek kell közvetlenül megszerveznie (az erre a célra használható formanyomtatvány mintáját a C. függelék tartalmazza).]

28. A látogatóknak a fogadó telephelyre való érkezésükkor érvényes személyazonosító igazolvánnyal vagy útlevéllel kell igazolniuk személyazonosságukat.

29. A látogatót fogadó telephelynek gondoskodnia kell arról, hogy valamennyi látogató szerepeljen a nyilvántartásban. A nyilvántartásban fel kell tüntetni a nevet, a képviselt szervezetet, (adott esetben) a személyi biztonsági tanúsítvány érvényességének lejártát, a látogatás dátumát és a meglátogatott személy nevét. Az európai adatvédelmi szabályok sérelme nélkül az ilyen nyilvántartásokat legalább öt évig vagy adott esetben a nemzeti szabályoknak és jogszabályi rendelkezéseknek megfelelően meg kell őrizni.

ÉRTÉKELŐ LÁTOGATÁSOK

30. A Bizottság biztonsági hatósága – az érintett nemzeti biztonsági hatósággal vagy kijelölt biztonsági hatósággal együttműködve – felkeresheti a kedvezményezettek vagy az alvállalkozók telephelyeit, hogy ellenőrizze az EU-minősített adatok kezelésére vonatkozó biztonsági követelmények teljesítését.

BIZTONSÁGI MINŐSÍTÉSI ÚTMUTATÓ

31. A biztonsági minősítési útmutató tartalmazza a támogatási megállapodás valamennyi olyan elemének felsorolását, amely minősített, vagy amelyet minősíteni kell a támogatási megállapodás teljesítése során, továbbá az erre vonatkozó szabályokat és az alkalmazandó biztonsági minősítési szintek leírását. A biztonsági minősítési útmutató e támogatási megállapodás szerves részét képezi, és megtalálható e melléklet B. függelékében.

B. függelék

BIZTONSÁGI MINŐSÍTÉSI ÚTMUTATÓ

[a konkrét szöveg a támogatási megállapodás tárgyától függően módosítandó]

C. függelék

LÁTOGATÁSI KÉRELEM (MINTA)

RÉSZLETES UTASÍTÁSOK A LÁTOGATÁSI KÉRELEM KITÖLTÉSÉHEZ

(A kérelem csak angol nyelven nyújtható be.)

HEADING	Jelölje meg a látogatás típusának és az adat típusának megfelelő négyzetet, és adja meg a felkeresendő helyek és a látogatók számát.
4. **ADMINISTRATIVE DATA**	A kérelmet benyújtó nemzeti biztonsági hatóság/kijelölt biztonsági hatóság tölti ki.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Adja meg a teljes nevet és a postacímet. Adott esetben adja meg a várost, az államot és a postai irányítószámot.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Adja meg a teljes nevet és a postacímet. Adja meg a várost, az államot, a postai irányítószámot, a telex- vagy faxszámot (adott esetben), a telefonszámot és az e-mail-címet. Adja meg a fő kapcsolattartó vagy annak a személynek a nevét és telefonszámát/faxszámát, valamint e-mail-címét, akivel megbeszélte a látogatást. Megjegyzések: 1) A helyes postai irányítószám megadása fontos, mert egy vállalatnak több különböző telephelye lehet. 2) Manuális kérelem esetén az 1. melléklet használható, ha ugyanazzal a témával kapcsolatban két vagy több telephelyet kell meglátogatni. Melléklet használata esetén a 3. pont szövege: „SEE ANNEX 1, NUMBER OF FAC.:..” (tüntesse fel a telephelyek számát).
7. **DATES OF VISIT (A látogatás napja)**	Adja meg a látogatás tényleges dátumát vagy időszakát (kezdő- és zárónapját) „nap – hónap – év” formátumban. Adott esetben zárójelben adjon meg egy másik dátumot vagy időszakot.
8. **TYPE OF INITIATIVE**	Adja meg, hogy a látogatást a kérelmező szervezet vagy telephely kezdeményezte vagy a meglátogatandó telephely meghívására kerül rá sor.
9. **THE VISIT RELATES TO:**	Adja meg a projekt, a szerződés vagy az ajánlati felhívás teljes nevét, kizárólag a gyakran használt rövidítések alkalmazásával.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Röviden ismertesse a látogatás okát. Ne használjon nem feloldott rövidítéseket. Megjegyzések: Ismétlődő látogatások esetén ebben a pontban az adatelem elején a „Recurring visits” szövegnek kell szerepelnie (például „Recurring visits to discuss_____”).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Lehetséges válaszok: SECRET UE/EU SECRET (S-UE/EU-S) vagy CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), a megfelelőt meg kell adni.

12. **PARTICULARS OF VISITOR**	Megjegyzés: ha kettőnél több látogató vesz részt a látogatáson, a 2. mellékletet kell használni.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Itt a kérelmező telephely biztonsági tisztviselőjének nevét, telefonszámát, faxszámát és e-mail-címét kell megadni.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Ezt a mezőt a tanúsító hatóság tölti ki. Megjegyzések a tanúsító hatóság számára: a) Adja meg a nevet, címet, telefonszámot, faxszámot és e-mail-címet (lehet előre nyomtatott formában). b) Ezt a pontot alá kell írni és bélyegzővel kell ellátni (adott esetben).
15. **REQUESTING SECURITY AUTHORITY**	Ezt a mezőt a nemzeti biztonsági hatóság/kijelölt biztonsági hatóság tölti ki. Megjegyzés a nemzeti biztonsági hatóság/kijelölt biztonsági hatóság számára: a) Adja meg a nevet, címet, telefonszámot, faxszámot és e-mail-címet (lehet előre nyomtatott formában). b) Ezt a pontot alá kell írni és bélyegzővel kell ellátni (adott esetben).

Minden mezőt ki kell tölteni, és a formanyomtatványt kormányközi csatornákon kell elküldeni ([9]).

