BESLUIT VAN DE COMMISSIE

van 4 mei 2010

betreffende het beveiligingsplan voor het centrale SIS II en de communicatie-infrastructuur

(2010/261/EU)

DE EUROPESE COMMISSIE,

Gelet op het Verdrag betreffende de werking van de Europese Unie,

Gelet op Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) [1], en met name op artikel 16,

Gelet op Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) [2], en met name op artikel 16,

Overwegende hetgeen volgt:

(1) In artikel 16 van Verordening (EG) nr. 1987/2006 en artikel 16 van Besluit 2007/533/JBZ wordt bepaald dat de beheersautoriteit, voor het centrale SIS II, en de Commissie, voor de communicatie-infrastructuur, de nodige maatregelen dienen te nemen, waartoe ook een beveiligingsplan behoort.

(2) In artikel 15, lid 4, van Verordening (EG) nr. 1987/2006 en artikel 15, lid 4, van Besluit 2007/533/JBZ wordt bepaald dat tijdens de overgangsperiode die aan de aanvang van de werkzaamheden van de beheersautoriteit voorafgaat, de Commissie met het operationele beheer van het centrale SIS II is belast.

(3) Aangezien de beheersautoriteit nog niet is ingesteld, dient het door de Commissie goed te keuren beveiligingsplan gedurende de overgangsperiode ook op het centrale SIS II van toepassing te zijn.

(4) Verordening (EG) nr. 45/2001van het Europees Parlement en de Raad [3] is van toepassing op de verwerking van persoonsgegevens door de Commissie bij het uitvoeren van haar taken op het gebied van het operationele beheer van SIS II.

(5) In artikel 15, lid 7, van Verordening (EG) nr. 1987/2006 en artikel 15, lid 7, van Besluit 2007/533/JBZ wordt bepaald dat indien de Commissie haar taken delegeert tijdens de overgangsperiode die aan de aanvang van de werkzaamheden van de beheersautoriteit voorafgaat, zij dient te waarborgen dat de delegatie niet ten koste gaat van de doeltreffendheid van de controlemechanismen van het EU-recht, ongeacht of het gaat om controle door het Hof van Justitie, de Rekenkamer of de Europese Toezichthouder voor gegevensbescherming.

(6) De beheersautoriteit dient, zodra zij haar werkzaamheden heeft aangevangen, haar eigen beveiligingsplan voor het centrale SIS II vast te stellen. Dat beveiligingsplan dient derhalve buiten werking te treden wanneer de beheersautoriteit haar werkzaamheden heeft aangevangen, voor zover het betrekking heeft op het centrale SIS II.

(7) In artikel 4, lid 3, van Verordening (EG) nr. 1987/2006 en artikel 4, lid 3, van Besluit 2007/533/JBZ wordt bepaald dat CS-SIS, dat voor technisch toezicht en beheer zorgt, zich in Straatsburg (Frankrijk) bevindt en een vervangend CS-SIS, dat alle functies van het hoofdsysteem van CS-SIS kan overnemen wanneer dit uitvalt, in Sankt Johann im Pongau (Oostenrijk).

(8) Het beveiligingsplan dient te voorzien in een systeembeveiligingsfunctionaris, die belast wordt met beveiligingstaken voor zowel het centrale SIS II als de communicatie-infrastructuur, en twee plaatselijke beveiligingsfunctionarissen, die belast worden met beveiligingstaken voor respectievelijk het centrale SIS II en de communicatie-infrastructuur. De taken van de beveiligingsfunctionarissen dienen te worden vastgesteld om te waarborgen dat op veiligheidsincidenten en meldingen daarvan doeltreffend en snel wordt gereageerd.

(9) Er dient een beveiligingsbeleid te worden vastgesteld, waarin alle technische en organisatorische details overeenkomstig dit besluit aan de orde komen.

(10) Er dienen maatregelen te worden vastgesteld om voor de werking van het centrale SIS II en de communicatie-infrastructuur een passend beveiligingsniveau te waarborgen,

[1] PB L 381 van 28.12.2006, blz. 4.
[2] PB L 205 van 7.8.2007, blz. 63.
[3] PB L 8 van 12.1.2001, blz. 1.

