KOMMISSIONENS BESLUT

av den 4 maj 2010

om en säkerhetsplan för det centrala SIS II och kommunikationsinfrastrukturen

(2010/261/EU)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) [1], särskilt artikel 16,

med beaktande av rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) [2], särskilt artikel 16, och

av följande skäl:

(1) I artikel 16 i förordning (EG) nr 1987/2006 och artikel 16 i beslut 2007/533/RIF föreskrivs att förvaltningsmyndigheten, med avseende på det centrala SIS II, och kommissionen, när det gäller kommunikationsinfrastrukturen, ska vidta de åtgärder som är nödvändiga, bland annat anta en säkerhetsplan.

(2) I artikel 15.4 i förordning (EG) nr 1987/2006 och artikel 15.4 i rådets beslut 2007/533/RIF föreskrivs att kommissionen ska ha ansvar för den operativa förvaltningen av SIS under en övergångsperiod innan förvaltningsmyndigheten övertar ansvaret.

(3) Eftersom förvaltningsmyndigheten ännu inte har inrättats bör den säkerhetsplan som ska antas av kommissionen även vara tillämplig på det centrala SIS II under en övergångsperiod.

(4) Europaparlamentets och rådets förordning (EG) nr 45/2001 [3] är tillämplig på kommissionens behandling av personuppgifter när den utövar sitt ansvar i samband med den operativa förvaltningen av SIS II.

(5) I artikel 15.7 i förordning (EG) nr 1987/2006 och artikel 15.7 i beslut 2007/533/RIF föreskrivs att om kommissionen delegerar sitt ansvar under övergångsperioden innan förvaltningsmyndigheten övertar ansvaret, ska den säkerställa att delegeringen inte inverkar negativt på någon av de kontrollmekanismer som följer av unionsrätten, oavsett om de utgörs av domstolen, revisionsrätten eller Europeiska datatillsynsmannen.

(6) Förvaltningsmyndigheten bör anta en egen säkerhetsplan för det centrala SIS II när den har börjat utöva sitt ansvar. Denna säkerhetsplan bör därför, i den utsträckning den rör det centrala SIS II, upphöra att gälla när förvaltningsmyndigheten övertar ansvaret.

(7) I artikel 4.3 i förordning (EG) nr 1987/2006 och artikel 4.3 i beslut 2007/533/RIF föreskrivs att CS-SIS, som står för teknisk tillsyn och administration, ska vara belägen i Strasbourg (Frankrike) och en reserv för CS-SIS, varigenom alla funktioner i den centrala delen av CS-SIS garanteras om detta system skulle sluta fungera, ska vara belägen i Sankt Johann im Pongau (Österrike).

(8) Säkerhetsplanen bör inbegripa en säkerhetsansvarig för hela systemet, som utför säkerhetsrelaterade uppgifter rörande såväl det centrala SIS II som kommunikationsinfrastrukturen, och två lokalt säkerhetsansvariga, som utför säkerhetsrelaterade uppgifter rörande det centrala SIS II respektive kommunikationsinfrastrukturen. De säkerhetsansvarigas uppgifter bör fastslås för att säkerställa snabba och effektiva åtgärder samt rapportering vid säkerhetstillbud.

(9) Det bör utarbetas en säkerhetsplan som tar upp alla tekniska och organisatoriska detaljer i enlighet med bestämmelserna i detta beslut.

(10) Det bör fastställas åtgärder för att säkerställa en lämplig säkerhetsnivå med avseende på driften av det centrala SIS II och kommunikationsinfrastrukturen.

[1] EUT L 381, 28.12.2006, s. 4.
[2] EUT L 205, 7.8.2007, s. 63.
[3] EGT L 8, 12.1.2001, s. 1.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Tillämpningsområde

1. Genom detta beslut fastställs en skyddsorganisation och åtgärder (dataskyddsplan) för att skydda det centrala SIS II och de uppgifter som behandlas i systemet mot hot mot uppgifternas tillgänglighet, integritet och konfidentialitet i den mening som avses i artikel 16.1 i förordning (EG) nr 1987/2006 och artikel 16.1 i beslut 2007/533/RIF om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) under en övergångsperiod fram till dess att förvaltningsmyndigheten inleder sin verksamhet.

