



Az Európai Unió
Tanácsa

Brüsszel, 2022. március 29.
(OR. en)

Intézményközi referenciaszám:
2022/0084(COD)

7670/22
ADD 5

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

JAVASLAT

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2022) 119 final - Annex 5
Tárgy:	MELLÉKLET a következőhöz: Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról

Mellékelten továbbítjuk a delegációknak a COM(2022) 119 final számú dokumentum V. mellékletét.

Melléklet: COM(2022) 119 final - Annex 5



EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.3.22.
COM(2022) 119 final

ANNEX 5

MELLÉKLET

a következőhöz:

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról

{SWD(2022) 65 final} - {SWD(2022) 66 final}

V. MELLÉKLET [...]

Az EU-minősített adatok (EUCI) védelme a minősített szerződésekben és támogatási megállapodásokban

E melléklet alkalmazásában a II. és IV. mellékletben foglalt fogalommeghatározásokon túlmenően a „telephelybiztonsági tanúsítvány” annak a nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság által történő hivatalos meghatározása, hogy egy adott létesítmény biztonsági szempontból megfelelő szintű védelmet tud nyújtani meghatározott biztonsági minősítésű szintű EU-minősített adatoknak.

A vállalkozók és a kedvezményezettek alkalmazottjainak hozzáférése az EU-minősített adatokhoz

1. Ajánlatkérő vagy engedélyező hatósággént minden uniós intézmény vagy szerv gondoskodik arról, hogy a minősített szerződések vagy a támogatási megállapodások tartalmazzanak olyan rendelkezéseket, amelyek értelmében a vállalkozók, az alvállalkozók vagy a kedvezményezettek azon alkalmazottja számára, akinek a minősített szerződés, alvállalkozói szerződés vagy támogatási megállapodás teljesítéséhez szüksége van az EU-minősített adatokhoz való hozzáférésre, a hozzáférés csak a következő feltételek teljesülése esetén adható meg:
 - 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 személyi biztonsági tanúsítványt állít ki;
 - 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. Ha a vállalkozó vagy kedvezményezett harmadik ország állampolgárát kívánja alkalmazni olyan pozícióban, amelyhez CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET szintű adatokhoz való hozzáférés szükséges, a vállalkozó vagy kedvezményezett kezdeményezi az adott személyre vonatkozó biztonsági ellenőrzési eljárás lefolytatását az abban az országban érvényes nemzeti jogszabályoknak és rendeleteknek megfelelően, ahol biztosítani tervezi az EU-minősített adatokhoz való hozzáférést.

Telephelybiztonsági tanúsítvány (FSC)

3. A telephelybiztonsági tanúsítványt valamely tagállam nemzeti biztonsági hatósága, kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatósága adja ki annak jelzésére, hogy – a nemzeti jogszabályokkal és rendelkezésekkel összhangban – a szervezet képes az EU-minősített adatok megfelelő minősítési szinten (CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET) való védelmére a létesítményein belül.
4. Az uniós intézménynek vagy szervnek mint ajánlatkérő vagy engedélyező hatóságnak biztonsági hatóságán keresztül értesítenie kell a megfelelő nemzeti biztonsági hatóságot, kijelölt biztonsági hatóságot vagy bármely más illetékes biztonsági hatóságot, amennyiben a szerződés vagy támogatási megállapodás teljesítéséhez telephelybiztonsági tanúsítványra van szükség.

5. Telephelybiztonsági tanúsítványra van szükség, ha a beszerzési vagy támogatás-odaítélési eljárás során CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokat kell a részvételre jelentkezők, az ajánlattevők vagy a pályázók létesítményeinek rendelkezésére bocsátani.
6. Az uniós intézménynek vagy szervnek mint ajánlatkérő vagy engedélyező hatóságnak az EU-minősített adatokhoz való hozzáférés megadása előtt a biztonsági hatóságán keresztül meg kell kapnia a részvételre jelentkező, az ajánlattevő vagy a vállalkozó, illetve a támogatást igénylő vagy a kedvezményezett telephelybiztonsági tanúsítványának megerősítését.
7. Amennyiben a tagállamok a nemzeti jogszabályok alapján nem állítanak ki telephelybiztonsági tanúsítványokat bizonyos létesítmények számára, az ajánlatkérő vagy engedélyező hatóságnak ellenőriznie kell az érintett nemzeti biztonsági hatóságnál vagy kijelölt biztonsági hatóságnál, hogy ezek a létesítmények képesek-e az EU-minősített adatok megfelelő szintű kezelésére.
8. A 7. pontban említett esetek kivételével az uniós intézmény vagy szerv mint ajánlatkérő szerv nem írhat alá minősített szerződést vagy minősített támogatási megállapodást azt megelőzően, hogy biztonsági hatóságán keresztül megerősítést kapna az érintett nemzeti biztonsági hatóságtól, kijelölt biztonsági hatóságtól vagy bármely más illetékes nemzeti hatóságtól arról, hogy megfelelő telephelybiztonsági tanúsítványt bocsátottak ki.
9. A telephelybiztonsági tanúsítványnak az illetékes nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság általi visszavonása elegendő indok arra, hogy az ajánlatkérő vagy engedélyező hatóság felmondja a minősített szerződést vagy támogatási megállapodást, vagy kizárjon egy részvételre jelentkezőt, ajánlattevőt vagy pályázót a versenyből.

