COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag **BEZOEKADRES** Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 **FAX** 070 - 88 88 501 **INTERNET** www.cbpweb.nl

College bescherming persoonsgegevens

Onderzoek beveiliging SIS II bij de Nederlandse Politie

Z2015-00126

OPENBARE VERSIE
Rapport definitieve bevindingen

DATUM

INHOUDOPGAVE

Samenvatting en Conclusies

Het verdrag van Schengen regelt het vrije verkeer van personen tussen 26 deelnemende landen in Europa. Tussen deze landen zijn de controles aan de binnengrenzen verdwenen, waardoor burgers vrij kunnen reizen.
Voor controle van inkomend en uitgaand personen- (en -goederenverkeer) in het Schengengebied is tussen de Schengenlidstaten het Schengen informatiesysteem (hierna: SIS II) ingericht.

Het SIS II heeft tot doel met behulp van SIS II te zorgen voor een hoog niveau van veiligheid in een ruimte van vrijheid, veiligheid en recht in de Europese Unie (…).
Personen uit niet tot het Schengengebied behorende landen die naar het Schengengebied reizen dienen om toegelaten te worden tot het Schengengebied een visum aan te vragen. Onderdeel van de visumaanvraag betreft de controle op signalering in het SIS II. Een van de voorwaarden is dat de aanvrager niet staat gesignaleerd ter fine van weigering van toegang in het SIS en/of in het nationaal register.

In het kader van de toezichthoudende taak heeft het CBP een ambtshalve onderzoek verricht conform artikel 60 Wet bescherming persoonsgegevens (hierna: Wbp), artikel 44 van 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) (hierna: de Verordening) en artikel 60 van het 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) (hierna: het Besluit).
Het onderzoek is gericht op het controleren of de beveiligingsvoorschriften voor het N.SIS II (nationale deel van het Schengen informatiesysteem) bij de verantwoordelijke autoriteit - de Nationale Politie – (hierna: de NP) conform artikel 10 van de Verordening en artikel 10 van het Besluit worden uitgevoerd en of de overige relevante bepalingen uit de Verordening en het Besluit in acht worden genomen.

De volgende vragen staan centraal in het onderzoek:

1) Heeft de Nationale Politie zijn verplichting om passende maatregelen te treffen ten aanzien van de beveiliging van N.SIS II, zoals een beveiligingsplan en controles op diverse onderdelen, op juiste wijze ingevuld.

2) Worden de bevragingen op het N.SIS II alleen door daartoe bevoegden - geautoriseerde medewerkers - uitgevoerd.

Op 1 juli 2015 heeft het CBP het rapport voorlopige bevindingen aan de NP gezonden. Op 22 juli 2015 heeft de NP een schriftelijke reactie gegeven op deze bevindingen. Op 25 augustus 2015 heeft de NP een aanvullende schriftelijke reactie gegeven op deze bevindingen. Het CBP heeft de reactie van de NP beoordeeld. Deze beoordeling is opgenomen in de bijlage.

Op grond van de bevindingen van het onderzoek komt het CBP daarbij tot de volgende conclusies.