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**	
Requester: To:	NSA/DSA RFV Reference No_____ Date *(dd/mm/yyyy)*: _____/_____/_____

([9]) Ha olyan megállapodás született, hogy közvetlenül megszervezhetők a CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET szintű EU-minősített adatokhoz való hozzáféréssel vagy potenciális hozzáféréssel járó látogatások, a kitöltött formanyomtatvány közvetlenül benyújtható a meglátogatandó létesítmény biztonsági tisztviselőjének.

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED *(Annex 1 to be completed)***

7. **DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____**

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):**

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S) *(Annex 2 to be completed)***

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

DATE *(dd/mm/yyyy)*:
_____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE:

DATE *(dd/mm/yyyy)*:
_____/_____/_____

16. **REMARKS *(Mandatory justification required in the case of an emergency visit)*:**

<A személyes adatokról szóló hatályos jogszabályokra való hivatkozás helye, illetve az érintett kötelező tájékoztatásával kapcsolatos hivatkozás helye, például hogyan kerül sor az általános adatvédelmi rendelet ([10]) 13. cikkének végrehajtására.>

([10]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, HL L 119., 2016.5.4., 1. o.).

ANNEX 1 to RFV FORM (A LÁTOGATÁSI KÉRELEMRE VONATKOZÓ FORMANYOMTATVÁNY 1. MELLÉKLETE)

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

<A személyes adatokról szóló hatályos jogszabályokra való hivatkozás helye, illetve az érintett kötelező tájékoztatásával kapcsolatos hivatkozás helye, például hogyan kerül sor az általános adatvédelmi rendelet ([11]) 13. cikkének végrehajtására.>

([11]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, HL L 119., 2016.5.4., 1. o.).

ANNEX 2 to RFV FORM (A LÁTOGATÁSI KÉRELEMRE VONATKOZÓ FORMANYOMTATVÁNY 2. MELLÉKLETE)

PARTICULARS OF VISITOR(S)
1. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
2. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION: ***(Continue as required)***

<A személyes adatokról szóló hatályos jogszabályokra való hivatkozás helye, illetve az érintett kötelező tájékoztatásával kapcsolatos hivatkozás helye, például hogyan kerül sor az általános adatvédelmi rendelet ([12]) 13. cikkének végrehajtására.>

([12]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, HL L 119., 2016.5.4., 1. o.).

D. függelék

A TELEPHELYBIZTONSÁGI TANÚSÍTVÁNYRA VONATKOZÓ ADATLAP (MINTA)

1. **BEVEZETÉS**

1.1 Mellékelve megtalálható a nemzeti biztonsági hatóság vagy a kijelölt biztonsági hatóság, az egyéb illetékes nemzeti biztonsági hatóságok és (a támogatást nyújtó hatóságok képviseletében) a Bizottság biztonsági hatósága közötti gyors információcserére szolgáló, a telephelybiztonsági tanúsítványra vonatkozó adatlap mintája a minősített támogatásokban vagy alvállalkozói szerződésekben érintett telephelyek telephelybiztonsági tanúsítványa tekintetében.

1.2. A telephelybiztonsági tanúsítványra vonatkozó adatlap csak az érintett nemzeti biztonsági hatóság, a kijelölt biztonsági hatóság vagy egyéb illetékes hatóság bélyegzőjével ellátva érvényes.

1.3. A telephelybiztonsági tanúsítványra vonatkozó adatlap a kérelemre és a válaszra osztható, és a fenti célokra vagy egyéb olyan célokra használható, amikor szükség van egy adott telephely telephelybiztonsági tanúsítvánnyal kapcsolatos státuszára. A kérelmező nemzeti biztonsági hatóság vagy kijelölt biztonsági hatóság a kérelemre vonatkozó szakasz 7. mezőjében meghatározza a kérelem okát.

1.4. A telephelybiztonsági tanúsítványra vonatkozó adatlapon szereplő részletek általában nem minősített adatok, így ennek megfelelően, ha szükség van az adatlap küldésére a nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságok/a Bizottság között, ezt lehetőség szerint elektronikus úton kell megoldani.

1.5. A nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságok mindent elkövetnek, hogy 10 munkanapon belül válaszoljanak a telephelybiztonsági tanúsítvány iránti kérelemre.

1.6. Amennyiben ezzel kapcsolatban minősített adatok továbbítására vagy támogatás vagy alvállalkozói szerződés odaítélésére kerül sor, tájékoztatni kell a tanúsítványt kiállító nemzeti biztonsági hatóságot vagy kijelölt biztonsági hatóságot.

Eljárások és utasítások a telephelybiztonsági tanúsítványra vonatkozó adatlap használatára vonatkozóan

Az alábbi részletes utasítások annak a nemzeti biztonsági hatóságnak vagy kijelölt biztonsági hatóságnak, illetve a támogatást nyújtó hatóságnak és a Bizottság biztonsági hatóságának szólnak, amely kitölti a telephelybiztonsági tanúsítványra vonatkozó adatlapot. A kérelmet lehetőleg nyomtatott nagybetűkkel kell kitölteni.

FEJLÉC	A kérelmező beilleszti a nemzeti biztonsági hatóság/kijelölt biztonsági hatóság és az ország teljes nevét.
1. **A KÉRELEM TÍPUSA**	A kérelmet benyújtó támogatást nyújtó hatóság bejelöli a telephelybiztonsági tanúsítványra vonatkozó adatlap tárgyát képező kérelem típusának megfelelő négyzetet. Fel kell tüntetni a kérelmezett biztonsági minősítési szintet. Az alábbi rövidítéseket kell használni: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = A minősített adatok kezelésére szolgáló kommunikációs és információs rendszerek.
2. **A TÁRGY RÉSZLETEI**	Az 1–6. mező magától értetődő. A 4. mezőben a szabványos, kétbetűs országkódot kell használni. Az 5. mező opcionális.
3. **A KÉRELEM INDOKA**	Tüntess fel a kérelem konkrét okát, adja meg a projektmutatókat, az ajánlati felhívás vagy a támogatás számát. Határozza meg a tárolási kapacitás iránti igényt, a kommunikációs és információs rendszer minősítési szintjét stb. Fel kell tüntetni minden olyan határidőt/lejárati napot/odaítélési dátumot, amely befolyásolhatja a telephelybiztonsági tanúsítvány kiállítását.

