KOMMISSIONENS AFGØRELSE

af 4. maj 2010

om sikkerhedsplanen for det centrale SIS II og kommunikationsinfrastrukturen

(2010/261/EU)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006 af 20. december 2006 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) [1], særlig artikel 16,

under henvisning til Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) [2], særlig artikel 16, og

ud fra følgende betragtninger:

(1) Artikel 16 i forordning (EF) nr. 1987/2006 og artikel 16 i afgørelse 2007/533/RIA foreskriver, at forvaltningsmyndigheden, i forbindelse med det centrale SIS II, og Kommissionen, i forbindelse med kommunikationsinfrastrukturen, skal vedtage de nødvendige foranstaltninger, herunder en sikkerhedsplan.

(2) Artikel 15, stk. 4, i forordning (EF) nr. 1987/2006 og artikel 15, stk. 4, i afgørelse 2007/533/RIA foreskriver, at Kommissionen i en overgangsperiode skal være ansvarlig for den operationelle forvaltning af det centrale SIS II, indtil forvaltningsmyndigheden indleder sin virksomhed.

(3) Da forvaltningsmyndigheden endnu ikke er oprettet, skal den sikkerhedsplan, som Kommissionen skal vedtage, også gælde for det centrale SIS II i en overgangsperiode.

(4) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 [3] gælder for Kommissionens behandling af personoplysninger, når den varetager sine forpligtelser i forbindelse med den operationelle forvaltning af SIS II.

(5) Artikel, 15, stk. 7, i forordning (EF) nr. 1987/2006 og artikel 15, stk. 7, i afgørelse 2007/533/RIA foreskriver, at Kommissionen ved uddelegering af sit ansvar i overgangsperioden, indtil forvaltningsmyndigheden indleder sin virksomhed, skal sikre, at denne uddelegering ikke negativt påvirker konkrete kontrolmekanismer i henhold til EU-retten, uanset om det drejer sig om kontrol udøvet af Domstolen, Revisionsretten eller den europæiske tilsynsførende for databeskyttelse.

(6) Forvaltningsmyndigheden skal vedtage sin egen sikkerhedsplan i forbindelse med det centrale SIS II, når den har indledt sin virksomhed. Denne sikkerhedsplan skal derfor ophæves, i det omfang den har relation til det centrale SIS II, når forvaltningsmyndigheden indleder sin virksomhed.

(7) Artikel 4, stk. 3, i forordning (EF) nr. 1987/2006 og artikel 4, stk. 3, i afgørelse 2007/533/RIA foreskriver, at CS-SIS, der står for teknisk tilsyn og forvaltning, placeres i Strasbourg (Frankrig), og en backup af CS-SIS, der kan sikre alle funktioner i det overordnede CS-SIS i tilfælde af systemsvigt, placeres i Sankt Johann i Pongau (Østrig).

(8) Sikkerhedsplanen skal indbefatte en sikkerhedsansvarlig for systemet, der udfører sikkerhedsrelaterede opgaver i forbindelse med både det centrale SIS II og kommunikationsinfrastrukturen samt to lokale sikkerhedsansvarlige, der udfører sikkerhedsrelaterede opgaver i forbindelse med hhv. det centrale SIS II og kommunikationsinfrastrukturen. De sikkerhedsansvarliges roller skal fastlægges for at sikre en effektiv og hurtig reaktion på sikkerhedsrelaterede hændelser og rapportering heraf.

(9) Der skal fastlægges en sikkerhedspolitik, som beskriver alle tekniske og organisatoriske detaljer i overensstemmelse med bestemmelserne i denne afgørelse.