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

1. Dit besluit betreft de organisatie van en de maatregelen voor de beveiliging (het beveiligingsplan) die vereist zijn ter bescherming van het centrale SIS II en de daarin verwerkte gegevens tegen bedreigingen van de beschikbaarheid, integriteit en vertrouwelijkheid daarvan, als bedoeld in artikel 16, lid 1, van Verordening (EG) nr. 1987/2006 en artikel 16, lid 1, van Besluit 2007/533/JBZ betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) gedurende een overgangsperiode, totdat de beheersautoriteit haar werkzaamheden aanvangt.

2. Dit besluit betreft de organisatie van en de maatregelen voor de beveiliging (het beveiligingsplan) die vereist zijn ter bescherming van de communicatie-infrastructuur tegen bedreigingen van de beschikbaarheid, integriteit en vertrouwelijkheid daarvan, als bedoeld in artikel 16 van Verordening (EG) nr. 1987/2006 en artikel 16 van Besluit 2007/533/JBZ betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II).

HOOFDSTUK II

ORGANISATIE, TAKEN EN INCIDENTBEHEERSING

Artikel 2

Taken van de Commissie

1. De Commissie voert de in dit besluit bedoelde beveiligingsmaatregelen voor het centrale SIS II uit en houdt toezicht op de effectiviteit van die beveiligingsmaatregelen.

2. De Commissie voert de in dit besluit bedoelde beveiligingsmaatregelen voor de communicatie-infrastructuur uit en houdt toezicht op de effectiviteit van die beveiligingsmaatregelen.

3. De Commissie wijst onder haar ambtenaren een systeembeveiligingsfunctionaris aan. De systeembeveiligingsfunctionaris wordt benoemd door de directeur-generaal van het directoraat-generaal Justitie, vrijheid en veiligheid van de Commissie. De taken van de systeembeveiligingsfunctionaris omvatten in het bijzonder:

a) formuleren van het beveiligingsbeleid als omschreven in artikel 7 van dit besluit;

b) toezicht houden op de doeltreffende uitvoering van de beveiligingsprocedures voor het centrale SIS II;

c) toezicht houden op de doeltreffende uitvoering van de beveiligingsprocedures voor de communicatie-infrastructuur;

d) bijdragen aan de verslaglegging over de beveiliging als bedoeld in artikel 50 van Verordening (EG) nr. 1987/2008 en artikel 66 van Besluit 2007/533/JBZ;

e) coördinatie- en bijstandstaken in verband met de controles en audits die worden uitgevoerd door de Europese Toezichthouder voor gegevensbescherming, als bedoeld in artikel 45 van Verordening (EG) nr. 1987/2006 en artikel 61 van Besluit 2007/533/JBZ, alsmede melden van incidenten als bedoeld in artikel 5, lid 2, aan de systeembeveiligingsfunctionaris van de Commissie;

f) erop toezien dat dit besluit en het beveiligingsbeleid correct en volledig worden toegepast door alle contractanten en subcontractanten die op welke wijze ook bij het beheer van het centrale SIS II betrokken zijn;

g) erop toezien dat dit besluit en het beveiligingsbeleid correct en volledig worden toegepast door alle contractanten en subcontractanten die op welke wijze ook bij het beheer van de communicatie-infrastructuur betrokken zijn;

h) bijhouden van een lijst van centrale nationale contactpunten voor de beveiliging van SIS II en delen van deze lijst met de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur.

i) delen van de onder h) bedoelde lijst met de plaatselijke beveiligingsfunctionaris voor het centrale SIS II.

Artikel 3

Plaatselijke beveiligingsfunctionaris voor het centrale SIS II

1. De Commissie wijst onder haar ambtenaren een plaatselijke beveiligingsfunctionaris voor het centrale SIS II aan, onverminderd het bepaalde in artikel 8. Belangenconflicten tussen de taken van de plaatselijke beveiligingsfunctionaris en andere officiële verplichtingen worden vermeden. De plaatselijke beveiligingsfunctionaris voor het centrale SIS II wordt benoemd door de directeur-generaal van het directoraat-generaal Justitie, vrijheid en veiligheid van de Commissie.