A minősített szerződések és támogatási megállapodások pályáztatására és végrehajtására vonatkozó rendelkezések

10. Amennyiben a közbeszerzési vagy kiválasztási eljárás során EU-minősített adatot bocsátanak a részvételre jelentkező, ajánlattevő vagy pályázó rendelkezésére, az ajánlati felhívásnak vagy pályázati felhívásnak tartalmaznia kell a ki nem választott részvételre jelentkező, ajánlattevő vagy pályázó arra vonatkozó kötelezettségét, hogy meghatározott időn belül valamennyi minősített dokumentumot visszaküldje.
11. Általános szabály, hogy a vállalkozó vagy a támogatás kedvezményezettje a minősített szerződés vagy támogatási megállapodás vagy a támogatási kedvezményezett részvételének lejártát követően köteles valamennyi EU-minősített adatot visszaszolgáltatni az ajánlatkérő vagy engedélyező hatóságnak.
12. Az EU-minősített adatoknak a minősített szerződés vagy támogatási megállapodás teljesítése során vagy azok lejártával történő megsemmisítésére vonatkozó egyedi rendelkezéseket a biztonsági vonatkozások záradékában kell lefektetni.
13. Amennyiben a vállalkozó vagy a támogatás kedvezményezettje engedélyt kap az EU-minősített adatok megtartására a minősített szerződés vagy támogatási megállapodás lejártát követően, továbbra is be kell tartani az e rendeletben foglalt minimumszabályokat, és a vállalkozónak vagy a támogatás kedvezményezettjének védenie kell az EU-minősített adatok bizalmasságát.
14. Az ajánlati felhívásban vagy a pályázati felhívásban, valamint a minősített szerződésben vagy támogatási megállapodásban meg kell határozni az EU-minősített

adatok védelmének azon feltételeit, amelyek mellett a vállalkozó vagy a kedvezményezett alvállalkozói szerződést köthet.

15. Mielőtt a vállalkozó vagy a kedvezményezett a minősített szerződés bármely részét vagy a támogatási megállapodás bármely minősített részét alvállalkozónak adná ki, be kell szereznie az ajánlatkérő vagy engedélyező hatóság engedélyét.
16. A vállalkozó vagy a kedvezményezett felel annak biztosításáért, hogy minden alvállalkozói tevékenységet az e rendeletben foglalt minimumszabályokkal összhangban folytassanak, és az alvállalkozó részére nem ad át EU-minősített adatot az az ajánlatkérő vagy engedélyező hatóság előzetes írásbeli engedélye nélkül.
17. A vállalkozó vagy a kedvezményezett által létrehozott EU-minősített adatok tekintetében az uniós intézmény vagy szerv – amely az ajánlatkérő vagy engedélyező hatóság – minősül kibocsátónak, és gyakorolja a kibocsátót megillető jogokat.
18. Amennyiben a tagállamok a nemzeti jogszabályaik és rendelkezéseik értelmében telephelybiztonsági vagy személyi biztonsági tanúsítványt írnak elő a RESTREINT UE/EU RESTRICTED minősítésű szerződések, támogatási megállapodások vagy alvállalkozói szerződések esetében, az uniós intézmények és szervek mint ajánlatkérő vagy engedélyező hatóságok e nemzeti követelményekkel nem írhatnak elő további kötelezettségeket más tagállamok számára, és nem zárhatják ki az olyan tagállamokból származó ajánlattevőket, pályázókat, vállalkozókat, kedvezményezetteket vagy alvállalkozókat, amelyek a kapcsolódó szerződések, 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.