(10) Der skal fastlægges foranstaltninger for at sikre et tilstrækkeligt sikkerhedsniveau for virkemåden af det centrale SIS II og kommunikationsinfrastrukturen —

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

VEDTAGET DENNE AFGØRELSE:

KAPITEL I

GENERELLE BESTEMMELSER

Artikel 1

Formål

1. Med denne afgørelse fastlægges sikkerhedsorganisationen og foranstaltningerne (sikkerhedsplanen) i forbindelse med beskyttelsen af det centrale SIS II og de heri behandlede data mod trusler i relation til deres tilgængelighed, integritet og fortrolighed i henhold til artikel 16, stk. 1, i forordning (EF) nr. 1987/2006 og i artikel 16, stk. 1, i afgørelse 2007/533/RIA om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) i en overgangsperiode, indtil forvaltningsmyndigheden indleder sin virksomhed.

2. Med denne afgørelse fastlægges sikkerhedsorganisationen og foranstaltningerne (sikkerhedsplanen) i forbindelse med beskyttelsen af kommunikationsinfrastrukturen mod trusler i relation til dens tilgængelighed, integritet og fortrolighed i henhold til artikel 16 i forordning (EF) nr. 1987/2006 og i artikel 16 i afgørelse 2007/533/RIA om oprettelse, drift og brug af anden generation af Schengen-informationssystemet (SIS II).

KAPITEL II

ORGANISATION, ANSVARSOMRÅDER OG HÆNDELSESSTYRING

Artikel 2

Kommissionens opgaver

1. Kommissionen skal gennemføre og overvåge effektiviteten af sikkerhedsforanstaltningerne i forbindelse med det centrale SIS II, der henvises til i denne afgørelse.

2. Kommissionen skal gennemføre og overvåge effektiviteten af de sikkerhedsforanstaltninger i forbindelse med den kommunikationsinfrastruktur, der henvises til i denne afgørelse.

3. Kommissionen skal udpege en sikkerhedsansvarlig for systemet blandt sine embedsmænd. Den sikkerhedsansvarlige for systemet skal udnævnes af generaldirektøren for Kommissionens Generaldirektorat for Retlige Anliggender, Frihed og Sikkerhed. Den systemsikkerhedsansvarlige skal især:

a) udarbejde sikkerhedspolitikken som beskrevet i artikel 7 i denne afgørelse

b) overvåge effektiviteten af gennemførelsen af sikkerhedsprocedurerne i forbindelse med det centrale SIS II

c) overvåge effektiviteten af gennemførelsen af sikkerhedsprocedurerne i forbindelse med kommunikationsinfrastrukturen

d) bidrage til udarbejdelsen af rapportering i forbindelse med sikkerhed som omhandlet i artikel 50 i forordning (EF) nr. 1987/2006 og i artikel 66 i afgørelse 2007/533/RIA

e) udføre koordinerende og understøttende opgaver i forbindelse med de kontroller og revisioner, der udøves af den europæiske tilsynsførende for databeskyttelse som omhandlet i artikel 45 i forordning (EF) nr. 1987/2006 og i artikel 61 i afgørelse 2007/533/RIA, samt anmelde hændelser i henhold til artikel 5, stk. 2, til Kommissionens databeskyttelsesansvarlige

f) overvåge, at denne afgørelse og sikkerhedspolitikken anvendes korrekt og fuldt ud af alle leverandører, herunder underleverandører, der på nogen måde er involveret i forvaltningen af det centrale SIS II

g) overvåge, at denne afgørelse og sikkerhedspolitikken anvendes korrekt og fuldt ud af alle leverandører, herunder underleverandører, der på nogen måde er involveret i forvaltningen af kommunikationsinfrastrukturen

h) føre en liste over nationale kontaktpunkter for SIS II-sikkerhed og dele den med den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen

i) dele den liste, der henvises til i litra h) med den lokale sikkerhedsansvarlige for det centrale SIS II.