2. De plaatselijke beveiligingsfunctionaris voor het centrale SIS II ziet erop toe dat de in dit besluit bedoelde beveiligingsmaatregelen worden uitgevoerd en dat de beveiligingsprocedures in het hoofdsysteem van CS-SIS worden nageleefd. Wat het vervangingssysteem voor CS-SIS betreft, ziet de plaatselijke beveiligingsfunctionaris voor het centrale SIS II erop toe dat de in dit besluit bedoelde beveiligingsmaatregelen, met uitzondering van die in artikel 9, worden uitgevoerd en dat de daarmee samenhangende beveiligingsprocedures worden nageleefd.

3. De plaatselijke beveiligingsfunctionaris voor het centrale SIS II kan elk van zijn taken uitbesteden aan ondergeschikt personeel. Belangenconflicten tussen deze taken en andere officiële verplichtingen worden vermeden. De plaatselijke beveiligingsfunctionaris of zijn dienstdoende plaatsvervanger is te allen tijde op hetzelfde telefoonnummer en adres bereikbaar.

4. De plaatselijke beveiligingsfunctionaris voor het centrale SIS II voert de taken uit die voortvloeien uit de beveiligingsmaatregelen die op de hoofdlocatie en de plaatsvervangende locatie van CS-SIS moeten worden genomen, met inachtneming van lid 1, en die in het bijzonder omvatten:

a) taken uitvoeren inzake de plaatselijke operationele beveiliging, zoals audit van de firewall en regelmatige beveiligingstests, -audits en -verslagen;

b) toezicht houden op de effectiviteit van het bedrijfscontinuïteitsplan en op geregelde beveiligingsoefeningen;

c) informatie verzamelen en rapporteren aan de systeembeveiligingsfunctionaris over alle incidenten die gevolgen kunnen hebben voor de veiligheid van het centrale SIS II of de communicatie-infrastructuur;

d) de systeembeveiligingsfunctionaris informeren indien het beveiligingsbeleid moet worden gewijzigd;

e) erop toezien dat dit besluit en het beveiligingsbeleid worden toegepast door alle contractanten en subcontractanten die op welke wijze ook bij het operationele beheer van het centrale SIS II betrokken zijn;

f) erop toezien dat alle personeelsleden op hun verplichtingen worden gewezen, en toezicht houden op de toepassing van het beveiligingsbeleid;

g) ontwikkelingen op het gebied van IT-beveiliging volgen en ervoor zorgen dat het personeel op dit gebied wordt opgeleid;

h) ondersteunende informatie en opties verzamelen voor de formulering, bijwerking en evaluatie van het beveiligingsbeleid overeenkomstig artikel 7.

Artikel 4

Plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur

1. De Commissie wijst onder haar ambtenaren een plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur aan, onverminderd het bepaalde in artikel 8. Belangenconflicten tussen de taken van de plaatselijke beveiligingsfunctionaris en andere officiële verplichtingen worden vermeden. De plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur wordt benoemd door de directeur-generaal van het directoraat-generaal Justitie, vrijheid en veiligheid van de Commissie.

2. De plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur bewaakt het functioneren van de communicatie-infrastructuur en ziet erop toe dat de beveiligingsmaatregelen worden uitgevoerd en de beveiligingsprocedures nageleefd.

3. De plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur kan elk van zijn taken uitbesteden aan ondergeschikt personeel. Belangenconflicten tussen deze taken en andere officiële verplichtingen worden vermeden. De plaatselijke beveiligingsfunctionaris of zijn dienstdoende plaatsvervanger is te allen tijde op hetzelfde telefoonnummer en adres bereikbaar.