2. Genom detta beslut fastställs en skyddsorganisation och åtgärder (dataskyddsplan) för att skydda kommunikationsinfrastrukturen mot hot mot uppgifternas tillgänglighet, integritet och konfidentialitet i den mening som avses i artikel 16 i förordning (EG) nr 1987/2006 och artikel 16 i beslut 2007/533/RIF om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II).

KAPITEL II

ORGANISATION, ANSVARSOMRÅDEN OCH TILLBUDSHANTERING

Artikel 2

Kommissionens uppgifter

1. Kommissionen ska säkerställa och övervaka att de säkerhetsåtgärder avseende det centrala SIS II som anges i detta beslut fungerar effektivt.

2. Kommissionen ska säkerställa och övervaka att de säkerhetsåtgärder avseende kommunikationsinfrastrukturen som anges i detta beslut fungerar effektivt.

3. Kommissionen ska utse en säkerhetsansvarig för systemet bland sina tjänstemän. Systemets säkerhetsansvarige ska utses av generaldirektören för kommissionens generaldirektorat för rättvisa, frihet och säkerhet. Uppgifterna för systemets säkerhetsansvarige ska särskilt omfatta

a) förberedelse av den säkerhetsplan som beskrivs i artikel 7 i detta beslut,

b) övervakning av att säkerhetsprocedurerna för det centrala SIS II genomförs effektivt,

c) övervakning av att säkerhetsprocedurerna för kommunikationsinfrastrukturen genomförs effektivt,

d) bidra till utarbetandet av rapporter om säkerheten i enlighet med artikel 50 i förordning (EG) nr 1987/2006 och artikel 66 i beslut 2007/533/RIF,

e) ansvara för samordning och stöd i samband med den kontroll och revision som europeiska datatillsynsmannen utför i enlighet med artikel 45 i förordning (EG) nr 1987/2006 och artikel 61 i beslut 2007/533/RIF, samt för rapportering till kommissionens uppgiftsskyddsombud av sådana tillbud som avses i artikel 5.2,

f) övervaka att detta beslut och säkerhetsplanen tillämpas korrekt och fullständigt av eventuella uppdragstagare och underleverantörer som på något sätt deltar i förvaltningen av det centrala SIS II,

g) övervaka att detta beslut och säkerhetsplanen tillämpas korrekt och fullständigt av eventuella uppdragstagare och underleverantörer som på något sätt deltar i förvaltningen av kommunikationsinfrastrukturen,

h) föra en förteckning över enskilda nationella kontaktpunkter för säkerhetsfrågor rörande SIS II och ställa den till förfogande för den lokalt säkerhetsansvariga för kommunikationsinfrastrukturen,

i) ställa den förteckning som avses i h till förfogande för den lokalt säkerhetsansvariga för det centrala SIS II.

Artikel 3

Den lokalt säkerhetsansvarige för det centrala SIS II

1. Utan att det påverkar tillämpningen av artikel 8 ska kommissionen bland sina tjänstemän utse en lokalt säkerhetsansvarig för det centrala SIS II. Intressekonflikter mellan den lokalt säkerhetsansvariges åtaganden och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige för det centrala SIS II ska utses av generaldirektören för kommissionens generaldirektorat för rättvisa, frihet och säkerhet.

2. Den lokalt säkerhetsansvarige för det centrala SIS II ska se till att de säkerhetsåtgärder som avses i detta beslut genomförs och att säkerhetsförfarandena följs i den ordinarie delen av CS-SIS. När det gäller reservsystemet för CS-SIS ska den lokalt säkerhetsansvarige för det centrala SIS II vidare säkerställa att de säkerhetsåtgärder som avses i detta beslut, med undantag för åtgärderna i artikel 9, genomförs och att de relevanta säkerhetsförfarandena följs.