Artikel 3

Lokal sikkerhedsansvarlig for det centrale SIS II

1. Med forbehold af artikel 8 skal Kommissionen udpege en lokal sikkerhedsansvarlig for det centrale SIS II blandt sine embedsmænd. Interessekonflikter mellem den lokale sikkerhedsansvarliges opgaver og andre officielle opgaver skal forhindres. Den lokale sikkerhedsansvarlige for det centrale SIS II skal udnævnes af generaldirektøren for Kommissionens Generaldirektorat for Retlige Anliggender, Frihed og Sikkerhed.

2. Den lokale sikkerhedsansvarlige for det centrale SIS II skal sikre gennemførelse af de sikkerhedsforanstaltninger, der henvises til i denne afgørelse, og at sikkerhedsprocedurerne følges i det overordnede CS-SIS. Hvad angår backuppen af CS-SIS, skal den lokale sikkerhedsansvarlige for det centrale SIS II sikre gennemførelse af de sikkerhedsforanstaltninger, der henvises til i denne afgørelse, bortset fra dem, der henvises til i artikel 9, og at sikkerhedsprocedurerne i relation hertil følges.

3. Den lokale sikkerhedsansvarlige for det centrale SIS II kan pålægge underordnet personale en hvilken som helst af sine opgaver. Interessekonflikter mellem den lokale sikkerhedsansvarliges opgaver og andre officielle opgaver skal forhindres. Et kontakttelefonnummer skal gøre det muligt når som helst at få fat i den lokale sikkerhedsansvarlige eller dennes underordnede, der har tjeneste.

4. Den lokale sikkerhedsansvarlige for det centrale SIS II skal udføre de opgaver, der er et resultat af sikkerhedsforanstaltninger, som skal træffes i de lokaler, hvor det overordnede CS-SIS og backuppen af CS-SIS er placeret, inden for de grænser, der er fastsat i stk. 1, herunder især:

a) lokale operationelle sikkerhedsopgaver, herunder firewall audit-funktioner, regelmæssig sikkerhedstestning, revision og rapportering

b) overvåge effektiviteten af kontinuitetsplanen og sikre, at der udføres regelmæssige kontroller

c) sikre dokumentation for og rapportere enhver hændelse til den sikkerhedsansvarlige for systemet, der kan have indvirkning på sikkerheden i det centrale SIS II eller kommunikationsinfrastrukturen

d) informere den sikkerhedsansvarlige for systemet, hvis det er nødvendigt at ændre sikkerhedspolitikken

e) overvåge, at denne afgørelse og sikkerhedspolitikken anvendes af alle leverandører, herunder underleverandører, der på nogen måde er involveret i den operationelle forvaltning af det centrale SIS II

f) sikre, at personalet er klar over dets forpligtelser og overvåge anvendelsen af sikkerhedspolitikken

g) overvåge it-sikkerhedsudviklingen og sikre, at personalet er uddannet i overensstemmelse hermed

h) forberede underliggende oplysninger og undersøge mulighederne for udarbejdelse, ajourføring og gennemgang af sikkerhedspolitikken i henhold til artikel 7.

Artikel 4

Lokal sikkerhedsansvarlig for kommunikationsinfrastrukturen

1. Med forbehold af artikel 8 skal Kommissionen udpege en lokal sikkerhedsansvarlig for kommunikationsinfrastrukturen blandt sine embedsmænd. Interessekonflikter mellem den lokale sikkerhedsansvarliges opgaver og andre officielle opgaver skal forhindres. Den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen skal udnævnes af generaldirektøren for Kommissionens Generaldirektorat for Retlige Anliggender, Frihed og Sikkerhed.

2. Den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen skal overvåge kommunikationsinfrastrukturens funktion og sikre, at sikkerhedsforanstaltningerne gennemføres, og at sikkerhedsprocedurerne følges.

3. Den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen kan pålægge underordnet personale en hvilken som helst af sine opgaver. Interessekonflikter mellem den lokale sikkerhedsansvarliges opgaver og andre officielle opgaver skal forhindres. Et kontakttelefonnummer skal gøre det muligt når som helst at få fat i den lokale sikkerhedsansvarlige eller dennes underordnede, der har tjeneste.

