A TÖRVÉNYSZÉK (EU) 2016/2387 HATÁROZATA

(2016. szeptember 14.)

az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott tájékoztatásokra vagy mellékletekre alkalmazandó biztonsági szabályokról

A TÖRVÉNYSZÉK,

Tekintettel az eljárási szabályzatra és különösen annak 105. cikke (11) bekezdésére,

Mivel:

(1) Az eljárási szabályzat 105. cikkének (1) és (2) bekezdése értelmében a felperes vagy az alperes – saját kezdeményezésére vagy a Törvényszék által elrendelt bizonyításfelvétel keretében – az Európai Uniónak, illetve egy vagy több tagállamának a biztonságát vagy nemzetközi kapcsolatainak irányítását érintő tájékoztatásokat vagy mellékleteket nyújthat be. E rendelkezés (3)–(10) bekezdése tartalmazza az ilyen tájékoztatásokra vagy mellékletekre alkalmazandó eljárási szabályokat.

(2) Figyelembe véve az érintett tájékoztatások vagy mellékletek érzékeny és bizalmas jellegét, az eljárási szabályzat 105. cikkében kialakított szabályok alkalmazása szükségessé teszi az e tájékoztatások vagy mellékletek magas szintű védelmének biztosítására irányuló megfelelő biztonsági rendelkezés megalkotását.

(3) Ennek érdekében a biztonsági rendelkezést alkalmazni kell az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott minden olyan tájékoztatásra vagy mellékletre, amelyek az Európai Unió minősített adatait képezik, illetve amelyekkel kapcsolatban az azokat benyújtó felperes vagy alperes jelzi, hogy az ellenérdekű felperessel vagy alperessel való közlésük sértené az Uniónak, illetve egy vagy több tagállamának a biztonságát vagy nemzetközi kapcsolatainak irányítását, ideértve azt az esetet is, ha az említett tájékoztatások vagy mellékletek nem képezik az Európai Unió minősített adatait.

(4) E tájékoztatások vagy mellékletek magas szintű védelmének biztosítása érdekében az említett tájékoztatások vagy mellékletek védelmét szolgáló alapelvek és biztonsági minimumszabályok azokat az alapelveket és biztonsági minimumszabályokat veszik alapul, amelyeket az uniós intézményeknek az Európai Unió minősített adatai (EUMA) védelmével kapcsolatos szabályai – különösen az Európai Unió Tanácsa, az Európai Parlament és az Európai Bizottság által elfogadott szabályok – szerint a SECRET UE / EU SECRET minősítésű adatok védelme érdekében alkalmaznak.

(5) Az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott tájékoztatásokat vagy mellékleteket külön az Európai Unió Bíróságára jellemző, úgynevezett „FIDUCIA” jelöléssel kell ellátni, amely meghatározza azokat a biztonsági szabályokat, amelyeket az ilyen tájékoztatásokra vagy mellékletekre a Törvényszék előtti eljárás, fellebbezés esetén pedig a Bíróság előtti eljárás során is mindvégig alkalmazni kell. A FIDUCIA jelölés rávezetése és annak törlése nincs hatással a Törvényszékkel közölt adatok minősítésére.

(6) A FIDUCIA adatokhoz való hozzáférést a „szükséges ismeret” elvének tiszteletben tartásával kell biztosítani,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Fogalmak

A jelen határozatban:

a) „biztonsági hatóság”: az Európai Unió Bíróságának biztonságáért felelős, az Európai Unió Bírósága által kijelölt hatóság, amely a jelen határozatban meghatározott feladatok ellátását egészben vagy részben átruházhatja;

b) „FIDUCIA iroda”: az Európai Unió Bíróságának a FIDUCIA adatokat kezelő irodája;

c) „birtokos”: olyan, megfelelő engedéllyel rendelkező, a „szükséges ismeret” feltételének eleget tévő személy, aki FIDUCIA adat birtokában van, és ennek megfelelően felel annak védelméért;

d) „dokumentum”: bármilyen adat, fizikai formájától vagy jellemzőitől függetlenül;

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

f) „az Európai Unió minősített adatai” (EUMA): az uniós intézményeken belül e tárgyban alkalmazandó szabályok alapján, az Európai Unió biztonsági minősítése szerint ilyenként megjelölt bármilyen adat vagy anyag, amely az alábbi minősítési szintek valamelyikébe tartozik:

— TRÈS SECRET UE / EU TOP SECRET;

— SECRET UE / EU SECRET;

— CONFIDENTIEL UE / EU CONFIDENTIAL;

— RESTREINT UE / EU RESTRICTED.

g) „FIDUCIA adat”: a FIDUCIA jelöléssel ellátott bármilyen adat;

h) FIDUCIA adat „kezelése”: azon tevékenységek összessége, amelyeknek a FIDUCIA adatok a Törvényszék előtti eljárás során mindvégig, legkésőbb pedig az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártáig tárgyát képezhetik. Így beletartozik az ilyen adatok nyilvántartásba vétele, az azokba való betekintés, azok előállítása, másolása, tárolása, visszaszolgáltatása és megsemmisítése.

2. cikk

Cél és hatály

(1) A jelen határozat megállapítja azokat az alapelveket és biztonsági minimumszabályokat, amelyek a Törvényszék előtti eljárás keretében, legkésőbb pedig az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártáig a FIDUCIA adatok védelmét szolgálják.

(2) Ezek az alapelvek és biztonsági minimumszabályok alkalmazandók valamennyi FIDUCIA adatra, hasonlóképp azok minden olyan írásbeli vagy szóbeli felhasználására, valamint másolataira, amelyeket a jelen határozatban megállapított biztonsági szabályokkal összhangban adott esetben végezhetnek vagy készíthetnek.