3. Den lokalt säkerhetsansvarige för det centrala SIS II får delegera sina arbetsuppgifter till underställd personal. Intressekonflikter mellan skyldigheten att utföra dessa uppgifter och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige eller dennes tjänstgörande underordnade ska när som helst kunna nås via ett särskilt telefonnummer och en särskild adress.

4. Den lokalt säkerhetsansvarige för det centrala SIS II ska utföra de uppgifter som är knutna till sådana säkerhetsåtgärder som ska vidtas på de platser där den ordinarie delen av det centrala CS-SIS respektive reservsystemet för CS-SIS är belägna, inom de ramar som fastställs i punkt 1, vilket särskilt innebär att han eller hon ska

a) utföra säkerhetsuppgifter i samband med driften lokalt, inklusive kontroll av brandväggar, regelbundna säkerhetstester, översyn och rapportering,

b) övervaka kontinuitetsplanens effektivitet och se till att regelbundna övningar genomförs,

c) säkra bevis för och rapportera till systemets säkerhetsansvarige om alla tillbud i det centrala SIS II som kan påverka säkerheten för det centrala SIS II eller kommunikationsinfrastrukturen,

d) underrätta systemets säkerhetsansvarige om säkerhetsplanen behöver ändras,

e) övervaka att detta beslut och skyddsstrategin tillämpas av eventuella uppdragstagare och underleverantörer som på något sätt är involverade i den operativa förvaltningen och av det centrala SIS II,

f) se till att personalen informeras om sina skyldigheter och övervaka tillämpningen av skyddsstrategin,

g) övervaka utvecklingen när det gäller it-säkerhet och se till att personalen får nödvändig fortbildning,

h) förbereda underlag och alternativ när det gäller att införa, uppdatera och se över skyddsstrategin i enlighet med artikel 7.

Artikel 4

Lokalt säkerhetsansvarig för kommunikationsinfrastrukturen

1. Utan att det påverkar tillämpningen av artikel 8 ska kommissionen bland sina tjänstemän utse en lokalt säkerhetsansvarig för kommunikationsinfrastrukturen. Intressekonflikter mellan den lokalt säkerhetsansvariges åtaganden och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen ska utses av generaldirektören för kommissionens generaldirektorat för rättvisa, frihet och säkerhet.

2. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen ska övervaka kommunikationsinfrastrukturens funktion och se till att säkerhetsåtgärderna genomförs och säkerhetsförfarandena följs.

3. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen får delegera sina arbetsuppgifter till underställd personal. Intressekonflikter mellan skyldigheten att utföra dessa uppgifter och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige eller dennes tjänstgörande underordnade ska när som helst kunna nås via ett särskilt telefonnummer och en särskild adress.

4. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen ska utföra sådana uppgifter som är förbundna med säkerhetsåtgärder rörande kommunikationsinfrastrukturen, särskilt

a) alla säkerhetsuppgifter som rör kommunikationsinfrastrukturen, inklusive kontroll av brandväggar, regelbundna säkerhetstester, översyn och rapportering,

b) övervaka kontinuitetsplanens effektivitet och se till att regelbundna övningar genomförs,

c) säkra bevis för och rapportera till systemets säkerhetsansvarige om alla tillbud i anslutning till kommunikationsinfrastrukturen som kan påverka säkerheten för det centrala SIS eller kommunikationsinfrastrukturen,

d) underrätta systemets säkerhetsansvarige om säkerhetsplanen behöver ändras,

e) övervaka att detta beslut och skyddsstrategin tillämpas av eventuella uppdragstagare och underleverantörer som på något sätt deltar i förvaltningen av kommunikationsinfrastrukturen,

f) se till att personalen informeras om sina skyldigheter och övervaka tillämpningen av säkerhetsplanen,

g) övervaka utvecklingen när det gäller it-säkerhet och se till att personalen får nödvändig fortbildning,

h) förbereda underlag och alternativ när det gäller att införa, uppdatera och se över skyddsstrategin i enlighet med artikel 7.

Artikel 5

Säkerhetstillbud

1. Varje händelse som har eller kan få en inverkan på säkerheten i SIS II och riskerar att orsaka skada eller förluster för SIS II ska anses som ett säkerhetstillbud, särskilt om systemet har utsatts för dataintrång eller om uppgifternas tillgänglighet, integritet och konfidentialitet har äventyrats eller kan ha äventyrats.