4. Den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen skal udføre de opgaver, der er et resultat af sikkerhedsforanstaltninger, som skal træffes i relation til kommunikationsinfrastrukturen, herunder især:

a) alle operationelle sikkerhedsopgaver i forbindelse med kommunikationsinfrastrukturen, herunder firewall audit-funktioner, regelmæssig sikkerhedstestning, revision og rapportering

b) overvåge effektiviteten af kontinuitetsplanen og sikre, at der udføres regelmæssige kontroller

c) sikre dokumentation for og rapportere enhver hændelse i kommunikationsinfrastrukturen til den sikkerhedsansvarlige for systemet, der kan have indvirkning på sikkerheden i det centrale SIS II eller kommunikationsinfrastrukturen

d) informere den sikkerhedsansvarlige for systemet, hvis det er nødvendigt at ændre sikkerhedspolitikken

e) overvåge, at denne afgørelse og sikkerhedspolitikken anvendes af alle leverandører, herunder underleverandører, der på nogen måde er involveret i forvaltningen af kommunikationsinfrastrukturen

f) sikre, at personalet er klar over dets forpligtelser, samt overvåge anvendelsen af sikkerhedspolitikken

g) overvåge it-sikkerhedsudviklingen og sikre, at personalet er uddannet i overensstemmelse hermed

h) forberede underliggende oplysninger og undersøge mulighederne for udarbejdelse, ajourføring og gennemgang af sikkerhedspolitikken i henhold til artikel 7.

Artikel 5

Sikkerhedsrelaterede hændelser

1. Enhver hændelse, der har eller kan have indvirkning på sikkerheden i SIS II og forårsage skade eller tab i forbindelse med SIS II, skal anses for at være en sikkerhedshændelse, især hvor adgang til oplysninger kan have forekommet, eller hvor tilgængeligheden, integriteten og fortroligheden af data er eller kan være blevet kompromitteret.

2. Sikkerhedsrelaterede hændelser skal styres for at sikre en hurtig, effektiv og behørig reaktion i overensstemmelse med sikkerhedspolitikken. Der skal fastlægges procedurer for genopretning efter en hændelse.

3. Oplysninger om en sikkerhedshændelse, der har eller kan have indvirkning på virkemåden af SIS II i en medlemsstat eller på tilgængeligheden, integriteten og fortroligheden af de data, som en medlemsstat har registreret eller sendt, skal videreformidles til den pågældende medlemsstat. Sikkerhedshændelser skal anmeldes til Kommissionens databeskyttelsesansvarlige.

Artikel 6

Hændelsesstyring

1. Alle ansatte og leverandører, der er involveret i udviklingen, forvaltningen og virkemåden af SIS II, skal registrere og rapportere enhver observeret eller formodet sikkerhedssvaghed i kommunikationsinfrastrukturen til den sikkerhedsansvarlige for systemet eller til den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen.

2. Hvis der konstateres en hændelse, der har eller kan have indvirkning på sikkerheden i forbindelse med SIS II, skal den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen så hurtigt som muligt informere den sikkerhedsansvarlige for systemet og, hvor det er relevant, det nationale kontaktpunkt for SIS II-sikkerhed, hvis der findes et sådant kontaktpunkt i den pågældende medlemsstat, skriftligt eller, i påtrængende hastetilfælde, via andre kommunikationskanaler. Rapporten skal indeholde beskrivelsen af sikkerhedshændelsen, risikoniveauet, mulige konsekvenser og de foranstaltninger, der er truffet eller skal træffes for at mindske risikoen.

3. Enhver dokumentation i forbindelse med sikkerhedshændelsen skal sikres øjeblikkeligt af den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen. I det omfang, det er muligt i henhold til gældende databeskyttelsesbestemmelser, skal denne dokumentation stilles til rådighed for den sikkerhedsansvarlige for systemet efter anmodning herom.

