A BIZOTTSÁG HATÁROZATA

(2010. május 4.)

a központi SIS II és a kommunikációs infrastruktúra működésére vonatkozó biztonsági tervről

(2010/261/EU)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló, 2006. december 20-i 1987/2006/EK európai parlamenti és tanácsi rendeletre [1] és különösen annak 16. cikkére,

tekintettel a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló, 2007. június 12-i 2007/533/IB tanácsi határozatra [2] és különösen annak 16. cikkére,

mivel:

(1) Az 1987/2006/EK rendelet 16. cikke és a 2007/533/IB határozat 16. cikke úgy rendelkezik, hogy az igazgató hatóság a központi SIS II-vel és a Bizottság a kommunikációs infrastruktúrával összefüggésben meghozza a szükséges intézkedéseket, beleértve a biztonsági terv elfogadását is.

(2) A 1987/2006/EK rendelet 15. cikkének (4) bekezdése és a 2007/533/IB határozat 15. cikkének (4) bekezdése úgy rendelkezik, hogy mielőtt az igazgató hatóság megkezdi tevékenységét, átmenetileg a Bizottság felel a központi SIS II üzemeltetési igazgatásáért.

(3) Mivel az igazgató hatóság még nem jött létre, a Bizottság által elfogadandó biztonsági terv átmeneti ideig a központi SIS II-re is alkalmazandó.

(4) A 45/2001/EK európai parlamenti és tanácsi rendeletet [3] alkalmazni kell akkor, amikor a Bizottság személyes adatokat dolgoz fel a SIS II üzemeltetési igazgatásával kapcsolatos feladatainak ellátása során.

(5) A 1987/2006/EK rendelet 15. cikkének (7) bekezdése és a 2007/533/IB határozat 15. cikkének (7) bekezdése úgy rendelkezik, hogy amennyiben a Bizottság az átmeneti időszakban, mielőtt az igazgató hatóság megkezdi tevékenységét, átruházza feladatát, biztosítania kell, hogy az átruházás ne érintse hátrányosan az akár a Bíróság, akár a Számvevőszék, akár az európai adatvédelmi biztos által, az uniós jog alapján végzett, hatékony ellenőrzési mechanizmusokat.

(6) Tevékenységének megkezdését követően az igazgató hatóság elfogadja a központi SIS-re vonatkozó saját biztonsági tervét. Ez a biztonsági terv ezért a központi SIS II tekintetében hatályát veszti, amikor az igazgató hatóság megkezdi tevékenységét.

(7) Az 1987/2006/EK rendelet 4. cikkének (3) bekezdése és a 2007/533/IB határozat 4. cikkének (3) bekezdése úgy rendelkezik, hogy a technikai felügyeletet és igazgatást ellátó elsődleges CS-SIS Strasbourgban (Franciaország), az e rendszer meghibásodása esetén az elsődleges CS-SIS minden funkcióját biztosítani képes tartalék CS-SIS pedig Sankt Johann im Pongauban (Ausztria) található.

(8) A biztonsági tervben elő kell irányozni egy rendszerbiztonsági tisztviselői pozíció létrehozását a központi SIS II és a kommunikációs infrastruktúra vonatkozásában felmerülő biztonsági feladatok ellátására, és elő kell irányozni egy-egy helyi biztonsági tisztviselői pozíció létrehozását egyrészről a központi SIS II, másrészről a kommunikációs infrastruktúra vonatkozásában felmerülő biztonsági feladatok ellátására. A biztonsági eseményekre való hatékony és azonnali válaszadás és a biztonsági eseményekkel kapcsolatos jelentéstétel érdekében meg kell határozni a biztonsági tisztviselők feladatait.

(9) Biztonsági politikát kell kidolgozni, amelyben e határozat rendelkezéseivel összhangban valamennyi technikai és szervezési részlet meghatározásra kerül.

(10) Meg kell állapítani a központi SIS II és a kommunikációs infrastruktúra működésének megfelelő biztonsági szintjét biztosító intézkedéseket,

[1] HL L 381., 2006.12.28., 4. o.
[2] HL L 205., 2007.8.7., 63. o.
[3] HL L 8., 2001.1.12., 1. o.