2. Säkerhetstillbud ska hanteras på ett sätt som säkerställer snabba, effektiva och välavvägda insatser. Det ska fastställas förfaranden för hur situationen ska återställas till det normala efter ett tillbud.

3. Information om ett säkerhetstillbud som har eller kan ha en inverkan på driften av SIS II i en medlemsstat, eller på tillgången till eller integriteten eller konfidentialiteten hos de uppgifter som matats in eller översänts av en medlemsstat, ska vidarebefordras till den berörda medlemsstaten. Säkerhetstillbud ska rapporteras till kommissionens uppgiftsskyddsombud.

Artikel 6

Hantering av tillbud

1. All personal och alla uppdragstagare som arbetar med att utveckla, förvalta eller driva SIS II ska vara skyldiga att notera och rapportera eventuella iakttagna eller misstänkta säkerhetsbrister i kommunikationsinfrastrukturen till systemets säkerhetsansvarige eller till den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen.

2. Vid ett tillbud som har eller kan ha en inverkan på säkerheten i samband med driften av SIS II ska den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen snarast möjligt underrätta systemets säkerhetsansvarige och, i tillämpliga fall, den nationella kontaktpunkten för säkerhetsfrågor rörande SIS II, om det finns en sådan kontaktpunkt i medlemsstaten i fråga; detta meddelande ska vara skriftligt, men om särskild skyndsamhet är påkallad får även andra kommunikationsmedel användas. Rapporten ska innehålla en beskrivning av säkerhetstillbudet, risknivån, de möjliga konsekvenserna och de åtgärder som har vidtagits eller bör vidtas för att minska risken.

3. Eventuella bevis med anknytning till säkerhetstillbudet ska säkras omedelbart av den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen. I den utsträckning det är möjligt enligt de tillämpliga bestämmelserna om uppgiftsskydd ska sådan bevisning göras tillgänglig för systemets säkerhetsansvarige på dennes begäran.

4. Återkopplingsprocesser ska fastställas i säkerhetsplanen för att säkerställa att information om typen, hanteringen och följderna av ett säkerhetstillbud vidarebefordras till systemets säkerhetsansvarige och den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen efter det att tillbudet har hanterats och situationen är löst.

5. Punkterna 1–4 ska i tillämpliga delar även gälla vid tillbud i det centrala SIS II. I relevanta fall ska därför alla hänvisningar till den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen i punkterna 1–4 förstås som hänvisningar till den lokalt säkerhetsansvarige för det centrala SIS II.

KAPITEL III

SÄKERHETSÅTGÄRDER

Artikel 7

Säkerhetsplan

1. Generaldirektören för generaldirektoratet för rättvisa, frihet och säkerhet ska fastställa, uppdatera och regelbundet se över en bindande säkerhetsplan i enlighet med detta beslut. Säkerhetsplanen ska omfatta detaljerade förfaranden och åtgärder för att skydda kommunikationsinfrastrukturens tillgänglighet, integritet och konfidentialitet, inklusive krisberedskap, i syfte att säkerställa en lämplig säkerhetsnivå i enlighet med detta beslut. Säkerhetsplanen ska vara utformad på ett sätt som överensstämmer med detta beslut.

2. Säkerhetsplanen ska grunda sig på en riskanalys. De åtgärder som beskrivs i säkerhetsplanen ska stå i proportion till de identifierade riskerna.

3. Riskanalysen och säkerhetsplanen ska uppdateras om det blir nödvändigt på grund av tekniska förändringar, nya hot eller andra omständigheter. Säkerhetsplanen ska under alla omständigheter ses över årligen för att säkerställa att den fortfarande överensstämmer med den senaste riskanalysen eller eventuella andra nyligen konstaterade tekniska förändringar, hot eller andra relevanta omständigheter.

4. Säkerhetsplanen ska utarbetas av systemets säkerhetsansvarige, i samarbete med den lokalt säkerhetsansvarige för det centrala SIS II och den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen.