A minősített szerződésekkel és támogatási megállapodásokkal kapcsolatos látogatások

19. Amennyiben az uniós intézményeknek és szerveknek, a vállalkozóknak, a kedvezményezetteknek vagy az alvállalkozóknak egy minősített szerződés vagy támogatási megállapodás végrehajtásához egymás telephelyén CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatokhoz kell hozzáférniük, a látogatásokat a nemzeti biztonsági hatóságokkal, a kijelölt biztonsági hatóságokkal vagy bármely más érintett illetékes biztonsági hatósággal egyeztetve kell megszervezni.
20. A 19. pontban említett látogatásokra az alábbi követelmények vonatkoznak:
 - a) a látogatásnak a minősített szerződéssel vagy támogatási megállapodással kapcsolatos hivatalos céljának kell lennie;
 - b) a minősített szerződés vagy támogatási megállapodás teljesítése során felhasznált vagy előállított EU-minősített adatokhoz való hozzáférés érdekében minden látogatónak előírt szintű személyi biztonsági tanúsítvánnyal kell rendelkeznie, és meg kell felelnie a szükséges ismeret feltételének.
 - c) a látogatásra vonatkozó hivatalos kérelmet a létesítmény illetékes nemzeti biztonsági hatóságához vagy kijelölt biztonsági hatóságához vagy az érintett uniós intézmény vagy szerv biztonsági hatóságához kell benyújtani legalább 15 nappal a látogatás időpontja előtt.
21. Konkrét projektek összefüggésében az érintett nemzeti biztonsági hatóságok vagy kijelölt biztonsági hatóságok és az érintett uniós intézmény vagy szerv biztonsági

hatósága megállapodhatnak olyan eljárásban, amelynek megfelelően egy adott minősített szerződés vagy támogatás vonatkozásában a látogató biztonsági tisztviselője és a meglátogatni kívánt telephely biztonsági tisztviselője közvetlenül szervezheti meg a látogatásokat. Az ilyen kivételes eljárásokat a program- vagy projektbiztonsági utasításokban vagy más konkrét megállapodásokban kell meghatározni.

22. A RESTREINT UE/EU RESTRICTED minősítésű adatokhoz való hozzáféréssel járó látogatásokat a küldő és a fogadó szervezetnek kell közvetlenül megszerveznie.

EU-minősített adatok elektronikus továbbítása minősített szerződésekkel és támogatási megállapodásokkal összefüggésben

23. Az EU-minősített adatok elektronikus kezelését és továbbítását az 5. fejezet 5. szakaszának megfelelően kell végezni.

A vállalkozó, kedvezményezett vagy alvállalkozó kommunikációs és információs rendszerét, amelyet az a szerződés vagy támogatási megállapodás teljesítésével összefüggésben az EU-minősített adatok kezelésére és tárolására használ, azon ország vagy nemzetközi szervezet biztonsági akkreditációs hatóságának kell akkreditálnia, amelynek felügyelete alatt a vállalkozó, a kedvezményezett vagy az alvállalkozó működik.

Az EU-minősített adatok minősített szerződések és támogatási megállapodások keretében történő elektronikus továbbítása esetén az adatok védelmét a 42. cikkel összhangban jóváhagyott kriptográfiai termékekkel kell biztosítani.

24. A vállalkozó vagy kedvezményezett RESTREINT UE/EU RESTRICTED szintű EU-minősített adatokat kezelő kommunikációs és információs rendszere és az összekapcsolás tekintetében a biztonsági akkreditáció elvégzése átruházható a vállalkozó vagy kedvezményezett biztonsági tisztviselőjére, amennyiben a nemzeti jogszabályok és rendelkezések azt lehetővé teszik.

A biztonsági akkreditációs feladat átruházása esetén a vállalkozó vagy kedvezményezett felelőssége, hogy akkor, amikor a kommunikációs és információs rendszerében RESTREINT UE/EU RESTRICTED minősítésű adatokat kezel, gondoskodjon a biztonsági vonatkozások záradékában meghatározott biztonsági követelmények teljesüléséről. Az érintett nemzeti biztonsági hatóságok vagy nemzeti biztonsági hatóságok és biztonsági akkreditációs hatóságok továbbra is felelősek a vállalkozó vagy kedvezményezett által kezelt vagy tárolt, RESTREINT UE/EU RESTRICTED minősítésű adatok védelméért, és joguk van megvizsgálni a vállalkozó vagy kedvezményezett által hozott biztonsági intézkedéseket.