ELFOGADTA EZT A HATÁROZATOT:

I FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

(1) Ez a határozat a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK európai parlamenti és tanácsi rendelet 16. cikkének (1) bekezdésének, és 2007/533/IB határozat 16. cikkének (1) bekezdésének értelmében átmeneti időszakra, az igazgató hatóság tevékenységének megkezdéséig létrehozza a központi SIS II és az abban feldolgozott adatok rendelkezésre állását, sértetlenségét és bizalmas természetét veszélyeztető fenyegetések elleni védelem biztosítását célzó biztonsági rendszert és intézkedéseket (biztonsági terv).

(2) Ez a határozat a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK európai parlamenti és tanácsi rendelet 16. cikkének (1) bekezdésének, és 2007/533/IB határozat 16. cikkének értelmében létrehozza a kommunikációs infrastruktúra rendelkezésre állását, sértetlenségét és bizalmas természetét veszélyeztető fenyegetések elleni védelem biztosítását célzó biztonsági rendszert és intézkedéseket (biztonsági terv).

II. FEJEZET

FELÉPÍTÉS, FELADATOK ÉS ESEMÉNYKEZELÉS

2. cikk

A Bizottság feladatai

(1) A Bizottság végrehajtja a központi SIS II-re vonatkozó, e határozatban említett biztonsági intézkedéseket, és nyomon követi azok eredményességét.

(2) A Bizottság végrehajtja a kommunikációs infrastruktúrára vonatkozó, e határozatban említett biztonsági intézkedéseket, és nyomon követi azok eredményességét.

(3) A Bizottság rendszerbiztonsági tisztviselőt jelöl ki tisztviselői közül. A rendszerbiztonsági tisztviselőt a Bizottság Jogérvényesülés, Szabadság és Biztonság Főigazgatóságának főigazgatója nevezi ki. A rendszerbiztonsági tisztviselő mindenekelőtt a következő feladatokat látja el:

a) kidolgozza az e határozat 7. cikkében meghatározott biztonsági politikát;

b) nyomon követi a központi SIS II-re vonatkozó biztonsági eljárások végrehajtásának hatékonyságát;

c) nyomon követi a kommunikációs infrastruktúrára vonatkozó biztonsági eljárások végrehajtásának hatékonyságát;

d) hozzájárul az 1987/2006/EK rendelet 50. cikkében és a 2007/533/IB határozat 66. cikkében említett, biztonsággal kapcsolatos jelentések kidolgozásához;

e) koordinációs és támogatási feladatokat lát el az európai adatvédelmi biztos által végzett, az 1987/2006/EK rendelet 45. cikkében és a 2007/533/IB határozat 61. cikkében említett ellenőrzések során, és a Bizottság adatvédelmi tisztviselőjét az 5. cikk (2) bekezdése értelmében értesíti a biztonsági eseményekről;

f) ellenőrzi, hogy ezt a határozatot és a biztonsági politikát a központi SIS II igazgatásában bármilyen módon részt vevő, valamennyi szerződő fél – az alvállalkozókat is beleértve – megfelelően és maradéktalanul alkalmazza;

g) ellenőrzi, hogy ezt a határozatot és a biztonsági politikát a kommunikációs infrastruktúra igazgatásában bármilyen módon részt vevő, valamennyi szerződő fél – az alvállalkozókat is beleértve – megfelelően és maradéktalanul alkalmazza;

h) kezeli a SIS II biztonságával foglalkozó nemzeti kapcsolattartási pontok listáját, és azt megküldi a kommunikációs infrastruktúra helyi biztonsági tisztviselője számára;

i) a h) pontban említett listát megküldi a központi SIS II helyi biztonsági tisztviselője számára.

3. cikk

A központi SIS II helyi biztonsági tisztviselője

(1) A 8. cikkben foglaltak sérelme nélkül a Bizottság tisztviselői közül kijelöli a központi SIS II helyi biztonsági tisztviselőjét. A helyi biztonsági tisztviselő kötelezettségei és bármely más hivatalos kötelezettség közötti összeférhetetlenséget el kell kerülni. A központi SIS II helyi biztonsági tisztviselőjét a Bizottság Jogérvényesülés, Szabadság és Biztonság Főigazgatóságának főigazgatója nevezi ki.