3. cikk

A benyújtás és a visszaszolgáltatás szabályai

A jelen határozatban kialakított szabályozás végrehajtása érdekében:

— a felperes vagy az alperes értesíti a Törvényszék Hivatalát arról, hogy az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése szerinti tájékoztatásokat vagy mellékleteket melyik napon nyújtja be,

— a felperes vagy az alperes az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése szerinti tájékoztatásokat vagy mellékleteket köteles a Hivatal képviselőjének kíséretében, a Hivatal nyitvatartási idejében benyújtani a FIDUCIA irodába,

— az a felperes vagy alperes, aki az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése szerinti tájékoztatásokat vagy mellékleteket benyújtotta, köteles azokat a FIDUCIA irodában, a Hivatal képviselőjének jelenlétében visszavenni, amennyiben az eljárási szabályzat 105. cikkének (4) bekezdése alapján nem járul hozzá a közlésükhöz; az eljárási szabályzat 105. cikkének (7) bekezdése szerinti visszavonásuk esetén haladéktalanul, illetve az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártakor haladéktalanul, kivéve ha e határidőn belül fellebbezést nyújtottak be,

— ha az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidőn belül a Törvényszék határozata ellen fellebbezést nyújtanak be, az ezen ügy keretében az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott tájékoztatásokat vagy mellékleteket a Bíróság rendelkezésére kell bocsátani. Ennek érdekében a Törvényszék hivatalvezetője azt követően, hogy értesítik őt e fellebbezésről, haladéktalanul levelet küld a Bíróság hivatalvezetőjének, amelyben értesíti őt arról, hogy az érintett tájékoztatásokat vagy mellékleteket a Bíróság rendelkezésére bocsátják. A Törvényszék hivatalvezetője ezzel egyidejűleg értesíti a biztonsági hatóságot arról, hogy az érintett tájékoztatásokat vagy mellékleteket a Bíróság rendelkezésére kell bocsátani, anélkül hogy az említett tájékoztatásokat vagy mellékleteket fizikailag elmozdítanák. Ezt az adatot a FIDUCIA iroda nyilvántartásba veszi. Az a felperes vagy alperes, aki e tájékoztatásokat vagy mellékleteket benyújtotta, köteles azokat a FIDUCIA irodában, a Bíróság Hivatala képviselőjének jelenlétében, a fellebbezési eljárást befejező határozat kézbesítését követően haladéktalanul visszavenni, kivéve ha az ügyet határozathozatal céljából visszautalták a Törvényszékhez,

— az ügynek a Törvényszékhez való visszautalása esetén a Bíróság az érintett tájékoztatásokat vagy mellékleteket a fellebbezési eljárást befejező határozat kézbesítését követően haladéktalanul a Törvényszék rendelkezésére bocsátja. Ennek érdekében a Bíróság hivatalvezetője levelet küld a Törvényszék hivatalvezetőjének, amelyben értesíti őt arról, hogy az érintett tájékoztatásokat vagy mellékleteket a Törvényszék rendelkezésére bocsátják. A Bíróság hivatalvezetője ezzel egyidejűleg értesíti a biztonsági hatóságot arról, hogy az érintett tájékoztatásokat vagy mellékleteket a Törvényszék rendelkezésére kell bocsátani, anélkül hogy az említett tájékoztatásokat vagy mellékleteket fizikailag elmozdítanák. Ezt az adatot a FIDUCIA iroda nyilvántartásba veszi. Az a felperes vagy alperes, aki e tájékoztatásokat vagy mellékleteket benyújtotta, köteles azokat a FIDUCIA irodában, a Törvényszék Hivatala képviselőjének jelenlétében, az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártakor haladéktalanul visszavenni, kivéve ha e határidőn belül fellebbezést nyújtottak be.

4. cikk

A FIDUCIA jelölés

(1) A FIDUCIA iroda az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott valamennyi tájékoztatáson vagy mellékleten elhelyezi a FIDUCIA jelölést.

(2) A FIDUCIA iroda a FIDUCIA jelölést elhelyezi az összes olyan adaton is, amely egészben vagy részben átveszi az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott tájékoztatások vagy mellékletek tartalmát, valamint az ilyen tájékoztatások vagy mellékletek minden egyes másolatán.

(3) A FIDUCIA iroda a FIDUCIA jelölést elhelyezi a FIDUCIA iroda által a jelen határozat alapján létrehozott azon dokumentumokon és nyilvántartásokon is, amelyek jogosulatlan hozzáférhetővé tétele sérthetné az Uniónak, illetve egy vagy több tagállamának a biztonságát vagy nemzetközi kapcsolatainak irányítását.

(4) A FIDUCIA jelölést a FIDUCIA adatok valamennyi oldalára és adathordozójára láthatóan kell rávezetni.

(5) A FIDUCIA jelölés rávezetése és e jelölésnek a III. mellékletben megállapított feltételek mellett történő törlése nincs hatással a Törvényszékkel közölt adatok minősítésére.

5. cikk

A FIDUCIA adatok védelme

(1) A FIDUCIA adatok védelme az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályokkal összhangban a SECRET UE / EU SECRET minősítésű EUMA-nak biztosított védelemmel egyenértékű.

(2) Bármely FIDUCIA adat birtokosa köteles azt a jelen határozattal összhangban védeni.

6. cikk

A biztonsági kockázat kezelése

(1) A FIDUCIA adatokat fenyegető kockázatokat olyan kockázatelemzési folyamat keretében kell kezelni, amelynek célja az ismert biztonsági kockázatok feltárása, az ilyen kockázatok elfogadható szintre történő csökkentésére irányuló biztonsági intézkedések meghatározása a jelen határozat alapelveivel és minimumszabályaival összhangban, valamint ezen intézkedések alkalmazása. Az ilyen intézkedések hatékonyságát a biztonsági hatóság folyamatosan értékeli.