4. De plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur voert de taken uit die voortvloeien uit de beveiligingsmaatregelen voor de communicatie-infrastructuur, in het bijzonder:

a) alle operationele beveiligingstaken met betrekking tot de communicatie-infrastructuur, zoals audit van de firewall en regelmatige beveiligingstests, -audits en -verslagen;

b) toezicht houden op de effectiviteit van het bedrijfscontinuïteitsplan en op geregelde beveiligingsoefeningen;

c) informatie verzamelen en rapporteren aan de systeembeveiligingsfunctionaris over alle incidenten in de communicatie-infrastructuur die gevolgen kunnen hebben voor de veiligheid van het centrale SIS II of de communicatie-infrastructuur;

d) de systeembeveiligingsfunctionaris informeren indien het beveiligingsbeleid moet worden gewijzigd;

e) erop toezien dat dit besluit en het beveiligingsbeleid worden toegepast door alle contractanten en subcontractanten die op welke wijze ook bij het beheer van de communicatie-infrastructuur betrokken zijn;

f) erop toezien dat alle personeelsleden op hun verplichtingen worden gewezen, en toezicht houden op de toepassing van het beveiligingsbeleid;

g) ontwikkelingen op het gebied van IT-beveiliging volgen en ervoor zorgen dat het personeel op dit gebied wordt opgeleid;

h) ondersteunende informatie en opties verzamelen voor de formulering, bijwerking en evaluatie van het beveiligingsbeleid overeenkomstig artikel 7.

Artikel 5

Veiligheidsincidenten

1. Elke gebeurtenis die gevolgen heeft of kan hebben voor de veiligheid van SIS II en die SIS II schade of verlies kan toebrengen, wordt beschouwd als een veiligheidsincident, met name wanneer toegang tot gegevens kan zijn verkregen of wanneer de beschikbaarheid, de integriteit en de vertrouwelijkheid van gegevens in gevaar is gekomen of kan zijn gekomen.

2. De beheersing van veiligheidsincidenten is gericht op een snelle, effectieve en passende respons overeenkomstig het beveiligingsbeleid. Er worden procedures opgezet voor herstel na een incident.

3. Informatie over een veiligheidsincident dat gevolgen heeft of kan hebben voor de werking van SIS II in een lidstaat of voor de beschikbaarheid, de integriteit en de vertrouwelijkheid van door een lidstaat ingevoerde of verzonden gegevens wordt verstrekt aan de betrokken lidstaat. Veiligheidsincidenten worden gemeld aan de gegevensbeschermingsfunctionaris van de Commissie.

Artikel 6

Incidentbeheersing

1. Alle personeelsleden en contractanten die betrokken zijn bij de ontwikkeling, het beheer en de werking van SIS II zijn verplicht alle geconstateerde of vermoede beveiligingslacunes in de communicatie-infrastructuur te melden aan de systeembeveiligingsfunctionaris of de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur.

2. Bij constatering van een incident dat gevolgen heeft of kan hebben voor de veiligheid van SIS II, meldt de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur dit zo snel mogelijk schriftelijk, of in uiterst spoedeisende gevallen via andere communicatiekanalen, aan de systeembeveiligingsfunctionaris en, waar van toepassing, het centrale nationale contactpunt voor de beveiliging van SIS II, indien zo'n contactpunt in de betrokken lidstaat bestaat. De melding omvat een beschrijving van het veiligheidsincident, het risiconiveau, de mogelijke gevolgen en de maatregelen die zijn of zouden moeten worden getroffen om het risico te verminderen.

3. Alle bewijsmateriaal betreffende het veiligheidsincident wordt door de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur onmiddellijk verzameld. Indien dat overeenkomstig de toepasselijke bepalingen inzake gegevensbescherming mogelijk is, wordt dit bewijsmateriaal desgevraagd ter beschikking gesteld van de systeembeveiligingsfunctionaris.

4. In het beveiligingsbeleid wordt voorzien in terugkoppelingsprocessen om te waarborgen dat informatie over de aard, de afhandeling en de gevolgen van een veiligheidsincident wordt meegedeeld aan de systeembeveiligingsfunctionaris en de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur, zodra het incident is afgehandeld en afgesloten.