(2) A központi SIS II helyi biztonsági tisztviselője az elsődleges CS-SIS tekintetében biztosítja az e határozatban említett biztonsági intézkedések végrehajtását és a biztonsági eljárások követését. A központi SIS II helyi biztonsági képviselője a tartalék CS-SIS tekintetében a 9. cikkben említett intézkedések kivételével biztosítja az e határozatban említett biztonsági intézkedések végrehajtását és az azokkal összefüggő biztonsági eljárások követését.

(3) A központi SIS helyi biztonsági tisztviselője bármely feladatát átruházhatja beosztottjaira. Az e feladatok ellátására vonatkozó kötelezettség és bármely más hivatalos kötelezettség közötti összeférhetetlenséget el kell kerülni. Biztosítani kell azt a telefonszámot és címet, amelyen a helyi biztonsági tisztviselő vagy szolgálatban lévő beosztottja mindenkor elérhető.

(4) A központi SIS II helyi biztonsági tisztviselője az (1) bekezdés szabta korlátok figyelembevételével elvégzi az elsődleges CS-SIS és a tartalék CS-SIS működési helyén foganatosítandó biztonsági intézkedésekből fakadó feladatokat, különös tekintettel a következőkre:

a) elvégzi a helyi operatív biztonsági feladatokat, köztük a tűzfalellenőrzést, a rendszeres biztonsági próbákat, az ellenőrzéseket, és elkészíti az ezekről szóló jelentéseket;

b) nyomon követi a rendszer működésének folytonosságát biztosító terv eredményességét, és biztosítja rendszeres gyakorlatok elvégzését;

c) összegyűjti a központi SIS II vagy a kommunikációs infrastruktúra biztonságát befolyásoló vagy befolyásolni képes, a központi SIS II-ben történő biztonsági eseményekkel kapcsolatos tényeket, és jelenti az ilyen eseményeket a rendszerbiztonsági tisztviselőnek;

d) tájékoztatja a rendszerbiztonsági tisztviselőt a biztonsági politika módosításának szükségességéről;

e) ellenőrzi, hogy ezt a határozatot és a biztonsági politikát a központi SIS II üzemeltetési igazgatásában bármilyen módon részt vevő, valamennyi szerződő fél – az alvállalkozókat is beleértve – alkalmazza;

f) biztosítja, hogy a személyi állomány tagjai tudatában legyenek kötelezettségeiknek, és nyomon követi a biztonsági politika végrehajtását;

g) nyomon követi az informatikai biztonság területén végbemenő fejleményeket, és biztosítja a személyi állomány ennek megfelelő képzését;

h) háttér-információkat és opciókat készít elő a biztonsági politika kidolgozása, naprakésszé tétele és felülvizsgálata céljából, a 7. cikknek megfelelően.

4. cikk

A kommunikációs infrastruktúra helyi biztonsági tisztviselője

(1) A 8. cikkben foglaltak sérelme nélkül a Bizottság tisztviselői közül kijelöli a kommunikációs infrastruktúra helyi biztonsági tisztviselőjét. A helyi biztonsági tisztviselő kötelezettségei és bármely más hivatalos kötelezettség közötti összeférhetetlenséget el kell kerülni. A kommunikációs infrastruktúra helyi biztonsági tisztviselőjét a Bizottság Jogérvényesülés, Szabadság és Biztonság Főigazgatóságának főigazgatója nevezi ki.

(2) A kommunikációs infrastruktúra helyi biztonsági tisztviselője nyomon követi a kommunikációs infrastruktúra működését, biztosítja a biztonsági intézkedések végrehajtását és a biztonsági eljárások követését.

(3) A kommunikációs infrastruktúra helyi biztonsági tisztviselője bármely feladatát átruházhatja beosztottjaira. Az e feladatok ellátására vonatkozó kötelezettség és bármely más hivatalos kötelezettség közötti összeférhetetlenséget el kell kerülni. Biztosítani kell azt a telefonszámot és címet, amelyen a helyi biztonsági tisztviselő vagy szolgálatban lévő beosztottja mindenkor elérhető.