(2) Azok a biztonsági intézkedések, amelyek a Törvényszék előtti eljárás során mindvégig, legkésőbb pedig az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártáig a FIDUCIA adatok védelmét szolgálják, arányban állnak különösen az érintett adatok vagy anyagok formájával, továbbá azok mennyiségével, a FIDUCIA iroda helyiségeinek elhelyezkedésével és felépítésével, valamint a szándékos károkozásokból és/vagy bűncselekményekből – a kémkedést, a szabotázst és a terrorizmust is ideértve – eredően helyi szinten fennálló fenyegetéssel.

(3) A jogosulatlan hozzáférés és hozzáférhetővé tétel, valamint az adatok és anyagok sértetlensége vagy rendelkezésre állása megszűnésének megelőzése érdekében az Európai Unió Bírósága belső szükséghelyzeti tervének figyelembe kell vennie a FIDUCIA adatok szükséghelyzet esetén való védelmének a szükségességét.

(4) A súlyos mulasztások vagy események által a FIDUCIA adatok kezelésére és tárolására gyakorolt hatások csökkentését szolgáló megelőző és helyreállító intézkedéseket az Európai Unió Bírósága belső szükséghelyzeti terve tartalmazza.

7. cikk

Személyekre vonatkozó biztonsági intézkedések

(1) A FIDUCIA adatokhoz való hozzáférés csak azon személyeknek biztosítható, akiknek:

— szükségük van azok ismeretére,

— a jelen cikk (2) bekezdésére is figyelemmel engedélyezték számukra a FIDUCIA adatokhoz való hozzáférést, valamint

— tájékoztatták őket a felelősségükről.

(2) A Törvényszék bíráit a jogállásuknál fogva úgy kell tekinteni, mint akik a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkeznek.

(3) Azon eljárás szabályait, amelynek célja annak eldöntése, hogy az Európai Unió Bíróságának valamely tisztviselője vagy egyéb alkalmazottja számára a lojalitását, feddhetetlenségét és megbízhatóságát figyelembe véve engedélyezhető-e a FIDUCIA adatokhoz való hozzáférés, az I. melléklet tartalmazza.

(4) A FIDUCIA adatokhoz való hozzáférés engedélyezését megelőzően, majd azt követően rendszeres időközönként valamennyi érintett személyt tájékoztatni kell a FIDUCIA adatok jelen határozat szerinti védelme területén őket terhelő felelősségről, az érintett személyeknek pedig e felelősséget írásban tudomásul kell venniük.

8. cikk

Fizikai biztonság

(1) A „fizikai biztonság” alatt a FIDUCIA adatokhoz való jogosulatlan hozzáférés megakadályozását célzó fizikai és technikai védelmi intézkedések alkalmazását kell érteni.

(2) A fizikai biztonsági intézkedések célja a FIDUCIA iroda helyiségeibe megtévesztés vagy erőszak útján történő bármilyen behatolás megakadályozása, a jogosulatlan cselekményektől való elrettentés, továbbá azok megakadályozása és felderítése, valamint a FIDUCIA adatokhoz a szükséges ismeret elvével összhangban hozzáférési engedéllyel rendelkező, illetve nem rendelkező személyek közötti különbségtétel lehetővé tétele. Ezeket az intézkedéseket kockázatkezelési eljárás alapján kell meghatározni.

(3) A fizikai biztonsági intézkedéseket a FIDUCIA iroda azon helyiségei tekintetében kell bevezetni, amelyekben a FIDUCIA adatokat kezelik és tárolják. Ezen intézkedések célja, hogy az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályokkal összhangban a SECRET UE / EU SECRET minősítésű EUMA-nak biztosított védelemmel egyenértékű védelmet biztosítsanak. Semmilyen FIDUCIA adat nem tárolható, sem pedig betekintés tárgyát nem képezheti a FIDUCIA iroda azon helyiségein kívül, amelyeket olyan területen belül alakítottak ki e célokra, amely maga is biztonsági terület.

(4) A FIDUCIA adatok védelmére csak olyan berendezések vagy eszközök használhatók, amelyek megfelelnek az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak.

(5) A jelen cikk alkalmazásának részletes szabályait a II. melléklet tartalmazza.

9. cikk

A FIDUCIA adatok kezelése

(1) A „FIDUCIA adatok kezelése" alatt azon adminisztratív intézkedések alkalmazását kell érteni, amelyek a FIDUCIA adatoknak a Törvényszék előtti eljárás során mindvégig, legkésőbb pedig az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártáig történő védelmére, valamint az ilyen adatok annak megelőzése és felderítése érdekében történő ellenőrzésére irányulnak, hogy azok szándékosan vagy véletlenszerűen illetéktelen személy tudomására jussanak vagy elvesszenek.

(2) A FIDUCIA adatok kezelésére irányuló intézkedések különösen a FIDUCIA adatok nyilvántartásba vételére, az azokba való betekintésre, azok előállítására, másolására, tárolására, visszaszolgáltatására és megsemmisítésére vonatkoznak.

(3) A FIDUCIA adatokat a kézhezvételük során és bármilyen kezelést megelőzően a FIDUCIA iroda nyilvántartásba veszi.

(4) A FIDUCIA iroda helyiségeit a biztonsági hatóság rendszeresen átvizsgálja.

(5) A jelen cikk alkalmazásának részletes szabályait a III. melléklet tartalmazza.

10. cikk

Az elektronikus úton kezelt FIDUCIA adatok védelme

(1) A FIDUCIA adatok kezelésére használt információs és kommunikációs rendszereket (számítógépeket és perifériákat) a FIDUCIA iroda helyiségeiben kell elhelyezni. E rendszereket minden informatikai hálózattól el kell szigetelni.