5. De leden 1 tot en met 4 zijn van overeenkomstige toepassing op incidenten bij het centrale SIS II. De verwijzingen in de leden 1 tot en met 4 naar de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur worden in dat verband gelezen als verwijzingen naar de plaatselijke beveiligingsfunctionaris voor het centrale SIS II.

HOOFDSTUK III

BEVEILIGINGSMAATREGELEN

Artikel 7

Beveiligingsbeleid

1. De directeur-generaal van het directoraat-generaal Justitie, vrijheid en veiligheid stelt overeenkomstig dit besluit een bindend beveiligingsbeleid op, werkt dit bij en evalueert het regelmatig. Het beveiligingsbeleid voorziet in gedetailleerde procedures en maatregelen ter bescherming tegen bedreigingen voor de beschikbaarheid, integriteit en vertrouwelijkheid van de communicatie-infrastructuur, alsmede in noodplannen om het door dit besluit voorgeschreven veiligheidsniveau te waarborgen. Het beveiligingsbeleid is in overeenstemming met dit besluit.

2. Het beveiligingsbeleid wordt gebaseerd op een beoordeling van het risico. De door het beveiligingsbeleid voorgeschreven maatregelen zijn evenredig met de vastgestelde risico's.

3. De risicobeoordeling en het beveiligingsbeleid worden bijgesteld indien technologische veranderingen, vaststelling van nieuwe bedreigingen of andere omstandigheden zulks noodzakelijk maken. Het beveiligingsbeleid wordt in ieder geval jaarlijks opnieuw bekeken om te waarborgen dat het een passende respons kan geven op de meest recente risicobeoordeling en op alle andere geconstateerde technologische veranderingen, bedreigingen of andere relevante omstandigheden.

4. Het beveiligingsbeleid wordt geformuleerd door de systeembeveiligingsfunctionaris, in coördinatie met de plaatselijke beveiligingsfunctionaris voor het centrale SIS II en de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur.

5. De leden 1 tot en met 4 zijn van overeenkomstige toepassing op het beveiligingsbeleid voor het centrale SIS II. De verwijzingen in de leden 1 tot en met 4 naar de plaatselijke beveiligingsfunctionaris voor de communicatie-infrastructuur worden in dat verband gelezen als verwijzingen naar de plaatselijke beveiligingsfunctionaris voor het centrale SIS II.

Artikel 8

Tenuitvoerlegging van de beveiligingsmaatregelen

1. De tenuitvoerlegging van de taken en vereisten die bij dit besluit en in het beveiligingsbeleid zijn vastgesteld, met inbegrip van de aanwijzing van een plaatselijke beveiligingsfunctionaris, mag worden uitbesteed of toevertrouwd aan particuliere of openbare instanties.

2. Indien dat het geval is, waarborgt de Commissie door middel van een juridisch bindende overeenkomst dat volledig wordt beantwoord aan de vereisten die in dit besluit en in het beveiligingsbeleid zijn vastgelegd. Indien de aanwijzing van een plaatselijke beveiligingsfunctionaris wordt gedelegeerd of uitbesteed, waarborgt de Commissie door middel van een juridisch bindende overeenkomst dat zij wordt geraadpleegd over de persoon die als plaatselijk beveiligingsfunctionaris zal worden aangewezen.

Artikel 9

Controle op de toegang tot de faciliteiten

1. Ter bescherming van gebieden waar zich faciliteiten voor gegevensverwerking bevinden, worden veiligheidszones ingesteld met passende fysieke barrières en toegangscontroles.

2. Binnen de veiligheidszones worden veilige gebieden aangewezen ter bescherming van de fysieke componenten, met inbegrip van hardware, gegevensdragers en werkstations, plannen en andere documenten betreffende SIS II, alsmede kantoren en andere arbeidsplaatsen van het personeel dat bij de werkzaamheden van SIS II betrokken is. Deze veilige gebieden worden beveiligd met passende toegangscontroles om te waarborgen dat slechts bevoegd personeel toegang heeft. Werkzaamheden binnen de veilige gebieden zijn onderworpen aan de gedetailleerde beveiligingsvoorschriften die onderdeel zijn van het beveiligingsbeleid.