(4) A kommunikációs infrastruktúra helyi biztonsági tisztviselője elvégzi a kommunikációs infrastruktúra tekintetében foganatosítandó biztonsági intézkedésekből fakadó feladatokat, különös tekintettel a következőkre:

a) elvégzi a kommunikációs infrastruktúrával kapcsolatos valamennyi operatív biztonsági feladatot, köztük a tűzfalellenőrzést, a rendszeres biztonsági próbákat, az ellenőrzéseket, és elkészíti az ezekről szóló jelentéseket;

b) nyomon követi a rendszer működésének folytonosságát biztosító terv eredményességét, és biztosítja rendszeres gyakorlatok elvégzését;

c) összegyűjti a központi SIS II vagy a kommunikációs infrastruktúra biztonságát befolyásolni képes biztonsági eseményekkel kapcsolatos tényeket, és jelenti az ilyen eseményeket a rendszerbiztonsági tisztviselőnek;

d) tájékoztatja a rendszerbiztonsági tisztviselőt a biztonsági politika módosításának szükségességéről;

e) ellenőrzi, hogy ezt a határozatot és a biztonsági politikát a kommunikációs infrastruktúra igazgatásában bármilyen módon részt vevő, valamennyi szerződő fél – az alvállalkozókat is beleértve – alkalmazza;

f) biztosítja, hogy a személyi állomány tagjai tudatában legyenek kötelezettségeiknek, és nyomon követi a biztonsági politika végrehajtását;

g) nyomon követi az informatikai biztonság területén végbemenő fejleményeket, és biztosítja a személyi állomány ennek megfelelő képzését;

h) háttér-információkat és opciókat készít elő a biztonsági politika kidolgozása, naprakésszé tétele és felülvizsgálata céljából, a 7. cikknek megfelelően.

5. cikk

Biztonsági események

(1) Biztonsági eseménynek kell tekinteni bármely olyan eseményt, amely veszélyezteti vagy veszélyeztetheti a SIS II biztonságát, és kárt vagy veszteséget okozhat a SIS II-ben, különösen akkor, ha hozzáférés történhetett az adatokhoz, vagy az adatok rendelkezésre állása, sértetlensége és bizalmas természete kárt szenvedett vagy szenvedhetett.

(2) A biztonsági események kezelése során gyors, eredményes és megfelelő választ kell adni az eseményekre, a biztonsági politika előírásaival összhangban. Meg kell állapítani azokat az eljárásokat, amelyek a biztonsági események kezeléséhez szükségesek.

(3) Valamely tagállamban a SIS II működését vagy a valamely tagállam által bevitt vagy továbbított adatok rendelkezésre állását, sértetlenségét vagy bizalmas természetét veszélyeztető vagy veszélyeztetni képes biztonsági eseményekkel kapcsolatos információkat az érintett tagállam rendelkezésére kell bocsátani. A biztonsági eseményekről értesíteni kell a Bizottság adatvédelmi tisztviselőjét.

6. cikk

A biztonsági események kezelése

(1) A SIS II kialakításában, igazgatásában és üzemeltetésében részt vevő személyi állománynak és szerződéses feleknek a kommunikációs infrastruktúra működésében észlelt vagy gyanított bármely biztonsági hiányosságról értesíteniük kell a rendszerbiztonsági tisztviselőt vagy a kommunikációs infrastruktúra helyi biztonsági tisztviselőjét, és arról jelentést kell tenniük számára.

(2) A SIS II biztonságát veszélyeztető vagy veszélyeztetni képes bármely esemény észlelése esetén a kommunikációs infrastruktúra helyi biztonsági tisztviselője a lehető leggyorsabban írásban – vagy rendkívül sürgős esetben más kommunikációs csatornákon keresztül – értesíti a rendszerbiztonsági tisztviselőt és – adott esetben, és amennyiben az érintett tagállamban létezik ilyen – a SIS II biztonságával foglalkozó nemzeti kapcsolattartási pontot. Az értesítés tartalmazza a biztonsági esemény leírását, a kockázati szintet, a lehetséges következményeket és a kockázat csökkentése érdekében foganatosított vagy foganatosítandó intézkedéseket.

(3) A kommunikációs infrastruktúra helyi biztonsági tisztviselője a biztonsági eseménnyel kapcsolatos bizonyítékokat késedelem nélkül biztonságba helyezi. E bizonyítékokat a rendszerbiztonsági tisztviselő erre irányuló kérése esetén az alkalmazandó adatvédelmi rendelkezések által lehetővé tett mértékben a rendszerbiztonsági tisztviselő rendelkezésére kell bocsátani.