4. **A KÉRELMEZŐ NEMZETI BIZTONSÁGI HATÓSÁG/KIJELÖLT BIZTONSÁGI HATÓSÁG**	Adja meg a (nemzeti biztonsági hatóság/kijelölt biztonsági hatóság nevében eljáró) kérelmező nevét, illetve számokkal (nn/hh/éééé) a kérelem dátumát.
5. **VÁLASZSZAKASZ**	1–5. mező: válassza ki a megfelelő mezőt. 2. mező: ha a telephelybiztonsági tanúsítvány kiállítása folyamatban van, ajánlott a kérelmező tudomására hozni (amennyiben ez az információ ismert) a feldolgozáshoz szükséges időt. 6. mező: a) Habár országonként vagy akár telephelyenként eltér a hitelesítés, ajánlott megadni a telephelybiztonsági tanúsítvány érvényességének lejártát. b) Azokban az esetekben, amikor a telephelybiztonsági tanúsítványról szóló igazolás korlátlan érvényességgel rendelkezik, ez a mező kihúzható. c) A vonatkozó nemzeti szabályoknak és jogszabályi rendelkezéseknek megfelelően a kedvezményezett vagy az alvállalkozó feladata a telephelybiztonsági tanúsítvány meghosszabbításának kérvényezése.
6. **MEGJEGYZÉSEK**	A telephelybiztonsági tanúsítvánnyal, a telephellyel vagy a fentiekkel kapcsolatos további információk feltüntetésére használható.
7. **A KIBOCSÁTÓ NEMZETI BIZTONSÁGI HATÓSÁG/KIJELÖLT BIZTONSÁGI HATÓSÁG**	Adja meg a (nemzeti biztonsági hatóság/kijelölt biztonsági hatóság nevében eljáró) kiállító hatóság nevét és szám formátumban (éééé/hh/nn) a válasz dátumát.

A TELEPHELYBIZTONSÁGI TANÚSÍTVÁNYRA VONATKOZÓ ADATLAP (MINTA)

Minden mezőt ki kell tölteni, és a formanyomtatványt kormányközi csatornákon vagy kormányok és nemzetközi szervezetek közötti csatornákon kell továbbítani.

A TELEPHELYBIZTONSÁGI TANÚSÍTVÁNNYAL KAPCSOLATOS IGAZOLÁSRA VONATKOZÓ KÉRELEM

TO: _____

(a nemzeti biztonsági hatóság/kijelölt biztonsági hatóság országa)

Kérjük, hogy adott esetben jelölje be a választ:

[ ] telephelybiztonsági tanúsítvánnyal kapcsolatos igazolás az alábbi szinten: [ ] S-UE/EU-S [ ] C-UE/EU-C

a lent megnevezett telephely számára

[ ] Beleértve minősített anyagok/adatok védelmét

[ ] Beleértve a minősített adatok kezelésére szolgáló kommunikációs és információs rendszereket

[ ] Közvetlenül vagy a kedvezményezett/alvállalkozó kérésére benyújtott, telephelybiztonsági tanúsítvány kiállítására vonatkozó kérelem ..... szinttel bezárólag, ... szintű védelemmel és ..... szintű kommunikációs és információs rendszerrel, ha a telephely jelenleg nem rendelkezik ezekkel a minősítésekkel.

Erősítse meg a telephellyel kapcsolatban lent megadott információkat, és szükség esetén javítsa ki/egészítse ki őket.

1. A telephely teljes neve:	Javítások/kiegészítések:
.....	.....
2. A telephely teljes címe:	
.....	.....
3. Postázási cím (ha eltér a 2. pontban megadott címtől):	
.....	.....
4. Postai irányítószám/város/ország:	
.....	.....
5. A biztonsági tisztviselő neve:	
.....	
.....	
6. A biztonsági tisztviselő telefonszáma/faxszáma/e-mail-címe:	
.....	.....
7. A kérés oka: (részletesen ismertesse a szerződést megelőző [az ajánlatkiválasztási] szakaszt, a támogatási megállapodást vagy alvállalkozói szerződést, a programot/projektet stb.):	
.....	

A kérelmező nemzeti biztonsági hatóság/kijelölt biztonsági hatóság/engedélyező hatóság: Név: .....

Dátum: (éééé/hh/nn) .....

VÁLASZ (10 munkanapon belül)

Igazoljuk, hogy

1. [ ] a fent említett telephely telephelybiztonsági tanúsítvánnyal rendelkezik [ ] S-UE/EU-S

   [ ] C-UE/EU-C szinttel bezárólag;

2. a fent említett telephely képes garantálni a minősített adatok/anyagok biztonságát:

   [ ] igen, szint: ..... [ ] nem.

3. a fent említett telephely akkreditált/jóváhagyott kommunikációs és információs rendszerrel rendelkezik:

   [ ] igen, szint: .... [] nem.

4. [ ] a fent említett kérelem vonatkozásában telephelybiztonsági tanúsítvány iránti eljárás kezdeményezésére került sor. Tájékoztatni fogjuk a telephelybiztonsági tanúsítvány kiállításakor vagy elutasításakor;

5. [ ] a fent említett telephely nem rendelkezik telephelybiztonsági tanúsítvánnyal.

6. A telephelybiztonsági tanúsítvány igazolása lejár: ..... (*éééé/hh/nn*) vagy a nemzeti biztonsági hatóság/kijelölt biztonsági hatóság által javasolt időpontban. Korábbi érvénytelenítés vagy a fenti információk bárminemű változása esetén tájékoztatjuk.

7. Megjegyzések:
   .....

*A kibocsátó nemzeti biztonsági hatóság/kijelölt biztonsági hatóság*Név: .....

Dátum (év/hónap/nap): .....

<A személyes adatokról szóló hatályos jogszabályokra való hivatkozás helye, illetve az érintett kötelező tájékoztatásával kapcsolatos hivatkozás helye, például hogyan kerül sor az általános adatvédelmi rendelet ([13]) 13. cikkének végrehajtására.>

([13]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, HL L 119., 2016.5.4., 1. o.).

