Az Európai Unió
Tanácsa

Brüsszel, 2022. március 29.
(OR. en)

Intézményközi referenciaszám:
2022/0084(COD)

7670/22
ADD 3

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

JAVASLAT

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2022. március 22.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2022) 119 final - Annex 3
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 III. mellékletét.

Melléklet: COM(2022) 119 final - Annex 3

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.3.22.
COM(2022) 119 final

ANNEX 3

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}

III. MELLÉKLET […]

Az EU-minősített adatok fizikai védelmére szolgáló intézkedések

Az EU-minősített adatok fizikai védelmére szolgáló berendezések és szervezeti intézkedések

1. Az adminisztratív zónának a következő követelményeknek kell megfelelnie:

   a) láthatóan kijelölt határvonallal kell rendelkeznie, amely lehetővé teszi a személyek és lehetőség szerint a járművek ellenőrzését;

   b) biztosítani kell, hogy a területen belül az EU-minősített adatokhoz való jogosulatlan vizuális hozzáférést lehetővé tevő ablakok átlátszatlanok legyenek, vagy fel legyenek szerelve redőnyökkel, függönyökkel vagy más sötétítő eszközökkel;

   c) a kíséret nélküli belépést csak az uniós intézmény biztonsági hatósága vagy más illetékes testület által kiadott megfelelő engedéllyel rendelkező személyek számára lehet megadni;

   d) minden más személy számára állandó kíséretet kell biztosítani vagy a személyt ezzel egyenértékű ellenőrzésnek kell alávetni.

2. Az 1. pontban előírt követelményeken túlmenően a biztonsági területnek a következő követelményeknek is meg kell felelnie:

   a) láthatóan kijelölt és védett határvonallal kell rendelkeznie, amelyen minden be- és kilépést folyamatosan ellenőriznek;

   b) a területen nem lehetnek engedély nélküli kommunikációs vonalak, engedély nélküli telefonvonalak és más engedély nélküli eszközök és elektromos vagy elektronikus berendezések;

   c) a területet belépési ellenőrzéssel és valós idejű ellenőrző behatolásjelző rendszerrel (IDS) kell felszerelni, valamint álljon rendelkezésre a biztonságért felelős elhárító személyzet;

   d) a területet a rendes munkaidő végén és a rendes munkaidőn kívül szúrópróbaszerűen ellenőrizni kell, amennyiben a területen nem tartózkodik napi 24 órán át munkavégző személyzet, és a területen nem működik valós idejű ellenőrző behatolásjelző rendszer;

   e) a területet képzett, felügyelt és megfelelő biztonsági ellenőrzésen átesett biztonsági személyzetnek kell kezelnie;

   f) biztonsági üzemeltetési eljárásokat kell meghatározni, beleértve a következő elemeket:

      i. a területen kezelt, tárgyalt és tárolt EU-minősített adatok minősítési szintje;

      ii. a fenntartandó ellenőrzési és védelmi intézkedések;

      iii. az EU-minősített adatokhoz való hozzáférési engedély és a szükséges ismeret elve alapján a területre kíséret nélkül való belépésre engedéllyel rendelkező személyek;

      iv. adott esetben a kíséretre vagy az EU-minősített adatok védelmére vonatkozó eljárások, amennyiben bármely más személynek engedélyezik a területre való belépést;

v. minden más vonatkozó intézkedés és eljárás.

3. Amennyiben a biztonsági területre való belépés az ott található minősített adatokhoz való közvetlen hozzáférést tesz lehetővé, a területet I. osztályú területnek kell tekinteni, amennyiben viszont nem ez az eset áll fenn, a területet II. osztályú területnek kell tekinteni.

Az érintett uniós intézmény vagy szerv biztonsági osztályának/tisztviselőjének az első albekezdésben említett mindkét osztály esetében és a 2. pontban előírt követelményeken túlmenően egyértelműen fel kell tüntetnie a területen általában tárolt információk legmagasabb biztonsági minősítésének szintjét, és egyértelműen meg kell határoznia azt a határvonalat, amely lehetővé teszi az egyének és – amennyiben lehetséges – a járművek ellenőrzését.

Az uniós intézményeknek és szerveknek biztosítaniuk kell, hogy a biztonsági területre belépő személyek teljesítik a következő kritériumokat:

a) a területre való belépéshez különleges engedéllyel rendelkeznek;

b) állandó kíséretet rendelnek mellékjük;

c) megfelelő biztonsági ellenőrzésen estek át, kivéve ha intézkedésekkel biztosított, hogy EU-minősített adatokhoz ne legyen lehetséges a hozzáférés.

4. A passzív és aktív lehallgatás ellen védett biztonsági területek a technikailag biztosított biztonsági terület megjelölést kapják. Ezekre a területekre a biztonsági területekre vonatkozó követelményeken felül a következő követelmények alkalmazandók:

a) az ilyen területeket behatolásjelző rendszerrel szerelik fel, használaton kívül zárva tartják, használat esetén pedig őrzik. Valamennyi kulcsot a 29 cikk (3) bekezdésével összhangban kell kezelni;

b) az érintett uniós intézmény vagy szerv biztonsági hatósága rendszeresen, fizikailag vagy technikailag, vagy mindkét módon ellenőrzi e területeket. Ezeket az ellenőrzéseket illetéktelen behatolás vagy annak gyanúja esetén is el kell végezni;

c) megfelelő akusztikus és TEMPEST-védelemmel kell rendelkezniük.