(4) A biztonsági politikában meg kell határozni azokat a visszacsatolási eljárásokat, amelyek biztosítják, hogy az esemény kezelését és lezárását követően a rendszerbiztonsági tisztviselő és a kommunikációs infrastruktúra helyi biztonsági tisztviselője tájékoztatást kapjon a biztonsági esemény típusáról, kezeléséről és következményeiről.

(5) Az (1)–(4) bekezdés értelemszerűen alkalmazandó a központi SIS II biztonsági eseményeire. Ebben az összefüggésben az (1)–(4) bekezdésben a kommunikációs infrastruktúra helyi biztonsági tisztviselőjére vonatkozó utalásokat a központi SIS II helyi biztonsági tisztviselőjére vonatkozó utalásokként kell értelmezni.

III. FEJEZET

BIZTONSÁGI INTÉZKEDÉSEK

7. cikk

Biztonsági politika

(1) A Jogérvényesülés, Szabadság és Biztonság Főigazgatóságának főigazgatója megállapítja, naprakészen tartja és rendszeresen felülvizsgálja az e határozatnak megfelelő, kötelező érvényű biztonsági politikát. A biztonsági politika részletes eljárásokat és intézkedéseket – egyebek mellett vészhelyzeti tervet – állapít meg a kommunikációs infrastruktúra rendelkezésre állását, sértetlenségét és bizalmas természetét veszélyeztető fenyegetések elleni védelem érdekében az e határozatban előírt megfelelő biztonsági szint biztosítása céljából. A biztonsági politika megfelel e határozat rendelkezéseinek.

(2) A biztonsági politika kockázatértékelésen alapul. A biztonsági politika által megállapított intézkedések arányosak az azonosított kockázatokkal.

(3) A kockázatértékelést és a biztonsági politikát naprakésszé kell tenni, amennyiben ezt technológiai változások, új fenyegetések azonosítása vagy bármely más körülmény szükségessé teszi. A biztonsági politikát minden esetben évente felül kell vizsgálni annak biztosítása érdekében, hogy továbbra is megfelelő választ adjon a legutóbbi kockázatértékelésre vagy bármely más újonnan azonosított technológiai változásra, fenyegetésre vagy egyéb releváns körülményre.

(4) A biztonsági politikát a rendszerbiztonsági tisztviselő dolgozza ki a központi SIS II helyi biztonsági tisztviselőjével és a kommunikációs infrastruktúra helyi biztonsági tisztviselőjével együttműködésben.

(5) Az (1)–(4) bekezdés értelemszerűen alkalmazandó a központi SIS II biztonsági eseményeire. Ebben az összefüggésben az (1)–(4) bekezdésben a kommunikációs infrastruktúra helyi biztonsági tisztviselőjére vonatkozó utalásokat a központi SIS II helyi biztonsági tisztviselőjére vonatkozó utalásokként kell értelmezni.

8. cikk

A biztonsági intézkedések végrehajtása

(1) Az e határozatban és a biztonsági politikában megállapított feladatok és követelmények végrehajtása, ideértve a helyi biztonsági tisztviselő kijelölését is, szerződés alapján vagy más módon átruházható magánszervezetekre vagy közhatóságokra.

(2) Ebben az esetben a Bizottság jogilag kötelező érvényű megállapodás révén biztosítja az e határozatban és a biztonsági politikában foglalt követelmények maradéktalan betartását. A helyi biztonsági tisztviselő kijelölésére irányuló feladat szerződés alapján vagy más módon történő átruházása esetén a Bizottság jogilag kötelező érvényű megállapodás révén biztosítja, hogy a helyi biztonsági tisztviselő személyéről egyeztetnek vele.

9. cikk

A létesítmény-hozzáférés ellenőrzése

(1) Az adatfeldolgozási létesítmények elhelyezésére szolgáló területeket megfelelő sorompókkal és beléptetési ellenőrzéssel védett biztonsági övezet veszi körül.

(2) A biztonsági övezeten belül védett területeket kell kijelölni a tárgyi összetevők (eszközök) – ideértve a hardverelemeket, adathordozókat és konzolokat, terveket a SIS II-ről szóló egyéb dokumentumokat – és a SIS II üzemeltetésében részt vevő személyi állomány irodái és egyéb munkaterületei védelmére. A védett területeket megfelelő beléptetési ellenőrzéssel kell védeni annak biztosítása érdekében, hogy oda csak az erre feljogosított személyek léphessenek be. A védett területeken történő munkavégzés szabályait a biztonsági politikában részletesen meg kell határozni.