E. függelék

A kedvezményezett kommunikációs és információs rendszerében kezelt RESTREINT UE/EU RESTRICTED szintű elektronikus EU-minősített adatok védelmére vonatkozó minimumkövetelmények

Általános előírások

1. A kedvezményezettnek biztosítania kell, hogy a RESTREINT UE/EU RESTRICTED minősítésű adatok védelme megfeleljen az ebben a biztonsági kikötésben ismertetett biztonsági minimumkövetelményeknek és az ajánlatkérő szerv vagy adott esetben a nemzeti biztonsági hatóság vagy a kijelölt biztonsági hatóság által ajánlott egyéb követelményeknek.

2. Az e dokumentumban meghatározott biztonsági követelmények teljesülésének biztosítása a kedvezményezett feladata.

3. E dokumentum alkalmazásában a „kommunikációs és információs rendszer” fogalma magában foglalja az EU-minősített adatok kezelésére, tárolására és továbbítására szolgáló valamennyi berendezést és készüléket, beleértve a munkaállomásokat, a nyomtatókat, a fénymásolókat, a faxgépeket, a szervereket, a hálózatkezelő rendszereket, a hálózatvezérlőket és a kommunikációs vezérlőket, a laptopokat, a notebookokat, a táblagépeket, az okostelefonokat és a hordozható tárolóeszközöket, például a pendrive-okat, a CD-ket, az SD-kártyákat stb. is.

4. A speciális berendezések és készülékek, például a kriptográfiai termékek védelmét a rájuk vonatkozó biztonsági üzemeltetési eljárásoknak megfelelően kell biztosítani.

5. A kedvezményezettnek létre kell hoznia a RESTREINT UE/EU RESTRICTED minősítésű adatokat kezelő kommunikációs és információs rendszer biztonságos üzemeltetéséért felelős struktúrát, és ki kell jelölnie az érintett telephelyért felelős biztonsági tisztviselőt.

6. A kedvezményezett személyzetének magántulajdonát képező IT-megoldások (hardver, szoftver vagy szolgáltatások) használata nem megengedett a RESTREINT UE/EU RESTRICTED minősítésű adatok tárolására vagy feldolgozására.

7. A kedvezményezett RESTREINT UE/EU RESTRICTED minősítésű adatokat kezelő kommunikációs és információs rendszerének akkreditációját vagy az érintett tagállam biztonsági akkreditációs hatóságának kell jóváhagynia, vagy pedig, amennyiben azt a nemzeti törvényi és rendeleti rendelkezések lehetővé teszik, ezt a feladatot a kedvezményezett biztonsági tisztviselőjére kell átruházni.

8. A támogatási megállapodás hatálya alá tartozó egyéb, nem minősített adatokkal azonos módon csak a jóváhagyott kriptográfiai termékekkel titkosított RESTREINT UE/EU RESTRICTED minősítésű adatok kezelhetők, tárolhatók vagy továbbíthatók (vezetékes vagy vezeték nélküli technikával). Az ilyen kriptográfiai termékeket az EU-nak vagy valamely tagállamnak jóvá kell hagynia.

9. A karbantartásban/javításban részt vevő külső telephelyeknek szerződésben kell kötelezniük magukat arra, hogy az ebben a dokumentumban foglaltaknak megfelelően betartják a RESTREINT UE/EU RESTRICTED minősítésű adatok kezelésére vonatkozó rendelkezéseket.

10. A támogatást nyújtó hatóság vagy az érintett nemzeti biztonsági hatóság/kijelölt biztonsági hatóság/biztonsági akkreditációs hatóság kérésére a kedvezményezettnek igazolnia kell, hogy eleget tesz a támogatási megállapodás biztonsági kikötésének. Ha a kérésnek a kedvezményezettek folyamataira és telephelyeire vonatkozó ellenőrzés vagy kivizsgálás is tárgya, akkor e követelmények teljesülésének biztosítása érdekében a kedvezményezettek lehetővé teszik a támogatást nyújtó hatóság, a nemzeti biztonsági hatóság, a kijelölt biztonsági hatóság és/vagy a biztonsági akkreditációs hatóság vagy az érintett uniós biztonsági hatóság képviselői számára az ellenőrzés vagy kivizsgálás elvégzését.

Fizikai biztonság

11. Megfelelő belépés-ellenőrző rendszerrel felszerelt, különálló, ellenőrzött területként kell létrehozni azokat a területeket, ahol a RESTREINT UE/EU RESTRICTED minősítésű adatok megjelenítésére, tárolására, feldolgozására vagy továbbítására szolgáló kommunikációs és információs rendszerek működnek, valamint azokat a területeket, ahol az ilyen kommunikációs és információs rendszerek szerverei, hálózatkezelő rendszerei, hálózatvezérlői és kommunikációs vezérlői találhatók. Az ezekre a különálló és ellenőrzött területekre való belépést csak a megfelelő engedéllyel rendelkező személyek számára szabad lehetővé tenni. A 8. pont sérelme nélkül a 3. pontban meghatározott berendezéseket és eszközöket ilyen különálló és ellenőrzött területeken kell tárolni.

12. Létre kell hozni olyan biztonsági mechanizmusokat és/vagy eljárásokat, amelyek szabályozzák a kommunikációs és információs rendszer alkotóelemeinek hordozható számítógépes adathordozókkal (például pendrive-okkal, nagy háttértárolókkal vagy újraírható kompakt lemezekkel [CD-RW]) való bővítését vagy ilyen eszközökhöz való csatlakoztatását.

Hozzáférés a kommunikációs és információs rendszerhez

13. A kedvezményezett EU-minősített adatokat kezelő kommunikációs és információs rendszeréhez való hozzáférés szigorúan a szükséges ismeret elve alapján és a személyzet erre történő felhatalmazásával engedélyezett.

14. Minden kommunikációs és információs rendszernek rendelkeznie kell az engedélyezett felhasználók naprakész listájával. Minden feldolgozási munkamenet kezdetén minden felhasználót hitelesíteni kell.