4. Der skal fastlægges feedbackprocesser i sikkerhedspolitikken for at sikre, at oplysninger om typen, håndteringen og resultatet af en sikkerhedshændelse videreformidles til den sikkerhedsansvarlige for systemet og til den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen, når hændelsen er blevet behandlet og ikke længere er i gang.

5. Stk. 1-4 finder tilsvarende anvendelse på hændelser i det centrale SIS II. For så vidt der henvises til den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen i stk. 1-4, skal dette anses for at være en henvisning til den lokale sikkerhedsansvarlige for det centrale SIS II.

KAPITEL III

SIKKERHEDSFORANSTALTNINGER

Artikel 7

Sikkerhedspolitik

1. Generaldirektøren for Kommissionens Generaldirektorat for Retlige Anliggender, Frihed og Sikkerhed skal fastlægge, ajourføre og regelmæssigt gennemgå en bindende sikkerhedspolitik i henhold til denne afgørelse. Sikkerhedspolitikken skal indeholde detaljerede procedurer og foranstaltninger for at beskytte mod trusler i relation til tilgængeligheden, integriteten og fortroligheden af kommunikationsinfrastrukturen, herunder nødplaner, med henblik på at sikre et tilstrækkeligt sikkerhedsniveau som foreskrevet i denne afgørelse. Sikkerhedspolitikken skal være i overensstemmelse med denne afgørelse.

2. Sikkerhedspolitikken skal baseres på en risikovurdering. De foranstaltninger, som foreskrives af sikkerhedspolitikken, skal stå i et rimeligt forhold til de identificerede risici.

3. Risikovurderingen og sikkerhedspolitikken skal opdateres, hvis teknologiske ændringer, identifikation af nye trusler eller andre forhold nødvendiggør dette. Sikkerhedspolitikken skal under alle omstændigheder gennemgås en gang om året for at sikre, at der fortsat reageres hensigtsmæssigt på den seneste risikovurdering eller en anden nyligt identificeret ændring, trussel eller et andet relevant forhold.

4. Sikkerhedspolitikken skal udarbejdes af den sikkerhedsansvarlige for systemet i samarbejde med den lokale sikkerhedsansvarlige for det centrale SIS II og den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen.

5. Stk. 1-4 finder tilsvarende anvendelse på sikkerhedspolitikken for det centrale SIS II. For så vidt der henvises til den lokale sikkerhedsansvarlige for kommunikationsinfrastrukturen i stk. 1-4, skal dette anses for at være en henvisning til den lokale sikkerhedsansvarlige for det centrale SIS II.

Artikel 8

Gennemførelse af sikkerhedsforanstaltningerne

1. Gennemførelsen af opgaver og krav, der er fastlagt i denne afgørelse og i sikkerhedspolitikken, herunder udpegelsen af en lokal sikkerhedsansvarlig, kan udliciteres eller overdrages til private eller offentlige organer.

2. I dette tilfælde skal Kommissionen gennem juridisk bindende aftaler sikre, at de krav, der er fastlagt i denne afgørelse og i sikkerhedspolitikken, overholdes fuldt ud. I tilfælde af uddelegering eller udlicitering af opgaven med udpegelse af en lokal sikkerhedsansvarlig skal Kommissionen gennem juridisk bindende aftaler sikre, at den vil blive konsulteret med hensyn til den person, der skal udpeges som lokal sikkerhedsansvarlig.

Artikel 9

Adgangskontrolfaciliteter

1. Der skal anvendes sikkerhedsperimetre med passende barrierer og adgangskontroller til at beskytte områder, der rummer databehandlingsfaciliteter.