- *Ten aanzien van een beveiligingsplan*
  De NP heeft geen beveiligingsplan vastgesteld met betrekking tot N.SIS II. Hierdoor overtreedt de NP artikel 10 lid 1 van het Besluit en handelt zij niet in overeenstemming met de NEN-norm.
- *Ten aanzien van toegangsrechten tot N.SIS II en personeelsprofielen*
  Niet alle partijen die toegangsrechten hebben tot N.SIS II staan in de autorisatiematrix en bij de in de matrix genoemde partijen worden niet alle typen van toegangsrechten vermeld. Nu de NP deze toegangsrechten niet juist heeft geregeld, handelt zij in strijd met artikel 10 lid onder f van de Verordening, artikel 10 lid 1 onder f van het Besluit en artikel 4 lid 3 van de Wpg.
  De NP heeft geen personeelsprofielen aan het CBP overgelegd. Het CBP neemt derhalve aan dat de NP deze profielen niet heeft opgesteld. De NP handelt hierdoor in strijd met artikel 10 lid 1 onder g van de Verordening en artikel 10 lid onder g van het Besluit.
- *Ten aanzien van het toekennen van autorisaties en controle op toegekende autorisaties*
  Met betrekking tot het toekennen van autorisaties heeft de NP geen specifieke schriftelijke procedure vastgelegd ten behoeve van het autoriseren van functioneel beheerders tot N.SIS II en dat is evenmin het geval ten aanzien van de medewerkers van de IND. Hierdoor overtreedt de NP artikel 32 lid 1 onder c van de Wpg en handelt zij niet in overeenstemming met artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.
  Met betrekking tot controle op toegekende autorisaties vinden er bij de NP geen (doorlopende) controles plaats op de aan functioneel beheerders en IND-medewerkers toegekende autorisaties en zijn er geen afspraken gemaakt met de regionale eenheden over de af te

leggen verantwoording. Hierdoor overtreedt de NP artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit.

- *Ten aanzien van beveiligingsincidenten*
  Er is geen snelle doeltreffende en ordelijke respons op een N.SIS II informatiebeveiligingsincident, neergelegd in een N.SIS II-procedure. De NP handelt hierdoor niet in overeenstemming met de NEN-norm en overtreedt hiermee artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit.
- *Ten aanzien van controle gebruik N.SIS II-logging*
  De logfiles worden door de NP niet (doorlopend) gecontroleerd en niet alle applicaties worden gelogd. Door het niet loggen van de mutaties in toegangsrechten in N.SIS II is controle op de werkzaamheden van functioneel beheerders en IND-medewerkers niet mogelijk. Hierdoor overtreedt de NP artikel 10 lid 1 onder i en k van de Verordening en artikel 10 lid 1 onder i en k van het Besluit en handelt niet in overeenstemming met de NEN-norm.
- *Ten aanzien van opleiding personeel*
  Het personeel van de NP krijgt geen specifieke en degelijke opleiding met betrekking tot de regels inzake gegevensbeveiliging en -bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. In de algemene opleiding wordt eveneens geen aandacht besteed aan N.SIS II. Hierdoor overtreedt de NP artikel 14 van de Verordening en artikel 14 van het Besluit.

1. Inleiding

1.1. Achtergrond onderzoek

Het verdrag van Schengen regelt het vrije verkeer van personen tussen 26[1] deelnemende landen in Europa. Tussen deze landen zijn de controles aan de binnengrenzen verdwenen, waardoor burgers vrij kunnen reizen.
Met het afschaffen van de controles aan de binnengrenzen tussen de deelnemende landen is er één enkele buitengrens gecreëerd waar de controles bij binnenkomst in de Schengen-ruimte volgens identieke procedures uitgevoerd worden. Ook zijn er gemeenschappelijke voorschriften vastgesteld inzake visa, asielrecht en controle bij de buitengrenzen, zodat het vrije verkeer van personen binnen de Schengen-ruimte niet ten koste gaat van de openbare orde.
Voor controle van inkomend en uitgaand personen- (en -goederenverkeer) in het Schengengebied is tussen de Schengenlidstaten het Schengen informatiesysteem (hierna: SIS II)[2] ingericht.
Het SIS II heeft tot doel met behulp van N.SIS II te zorgen voor een hoog niveau van veiligheid in en ruimte van vrijheid, veiligheid en recht in de Europese Unie (…).[3]
Personen uit niet tot het Schengengebied behorende landen die naar het Schengengebied reizen dienen om toegelaten te worden tot het Schengengebied een visum aan te vragen. Onderdeel van de visumaanvraag betreft de controle op signalering in het SIS II. Een van de voorwaarden is dat de aanvrager niet staat gesignaleerd ter fine van weigering van toegang in het SIS en/of in het nationaal register.[4]
Ook voor verkeer van personen en goederen naar het Schengengebied geldt dat er aan bepaalde voorwaarden moet worden voldaan. Voor het verwerken, waaronder onder meer wordt verstaan het vastleggen, raadplegen en muteren van SIS II-gegevens zijn de Verordening (EG) Nr. 1987/2006[5] (hierna: de Verordening) en het Besluit