5. Punkterna 1–4 ska i tillämpliga delar även gälla vid tillbud i det centrala SIS II. I relevanta fall ska således alla hänvisningar till den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen i punkterna 1–4 förstås som en hänvisning till den lokalt säkerhetsansvarige för det centrala SIS II.

Artikel 8

Genomförandet av säkerhetsåtgärderna

1. Genomförandet av de uppgifter och krav som fastställs i detta beslut och i säkerhetsplanen, inklusive uppgiften att utse en lokalt säkerhetsansvarig, kan läggas ut på eller anförtros privata eller offentliga organisationer.

2. I så fall ska kommissionen genom rättsligt bindande avtal se till att de krav som fastställs i detta beslut och i säkerhetsplanen uppfylls fullt ut. Vid delegering eller utläggning av uppgiften att utse en lokal säkerhetsansvarig ska kommissionen genom rättsligt bindande avtal se till att den ges tillfälle att yttra sig om den person som valet faller på.

Artikel 9

Kontroll av tillträdet till anläggningen

1. Yttre säkerhetsgränser med lämpliga barriärer och inträdeskontroller ska användas för att skydda områden där det finns databehandlingsutrustning.

2. Inom dessa yttre säkerhetsgränser ska det finnas säkerhetszoner för att skydda de fysiska beståndsdelarna (anläggningstillgångar), inklusive hårdvara, databärare och konsoler, men även planer och annan dokumentation över SIS II samt kontor och andra arbetsutrymmen för personal som deltar i driften av SIS II. Dessa säkerhetszoner ska skyddas genom för ändamålet avpassade tillträdeskontroller för att säkerställa att endast auktoriserad personal ges tillträde. Arbete som utförs inom säkerhetszoner ska omfattas av säkerhetsbestämmelser som fastställs närmare i säkerhetsplanen.

3. Åtgärder ska planeras och vidtas för att säkerställa den fysiska säkerheten med avseende på kontor och andra lokaler och installationer. Lastnings- och avlastningsplatser och andra ställen där obehöriga kan ta sig in på området ska övervakas och, om möjligt, hållas avskilda från databehandlingsanläggningar för att undvika att obehöriga får tillträde.

4. Ett fysiskt skydd för de yttre säkerhetsgränserna mot skador från naturkatastrofer eller katastrofer orsakade av människan ska utformas och användas på ett sätt som står i proportion till den risk som föreligger.

5. Utrustning ska skyddas från fysiska och miljörelaterade hot samt mot risken för obehörigt tillträde.

6. Om kommissionen har tillgång till sådan information ska den komplettera den förteckning som avses i artikel 2.3 h med uppgifter om en kontaktpunkt för övervakning av hur bestämmelserna i denna artikel tillämpas på den plats där reservsystemet för CS-SIS är placerat.

Artikel 10

Kontroll av databärare och tillgångar

1. Flyttbara databärare som innehåller data ska skyddas mot obehörig åtkomst, missbruk eller förvanskning och vara läsbara under uppgifternas hela livstid.

2. Databärarna ska skaffas undan på ett säkert sätt när de har spelat ut sin roll, i enlighet med de förfaranden som fastställs närmare i säkerhetsplanen.

3. Förteckningar ska säkerställa att uppgifter om lagringsplats, lagringsperioder och åtkomsträttigheter finns tillgängliga.

4. Alla viktiga tillgångar som hör till kommunikationsinfrastrukturen ska identifieras, så att de kan skyddas i förhållande till deras betydelse. Ett uppdaterat register över relevant it-utrustning ska föras.

5. Det ska finnas uppdaterad dokumentation rörande kommunikationsinfrastrukturen. Denna dokumentation ska skyddas mot obehörig åtkomst.

6. Punkterna 1–5 ska i tillämpliga delar även gälla vid tillbud i det centrala SIS II. I relevanta fall ska därför alla hänvisningar till kommunikationsinfrastrukturen förstås som hänvisningar till det centrala SIS II.