2. Inden for sikkerhedsperimetrene skal der defineres sikre områder for at beskytte de fysiske komponenter (aktiver), herunder hardware, datamedier og konsoller, planer og andre dokumenter i SIS II samt kontorer og andre arbejdssteder, hvor personale er involveret i driften af SIS II. Disse sikre områder skal beskyttes ved hjælp af passende adgangskontroller for at sikre, at kun autoriseret personale har adgang hertil. Arbejde i sikre områder skal være omfattet af de detaljerede sikkerhedsregler, der er fastlagt i sikkerhedspolitikken.

3. Der skal tages højde for og installeres fysisk sikkerhed i kontorer, rum og faciliteter. Adgangspunkter, f.eks. af- og pålæsningsområder, og andre punkter, hvor uautoriserede personer kan få adgang til lokalerne, skal kontrolleres og om muligt isoleres fra databehandlingsfaciliteter for at undgå uautoriseret adgang.

4. Der skal konstrueres en fysisk beskyttelse af sikkerhedsperimetrene mod skader, der forårsages af naturlige eller menneskeskabte katastrofer, og de skal anvendes proportionalt i forhold til risikoen.

5. Udstyr skal beskyttes mod fysiske og miljømæssige trusler samt mod risikoen for uautoriseret adgang.

6. Hvis Kommissionen har adgang til sådanne oplysninger, skal den tilføje et kontaktpunkt på den liste, der henvises til i artikel 2, stk. 3, litra h), i forbindelse med overvågning af gennemførelsen af bestemmelserne i denne artikel i de lokaler, hvor backuppen af CS-SIS er placeret.

Artikel 10

Datamedier og kontrol med aktiver

1. Flytbare medier, som indeholder data, skal beskyttes mod uautoriseret adgang, misbrug eller forvanskning, og læseligheden heraf skal sikres i hele deres levetid.

2. Medier skal bortskaffes på en forsvarlig og sikker måde, når de ikke længere skal anvendes, i overensstemmelse med de detaljerede procedurer, der skal fastlægges i sikkerhedspolitikken.

3. Fortegnelser skal sikre, at oplysninger om lagringsplaceringen, den gældende opbevaringsperiode og adgangsrettigheder er tilgængelige.

4. Alle vigtige aktiver i forbindelse med kommunikationsinfrastrukturen skal identificeres, således at de kan beskyttes i overensstemmelse med deres vigtighed. Der skal føres et opdateret register over relevant it-udstyr.

5. Der skal forefindes opdateret dokumentation for kommunikationsinfrastrukturen. Denne dokumentation skal beskyttes mod uautoriseret adgang.

6. Stk. 1-5 finder tilsvarende anvendelse på det centrale SIS II. For så vidt der henvises til kommunikationsinfrastrukturen, skal dette anses for at være en henvisning til det centrale SIS II.

Artikel 11

Lagringskontrol

1. Der skal træffes passende foranstaltninger til at sikre korrekt lagring af data og forhindre uautoriseret adgang hertil.

2. Alt udstyr, der indeholder lagringsmedier, skal kontrolleres for at sikre, at følsomme data er blevet fjernet eller fuldstændig overskrevet inden bortskaffelse, eller det skal destrueres sikkert.

Artikel 12

Passwordkontrol

1. Alle adgangskoder skal opbevares sikkert og behandles fortroligt. Hvis der er mistanke om, at en adgangskode er blevet afsløret, skal adgangskoden ændres øjeblikkeligt, eller den pågældende konto skal deaktiveres. Der skal anvendes entydige og individuelle bruger-id'er.

2. Der skal fastlægges procedurer i sikkerhedspolitikken for log-in/log-off for at forhindre uautoriseret adgang.

Artikel 13

Adgangskontrol

1. Sikkerhedspolitikken skal fastlægge en formel procedure for registrering og afregistrering af personale i forbindelse med at tildele og inddrage adgangsrettigheder til SIS II-hardware og -software i forbindelse med den operationelle forvaltning. Tildelingen og brugen af de fornødne adgangsrettigheder (adgangskoder eller andre egnede midler) skal kontrolleres ved hjælp af en formel forvaltningsproces som fastsat i sikkerhedspolitikken.