---

[1] Van de 26 deelnemende landen zijn er ook vier niet EU-landen (IJsland, Liechtenstein, Noorwegen en Zwitserland). IJsland en Noorwegen zijn geassocieerd lid. De volgende landen nemen niet deel: Bulgarije, Kroatië, Cyprus, Ierland, Roemenië en het Verenigd Koninkrijk.
[2] Het SIS II bevat informatie over personen (mogelijke betrokkenheid bij een zwaar misdrijf, personen die geen toegang zouden mogen hebben tot het Schengengebied, vermiste personen – met name kinderen-) en over gestolen of verloren goederen (zoals bankbiljetten, voertuigen, vuurwapens en identiteitsbewijzen die gestolen, verloren of verduisterd zijn).
[3] Artikel 1 van de Verordening en artikel 1 van het Besluit.
[4] Verordening (EG) Nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (VIS-verordening).
[5] 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).

2007/533/JBZ[6] (hierna: het Besluit) van toepassing. Deze verordening is met ingang van 9 april 2013 van toepassing op de lidstaten die deelnemen aan SIS I +.[7]
Lidstaten zijn verplicht de in de Verordening en het Besluit opgenomen bepalingen toe te passen.[8] Hierop dient periodiek zowel door de verantwoordelijke autoriteit de NP als door de Nationale Toezichthouder in Nederland het College Bescherming Persoonsgegevens (hierna: het CBP) gecontroleerd te worden.
Voorts zijn de nationale bepalingen die zijn neergelegd in het wettelijke kader onder 1.3 van toepassing.[9]
Dit onderzoeksrapport betreft het door het CBP uitgevoerde onderzoek bij de Nationale Politie.

1.2. Doel, reikwijdte en uitvoering van het onderzoek

Het CBP is toezichthouder op het Nederlandse deel van het Schengen Informatiesysteem, dit betreft het N.SIS II-informatiesysteem. In het kader van de toezichthoudende taak heeft het CBP een ambtshalve onderzoek verricht conform artikel 60 Wet bescherming persoonsgegevens (hierna: Wbp), artikel 44 van de Verordening en artikel 60 van het Besluit.[10]
Het onderzoek is gericht op het controleren of de beveiligingsvoorschriften voor het N.SIS II (nationale deel van het Schengen informatiesysteem) bij de verantwoordelijke autoriteit - de Nationale Politie - conform artikel 10 van de Verordening en artikel 10 van het Besluit worden uitgevoerd en of de overige van toepassing zijnde bepalingen uit de Verordening en het Besluit in acht worden genomen. Uit deze artikelen blijkt dat de lidstaat voor N. SIS II passende beveiligingsmaatregelen dient te treffen.
Op grond van artikel 7 lid 1 van de Verordening en artikel 7 lid 1 van het Besluit is in Nederland de NP aangewezen als autoriteit die de centrale verantwoordelijkheid heeft voor N.SIS II. De NP is verantwoordelijk voor de goede werking en beveiliging van N.SIS II. Daarnaast is de NP ook op grond van artikel 27 Verordening en artikel 27 van het Besluit een van de autoriteiten met toegangsrecht tot signaleringen en staan zij als zodanig opgenomen in de in artikel 27 lid 4 van de Verordening genoemde lijst.

De volgende vragen staan centraal in het onderzoek.

1) Heeft de Nationale Politie zijn verplichting om passende maatregelen te treffen ten aanzien van de beveiliging van N.SIS II, zoals een beveiligingsplan en controles op diverse onderdelen, op juiste wijze ingevuld.