3. Kantoren, andere vertrekken en faciliteiten worden fysiek beveiligd. Toegangspunten, zoals los- en laadplaatsen en andere plaatsen waarlangs onbevoegden het terrein kunnen betreden, moeten onder toezicht staan en zo mogelijk worden geïsoleerd van de gegevensverwerkingsfaciliteiten, teneinde ongeoorloofde toegang te voorkomen.

4. De veiligheidsbarrières worden, op een wijze die evenredig is met het risico, beschermd tegen schade door natuurrampen en door de mens veroorzaakte rampen.

5. Alle uitrusting wordt beschermd tegen fysieke bedreigingen en milieurisico's en tegen de mogelijkheid van ongeoorloofde toegang.

6. De Commissie voegt aan de lijst bedoeld in artikel 2, lid 3, onder f), een centraal contactpunt toe voor het toezicht op de tenuitvoerlegging van dit artikel op het terrein waar het vervangende systeem van CS-SIS is gehuisvest.

Artikel 10

Controle van fysieke componenten en gegevensdragers

1. Verwijderbare gegevensdragers waarop gegevens zijn opgenomen, worden beschermd tegen ongeoorloofde toegang, misbruik of gegevensverminking; tijdens de gehele levensduur van de gegevens wordt de leesbaarheid van de gegevens gegarandeerd.

2. Gegevensdragers worden, wanneer zij niet langer benodigd zijn, veilig verwijderd overeenkomstig de in het beveiligingsbeleid opgenomen gedetailleerde procedures.

3. Door middel van inventarisatie wordt gewaarborgd dat informatie over de opslaglocatie, de toepasselijke bewaartermijn en de toegangsbevoegdheden beschikbaar is.

4. Alle belangrijke componenten van de communicatie-infrastructuur worden geïdentificeerd, zodat zij overeenkomstig hun belang kunnen worden beschermd. Van relevante IT-uitrusting wordt een geactualiseerd register bijgehouden.

5. Inzake de communicatie-infrastructuur is geactualiseerde documentatie beschikbaar. Deze documentatie wordt tegen ongeoorloofde toegang beveiligd.

6. De leden 1 tot en met 5 zijn van overeenkomstige toepassing op het centrale SIS II. Verwijzingen naar de communicatie-infrastructuur worden in dat verband gelezen als verwijzingen naar het centrale SIS II.

Artikel 11

Controle van opslag

1. Er worden passende maatregelen genomen om de correcte opslag van gegevens te waarborgen en ongeoorloofde toegang tot die informatie te voorkomen.

2. Alle uitrustingonderdelen die gegevensdragers bevatten, worden gecontroleerd om te waarborgen dat gevoelige gegevens voor de verwijdering van de drager zijn gewist of volledig overschreven, of worden veilig vernietigd.

Artikel 12

Wachtwoordcontrole

1. Alle wachtwoorden worden veilig bewaard en als vertrouwelijk behandeld. Wanneer het vermoeden bestaat dat een wachtwoord bekend is geraakt, wordt het wachtwoord onmiddellijk gewijzigd of het betrokken account gedeactiveerd. Alle gebruikersidentiteiten zijn uniek en individueel.

2. Ter voorkoming van ongeoorloofde toegang worden in het beveiligingsbeleid procedures voor aanmelding en afmelding opgenomen.

Artikel 13

Toegangscontrole

1. Het beveiligingsbeleid voorziet in een formele procedure voor de inschrijving en uitschrijving van personeel, waarmee de toegangsrechten voor de apparatuur en programmatuur van SIS II kunnen worden toegekend en ingetrokken met het oog op het operationele beheer. De toewijzing en het gebruik van passende toegangscodes (wachtwoorden en andere geschikte middelen) wordt gecontroleerd door middel van een formeel beheersproces, dat in het beveiligingsbeleid wordt vastgelegd.