(3) Gondoskodni kell az irodák, helyiségek és létesítmények fizikai biztonságáról. A jogosulatlan hozzáférés megakadályozása érdekében ellenőrizni kell, és amennyiben lehetséges, az adatfeldolgozási létesítményektől el kell választani azokat a pontokat, például a szállítási, be- és kirakodási területeket, ahol fel nem jogosított személyek beléphetnek az intézmény területére.

(4) A biztonsági övezetek természetes vagy ember által okozott csapások elleni fizikai védelmét a kockázattal arányos mértékben kell megtervezni és biztosítani.

(5) A berendezéseket védeni kell a fizikai és környezeti veszélyektől és a jogosulatlan hozzáférés lehetőségétől.

(6) Amennyiben ilyen információ rendelkezésére áll, a Bizottság a 2. cikk (3) bekezdésének h) pontjában említett listát kiegészíti az e cikk rendelkezéseinek a tartalék CS-SIS üzemeltetési helyén történő végrehajtását nyomon követő kapcsolattartási ponttal.

10. cikk

Az adathordozók és más eszközök ellenőrzése

(1) Az eltávolítható adathordozókat védeni kell a jogosulatlan hozzáféréstől, helytelen felhasználástól és rongálódástól, és olvashatóságukat az adatok teljes élettartama alatt biztosítani kell.

(2) A szükségtelenné vált adathordozókat biztonságos módon, a biztonsági politikában megállapított részletes eljárásoknak megfelelően kell használaton kívül helyezni.

(3) Készletnyilvántartás révén biztosítani kell a tárolás helyével, a megőrzés előírt időtartamával és a hozzáférésre vonatkozó engedélyekkel kapcsolatos információk elérhetőségét.

(4) A kommunikációs infrastruktúra minden fontos eszközét azonosítani kell a fontosságuknak megfelelő védelem biztosítása érdekében. Naprakész nyilvántartást kell vezetni a releváns informatikai berendezésekről.

(5) Naprakész dokumentációval kell rendelkezni a kommunikációs infrastruktúráról. Ezt a dokumentációt védeni kell a jogosulatlan hozzáféréstől.

(6) Az (1)–(5) bekezdés értelemszerűen alkalmazandó a központi SIS II esetében. Ebben az összefüggésben a kommunikációs infrastruktúrára vonatkozó utalásokat a központi SIS II-re vonatkozó utalásokként kell értelmezni.

11. cikk

Az adattárolás ellenőrzése

(1) Megfelelő intézkedéseket kell hozni az információk helyes tárolása és az információkhoz való jogosulatlan hozzáférés megakadályozása érdekében.

(2) Az adatok tárolására szolgáló eszközöket tartalmazó berendezéseket ellenőrizni kell abból a szempontból, hogy a használaton kívül helyezést megelőzően a különleges adatokat azokból eltávolították-e vagy azokban teljes mértékben felülírták-e, illetőleg e berendezéseket biztonságos módon meg kell semmisíteni.

12. cikk

Jelszóellenőrzés

(1) A jelszavakat biztonságos módon kell tárolni, és bizalmasan kell kezelni. Jelszó felfedésének gyanúja esetén a jelszót késedelem nélkül meg kell változtatni, vagy a felhasználó fiókját le kell tiltani. A felhasználó-azonosítóknak egyedieknek és személyre szólóaknak kell lenniük.

(2) A biztonsági politika keretében be- és kijelentkezési eljárásokat kell megállapítani a jogosulatlan hozzáférés megakadályozása érdekében.

13. cikk

A hozzáférés ellenőrzése

(1) A biztonsági politika keretében a központi SIS II üzemeltetésének igazgatása érdekében a személyi állomány számára formális regisztrációs eljárást kell meghatározni a VIS hardver- és szoftverelemeihez történő hozzáférés engedélyezése és visszavonása céljából. A hozzáférést biztosító megfelelő meghatalmazások (jelszó vagy más megfelelő eszköz) kiadását és használatát a biztonsági politikában meghatározott formális irányítási folyamat révén kell ellenőrizni.