(2) Biztonsági intézkedéseket kell tenni a FIDUCIA adatok kezelésére használt informatikai berendezések az ellen történő védelme érdekében, hogy az ilyen adatok nem szándékos elektromágneses kisugárzás folytán illetéktelen személy tudomására jussanak (az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályokkal összhangban a SECRET UE / EU SECRET minősítésű EUMA vonatkozásában alkalmazott biztonsági intézkedésekkel egyenértékű biztonsági intézkedések).

(3) Az információs és kommunikációs rendszereket a biztonsági hatóságnak akkreditálnia kell, amelynek meg kell győződnie arról, hogy e rendszerek megfelelnek az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak.

(4) A jelen cikk alkalmazásának részletes szabályait a IV. melléklet tartalmazza.

11. cikk

Külső beavatkozás esetén irányadó biztonság

(1) A „külső beavatkozás esetén irányadó biztonság" alatt a FIDUCIA adatok védelmének biztosítását szolgáló intézkedések olyan szerződő felek általi alkalmazását kell érteni, akiknek az informatikai hálózattól elszigetelt információs és kommunikációs rendszerek karbantartása keretében, vagy pedig a FIDUCIA adatok abból a célból történő sürgős elmozdítását igénylő beavatkozás során kell közreműködniük, hogy azokat biztonságos helyen helyezzék el.

(2) A biztonsági hatóság a valamely tagállamban nyilvántartásba vett szerződő feleket bízhat meg olyan feladatok elvégzésével, amelyek a szerződésük értelmében a FIDUCIA adatokhoz való hozzáféréssel járnak, vagy azt szükségessé teszik.

(3) A biztonsági hatóság gondoskodik arról, hogy a szerződések odaítélése során tiszteletben tartsák a jelen határozatban megállapított és a szerződésben említett biztonsági minimumszabályokat.

(4) Valamely szerződő fél személyi állományának tagjai csak azt követően férhetnek hozzá a FIDUCIA adatokhoz, hogy a biztonsági hatóság a Nemzeti Biztonsági Hatóság vagy bármely más illetékes biztonsági hatóság által a nemzeti jogszabályoknak és rendelkezéseknek megfelelően kibocsátott személyi biztonsági tanúsítvány alapján erre engedélyt adott nekik.

(5) A jelen cikk alkalmazásának részletes szabályait az V. melléklet tartalmazza.

12. cikk

A FIDUCIA adatok digitális terjesztésének, valamint közlésének és cseréjének kizártsága

(1) A FIDUCIA adatok digitális formában semmilyen esetben nem terjeszthetők.

(2) A Törvényszék a FIDUCIA adatokat sem az uniós intézmények, szervek, hivatalok vagy ügynökségek, sem a tagállamok, sem a jogvitában részt vevő egyéb felek, sem pedig harmadik személy részére nem továbbítja.

13. cikk

A biztonsági szabályok megsértése és a FIDUCIA adatok illetéktelen személy tudomására jutása

(1) A biztonsági szabályok megsértése valamely személy olyan cselekményét vagy mulasztását jelenti, amely ellentétes a jelen határozatban megállapított biztonsági szabályokkal.

(2) Az illetéktelen személy tudomására jutás akkor következik be, ha a biztonsági szabályok megsértése folytán egyes FIDUCIA adatok olyan személyek részére váltak egészben vagy részben hozzáférhetővé, akik nem rendelkeznek engedéllyel, vagy nem tekinthetők engedéllyel rendelkezőnek.

(3) A biztonsági szabályok minden tényleges vagy feltételezett megsértését haladéktalanul jelezni kell a biztonsági hatóságnak.

(4) Ha bebizonyosodik, vagy ésszerű indokok alapján feltételezhető, hogy egyes FIDUCIA adatok illetéktelen személy számára hozzáférhetővé váltak vagy elvesztek, a biztonsági hatóság a Törvényszék elnökével és hivatalvezetőjével szorosan együttműködve, az alkalmazandó rendelkezésekkel összhangban megtesz minden megfelelő intézkedést annak érdekében, hogy:

a) erről értesítse azt a felperest vagy alperest, aki az érintett tájékoztatásokat vagy mellékleteket benyújtotta;

b) a hatáskörrel rendelkező hatóságot közigazgatási vizsgálat megindítására hívja fel;

c) értékelje az Uniónak, illetve egy vagy több tagállamának a biztonsága vagy nemzetközi kapcsolatainak irányítása tekintetében okozott esetleges kárt;

d) elkerülje a tényállás megismétlődését, valamint

e) a hatáskörrel rendelkező hatóságokat értesítse a megtett intézkedésekről.

(5) A jelen határozatban megállapított biztonsági szabályok megsértéséért felelős bármely személlyel szemben az irányadó rendelkezésekkel összhangban fegyelmi szankció alkalmazható. A FIDUCIA adatok illetéktelen személy tudomására jutásáért vagy elvesztéséért felelős bármely személlyel szemben az irányadó rendelkezésekkel összhangban fegyelmi szankció alkalmazható, és/vagy bírósági eljárás indítható.

14. cikk

A Törvényszék biztonsági szervezete

(1) A FIDUCIA adatoknak a jelen határozat alkalmazásával történő védelméről a FIDUCIA iroda gondoskodik.

(2) A jelen határozat megfelelő alkalmazásáért a biztonsági hatóság felelős. Ennek érdekében a biztonsági hatóság:

a) alkalmazza az Európai Unió Bíróságának biztonsági politikáját, és azt időszakonként felülvizsgálja;

b) ellenőrzi a jelen határozatnak a FIDUCIA iroda általi végrehajtását;

c) adott esetben, a 13. cikkben megállapított feltételek mellett vizsgálatot rendel el a FIDUCIA adatok illetéktelen személy tudomására jutásának vagy elvesztésének bármely tényleges vagy feltételezett esete tárgyában;

d) lefolytatja a FIDUCIA adatok védelmének biztosítására szolgáló, a FIDUCIA iroda helyiségeiben érvényes biztonsági intézkedések időszakos felülvizsgálatait.