---

[6] Van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II).
[7] Besluit van de Raad van 7 maart 2013 tot vaststelling van de datum van toepassing van Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II), artikel 1.
[8] Verordening (EU) Nr. 1053/2013 van 7 oktober 2013.
[9] Wet bescherming persoonsgegevens, hoofdstuk 9 Toezicht, paragraaf 1, artikelen 51-61.
[10] In de Verordening en het Besluit is bepaald dat nationale controleautoriteiten zelfstandig waken over de rechtmatigheid van de verwerking van SIS II-persoonsgegevens op hun grondgebied (…).

2) Worden de bevragingen op het N.SIS II alleen door daartoe bevoegden - geautoriseerde medewerkers - uitgevoerd.

Bij brief van 20 februari 2015 heeft het CBP bij de NP het onderzoek aangekondigd en de relevante schriftelijke stukken opgevraagd waaronder het beveiligingsplan N.SIS II, alsmede de rapportage van de laatst uitgevoerde interne controle op het N.SIS II, de procedures die worden gehanteerd bij het toekennen, wijzigen en beëindigen van autorisaties tot het N.SIS II en een overzicht van de toegekende autorisaties die van toepassing zijn voor de toegang tot SIS II-gegevens in de periode van 1 januari 2015 tot en met 15 februari 2015.
De NP heeft bij brief van 23 maart 2015 geantwoord en een aantal bescheiden aan het CBP verstrekt. Naar aanleiding hiervan heeft het CBP bij brief van 2 april 2015 nadere informatie opgevraagd. Hierop is bij brief van 9 april 2015 door de NP gereageerd.
Op 11 mei 2015 heeft een onderzoek ter plaatse bij de Dienst ICT van de NP plaatsgevonden, waarbij het CBP interviews heeft gehouden met diverse medewerkers van de NP en kennis heeft genomen van de werking van N.SIS II. Daarnaast heeft het CBP ter plaatse de relevante documentatie opgevraagd. Een groot deel van de documentatie heeft de NP op 12, 20 en 26 mei 2015 ten kantore van het CBP overgelegd.
De logbestanden zijn op 26 mei 2015 door een medewerker van de Dienst ICT ten kantore van het CBP afgegeven.
Het CBP heeft op 30 juni 2015 het rapport voorlopige bevindingen vastgesteld.
Het CBP heeft op 22 juli 2015 de schriftelijke reactie (hierna: zienswijze) van de NP ontvangen op het rapport voorlopige bevindingen. Naar aanleiding van deze reactie heeft het CBP aan de NP gevraagd haar standpunt nader te onderbouwen en hiertoe alle relevante informatie te verstrekken. De NP heeft gereageerd door middel van haar brief van 22 augustus 2015.

1.3. Wettelijk kader

De Europese regelgeving betreffende SIS II is vastgelegd in de Verordening en het Besluit.
Ten aanzien van het verwerken van SIS II-gegevens voor handhavingsdoeleinden – als bedoeld in het Besluit – zijn de Wet politiegegevens (hierna: Wpg) en het Besluit politiegegevens (hierna: Bpg) van toepassing. Ten aanzien van het verwerken van SIS II-gegevens voor signaleringsdoeleinden – als bedoeld in de Verordening – is de Wbp van toepassing.
De bevindingen van dit onderzoek zijn getoetst aan het volgende wettelijke kader.

- Artikelen 4, derde lid, 6 en 32 Wet politiegegevens
- Artikelen 13, 33 en 34 Wet bescherming persoonsgegevens
- Artikelen 7, 10, 13, 31 en 44, tweede lid, van 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)
- Artikelen 7, 10, 13, 46 en 60, tweede lid, van het Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende instelling, werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II).

2. Organisatie Nationale Politie

Vanaf 1 januari 2013 vormt de politie één korps. Eén korpschef heeft de leiding over deze organisatie die bestaat uit tien regionale eenheden, de Landelijke Eenheid voor regio/overschrijdend en specialistisch politiewerk en het Politiedienstencentrum voor ondersteunende taken.
Onderdeel van het Politiedienstencentrum is onder meer de dienst ICT. Deze dienst focust zich op het brede terrein van ICT-diensten, waaronder het aansturen van 7 rekencentra en het realiseren van een landelijk gestandaardiseerde ICT-structuur voor de politie.
De dienst ICT is verantwoordelijk voor het beheer en onderhoud van het N.SIS II systeem.