15. A legtöbb azonosítási és hitelesítési célú biztonsági intézkedés részét képező jelszavaknak legalább kilenc karakterből kell állniuk, és számokat, speciális karaktereket (amennyiben a rendszer ezt engedélyezi) és betűket kell tartalmazniuk. A jelszavakat legalább 180 naponta meg kell változtatni. A jelszavakat a lehető leghamarabb meg kell változtatni, ha illetéktelenek tudomására jutnak, vagy fennáll ennek gyanúja.

16. Minden kommunikációs és információs rendszernek belső hozzáférés-ellenőrzéssel kell rendelkeznie annak megakadályozására, hogy illetéktelenek hozzáférjenek a RESTREINT UE/EU RESTRICTED minősítésű adatokhoz vagy módosítsák őket, vagy módosítsák a rendszer- és a biztonsági ellenőrző funkciókat. Ha a terminál meghatározott ideig inaktív, a felhasználókat automatikus ki kell léptetni a kommunikációs és információs rendszerből vagy a kommunikációs és információs rendszernek 15 perc inaktivitás után be kell kapcsolnia egy jelszóval védett képernyővédőt.

17. A kommunikációs és információs rendszer minden felhasználójának egyedi felhasználói fiókkal és azonosítóval kell rendelkeznie. A felhasználói fiókokat, legalább öt egymást követő helytelen bejelentkezési kísérletet követően automatikusan le kell zárni.

18. A kommunikációs és információs rendszer valamennyi felhasználójának tisztában kell lennie felelősségével, és ismernie kell a RESTREINT UE/EU RESTRICTED minősítésű adatoknak a kommunikációs és információs rendszerben történő védelme érdekében követendő eljárásokat. A felelősség tartalmát és a követendő eljárásokat írásban dokumentálni kell, és a felhasználóknak írásban nyilatkozniuk kell azok tudomásulvételéről.

19. A biztonsági üzemeltetési eljárásoknak elérhetőknek kell lenniük a felhasználók és az adminisztrátorok számára, és tartalmazniuk kell a biztonsági feladatkörök leírását, valamint a feladatok, utasítások és tervek kapcsolódó jegyzékét.

Számvitel, ellenőrzés és az incidensekre való reagálás

20. A kommunikációs és információs rendszerhez való minden hozzáférést naplózni kell.

21. Az alábbi eseményeket kell rögzíteni:

    a) minden bejelentkezési kísérletet, akár sikeres volt, akár meghiúsult;

    b) kijelentkezés (beleértve adott esetben az időkorlát miatti kiléptetést);

    c) hozzáférési jogok és privilégiumok létrehozása, törlése vagy módosítása;

    d) jelszavak létrehozása, törlése vagy módosítása.

22. A fent említett események tekintetében legalább az alábbi információkat meg kell adni:

    a) az esemény típusa;

    b) felhasználói azonosító;

    c) dátum és időpont;

    d) a készülék azonosítója.

23. A számviteli nyilvántartások a biztonsági tisztviselő segítségére vannak a lehetséges biztonsági incidensek kivizsgálása során. Emellett biztonsági incidensek esetében a jogi vizsgálatok támogatására is felhasználhatók. Valamennyi biztonsági nyilvántartást rendszeresen ellenőrizni kell a lehetséges biztonsági incidensek azonosítása céljából. A számviteli nyilvántartásokat védeni kell a jogosulatlan törléstől és módosításoktól.

24. A kedvezményezettnek a biztonsági incidensekre vonatkozóan kidolgozott válaszstratégiával kell rendelkeznie. Utasításokat kell adni a felhasználók és adminisztrátorok részére az incidensekre való reagálással, az incidensek jelentésével és a szükséghelyzeti teendőkkel kapcsolatban.

25. A RESTREINT UE/EU RESTRICTED minősítésű adatokkal való visszaéléseket vagy feltételezett visszaéléseket jelenteni kell a támogatást nyújtó hatóságnak. A jelentésben fel kell tüntetni az érintett adatok leírását, valamint az adatokkal való visszaélés vagy feltételezett visszaélés körülményeit. A kommunikációs és információs rendszer valamennyi felhasználójának tudnia kell, hogyan kell bejelenteni a tényleges vagy feltételezett biztonsági incidenseket a biztonsági tisztviselőnek.

Hálózatépítés és összekapcsolás

26. Amikor a kedvezményezettnek a RESTREINT UE/EU RESTRICTED minősítésű adatokat kezelő kommunikációs és információs rendszere nem akkreditált kommunikációs és információs rendszerhez kapcsolódik, jelentősen nő a kommunikációs és információs rendszer és az általa kezelt RESTREINT UE/EU RESTRICTED minősítésű adatok biztonságát fenyegető veszély. Idetartozik az internet és egyéb olyan nyilvános vagy magán kommunikációs és információs rendszer, mint például a kedvezményezett vagy alvállalkozó egyéb kommunikációs és információs rendszere. Ebben az esetben a kedvezményezettnek kockázatértékelést kell végeznie annak meghatározására, hogy milyen további biztonsági követelményeket kell végrehajtani a biztonsági akkreditációs folyamat részeként. A kedvezményezett bemutatja a támogatást nyújtó hatóságnak – és amennyiben a nemzeti törvényi és rendeleti rendelkezések előírják, az illetékes biztonsági akkreditációs hatóságoknak – a megfelelőségi nyilatkozatot, amely tanúsítja, hogy a kedvezményezett kommunikációs és információs rendszere és az összekapcsolás akkreditációval rendelkezik a RESTREINT UE/EU RESTRICTED szintű EU-minősített adatok kezelésére.

27. Az egyéb rendszerekből a LAN szolgáltatásokhoz való távoli hozzáférés (például az e-mailekhez való távoli hozzáférés és a távoli rendszertámogatás) csak abban az esetben megengedett, ha a támogatást nyújtó hatósággal egyeztetett – és amennyiben a nemzeti törvényi és rendeleti rendelkezések előírják, az illetékes biztonsági akkreditációs hatóság által jóváhagyott – egyedi biztonsági intézkedések végrehajtására kerül sor.