15. cikk

Gyakorlati végrehajtási szabályok

A jelen határozat gyakorlati végrehajtási szabályait a biztonsági hatóság a Törvényszék hivatalvezetőjével egyetértésben állapítja meg.

16. cikk

Hatálybalépés

A jelen határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon lép hatályba.

Kelt Luxembourgban, 2016. szeptember 14-én.

E. COULON	M. JAEGER
hivatalvezető	*elnök*

I. MELLÉKLET

SZEMÉLYEKRE VONATKOZÓ BIZTONSÁGI INTÉZKEDÉSEK

1. A jelen melléklet a határozat 7. cikke alkalmazásának szabályait tartalmazza.

2. A Törvényszék hivatalvezetőjének feladata, hogy – saját felelősségi körén belül és szigorúan a szükséges mértékben – összeállítsa azon álláshelyek jegyzékét, amelyek esetében szükséges a FIDUCIA adatokhoz való hozzáférés, és amelyek következésképpen megkövetelik, hogy a Törvényszéken belül a szóban forgó álláshelyeket betöltő tisztviselők és egyéb alkalmazottak számára engedélyezzék a FIDUCIA adatokhoz való hozzáférést.

3. A FIDUCIA adatokhoz való hozzáférés engedélyezése érdekében a FIDUCIA iroda az érintett tisztviselő vagy egyéb alkalmazott által kitöltött biztonsági kérdőívet megküldi azon tagállam Nemzeti Biztonsági Hatóságának, amely tagállamnak az érintett személy az állampolgára, vagy bármely más illetékes, az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályokban megjelölt nemzeti hatóságnak (a továbbiakban: illetékes NBH), és felkéri, hogy folytasson le a SECRET UE / EU SECRET minősítési szintnek megfelelő biztonsági ellenőrzést.

4. Az illetékes NBH a biztonsági ellenőrzés végén, az érintett tagállamban hatályos jogszabályoknak és rendelkezéseknek megfelelően eljárva értesíti a FIDUCIA irodát a szóban forgó ellenőrzés eredményéről.

5. Amennyiben a biztonsági ellenőrzés végén az illetékes NBH bizonyosságot szerzett arról, hogy nincs olyan kedvezőtlen tájékoztatás, amely kétségbe vonhatná az érintett személy lojalitását, feddhetetlenségét és megbízhatóságát, az illetékes kinevezésre jogosult hatóság megadhatja ezen érintett személynek a FIDUCIA adatokhoz való hozzáférési engedélyt.

6. Amennyiben a biztonsági ellenőrzés végén a fenti 5. pontban foglaltakról nem lehetett bizonyosságot szerezni, a kinevezésre jogosult hatóság erről értesíti az érintett személyt. Ilyen esetben a FIDUCIA iroda a kinevezésre jogosult hatóság utasítása alapján eljárva felkérheti az illetékes NBH-t, hogy adjon meg minden olyan további felvilágosítást, amelyet a rá vonatkozó nemzeti jogszabályoknak és rendelkezéseknek megfelelően megadhat. A biztonsági vizsgálat eredményének megerősítése esetén a FIDUCIA adatokhoz való hozzáférési engedély nem adható meg.

7. A FIDUCIA adatokhoz való hozzáférési engedély öt évre érvényes. Az engedélyt vissza kell vonni, ha az érintett személy elhagyja azt az álláshelyet, amelynek esetében szükséges a FIDUCIA adatokhoz való hozzáférés, illetve ha a kinevezésre jogosult hatóság szerint olyan indokok állnak fenn, amelyek az engedély visszavonását igazolják.

8. A FIDUCIA adatokhoz való hozzáférési engedély a 3–5. pont szerinti eljárásnak megfelelően megújítható.

9. A FIDUCIA iroda a FIDUCIA adatokhoz való hozzáférési engedélyekről nyilvántartást vezet.

10. Amennyiben olyan biztonsági kockázattal kapcsolatos információk jutnak a FIDUCIA iroda tudomására, amelyet a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkező személy jelent, a FIDUCIA iroda erről értesíti az illetékes kinevezésre jogosult hatóságot, a kinevezésre jogosult hatóság pedig felfüggesztheti a FIDUCIA adatokhoz való hozzáférést, vagy visszavonhatja az ilyen adatokhoz való hozzáférési engedélyt.

11. Sürgős esetben a kinevezésre jogosult hatóság – az illetékes NBH-val folytatott konzultációt követően és a kedvezőtlen tájékoztatások hiányáról való meggyőződés érdekében lefolytatott előzetes vizsgálatok eredményeitől függően – az érintett tisztviselőknek és egyéb alkalmazottaknak a FIDUCIA adatokhoz való ideiglenes hozzáférési engedélyt adhat. Ezen ideiglenes engedély érvényessége a 3–5. pont szerinti eljárás végéig áll fenn, azonban nem haladhatja meg a biztonsági ellenőrzés lefolytatása iránti kérelemnek az illetékes NBH-hoz való benyújtásától számított hat hónapot.

12. Azoknak a személyeknek, akik erre engedélyt kaptak, a FIDUCIA adatokhoz való hozzáférés előtt képzésen kell részt venniük, amelynek célja felkészíteni őket a FIDUCIA adatok kezelésével kapcsolatos felelősségük vállalására. A FIDUCIA adatokhoz való hozzáférés ténylegesen csak e képzést és a felelősség írásbeli tudomásulvételét követően gyakorolható.