2. De toegang tot de apparatuur en de programmatuur van SIS II op de locatie van CS-SIS:

i) wordt beperkt tot bevoegde personen;

ii) wordt slechts toegestaan indien een legitiem doel als bedoeld in artikel 45 van Verordening (EG) nr. 1987/2006 en artikel 61 van Besluit 2007/533/JBZ of artikel 50, lid 2, van Verordening (EG) nr. 1987/2006 en artikel 66, lid 2, van Besluit 2007/533/JBZ kan worden vastgesteld;

iii) mag niet langer duren en niet meer omvatten dan voor het doel van de toegang vereist is, en

iv) mag slechts plaatsvinden in overeenstemming met een in het veiligheidbeleid vast te leggen toegangscontrolebeleid.

3. In CS-SIS worden slechts werkstations en programmatuur gebruikt die door de plaatselijke beveiligingsfunctionaris voor het centrale SIS II zijn toegestaan. Het gebruik van systeemhulpprogramma's waarmee de systeem- en toepassingscontroles kunnen worden omzeild, wordt beperkt en gecontroleerd. Er worden procedures ingesteld om de installatie van programmatuur te controleren.

Artikel 14

Communicatiecontrole

De communicatie-infrastructuur staat onder controle teneinde de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie-uitwisseling te waarborgen. Ter bescherming van de gegevens die via de communicatie-infrastructuur worden doorgegeven, wordt gebruikgemaakt van versleuteling.

Artikel 15

Inputcontrole

Op de accounts van personen die toegangsbevoegdheid hebben tot de SIS II-programmatuur vanuit CS-SIS wordt toezicht uitgeoefend door de plaatselijke beveiligingsfunctionaris voor het centrale SIS II. Het gebruik van deze accounts, met inbegrip van de tijdsduur en de identiteit van de gebruiker, wordt geregistreerd.

Artikel 16

Controle op doorgifte en vervoer

1. In het beveiligingsbeleid worden passende maatregelen opgenomen om te voorkomen dat persoonsgegevens tijdens de doorgifte van of naar SIS II of tijdens het vervoer van gegevensdragers ongeoorloofd worden gelezen, gekopieerd, gewijzigd of gewist. In het beveiligingsbeleid worden bepalingen opgenomen betreffende de toegestane wijzen van verzending of vervoer en de procedures voor de verantwoording van het vervoer van voorwerpen en de aankomst op de plaats van bestemming. Gegevensdragers mogen naast de te verzenden gegevens geen andere gegevens bevatten.

2. Door derden verleende diensten die de toegang tot of de verwerking of verzending van gegevens of het beheer van gegevensverwerkingsfaciliteiten, dan wel aanvullende producten of diensten voor gegevensverwerkingsfaciliteiten omvatten, zijn voorzien van passende geïntegreerde veiligheidscontroles.

Artikel 17

Beveiliging van de communicatie-infrastructuur

1. De communicatie-infrastructuur wordt op passende wijze beheerd en gecontroleerd om deze te beschermen tegen bedreigingen en de veiligheid te waarborgen van de communicatie-infrastructuur zelf en van het centrale SIS II, met inbegrip van de via deze systemen uitgewisselde gegevens.

2. De beveiligingskenmerken, het dienstverleningsniveau en de beheersvereisten worden voor alle netwerkdiensten vastgelegd in de netwerkdienstenovereenkomst met de dienstverlener.

3. Niet alleen de toegangspunten tot SIS II, maar ook alle aanvullende door de communicatie-infrastructuur gebruikte diensten worden beschermd. Hiertoe worden passende maatregelen vastgelegd in het beveiligingsbeleid.

Artikel 18

Monitoring

1. Informatie betreffende alle toegang tot CS-SIS en betreffende alle uitwisseling van persoonsgegevens binnen CS-SIS, zoals bedoeld in artikel 18, lid 1, van Verordening (EG) nr. 1987/2006 en artikel 18, lid 1, van Besluit 2007/533/JBZ, wordt geregistreerd en veilig opgeslagen op de locaties van het hoofdsysteem en het vervangende systeem van CS-SIS en toegankelijk gemaakt vanaf die locaties, gedurende de periode bedoeld in artikel 18, lid 3, van Verordening (EG) nr. 1987/2006 en artikel 18, lid 3, van Besluit 2007/533/JBZ.