Konfigurációkezelés

28. Az akkreditációs/jóváhagyási dokumentációban (beleértve a rendszer- és hálózati diagramokat) szereplő részletes hardver- és szoftverkonfigurációnak elérhetőnek kell lennie, és azt rendszeresen karban kell tartani.

29. A kedvezményezett biztonsági tisztviselője ellenőrzi a hardver- és szoftverkonfigurációt, hogy meggyőződjön arról, nem került-e sor jogosulatlan hardver vagy szoftver alkalmazására.

30. A biztonsági tisztviselőnek – és amennyiben a nemzeti törvényi és rendeleti rendelkezések előírják, a biztonsági akkreditációs hatóságnak – a biztonsági következmények szempontjából értékelnie kell a kedvezményezett kommunikációs és információs rendszere konfigurációjának változásait, és jóvá kell hagynia azokat.

31. A rendszert legalább háromhavonta át kell vizsgálni a biztonsági sebezhetőség szempontjából. A rosszindulatú számítógépes programok észlelésére szolgáló szoftvert kell telepíteni, és ezt rendszeresen frissíteni kell. Amennyiben lehetséges, az ilyen szoftvernek nemzeti vagy elismert nemzetközi jóváhagyással kell rendelkeznie, vagy széles körben elfogadott iparági szabványnak kell lennie.

32. A kedvezményezett üzletmenet-folytonossági tervet dolgoz ki. Biztonsági mentési eljárásokat kell kidolgozni az alábbiak tekintetében:

    a) a biztonsági mentések gyakorisága;

    b) helyszíni (tűzálló tárolási lehetőségek) és helyszínen kívüli tárolási követelmények;

    c) a biztonsági mentéshez való engedélyezett hozzáférés ellenőrzése.

Megtisztítás és megsemmisítés

33. A bármikor RESTREINT UE/EU RESTRICTED minősítésű adatokat tartalmazó kommunikációs és információs rendszerek vagy adattároló eszközök esetében az alábbi tisztítást kell elvégezni a teljes rendszeren vagy tárolóeszközön a használata beszüntetését megelőzően:

a) a flash memóriát (például pendrive-ot, SD-kártyát, szilárdtestmeghajtót, hibrid merevlemezt) legalább háromszor felül kell írni, majd ellenőrizni kell, hogy az eredeti tartalom nem állítható vissza, vagy jóváhagyott törlési szoftverrel törölni kell azt;

b) a mágneses adathordozókat (például merevlemezeket) felül kell írni vagy demagnetizálni kell;

c) az optikai eszközöket (például a CD-ket és DVD-ket) fel kell aprítani;

d) bármely egyéb tárolóeszköz esetében konzultálni kell a támogatást nyújtó hatósággal vagy adott esetben a nemzeti biztonsági hatósággal, a kijelölt biztonsági hatósággal vagy a biztonsági akkreditációs hatósággal a biztonsági követelményekről.

34. A RESTREINT UE/EU RESTRICTED minősítésű adatokat minden adathordozón meg kell tisztítani, mielőtt olyan szervekhez kerülnek (például karbantartás céljából), amely nem jogosult a RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáférésre.

IV. MELLÉKLET

A RESTREINT UE/EU RESTRICTED minősítésű adatokat kezelő kedvezményezettek vagy alvállalkozók telephelybiztonsági és személyi biztonsági tanúsítványa és a RESTREINT UE/EU RESTRICTED szintű minősített támogatási megállapodásokról értesítendő nemzeti biztonsági hatóságok/kijelölt biztonsági hatóságok ([1])

Tagállam	TELEPHELYBIZTONSÁGI TANÚSÍTVÁNY		Az R-UE/EU-R minősítésű adatokat érintő támogatási megállapodások vagy alvállalkozói szerződések bejelentése a nemzeti biztonsági hatóságnak és/vagy kijelölt biztonsági hatóságnak		Személyi biztonsági tanúsítvány	
	IGEN	NEM	IGEN	NEM	IGEN	NEM
Belgium		**X**		**X**		**X**
Bulgária		**X**		**X**		**X**
Csehország		**X**		**X**		**X**
Dánia	**X**		**X**		**X**	
Németország		**X**		**X**		**X**
Észtország	**X**		**X**			**X**
Írország		**X**		**X**		**X**
Görögország	**X**			**X**	**X**	
Spanyolország		**X**	**X**			**X**
Franciaország		**X**		**X**		**X**
Horvátország		**X**	**X**			**X**
Olaszország		**X**	**X**			**X**
Ciprus		**X**	**X**			**X**
Lettország		**X**		**X**		**X**
Litvánia	**X**		**X**			**X**
Luxemburg	**X**		**X**		**X**	
Magyarország		**X**		**X**		**X**
Málta		**X**		**X**		**X**
Hollandia	**X** (csak védelmi vonatkozású támogatási megállapodások és alvállalkozói szerződések esetében)		**X** (csak védelmi vonatkozású támogatási megállapodások és alvállalkozói szerződések esetében)			**X**
Ausztria		**X**		**X**		**X**
Lengyelország		**X**		**X**		**X**

([1]) A telephelybiztonsági és személyi biztonsági tanúsítványokra és a RESTREINT UE/EU RESTRICTED minősítésű adatokat érintő támogatási megállapodások bejelentésére vonatkozó nemzeti követelmények nem róhatnak további kötelezettségeket más tagállamokra vagy a joghatóságuk alatt álló kedvezményezettekre.
N.B. A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat érintő támogatási megállapodások bejelentése kötelező.