2. Adgang til SIS II-hardware og -software i forbindelse med CS-SIS skal:

i) være begrænset til autoriserede personer

ii) være begrænset til tilfælde, hvor der kan identificeres et lovligt formål i henhold til artikel 45 i forordning (EF) nr. 1987/2006 og artikel 61 i afgørelse 2007/533/RIA, eller i henhold til artikel 50, stk. 2, i forordning (EF) nr. 1987/2006 og artikel 66, stk. 2, i afgørelse 2007/533/RIA

iii) ikke overskride den varighed og det omfang, der er nødvendigt i forbindelse med formålet med adgangen og

iv) kun ske i overensstemmelse med en adgangskontrolpolitik, der skal defineres i sikkerhedspolitikken.

3. Kun konsoller og software, der er autoriseret af den lokale sikkerhedsansvarlige for det centrale SIS II, skal anvendes i forbindelse med CS-SIS. Brugen af systemværktøjer, der eventuelt kan overstyre system- og applikationskontroller, skal begrænses og kontrolleres. Der skal være procedurer med henblik på kontrol af softwareinstallationer.

Artikel 14

Kommunikationskontrol

Kommunikationsinfrastrukturen skal overvåges med henblik på at skabe tilgængelighed, integritet og fortrolighed i forbindelse med informationsudvekslingen. Krypteringsværktøjer skal anvendes for at sikre de data, der overføres i kommunikationsinfrastrukturen.

Artikel 15

Inputkontrol

Konti for personer, der er autoriseret til at have adgang til SIS II-software fra CS-SIS, skal overvåges af den lokale sikkerhedsansvarlige for det centrale SIS II. Brugen af disse konti, herunder varighed og bruger-id, skal registreres.

Artikel 16

Overførselskontrol

1. Der skal træffes de nødvendige foranstaltninger i sikkerhedspolitikken med henblik på at forhindre uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger under overførsler af disse til eller fra SIS II eller under transport af databærere. Der skal fastsættes bestemmelser i sikkerhedspolitikken med hensyn til tilladte typer af forsendelse eller transport samt med hensyn til ansvarsprocedurer i forbindelse med transport af udstyr og dets ankomst på bestemmelsesstedet. Datamediet må ikke indeholde nogen andre data end dem, der skal sendes.

2. Tjenester, der leveres af tredjeparter, og som involverer vurdering, behandling, kommunikation eller forvaltning af databehandlingsfaciliteter eller tilføjelse af produkter eller tjenester til databehandlingsfaciliteter, skal have passende indbyggede sikkerhedskontroller.

Artikel 17

Sikkerheden af kommunikationsinfrastrukturen

1. Kommunikationsinfrastrukturen skal forvaltes og kontrolleres tilfredsstillende med henblik på at beskytte den mod trusler og garantere sikkerheden for selve kommunikationsinfrastrukturen og for det centrale SIS II, herunder oplysninger, der udveksles herigennem.

2. Sikkerhedsfunktioner, serviceniveauer og forvaltningskrav i forbindelse med alle netværkstjenester skal identificeres i serviceaftalen med tjenesteudbyderen.

3. Ud over at beskytte SIS II-adgangspunkterne skal enhver yderligere tjeneste, der anvendes af kommunikationsinfrastrukturen, også beskyttes. Der skal defineres passende foranstaltninger i sikkerhedspolitikken.

Artikel 18

Overvågning

1. Logs, som registrerer de oplysninger, der henvises til i artikel 18, stk. 1, i forordning (EF) nr. 1987/2006 og artikel 18, stk. 1, i afgørelse 2007/533/RIA, om hver adgang til og alle udvekslinger af personoplysninger inden for CS-SIS skal lagres forsvarligt og sikkert i og være tilgængelige fra de lokaler, hvor det overordnede CS-SIS og backuppen af CS-SIS er placeret i den maksimale periode, der henvises til i artikel 18, stk. 3, i forordning (EF) nr. 1987/2006 og artikel 18, stk. 3, i afgørelse 2007/533/RIA.