A vállalkozó vagy kedvezményezett emellett bemutatja az uniós intézménynek vagy szervnek mint ajánlatkérő vagy engedélyező hatóságnak – és amennyiben a nemzeti jogszabályok és rendeletek előírják, az illetékes nemzeti biztonsági akkreditációs hatóságnak – a megfelelőségi nyilatkozatot, amely tanúsítja, hogy a vállalkozó vagy kedvezményezett kommunikációs és információs rendszere és a vonatkozó összekapcsolás akkreditációval rendelkezik a RESTREINT UE/EU RESTRICTED szintű EU-minősített adatok kezelésére és tárolására.

EU-minősített adatok kézi szállítása minősített szerződésekkel és támogatási megállapodásokkal összefüggésben

25. A minősített szerződésekhez és támogatási megállapodásokhoz kapcsolódó minősített adatok kézi szállítására szigorú biztonsági követelményeknek kell vonatkozniuk.
26. A RESTREINT UE/EU RESTRICTED minősítésű adatokat a vállalkozó vagy kedvezményezett alkalmazottjai az Európai 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 minősített adatok mindvégig a szállítónál maradnak;
 - c) a borítékot vagy a csomagot a végső rendeltetési hely eléréséig nem szabad felnyitni.
27. 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 vállalkozó vagy 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. A 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 adatok mindvégig a szállítónál maradnak;
 - d) a borítékot vagy a csomagot a végső rendeltetési hely eléréséig nem szabad felnyitni;
 - e) a boríték vagy csomag szállítása olyan zárható aktatáskában vagy olyan méretű és súlyú hasonló jóváhagyott táskában történik, amelyet a szállító mindvégig magánál tud tartani;
 - f) a futár olyan, az illetékes biztonsági hatósága által kiállított tanúsítvánnyal rendelkezik, amely felhatalmazza a meghatározott minősített szállítmány szállítására.
28. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy SECRET UE/EU SECRET minősítésű adatoknak a vállalkozó vagy kedvezményezett alkalmazottja általi, uniós tagállamok közötti kézi szállítására a 27. pontban meghatározott követelményeken kívül 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(ok) végén a futár tanúsítványát és a kapcsolódó dokumentumokat vissza kell juttatni a dokumentumokat kiállító nemzeti biztonsági hatósághoz vagy kijelölt biztonsági hatósághoz, vagy a futártanúsítvány átvevőjének 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.

Amennyiben 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.

29. A legfeljebb SECRET UE/EU SECRET minősítésű adatoknak a vállalkozó vagy kedvezményezett alkalmazottja általi, harmadik országba vagy nemzetközi szervezetnek való kézi szállítására az Európai Unió és az érintett harmadik ország vagy nemzetközi szervezet közötti adatbiztonsági megállapodás rendelkezései irányadók.

EU-minősített adatok kereskedelmi futárszolgálattal és szállítmányként való szállítása minősített szerződésekkel és támogatási megállapodásokkal összefüggésben

30. Az EU-minősített adatok kereskedelmi futárszolgálat általi szállítását a IV. melléklet vonatkozó rendelkezéseivel összhangban kell végezni.
31. Az EU-minősített adatok szállítmányként való szállítása biztonsági előírásainak meghatározása során az alábbi elveket kell alkalmazni:
- a) a szállítás valamennyi szakasza alatt garantálni kell a biztonságot, a kiindulási helytől a végső úti célig;
 - b) egy adott szállítmányra megállapított védelmi szintet az abban foglalt anyag legmagasabb minősítési szintje határozza meg;
 - c) a szállítást végző vállalatoknak megfelelő szintű telephelybiztonsági tanúsítvánnyal kell rendelkezniük. Ilyen esetekben a szállítmányt kezelő személyzetnek biztonsági ellenőrzésen kell átesnie;
 - d) a CONFIDENTIEL UE/EU CONFIDENTIEL vagy SECRET UE/EU SECRET minősítésű anyag határokon keresztül bármilyen szállítását megelőzően a feladó szállítási tervet készít, amelyet a nemzeti biztonsági hatóság, a kijelölt biztonsági hatóság vagy bármely más illetékes biztonsági hatóság jóváhagy;
 - e) lehetőség szerint közvetlen útvonalakat kell használni, és a szállítást a körülményekhez képest a lehető leggyorsabban kell végrehajtani;

- f) lehetőség szerint kizárólag a tagállamokat érintő útvonalakat kell használni. Harmadik országokon keresztül vezető útvonalak kizárólag mind a feladó, mind a címzett államának nemzeti biztonsági hatósága, kijelölt biztonsági hatósága vagy bármely más illetékes biztonsági hatósága által kiadott engedély birtokában alkalmazhatók.