Artikel 11

Lagringskontroll

1. Lämpliga åtgärder ska vidtas för att säkerställa en säker lagring av uppgifter och förebygga obehörig åtkomst.

2. All utrustning som innehåller lagringsmedier ska antingen kontrolleras för att säkerställa att känsliga uppgifter har avlägsnats eller skrivits över före bortskaffandet, eller förstöras på ett säkert sätt.

Artikel 12

Kontroll av lösenord

1. Alla lösenord ska förvaras säkert och behandlas konfidentiellt. Vid misstanke om att ett lösenord har röjts ska lösenordet omedelbart bytas ut eller det berörda kontot avaktiveras. Unika och individuella användaridentiteter ska användas.

2. Procedurer för inloggning och utloggning ska fastställas i säkerhetsplanen, i syfte att förhindra obehörig åtkomst.

Artikel 13

Tillträdeskontroll

1. Säkerhetsplanen ska fastställa ett formellt förfarande för registrering och avregistrering av personal, som gör det möjligt att bevilja och återkalla tillträde till SIS II-hårdvara och SIS II-programvara för operativa förvaltningsändamål. Tilldelningen och användningen av nödvändiga åtkomstuppgifter (lösenord eller liknande) ska kontrolleras genom ett formellt förvaltningsförfarande i enlighet med säkerhetsplanen.

2. Tillträdet till SIS II-hårdvara och programvara i CS-SIS ska

i) vara begränsad till auktoriserade personer,

ii) vara begränsat till fall där det är möjligt att fastställa ett legitimt syfte i enlighet med artikel 45 i förordning (EG) nr 1987/2006 och artikel 61 i beslut 2007/533/RIF, eller artikel 50.2 i förordning (EG) nr 1987/2006 och artikel 66.2 i beslut 2007/533/RIF.

iii) inte i tid och omfattning överstiga vad som är nödvändigt för ändamålet för tillträdet, och

iv) endast ske i enlighet med en policy för tillträdeskontroll som ska fastställas i säkerhetsplanen.

3. Endast konsoler och programvara som godkänts av den lokalt säkerhetsansvarige för det centrala SIS II ska användas vid CS-SIS. Användningen av hjälpprogram varmed kontrollen av system och applikationer skulle kunna kringgås ska begränsas och kontrolleras. Förfaranden för att kontrollera installationen av programvara ska inrättas.

Artikel 14

Kommunikationskontroll

Kommunikationsinfrastrukturen ska stå under kontroll för att säkerställa tillgänglighet, integritet och konfidentialitet i informationsutbytet. Kryptering ska användas för att skydda de uppgifter som överförs i kommunikationsinfrastrukturen.

Artikel 15

Kontroll av indata

Konton för personer som givits tillgång till SIS II-programvara från CS-SIS ska övervakas av den lokalt säkerhetsansvarige för det centrala SIS II. Användningen av dessa konton, inklusive tidsuppgifter och användaridentitet, ska registreras.

Artikel 16

Kontroll av transport

1. I säkerhetsplanen ska lämpliga åtgärder fastställas för att förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter vid överföring till eller från SIS II eller i samband med transport av databärare. Säkerhetsplanen ska även omfatta bestämmelser om tillåtna former av försändelse eller transport och om ansvarsförfaranden i samband med transport av föremål och deras ankomst till bestämmelseorten. Databärarna ska inte innehålla några andra data än de som ska översändas.

2. Tjänster som tillhandahålls av tredje man, och som innebär åtkomst till, behandling av eller vidarebefordran av uppgifter, förvaltning av databehandlingsinstallationer eller att databehandlingsinstallationer tillförs produkter eller tjänster, ska omfattas av lämpliga integrerade säkerhetskontroller.

Artikel 17

Kommunikationsinfrastrukturens säkerhet

1. Kommunikationsinfrastrukturen ska förvaltas och kontrolleras på ett tillfredsställande sätt för att skydda den mot hot och garantera säkerheten för kommunikationsinfrastrukturen i sig och för det centrala SIS II, inklusive de uppgifter som utbyts genom den.

2. För alla nätverkstjänster gäller att krav på säkerhetsanordningar, servicenivåer och förvaltning ska fastställas i nätserviceavtalet med tjänsteleverantören.