Portugália		**X**		**X**		**X**
Románia		**X**		**X**		**X**
Szlovénia	**X**		**X**			**X**
Szlovákia	**X**		**X**			**X**
Finnország		**X**		**X**		**X**
Svédország		**X**		**X**		**X**

V. MELLÉKLET

AZ IPARBIZTONSÁGGAL KAPCSOLATOS KEZELÉSI ELJÁRÁSOKKAL FOGLALKOZÓ NEMZETI BIZTONSÁGI HATÓSÁGOK/KIJELÖLT BIZTONSÁGI HATÓSÁGOK JEGYZÉKE

BELGIUM

Nemzeti biztonsági hatóság
FPS Foreign Affairs (Szövetségi Külügyi Közszolgálat)
Rue des Petits Carmes 15
1000 Bruxelles/Brussel

Tel.: +32 25014542 (Titkárság)

Fax: +32 25014596

E-mail-cím: nvo-ans@diplobel.fed.be

BULGÁRIA

1. State Commission on Information Security (Információbiztonsági Állami Bizottság – nemzeti biztonsági hatóság)
   4 Kozloduy Street
   1202 Sofia
   Tel.: +359 29835775
   Fax: +359 29873750
   E-mail-cím: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (Védelmi Információs Szolgálat a Védelmi Minisztériumban) (biztonsági szolgálat)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel.: +359 29227002
   Fax: +359 29885211
   E-mail-cím: office@iksbg.org

3. State Intelligence Agency (Állami Hírszerzési Ügynökség) (biztonsági szolgálat)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel.: +359 29813221
   Fax: +359 29862706
   E-mail-cím: office@dar.bg

4. State Agency for Technical Operations (Technikai Műveletek Állami Ügynöksége) (biztonsági szolgálat)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel.: +359 29824971
   Fax: +359 29461339
   E-mail-cím: dato@dato.bg

(A fent felsorolt illetékes hatóságok folytatják le az ellenőrzési eljárásokat a minősített szerződéseket kötni szándékozó jogi személyek telephelybiztonsági tanúsítványának kibocsátása, illetve az ilyen hatóságok szükségleteinek megfelelően a minősített szerződéseket végrehajtó egyének személyi biztonsági tanúsítványának kibocsátása tekintetében.)

5. State Agency National Security (Állami Nemzeti Biztonsági Ügynökség) (biztonsági szolgálat)

   45 Cherni Vrah Blvd.
   1407 Sofia
   Tel.: +359 28147109
   Fax: +359 29632188, +359 28147441
   E-mail-cím: dans@dans.bg

(A fenti biztonsági szolgálat folytatja le az ellenőrzési eljárást a telephelybiztonsági tanúsítványok és a személyi biztonsági tanúsítványok kibocsátása tekintetében minden egyéb olyan természetes vagy jogi személy esetében, aki/amely minősített szerződést vagy minősített támogatási megállapodást kíván kötni, vagy minősített szerződést vagy minősített támogatási megállapodást kíván végrehajtani.)

CSEHORSZÁG

Nemzeti biztonsági hatóság
Industrial Security Department (Iparbiztonsági Osztály)
PO BOX 49
150 06 Praha 56
Tel.: +420 257283129
E-mail-cím: sbr@nbu.cz

DÁNIA

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

2. Forsvarets Efterretningstjeneste
   (Dán Védelmi Hírszerző Szolgálat)
   Kastellet 30
   2100 Copenhagen Ø
   Tel.: +45 33325566
   Fax: +45 33931320

NÉMETORSZÁG

1. Az iparbiztonsági politikával, a telephelybiztonsági tanúsítványokkal és a szállítási tervekkel kapcsolatos ügyekben (kivéve a titkosítást/bizalmas üzleti információkat):
   Federal Ministry for Economic Affairs and Energy (Szövetségi Gazdasági és Energiaügyi Minisztérium)
   Industrial Security Division - RS3 (Iparbiztonsági Részleg – ZB3)
   Villemombler Str. 76
   53123 Bonn
   Tel.: +49 228996154028
   Fax: +49 228996152676
   E-mail-cím: dsagermany-rs3@bmwi.bund.de (az iroda e-mail-címe)

2. A német vállalatokat érintő szabványos látogatási kérelmekkel kapcsolatos ügyekben:

   Federal Ministry for Economic Affairs and Energy (Szövetségi Gazdasági és Energiaügyi Minisztérium)

   Industrial Security Division – RS2 (Iparbiztonsági Részleg – ZB2)
   Villemombler Str. 76
   53123 Bonn

   Tel.: +49 228996152401

   Fax: +49 228996152603

   E-mail-cím: rs2-international@bmwi.bund.de (irodai e-mail-cím)

3. Titkosított anyagok szállítási terve:

   Federal Office for Information Security (Információbiztonsági Szövetségi Hivatal, BSI)
   National Distribution Agency (Nemzeti Elosztási Ügynökség)/NDA-EU DEU
   Mainzer Str. 84
   53179 Bonn

   Tel.: +49 2289995826052

   Fax: +49 228991095826052

   E-mail-cím: NDAEU@bsi.bund.de

ÉSZTORSZÁG

National Security Authority Department (Nemzeti Biztonsági Hatósági Osztály)
Estonian Foreign Intelligence Service (Észt Külföldi Hírszerző Szolgálat)
Rahumäe tee 4B
11316 Tallinn

Tel.: +372 6939211

Fax: +372 6935001

E-mail-cím: nsa@fis.gov.ee

ÍRORSZÁG

National Security Authority Ireland (Nemzeti Biztonsági Hatóság, Írország)
Department of Foreign Affairs and Trade (Külpolitikai és Külkereskedelmi Osztály)
76-78 Harcourt Street
Dublin 2
D02 DX45

Tel.: +353 14082724

E-mail-cím: nsa@dfa.ie

GÖRÖGORSZÁG

Hellenic National Defence General Staff (Görög Nemzetvédelmi Vezérkar)
E' Division (Security INTEL, CI BRANCH) (E részleg, Security INTEL, CI BRANCH)
E3 Directorate (E3 Igazgatóság)
Industrial Security Office (Iparbiztonsági Hivatal)
227-231 Mesogeion Avenue
15561 Holargos, Athens

Tel.: +30 2106572022, +30 2106572178

Fax: +30 2106527612

E-mail-cím: daa.industrial@hndgs.mil.gr

SPANYOLORSZÁG

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tel.: +34 912832583, +34 912832752, +34 913725928

Fax: +34 913725808

E-mail-cím: nsa-sp@areatec.com

A minősített programokkal kapcsolatos információk esetében: programas.ons@areatec.com