3. Definitieve bevindingen onderzoek

3.1.Beveiligingsplan

3.1.1 Norm

In artikel 13 van de Verordening en artikel 13 van het Besluit is bepaald dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van deze verordening en dit besluit (…). Uit deze artikelen blijkt dat de NP – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

In artikel 10 lid 1 van de Verordening is bepaald dat elke lidstaat passende maatregelen neemt, waaronder de vaststelling van een veiligheidsplan en in artikel 10 lid 1 van het Besluit is bepaald dat elke lidstaat voor zijn N.SIS II–systeem passende maatregelen neemt waaronder de vaststelling van een beveiligingsplan.

3.1.2 Definitieve bevindingen

Er bestaat geen specifiek beveiligingsplan met betrekking tot N.SIS II. De NP beschikt over een generiek Informatiebeveiligingsbeleid en een document met betrekking tot informatiebeveiliging. Het verstrekte en meeste recente informatiebeveiligingsbeleid van oktober 2013 betreft een definitieve versie.
De in het informatiebeveiligingsbeleid geformuleerde doelstellingen voor informatiebeveiliging zijn nader uitgewerkt in twee documenten. In deze documenten wordt verwezen naar de veranderde aanpak van Informatiebeveiliging bij de NP. De NP is van een baseline denken (informatiebeveiliging inrichten vanuit maatregelen) overgegaan naar een generieke invulling van de Informatiebeveiliging gebaseerd op actuele inschatting van risico's in de werkprocessen waarin de informatie en informatiesystemen worden toegepast. Volgens de NP is "*tot op heden uit dergelijke analyses geen aanleiding naar voren gekomen om de beveiliging van N.SIS II anders te behandelen dan de generieke aanpak voorschrijft*".
Door de meer generieke op risico's gebaseerde aanpak bevindt de NP zich volgens de CISO[11] thans in een transitie.

[11] Chief Information Security Officer.

De laatst risicoanalyse is uitgevoerd op het N.SIS I systeem. In 2013 is een zelf-assessment op N.SIS II uitgevoerd.
Noch in het informatiebeveiligingsbeleid, noch in het document met betrekking tot informatiebeveiliging wordt specifiek ingegaan op te realiseren doelen en de te treffen maatregelen voor het N.SIS II-systeem. Alhoewel de beide documenten componenten bevatten die betrekking hebben op te nemen beveiligingsmaatregelen die ook N.SIS II zouden kunnen raken, kan niet gesproken worden van een beveiligingsplan dat specifiek betrekking heeft op N.SIS II, omdat de documenten met betrekking tot informatie beleidsbeleid en informatiebeveiliging algemene doelen en maatregelen bevatten.
Er is voorts een document in de vorm van een aantal 'sheets' verstrekt. Het document bevat onder meer de belangrijkste te behalen speerpunten voor de CISO in 2015. De status van dit document wordt niet vermeld.
Ten slotte wordt opgemerkt dat uit het informatiebeveiligingsbeleidsstuk van de NP, blijkt dat de NP de uitvoering van haar jaarplan dient te bewaken door middel van het opstellen van voortgangsrapportages. Desgevraagd is door de CISO verklaard dat er geen voortgangsrapportages beschikbaar zijn maar thans een format voor de voortgangsrapportage wordt ontwikkeld.

3.1.3 Beoordeling

In artikel 13 van het Besluit is neergelegd dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van het Besluit. In artikel 10 lid 1 van het Besluit is bepaald dat de lidstaat - in casu de NP - een beveiligingsplan dient vast te stellen.

De NP heeft een aantal documenten overgelegd.