II. MELLÉKLET

FIZIKAI BIZTONSÁG

I. BEVEZETÉS

1. A jelen melléklet a határozat 8. cikke alkalmazásának szabályait tartalmazza. Megállapítja a FIDUCIA iroda azon helyiségeinek fizikai védelmére vonatkozó minimumszabályokat, amelyekben a FIDUCIA adatokat kezelik és tárolják.

2. A fizikai biztonsági intézkedések célja a FIDUCIA adatokhoz való jogosulatlan hozzáférés megakadályozása az alábbiak révén:

   a) a FIDUCIA adatok megfelelő módon való kezelésének és tárolásának biztosítása;

   b) a FIDUCIA adatokhoz a szükséges ismeret elvével összhangban hozzáférési engedéllyel rendelkező, illetve nem rendelkező személyek közötti különbségtétel lehetővé tétele;

   c) elrettentő hatás a jogosulatlan cselekmények megakadályozásával és felderítésével, valamint

   d) a FIDUCIA iroda helyiségeibe megtévesztés vagy erőszak útján történő bármilyen behatolás megakadályozásával, illetve késleltetésével.

3. A fizikai biztonsági intézkedéseket a FIDUCIA adatok fenyegetettségének értékelése alapján kell megválasztani. Ezek az intézkedések figyelembe veszik a FIDUCIA iroda helyiségeinek elhelyezkedését és felépítését. A biztonsági hatóság megállapítja az alábbi fizikai intézkedések mindegyike esetében elérendő biztonsági szintet:

   a) a védelmet igénylő terület határait védő kordon;

   b) az Európai Unió Bíróságának biztonsági irányítóközpontjával összekötött behatolásjelző rendszer;

   c) elektronikus vagy elektromechanikus eszközökkel működő és a biztonsági személyi állomány tagja által működtetett belépés-ellenőrzési rendszer;

   d) képzett, felügyelt és a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkező biztonsági személyi állomány;

   e) a biztonsági személyi állomány által működtetett és a behatolásjelző rendszerrel, valamint a belépés-ellenőrzési rendszerrel összekötött zártláncú videomegfigyelő rendszer;

   f) közvetlen vagy a videomegfigyelő rendszeren keresztüli hatékony megfigyelést lehetővé tevő biztonsági világítás;

   g) bármely más megfelelő fizikai intézkedés, amelynek célja a jogosulatlan belépéssel szembeni elrettentés vagy az ilyen belépés felderítése, illetve a valamely FIDUCIA adatba való betekintésnek, továbbá az ilyen adat elvesztésének vagy megrongálódásának a megelőzése.

II. A FIDUCIA ADATOK TÁROLÁSÁRA ÉS AZ AZOKBA VALÓ BETEKINTÉSRE SZOLGÁLÓ HELYISÉGEK

Fizikailag védett tárolási és betekintési helyiségek kialakítása

4. A FIDUCIA adatok tárolása és az azokba való betekintés céljából biztonsági helyiségeket kell kialakítani. A FIDUCIA adatok tárolása és az azokba való betekintés csak a FIDUCIA iroda olyan helyiségeiben történhet, amelyek minden szempontból megfelelnek az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak.

5. E helyiségeken belül a FIDUCIA adatokat olyan biztonsági tárolóeszközökben kell tárolni, amelyek szintén minden szempontból megfelelnek az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak.

6. A FIDUCIA iroda helyiségeibe semmilyen kommunikációs rendszer (telefon vagy egyéb elektronikai eszköz) nem vezethető be.

7. A FIDUCIA iroda tárgyalóhelyiségét védeni kell a lehallgatással szemben. E helyiségben rendszeres időközönként elektronikus biztonsági átvizsgálást kell lefolytatni.

Belépés a tárolási és betekintési helyiségekbe

8. A FIDUCIA irodába való belépést videomegfigyelés alatt álló azonosító zsilipkapuval kell ellenőrizni.

9. Azok a személyek, akik a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkeznek, továbbá akiket engedéllyel rendelkezőknek kell tekinteni, a FIDUCIA adatokba való betekintés céljából a jelen határozat 7. cikkének (1) és (2) bekezdésében megállapított feltételek mellett léphetnek be a FIDUCIA iroda helyiségeibe.

10. A biztonsági hatóság kivételesen belépési engedélyt adhat engedéllyel nem rendelkező olyan személyeknek is, akiknek a FIDUCIA irodában való tartózkodása elengedhetetlenül szükséges, azzal a feltétellel, hogy az e helyiségekbe való belépés nem jelent hozzáférést a FIDUCIA adatokhoz, amelyek a biztonsági tárolóeszközökben elzárva maradnak. E személyek csak a FIDUCIA irodához tartozó olyan személy kíséretében és állandó felügyelete mellett léphetnek be, aki a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkezik.

11. A FIDUCIA iroda helyiségeibe történő valamennyi belépést rögzíteni kell a belépések nyilvántartásában. E nyilvántartást az e helyiségekben elhelyezett munkaállomáson kell vezetni. Az e célra használt információs és kommunikációs rendszernek meg kell felelnie a határozat 10. cikkében, valamint IV. mellékletében megállapított biztonsági követelményeknek.

12. A FIDUCIA adatok írásbeli felhasználását szabályozó védelmi intézkedések ugyanezen adatok szóbeli felhasználása esetén is alkalmazandók.

III. A FIDUCIA ADATOK VÉDELMÉRE SZOLGÁLÓ KULCSOK ÉS KOMBINÁCIÓK ELLENŐRZÉSE

13. A biztonsági hatóság meghatározza a FIDUCIA iroda helyiségei és a biztonsági tárolóeszközök kulcsainak és kombinációinak kezelésére vonatkozó eljárásokat. Ezek az eljárások a jogosulatlan hozzáféréssel szembeni védelmet biztosítják.