A személyi biztonsági tanúsítványokkal kapcsolatos ügyekben: hps.ons@areatec.com

A szállítási tervekkel és nemzetközi látogatásokkal kapcsolatos ügyekben: sp-ivtco@areatec.com

FRANCIAORSZÁG

Nemzeti biztonsági hatóság (a szakpolitikával és a védelmi iparon kívüli végrehajtással kapcsolatban)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel.: +33 171758193

Fax: +33 171758200

E-mail-cím: ANSFrance@sgdsn.gouv.fr

Kijelölt biztonsági hatóság (a védelmi iparban történő végrehajtással kapcsolatban)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15

Tel.: +33 988670421

E-mail-cím: formanyomtatványok és kimenő látogatási kérelmek ügyében: dga-ssdi.ai.fct@intradef.gouv.fr

bejövő látogatási kérelmek ügyében: dga-ssdi.visit.fct@intradef.gouv.fr

HORVÁTORSZÁG

Ured Vijeća za nacionalnu sigurnost
Horvát Nemzeti Biztonsági Hatóság
Jurjevska 34
10000 Zagreb

Tel.: +385 14681222

Fax: +385 14686049

E-mail-cím: NSACroatia@uvns.hr

OLASZORSZÁG

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma

Tel.: +39 0661174266

Fax: +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

E-mail-cím: cynsa@mod.gov.cy

Védelmi Minisztérium
Nemzeti Biztonsági Hatóság
172-174, Strovolos Avenue
2048 Strovolos, Nicosia

Tel.: +357 22807569, +357 22807764

Fax: +357 22302351

E-mail-cím: cynsa@mod.gov.cy

LETTORSZÁG

Nemzeti biztonsági hatóság
Constitution Protection Bureau of the Republic of Latvia (A Lett Köztársaság Alkotmányvédelmi Hivatalának Nemzeti Biztonsági Hatósága)
PO Box 286
Riga LV-1001

Tel.: +371 67025418, +371 67025463

Fax: +371 67025454

E-mail-cím: ndi@sab.gov.lv, ndi@zd.gov.lv

LITVÁNIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(A Litván Köztársaság Titokvédelmi Koordinációs Bizottsága)
Nemzeti biztonsági hatóság
Pilaitės pr. 19
LT-06264 Vilnius

Tel.: +370 70666128

E-mail-cím: nsa@vsd.lt

LUXEMBURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxemburg

Tel.: +352 24782210

E-mail-cím: ans@me.etat.lu

MAGYARORSZÁG

Nemzeti Biztonsági Felügyelet
H-1399 Budapest, P.O. Box 710/50
1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel.: +36 13911862

Fax: +36 13911889

E-mail-cím: nbf@nbf.hu

MALTA

Szabványügyi igazgató
Iparbiztonsági kijelölt biztonsági hatóság
Standards & Metrology Institute (Szabványügyi és Metrológiai Intézet)
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010

Tel.:+356 23952000

Fax: +356 21242406

E-mail-cím: certification@mccaa.org.mt

HOLLANDIA

1. Ministry of the Interior and Kingdom Relations (A Belügyekért és Királysági Kapcsolatokért Felelős Minisztérium)

   PO BOX 20010.
   2500 EA The Hague

   Tel.: +31 703204400

   Fax: +31 703200733

   E-mail-cím: nsa-nl-industry@minbzk.nl

2. Védelmi Minisztérium

   Industrial Security Department (Iparbiztonsági Osztály)

   PO BOX 20701
   2500 ES The Hague

   Tel.: +31 704419407

   Fax: +31 703459189

   E-mail-cím: indussec@mindef.nl

AUSZTRIA

1. Federal Chancellery of Austria (Osztrák Szövetségi Kancellária)

   Department I/10, Office for Information Security (I/10. osztály, Információbiztonsági Szövetségi Hivatal)

   Ballhausplatz 2
   10104 Vienna

   Tel.: +43 153115202594

   E-mail-cím: isk@bka.gv.at

2. Kijelölt biztonsági hatóság katonai ügyekben:

   BMLVS/Abwehramt

   Postfach 2000
   1030 Vienna

   E-mail-cím: abwa@bmlvs.gv.at

LENGYELORSZÁG

Internal Security Agency (Belbiztonsági Ügynökség)
Department for the Protection of Classified Information (A Minősített Adatok Védelmével Foglalkozó Osztály)
Rakowiecka 2A
00-993 Warsaw

Tel.: +48 225857944

Fax: +48 225857443

E-mail-cím: nsa@abw.gov.pl

PORTUGÁLIA

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon

Tel.: +351 213031710

Fax: +351 213031711

E-mail-cím: sind@gns.gov.pt, franco@gns.gov.pt

ROMÁNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
(Román nemzeti biztonsági hatóság – ORNISS – Minősített Adatok Nemzeti Nyilvántartó Hivatala)
4th Mures Street
012275 Bucharest

Tel.: +40 212075115

Fax: +40 212245830

E-mail-cím: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SZLOVÉNIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel.: +386 14781390

Fax: +386 14781399

E-mail-cím: gp.uvtp@gov.si

SZLOVÁKIA

Národný bezpečnostný úrad
(Nemzeti Biztonsági Hatóság)
Security Clearance Department (Biztonsági Ellenőrzési Osztály)
Budatínska 30
851 06 Bratislava

Tel.: +421 268691111

Fax: +421 268691700

E-mail-cím: podatelna@nbu.gov.sk

FINNORSZÁG

Nemzeti biztonsági hatóság
Külügyminisztérium
PO Box 453
FI-00023 Government

E-mail-cím: NSA@formin.fi

SVÉDORSZÁG

1. Nemzeti biztonsági hatóság

   Utrikesdepartementet (Külügyminisztérium)
   UD SÄK / NSA
   SE-103 39 Stockholm
   Tel.: +46 84051000
   Fax: +46 87231176
   E-mail-cím: ud-nsa@gov.se

2. Kijelölt biztonsági hatóság

   Försvarets Materielverk (Svéd Védelmianyag-hivatal)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel.: +46 87824000
   Fax: +46 87826900
   E-mail-cím: security@fmv.se