(2) A központi SIS II hardver- és szoftverelemeihez történő hozzáférés:

i. csak az arra feljogosított személyek számára biztosítható;

ii. azokra az esetekre korlátozandó, amelyekben megállapítható az 1987/2006/EK rendelet 45. cikkének és a 2007/533/IB határozat 61. cikkének, vagy az 1987/2006/EK rendelet 50. cikke (2) bekezdésének és a 2007/533/IB határozat 66. cikke (2) bekezdésének megfelelő jogos cél;

iii. nem haladhatja meg a hozzáférés céljához szükséges időtartamot és mértéket; valamint

iv. csak a biztonsági politikában meghatározott hozzáférés-ellenőrzési politika szabályainak megfelelően történhet.

(3) A CS-SIS üzemeltetési helyén csak a helyi biztonsági tisztviselő által a központi SIS II számára engedélyezett konzolok és szoftverek használhatók. A rendszer és az alkalmazások beállításait felülírni képes programok használatát korlátozni és ellenőrizni kell. Eljárásokat kell megállapítani a szoftverek telepítésének ellenőrzésére.

14. cikk

A kommunikáció ellenőrzése

Az információcsere rendelkezésre állásának, sértetlenségének és bizalmas természetének biztosítása érdekében ellenőrizni kell a kommunikációs infrastruktúrát. A kommunikációs infrastruktúrán keresztül továbbított adatokat kriptográfiai eszközökkel kell védeni.

15. cikk

Az adatrögzítés ellenőrzése

A CS-SIS-ből a SIS II-szoftverhez hozzáférni jogosult személyek felhasználói fiókjait a központi SIS II helyi biztonsági tisztviselője ellenőrzi. Az e fiókok használatára vonatkozó információkról, ideértve a felhasználás idejét és a felhasználó kilétét is, nyilvántartást kell vezetni.

16. cikk

Az adathordozók szállításának ellenőrzése

(1) A biztonsági politika keretében megfelelő intézkedéseket kell megállapítani annak érdekében, hogy meg lehessen akadályozni a személyes adatok a SIS II-ből vagy SIS II-be történő adattovábbítás vagy az adathordozók szállítása során történő, esetleges jogosulatlan olvasását, másolását, módosítását vagy törlését. A biztonsági politika keretében rendelkezni kell a továbbítás vagy szállítás megengedhető módozatairól, valamint a tételek szállítására és a rendeltetési helyre történő megérkezésére vonatkozó elszámoltathatósági eljárásokról. Az adathordozó a küldendő adatokon kívül más adatot nem tartalmazhat.

(2) A harmadik felek által nyújtott azon szolgáltatásoknak, amelyek kiterjednek adatfeldolgozó létesítményekhez történő hozzáférésre, adatok feldolgozására, továbbítására, adatfeldolgozó létesítmények irányítására vagy adatfeldolgozó létesítmények termékeinek vagy szolgáltatásainak bővítésére, megfelelő, integrált biztonsági ellenőrző rendszerrel kell rendelkezniük.

17. cikk

A kommunikációs infrastruktúra biztonsága

(1) A kommunikációs infrastruktúrát megfelelően irányítani és ellenőrizni kell a fenyegetésektől való védelem, valamint a kommunikációs infrastruktúra és a központi SIS II biztonságának megőrzése érdekében, ideértve a kommunikációs infrastruktúrán keresztül továbbított adatok biztonságát is.

(2) A hálózati szolgáltatások biztonsági jellemzőit, szolgáltatási szintjeit és irányítási követelményeit a szolgáltatóval kötött hálózati szolgáltatási megállapodásban kell meghatározni.

(3) A SIS II hozzáférési pontok védelmén kívül biztosítani kell a kommunikációs infrastruktúra vonatkozásában igénybe vett egyéb kiegészítő szolgáltatások védelmét is. A megfelelő intézkedéseket a biztonsági politikában kell megállapítani.

18. cikk

Nyomon követés

(1) Azokat a nyilvántartásokat, amelyek a CS-SIS-ben tárolt személyes adatokhoz történő hozzáférésekre, és ezen adatok cseréire vonatkozó, az 1987/2006/EK rendelet 18. cikkének (1) bekezdésében és a 2007/533/IB határozat 18. cikkének (1) bekezdésében említett információkat tartalmazzák, az 1987/2006/EK rendelet 18. cikkének (3) bekezdésében és a 2007/533/IB határozat 18. cikkének (3) bekezdésében említett leghosszabb időtartam alatt biztonságos módon kell tárolni az elsődleges és a tartalék CS-SIS üzemeltetési helyén, illetve hozzáférhetővé kell tenni ezek üzemeltetési helyéről.