14. A kombinációkat meg kell jegyezniük a személyi állomány lehető legkisebb számú azon tagjainak, akiknek azokat ismerniük kell. A FIDUCIA adatok tárolására szolgáló biztonsági tárolóeszközök kombinációit az alábbi esetekben meg kell változtatni;

a) új tárolóeszköz átvételekor;

b) a kombinációt ismerő személyi állomány minden változásakor;

c) ha az adatok ténylegesen vagy feltételezhetően illetéktelen személy tudomására jutottak;

d) ha a záron karbantartást vagy javítást végeztek;

e) legalább tizenkét havonta.

15. A FIDUCIA adatok fizikai védelmét szolgáló műszaki berendezésnek meg kell felelnie az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak. E szabályok betartásáért a biztonsági hatóság felelős.

16. A műszaki berendezést időszakosan át kell vizsgálni, és rendszeres időközönként karban kell tartani. A karbantartás során figyelembe kell venni az átvizsgálások eredményét annak biztosítása érdekében, hogy a berendezés folyamatosan a lehető leghatékonyabban működjön.

17. A különböző biztonsági intézkedések és a teljes biztonsági rendszer hatékonyságát minden egyes átvizsgálás során újra kell értékelni.

III. MELLÉKLET

A FIDUCIA ADATOK KEZELÉSE

I. BEVEZETÉS

1. A jelen melléklet a határozat 9. cikke alkalmazásának szabályait tartalmazza. Megállapítja azon adminisztratív intézkedéseket, amelyek a FIDUCIA adatoknak a Törvényszék előtti eljárás során mindvégig, legkésőbb pedig az Európai Unió Bírósága alapokmánya 56. cikkének első bekezdése szerinti határidő lejártáig történő védelmére, valamint az ilyen adatok annak megelőzése és felderítése érdekében történő ellenőrzésére irányulnak, hogy azok szándékosan vagy véletlenszerűen illetéktelen személy tudomására jussanak vagy elvesszenek.

II. A FIDUCIA ADATOK NYILVÁNTARTÁSA

2. Létre kell hozni a FIDUCIA adatok nyilvántartását. A FIDUCIA iroda e nyilvántartást a FIDUCIA iroda helyiségeiben elhelyezett munkaállomáson vezeti. Az e nyilvántartás vezetésére használt információs és kommunikációs rendszernek meg kell felelnie a határozat 10. cikkében, valamint IV. mellékletében megállapított biztonsági követelményeknek.

III. A FIDUCIA ADATOK NYILVÁNTARTÁSBA VÉTELE

3. A jelen határozat alkalmazásában a biztonsági célú nyilvántartásba vétel (a továbbiakban: nyilvántartásba vétel) alatt olyan eljárások alkalmazását kell érteni, amelyek lehetővé teszik a FIDUCIA adat életciklusának nyomon követését, ideértve a megsemmisítését is.

4. A FIDUCIA adatok nyilvántartásba vételéről a FIDUCIA iroda gondoskodik.

5. A FIDUCIA iroda az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott tájékoztatásokon vagy mellékleteken automatikusan elhelyezi a FIDUCIA jelölést. A FIDUCIA iroda a FIDUCIA adatot felveszi a FIDUCIA adatok nyilvántartásába.

6. A FIDUCIA iroda a FIDUCIA adatok nyilvántartásához mellékelt jelentést készít, amelyben pontosan megjelöli az adat kézhezvételének körülményeit. Az adatot ezt követően az előző pontban megállapított szabályok szerint kell kezelni.

7. A FIDUCIA adatnak az 5. és 6. pont alapján a FIDUCIA adatok nyilvántartásába történő felvétele azon eljárási nyilvántartásba vétel sérelme nélkül történik, amelyet a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkező személyek a Hivatalon belül végeznek.

IV. A FIDUCIA ADATOK KEZELÉSE

Jelölés

8. Ha az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése keretében EUMA-t vagy bármely egyéb olyan adatot nyújtanak be, amellyel kapcsolatban jelzik, hogy annak közlése sértené az Uniónak, illetve egy vagy több tagállamának a biztonságát vagy nemzetközi kapcsolatainak irányítását, a FIDUCIA iroda az ilyen adaton elhelyezi a FIDUCIA jelölést.

9. A FIDUCIA jelölést a dokumentum minden egyes részén világosan és szabályosan el kell helyezni, függetlenül attól, hogy az adat milyen formában jelenik meg: papírváltozatban, hanganyagként, elektronikus vagy egyéb formában.

FIDUCIA adat létrehozása

10. A jelen határozat 4. cikkének (2) és (3) bekezdésében megjelölt FIDUCIA adatot csak olyan személy hozhat létre, aki a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkezik, vagy akit engedéllyel rendelkezőnek kell tekinteni.

11. A FIDUCIA iroda minden létrehozott FIDUCIA adatot felvesz a FIDUCIA adatok nyilvántartásába.

12. Minden létrehozott FIDUCIA adatra alkalmazandó a FIDUCIA adatok kezelésére vonatkozó, a jelen határozatban és annak mellékleteiben megállapított valamennyi szabály.

A FIDUCIA jelölés törlése

13. A FIDUCIA adatok jelölése két esetben kerül eltávolításra:

    a) Ha az a felperes vagy alperes, aki a FIDUCIA adatot benyújtotta, engedélyezi annak az ellenérdekű felperes vagy alperes részére történő megküldését, akkor az eredetileg megküldött adat, valamint az ezen adat alapján létrehozott valamennyi adat FIDUCIA jelölését el kell távolítani;

    b) Ha a FIDUCIA adatot visszaadják annak a felperesnek vagy alperesnek, aki azt benyújtotta.