5. A technikailag biztosított biztonsági területekre belépő valamennyi személynek meg kell felelnie a 3. pontban meghatározott követelményeknek.

6. Biztonsági területeket és technikailag biztosított biztonsági területeket ideiglenesen is fel lehet állítani valamely adminisztratív zónán belül, minősített üléshez vagy más hasonló célból.

7. A biztonsági területeken megerősített helyiségeket kell kialakítani. A megerősített helyiség olyan megerősített fizikai létesítmény, amelynek falát, padlóját, plafonját, ablakait és zárható ajtajait az érintett uniós intézmény vagy szerv biztonsági hatósága hagyja jóvá. Az ilyen helyiségeknek az ugyanilyen minősítési szintű EU-minősített adat tárolásához jóváhagyott tárolóeszköz által nyújtottal egyenértékű védelmet kell biztosítaniuk.

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

8. A RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatokat az alábbi területek valamelyikén kell kezelni és tárolni:

a) biztonsági területen;

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

c) biztonsági területen vagy adminisztratív zónán kívül, amennyiben az adat birtokosa vállalja, hogy eleget tesz az érintett uniós intézmény vagy szerv biztonsági hatósága által meghatározott kiegészítő intézkedéseknek.

9. A RESTREINT UE/EU RESTRICTED minősítésű EU-minősített adatokat zárható irodabútorokban kell tárolni az adminisztratív zónában vagy biztosított területen. Az adatokat ideiglenesen adminisztratív zónán vagy biztonsági területen kívül is lehet tárolni, amennyiben az adat birtokosa vállalja, hogy az érintett dokumentumokat megfelelően zárható irodabútorokban tárolja, amikor azokat nem olvassák vagy nem tárgyalják.

10. Az uniós intézmények és szervek a RESTREINT UE/EU RESTRICTED minősítésű adatokat a székhelyeiken kívül is kezelhetik és tárolhatják, feltéve, hogy a vonatkozó információk megfelelő védelemben részesülnek. E célból az uniós intézményeknek és szerveknek meg kell felelniük a 8. pont c) alpontjában előírt intézkedéseknek.

11. A CONFIDENTIEL UE/EU CONFIDENTIAL és SECRET UE/EU SECRET minősítésű adatokat a következő területek valamelyikén kell kezelni és tárolni:

a) biztonsági területen;

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

c) biztonsági területen vagy adminisztratív zónán kívül korlátozott mennyiségben és időtartamban, amennyiben az adat birtokosa vállalja, hogy eleget tesz az érintett uniós intézmény vagy szerv biztonsági hatósága által meghatározott kiegészítő intézkedéseknek. Ezen túlmenően az EU-minősített adatok birtokosának a következő lépéseket kell tennie:

i. értesítenie kell az illetékes nyilvántartó hivatalt arról, hogy a minősített dokumentumokat védett területen kívül kezelik;

ii. a dokumentumot mindenkor személyes felügyelete alatt kell tartania.

12. A CONFIDENTIEL UE/EU CONFIDENTIAL és a SECRET UE/EU SECRET minősítésű adatokat olyan biztonsági területen – biztonsági tárolóeszközben vagy megerősített helyiségben – kell tárolni, amelyet az érintett uniós intézmény vagy szerv illetékes biztonsági akkreditációs hatósága ezen a szinten akkreditált.

13. A CONFIDENTIEL UE/EU CONFIDENTIAL vagy annál magasabb minősítésű dokumentumokról csak az illetékes nyilvántartó hivatal készíthet másolatot.

14. A TRÈS SECRET UE/EU TOP SECRET minősítésű adatokat az ezen a szinten akkreditált biztonsági területen kell kezelni és tárolni. E célból az uniós intézmények és szervek megköthetik a szükséges megállapodásokat ahhoz, hogy egy másik uniós intézmény és szerv biztonsági akkreditációs hatósága által üzemeltetett és a megfelelő szinten akkreditált biztonsági területet használjanak.

15. A TRÈS SECRET UE/EU TOP SECRET minősítésű adatokat az érintett illetékes uniós intézmény vagy szerv biztonsági akkreditációs hatósága által ezen a szinten akkreditált biztonsági területen kell tárolni, az alábbi feltételek egyike mellett:

a) az egyes uniós intézmények és szervek biztonsági hatóságai által jóváhagyott biztonsági tárolóeszközben, a következő kiegészítő ellenőrzések egyike mellett:

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

   ii. jóváhagyott behatolásjelző rendszer, a biztonságért felelős elhárító személyzet alkalmazása mellett;

b) behatolásjelző rendszerrel ellátott megerősített helyiségben, a biztonságért felelős elhárító személyzet alkalmazása mellett.