(2) A biztonsági politikában meg kell állapítani az adatfeldolgozási létesítmények használatának és hibáinak nyomon követésére vonatkozó eljárásokat, és a nyomonkövetési tevékenységek eredményeit rendszeresen ellenőrizni kell. Szükség esetén meg kell tenni a megfelelő lépéseket.

(3) A bizonyítékok megőrzésére vonatkozó időtartam folyamán betartandó adatgyűjtési és -megőrzési követelmények teljesítése érdekében a nyilvántartásra szolgáló létesítményeket és a nyilvántartásokat védeni kell a manipulációtól és a jogosulatlan hozzáféréstől.

19. cikk

Kriptográfiai intézkedések

Az információk védelme céljából megfelelő esetben kriptográfiai intézkedések alkalmazandók. Ezek használatát, céljait és feltételeit a rendszerbiztonsági tisztviselő előzetesen hagyja jóvá.

IV. FEJEZET

EMBERIERŐFORRÁS-BIZTONSÁG

20. cikk

Személyi állományi profilok

(1) A biztonsági politika meghatározza azon személyek funkcióit és feladatait, akik hozzáférnek a központi SIS II-höz és a kommunikációs infrastruktúrához.

(2) A biztonsági politika meghatározza azon személyek funkcióit és feladatait, akik hozzáférnek a kommunikációs infrastruktúrához.

(3) Az üzemeltetési igazgatásban részt vevő bizottsági alkalmazottak, szerződéses felek és személyi állomány biztonsággal kapcsolatos szerepköreit és feladatait meg kell határozni, és dokumentálni kell; e szerepkörökről és feladatokról tájékoztatni kell az érintett személyeket. A szerepköröket és feladatokat a bizottsági alkalmazottak esetében a munkaköri leírásban és célkitűzésekben, a szerződéses felek esetében a szerződésekben vagy a szolgálati szintű megállapodásokban kell megállapítani.

(4) Mindazon személyekkel, akiket nem kötnek európai uniós vagy tagállami közszolgálati szabályok, a bizalmas kezelésre és titoktartásra vonatkozó megállapodást kell kötni. A SIS II-adatokkal dolgozó személyi állománynak rendelkeznie kell a feladatkör ellátásához szükséges biztonsági engedélyekkel és igazolásokkal a biztonsági politikában megállapított részletes eljárásoknak megfelelően.

21. cikk

A személyi állomány tájékoztatása

(1) A személyi állomány tagjai és a szerződéses felek megfelelő képzés keretében – feladataik ellátásához szükséges mértékben – tájékoztatást kapnak a biztonsági kérdésekről, jogi követelményekről, elvekről és eljárásokról.

(2) A foglalkoztatási jogviszony megszűnte vagy a szerződés lejárta esetére a biztonsági politika a személyi állomány és a szerződéses felek tekintetében meghatározza a munkahelyváltással vagy a foglalkoztatás megszűntével összefüggésben elvégzendő feladatokat, és megállapítja az eszközök visszaszolgáltatására és a hozzáférési jogok megszüntetésére irányadó eljárásokat.

V. FEJEZET

ZÁRÓ RENDELKEZÉS

22. cikk

Időbeli hatály

(1) Ez a határozat a Tanács által az 1987/2006/EK rendelet 55. cikke (2) bekezdésének és a 2007/533/IB határozat 71. cikke (2) bekezdésének megfelelően megállapított időponttól lép hatályba.

(2) Az 1. cikk (1) bekezdése, a 2. cikk (1) bekezdése, (3) bekezdésének b), d), f) és i) pontja, 3. cikke, 6. cikkének (5) bekezdése, 7. cikkének (5) bekezdése, 9. cikkének (6) bekezdése, 10. cikkének (6) bekezdése, 13. cikkének (2) és (3) bekezdése, 15. cikke, 18. cikke és 20. cikkének (1) bekezdése akkor veszti hatályát, amikor az igazgató hatóság megkezdi tevékenységét.

Kelt Brüsszelben, 2010. május 4-én.

a Bizottság részéről

az elnök

José Manuel BARROSO