2. In het beveiligingsbeleid worden procedures opgenomen voor het toezicht op het gebruik van de gegevensverwerkingsfaciliteiten en voor het opsporen van fouten in die faciliteiten; de resultaten van deze toezicht- en opsporingsactiviteiten worden regelmatig getoetst. Indien nodig worden passende maatregelen getroffen.

3. De faciliteiten voor de registratie en de registratiebestanden worden beschermd tegen ongeoorloofde wijziging en ongeoorloofde toegang, teneinde te voldoen aan de eisen inzake verzameling en bewaring van bewijsmateriaal gedurende de voorgeschreven periode.

Artikel 19

Versleuteling

Waar nodig wordt ter bescherming van informatie versleuteling toegepast. De toepassing daarvan, alsmede het doel en de voorwaarden, worden door de systeembeveiligingsfunctionaris van tevoren goedgekeurd.

HOOFDSTUK IV

BEVEILIGING VAN PERSONEEL

Artikel 20

Personeelsprofielen

1. In het beveiligingsbeleid worden de taken en verantwoordelijkheden vastgelegd van de personen die toegang hebben tot het centrale SIS II.

2. In het beveiligingsbeleid worden de taken en verantwoordelijkheden vastgelegd van de personen die toegang hebben tot de communicatie-infrastructuur.

3. De beveiligingstaken en -verantwoordelijkheden van Commissiepersoneel, contractanten en personeel dat bij het operationele beheer is betrokken, worden vastgesteld en gedocumenteerd en aan de betrokkenen meegedeeld. Voor personeel van de Commissie worden deze taken en verantwoordelijkheden in de functieomschrijving en de doelstellingen opgenomen; voor contractanten in het contract of de overeenkomst inzake het dienstverleningsniveau.

4. Met alle personen op wie geen overheidsdienstvoorschriften van de Europese Unie of een lidstaat van toepassing zijn, wordt een vertrouwelijkheids- en geheimhoudingsovereenkomst gesloten. Personeel dat met SIS II-gegevens moet werken, dient te beschikken over de noodzakelijke veiligheidsmachtiging of -certificatie overeenkomstig de in het beveiligingsbeleid opgenomen gedetailleerde procedures.

Artikel 21

Informatie van personeel

1. Alle personeelsleden en contractanten krijgen een passende opleiding op het gebied van beveiligingsbewustzijn, juridische vereisten, beleid en procedures, voor zover noodzakelijk voor de uitvoering van hun taken.

2. In het beveiligingsbeleid wordt vastgelegd welke plichten bij beëindiging van het dienstverband of het contract rusten op personeelsleden en contractanten wat verandering van werkzaamheden of beëindiging van de arbeidsrelatie betreft, en welke procedures gelden voor de teruggave van apparatuur en de intrekking van toegangsbevoegdheden.

HOOFDSTUK V

SLOTBEPALING

Artikel 22

Toepasselijkheid

1. Dit besluit is van toepassing met ingang van de datum die door de Raad wordt vastgesteld overeenkomstig artikel 55, lid 2, van Verordening (EG) nr. 1987/2006 en artikel 71, lid 2, van Besluit 2007/533/JBZ.

2. Artikel 1, lid 1, artikel 2, lid 1, artikel 2, lid 3, onder b), d), f) en i), artikel 3, artikel 6, lid 5, artikel 7, lid 5), artikel 9, lid 6), artikel 10, lid 6, artikel 13, leden 2 en 3, artikel 15, artikel 18 en artikel 20, lid 1, komen te vervallen wanneer de beheersautoriteit met haar werkzaamheden begint.

Gedaan te Brussel, 4 mei 2010.

Voor de Commissie

De voorzitter

José Manuel BARROSO