2. Procedurer for overvågning af brug eller fejl i databehandlingsfaciliteter skal fastlægges i sikkerhedspolitikken, og resultaterne af overvågningsaktiviteterne skal gennemgås regelmæssigt. Om nødvendigt skal der træffes passende foranstaltninger.

3. Logningsfaciliteter og logs skal beskyttes mod manipulation og uautoriseret adgang med henblik på at overholde kravene til indsamling og opbevaring af dokumentation i opbevaringsperioden.

Artikel 19

Krypteringsteknikker

Krypteringsteknikker skal anvendes, hvor det er relevant, til beskyttelse af oplysninger. Anvendelsen heraf skal, sammen med formål og betingelser, godkendes af den sikkerhedsansvarlige for systemet på forhånd.

KAPITEL IV

SIKKERHEDEN I FORBINDELSE MED MENNESKELIGE RESSOURCER

Artikel 20

Personaleprofiler

1. Sikkerhedspolitikken skal definere funktionerne og ansvarsområderne for de personer, der er autoriseret til at have adgang til det centrale SIS II.

2. Sikkerhedspolitikken skal definere funktionerne og ansvarsområderne for de personer, der er autoriseret til at have adgang til kommunikationsinfrastrukturen.

3. Sikkerhedsroller og ansvarsområder for Kommissionens ansatte, leverandører og personale, der er involveret i den operationelle forvaltning, skal fastlægges, dokumenteres og meddeles til de pågældende personer. I jobbeskrivelsen og målene skal disse roller og ansvarsområder for Kommissionens tjenestegrene være angivet. For leverandører skal disse være indeholdt i kontrakter eller serviceniveauaftaler.

4. Der skal indgås aftaler om fortrolighed og tavshedspligt med alle personer, for hvem der ikke gælder nogen public service-regler på EU-plan eller medlemsstatsplan. Personale, der skal arbejde med SIS II-data, skal have den nødvendige sikkerhedsgodkendelse eller autorisation i overensstemmelse med de detaljerede procedurer, der skal fastlægges i sikkerhedspolitikken.

Artikel 21

Information af personale

1. Alt personale skal gennemføre relevante kurser i sikkerhedsbevidsthed, lovkrav, politikker og procedurer i det omfang, som deres arbejdsopgaver nødvendiggør det.

2. Ved ansættelsesforholdets eller kontraktens udløb skal ansvarsområder i forbindelse med jobskifte eller ansættelsesforholdets ophør fastsættes for ansatte og leverandører i sikkerhedspolitikken, og der skal fastlægges procedurer i sikkerhedspolitikken med henblik på at forvalte returneringen af aktiver og inddragelsen af adgangsrettigheder.

KAPITEL V

AFSLUTTENDE BESTEMMELSER

Artikel 22

Anvendelsesområde

1. Denne afgørelse finder anvendelse fra den dato, der fastsættes af Rådet i overensstemmelse med artikel 55, stk. 2, i forordning (EF) nr. 1987/2006 og artikel 71, stk. 2, i afgørelse 2007/533/RIA.

2. Artikel 1, stk. 1, artikel 2, stk. 1, artikel 2, stk. 3, litra b), d), f) og i), artikel 3, artikel 6, stk. 5, artikel 7, stk. 5, artikel 9, stk. 6 artikel 10, stk. 6, artikel 13, stk. 2 og 3, artikel 15, 18 og artikel 20, stk. 1, ophæves, når forvaltningsmyndigheden indleder sin virksomhed.

Udfærdiget i Bruxelles, den 4. maj 2010.

For Kommissionen

José Manuel BARROSO

Formand