14. A FIDUCIA jelölés törlését a FIDUCIA iroda végzi el, amely e törlést felveszi a FIDUCIA adatok nyilvántartásába.

15. A FIDUCIA jelölés törlése nem jelenti az EUMA minősítésének megszüntetését.

V. A FIDUCIA ADATOK MÁSOLATAI

16. A FIDUCIA adatokról nem készíthetők másolatok, kivéve ha azok elengedhetetlenül szükségesek. Ez utóbbi esetben a másolatokat a FIDUCIA iroda készíti el, amely azokat számozással látja el és nyilvántartásba veszi.

17. A másolatokra alkalmazandó a jelen határozatban és annak mellékleteiben megállapított valamennyi biztonsági szabály.

VI. A FIDUCIA ADATOK MEGSEMMISÍTÉSE

18. Ha az eljárási szabályzat 105. cikkének (1) vagy (2) bekezdése alapján benyújtott tájékoztatásokat vagy mellékleteket visszaadják annak a felperesnek vagy alperesnek, aki azokat benyújtotta, akkor minden olyan adatot, amely egészben vagy részben átveszi az ilyen tájékoztatások vagy mellékletek tartalmát, az esetleg készített másolatokkal együtt meg kell semmisíteni.

19. A FIDUCIA adatoknak a 18. pont szerinti megsemmisítését a FIDUCIA iroda az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak megfelelő módszerek alkalmazásával végzi annak érdekében, hogy megakadályozza azok teljes vagy részleges rekonstruálását.

20. A FIDUCIA adatoknak a 18. pont szerinti megsemmisítését olyan tanú jelenlétében kell végezni, aki a FIDUCIA adatokhoz való hozzáférési engedéllyel rendelkezik.

21. A FIDUCIA iroda a megsemmisítésről jegyzőkönyvet készít.

22. A megsemmisítésről készített jegyzőkönyvet mellékelni kell a FIDUCIA adatok nyilvántartásához. A jegyzőkönyv egy másolatát meg kell küldeni annak a felperesnek vagy alperesnek, aki az érintett dokumentumot benyújtotta.

IV. MELLÉKLET

AZ ELEKTRONIKUS ÚTON KEZELT FIDUCIA ADATOK VÉDELME

1. A jelen melléklet a határozat 10. cikke alkalmazásának szabályait tartalmazza.

2. A FIDUCIA adatok kezelésére csak olyan elektronikai készülékek (munkaállomások, nyomtatók, fénymásolók) használhatók, amelyek nincsenek összekötve az informatikai hálózattal, és amelyeket a FIDUCIA iroda helyiségeiben helyeztek el.

3. A FIDUCIA adatok kezelésére használt valamennyi elektronikai készüléknek meg kell felelnie az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak. E készülékek biztonságáról a teljes életciklusuk alatt gondoskodni kell.

4. Az internethez és az egyéb eszközökhöz (LAN, WLAN, Bluetooth stb.) való bármilyen kapcsolódás lehetőségét állandó jelleggel ki kell iktatni.

5. A munkaállomásokat megfelelő vírusvédelemmel kell ellátni. A vírusvédelmet olyan CD-ROM-mal vagy USB-kulccsal kell frissíteni, amelyeket kizárólag erre a célra használnak.

6. A nyomtatók és a fénymásolók memóriáit minden karbantartási művelet előtt törölni kell.

7. Az I. melléklet szerinti ellenőrzések lefolytatására irányuló felkérések kezelésére csak az uniós intézményeken belül az EUMA védelme tárgyában alkalmazandó szabályoknak megfelelően jóváhagyott kriptográfiai termékek használhatók.

V. MELLÉKLET

KÜLSŐ BEAVATKOZÁS ESETÉN IRÁNYADÓ BIZTONSÁG

1. A jelen melléklet a határozat 11. cikke alkalmazásának szabályait tartalmazza.

2. A szerződő felek csak az informatikai hálózattól elszigetelt információs és kommunikációs rendszerek karbantartása keretében, vagy pedig a FIDUCIA adatok abból a célból történő sürgős elmozdítását igénylő beavatkozás során férhetnek hozzá a FIDUCIA adatokhoz, hogy azokat biztonságos helyen helyezzék el.

3. A biztonsági hatóság a külső beavatkozásra vonatkozó olyan iránymutatásokat dolgoz ki, amelyek kiterjednek különösen a szerződő felek személyi biztonsági tanúsítványára, valamint az e melléklet szerinti szerződések tartalmára.

4. Az informatikai hálózattól elszigetelt információs és kommunikációs rendszerek karbantartására irányuló pályázati eljárásokkal kapcsolatos dokumentumokat, valamint az e tárgyban kötött szerződést FIDUCIA jelöléssel kell ellátni, amennyiben azok olyan adatokat tartalmaznak, amelyek jogosulatlan hozzáférhetővé tétele sérthetné az Uniónak, illetve egy vagy több tagállamának a biztonságát vagy nemzetközi kapcsolatainak irányítását. E szerződés biztonsági melléklete tartalmazza azokat a rendelkezéseket, amelyek a szerződő féllel szemben előírják a jelen határozatban megállapított minimumszabályok tiszteletben tartását. E minimumszabályok tiszteletben tartásának elmulasztása elegendő indokot jelenthet a szerződés felbontására.

5. Annak a szerződésnek, amely a FIDUCIA adatok abból a célból történő sürgős elmozdítását igénylő beavatkozásokkal jár, hogy azokat biztonságos helyen helyezzék el, tartalmaznia kell azon biztonsági őrök számát, akiknek személyi biztonsági tanúsítvánnyal kell rendelkezniük. E szerződés a lefolytatandó eljárásokat illetően semmilyen konkrét adatot nem tartalmazhat. E szerződést nem látják el FIDUCIA jelöléssel.

6. A szerződő fél nem vehet igénybe alvállalkozót a pályázati felhívásban és a szerződésben megjelölt olyan tevékenységek elvégzésére, amelyek a FIDUCIA adatokhoz való hozzáféréssel járnak, vagy azt szükségessé teszik.