3. Skyddskraven omfattar inte endast accesspunkterna till SIS II, utan även eventuella andra tjänster som används av kommunikationsinfrastrukturen. Lämpliga åtgärder ska fastställas i säkerhetsplanen.

Artikel 18

Övervakning

1. Loggningsnoteringar om all konsultation och allt utbyte av personuppgifter i CS-SIS, i den mening som avses i artikel 18.1 i förordning (EG) nr 1987/2006 och artikel 18.1 i beslut 2007/533/RIF, ska lagras på ett säkert sätt på de platser där den ordinarie delen av CS-SIS och reservsystemet är belägna och finnas åtkomliga där under den maximiperiod som anges i artikel 18.3 i förordning (EG) nr 1987/2006 och artikel 18.3 i beslut 2007/533/RIF.

2. Förfaranden för att övervaka användningen av och eventuella brister i databehandlingsutrustningen ska fastställas i säkerhetsplanen, och resultaten av övervakningen ska gås igenom regelbundet. Om nödvändigt ska lämpliga åtgärder vidtas.

3. Loggfunktioner och loggar ska skyddas mot manipulation och obehörigt tillträde för att uppfylla kraven på insamling och bevarande av bevismaterial under den för ändamålet föreskrivna perioden.

Artikel 19

Kryptering

Krypteringsmetoder ska användas när det är lämpligt för att skydda information. Användningen av sådana krypteringsmetoder ska, tillsammans med syften och villkor, godkännas på förhand av systemets säkerhetsansvarige.

KAPITEL IV

PERSONALSÄKERHET

Artikel 20

Personalprofiler

1. Säkerhetsplanen ska fastställa funktioner och ansvarsområden för de personer som beviljats tillträde till det centrala SIS II.

2. Säkerhetsplanen ska fastställa funktioner och ansvarsområden för de personer som beviljats tillträde till kommunikationsinfrastrukturen.

3. Säkerhetsuppgifter och ansvarsområden för kommissionens anställda, uppdragstagare och andra medarbetare som är involverade i den operativa förvaltningen ska fastställas, dokumenteras och meddelas de berörda personerna. Dessa uppgifter och ansvarsområden ska för kommissionsanställdas del fastställas i arbetsbeskrivningen och målen. Motsvarande uppgifter för uppdragstagare ska fastställas i kontrakt eller tjänstenivåavtal.

4. Avtal om sekretess och tystnadsplikt ska ingås med alla berörda som inte omfattas av särskilda regler för offentliganställda på EU- eller medlemsstatsnivå. Personal som arbetar med SIS II-data ska ha nödvändigt säkerhetsgodkännande eller certifiering i enlighet med de närmare bestämmelser som ska fastställas i säkerhetsplanen.

Artikel 21

Information till personal

1. Alla anställda och uppdragstagare ska i den omfattning som krävs för deras tjänsteutövning erhålla lämplig fortbildning när det gäller säkerhetsmedvetande, rättsliga krav, politik och förfaranden.

2. Det ansvar som åligger anställda och uppdragstagare i samband med att en anställning upphör eller ett uppdrag avslutas ska fastställas i säkerhetsplanen, som också ska omfatta förfaranden för att förvalta återlämnande av egendom och återkalla tillträdesrätt i ovannämnda situationer.

KAPITEL V

SLUTBESTÄMMELSER

Artikel 22

Tillämpning

1. Detta beslut ska tillämpas från och med den dag som rådet fastställer i enlighet med artikel 55.2 i förordning (EG) nr 1987/2006 och artikel 71.2 i beslut 2007/533/RIF.

2. Artiklarna 1.1, 2.1 och 2.3 b, d, f och i samt artiklarna 3, 6.5, 7.5, 9.6, 10.6, 13.2 och 13.3, 15, 18 och 20.1 ska upphöra att gälla när förvaltningsmyndigheten övertar ansvaret.

Utfärdat i Bryssel den 4 maj 2010.

På kommissionens vägnar

José Manuel BARROSO

Ordförande