Het document met betrekking tot Informatiebeveiligingsbeleid en het document met betrekking tot informatiebeveiliging bevatten slechts componenten die betrekking hebben op te nemen beveiligingsmaatregelen die ook N.SIS II zouden kunnen raken. Het document dat in de vorm van een aantal sheets is verstrekt, bevat slechts de belangrijkste te behalen speerpunten voor de CISO in 2015. Niet gesproken kan echter worden van een beveiligingsplan dat specifiek betrekking heeft op N.SIS II, omdat de beide stukken algemene doelen en maatregelen bevatten en de sheets slechts de te behalen speerpunten voor de CISO in 2015. Hierdoor zijn deze plannen niet aan te merken als een beveiligingsplan in de zin van artikel 10 van het Besluit. Nu de NP geen specifiek beveiligingsplan heeft vastgesteld met betrekking tot N.SIS II overtreedt zij artikel 10 lid 1 van het Besluit.
Ten slotte wordt opgemerkt dat de NP geen voortgangsrapportages aan het CBP beschikbaar heeft gesteld, en dat zij heeft verklaard dat hier thans een format voor wordt ontwikkeld. Nu bij de NP voortgangsrapportages ontbreken handelt zij in strijd met haar eigen beleid. In het beleidsstuk van de NP wordt immers vermeld dat de NP de uitvoering van haar jaarplan dient te bewaken door middel van het opstellen van voortgangsrapportages.

3.2. *Toegangsrechten tot N.SIS II en Personeelsprofielen*

3.2.1 Norm

In artikel 13 van de Verordening en artikel 13 van het Besluit is bepaald dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van deze verordening en dit besluit (…). Uit deze artikelen blijkt dat de NP – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

Uit artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit volgt dat medewerkers van de NP die bevoegd zijn een systeem voor automatische gegevensverwerking te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend middels persoonlijke en unieke gebruikersidentiteiten en geheime toegangsprocedures. Deze artikelen zijn nader uitgewerkt in de Wet politiegegevens (hierna: Wpg).

Artikel 4 lid 3 van de Wpg legt aan de NP eveneens de verplichting op om passende technische en organisatorische maatregelen ten uitvoer te leggen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via direct geautomatiseerde toegang omvat, en tegen alle andere vormen van onrechtmatige verwerking, waarbij met name rekening wordt gehouden met de risico's van de verwerking en de aard van de te beschermen gegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's van de verwerking en de aard van de politiegegevens.

Op grond van artikel 10 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit dient de NP profielen op te stellen waarin de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om gegevens in te zien, in te voeren, bij te werken, te wissen en te doorzoeken (…).

3.2.2 Definitieve bevindingen

<u>Toegangsrechten tot N.SIS II</u>
De hieronder beschreven bevindingen baseert het CBP op van de NP ontvangen documenten en tijdens het onderzoek ter plaatse ontvangen informatie tijdens de interviews.
Het CBP heeft de NP schriftelijk, bij brief van 20 februari 2015 verzocht een overzicht van toegekende autorisaties (gerangschikt per instantie met toegangsrecht tot SIS II-gegevens) die van toepassing zijn voor toegang tot SIS II-gegevens over de periode van 1 januari 2015 tot en met 15 februari 2015. Het CBP heeft van de NP een autorisatiematrix ontvangen met de verschillende rollen (*actoren*) die aan de medewerkers van de verschillende op N.SIS II aangesloten partijen kunnen worden toegekend. Per partij worden de rollen vermeld en aan elke rol zijn toegangsrechten gekoppeld.

De autorisatielijst bevat de namen en de toegangsrechten van alle tot N.SIS-II geautoriseerde medewerkers op alfabetische volgorde. Dit bestand is vergeleken met de autorisatiematrix.
Uit de vergelijking met de autorisatiematrix blijkt dat niet alle toegangsrechten daar in voorkomen en/of niet gekoppeld zijn aan een bepaalde rol. Daarnaast constateert het CBP dat de toegangsrechten aan drie actoren zijn toegekend die niet genoemd zijn in de autorisatiematrix.

Met betrekking tot de IND en SIRENE merkt het CBP op dat op de autorisatielijst medewerkers voorkomen die toegangsrechten hebben die niet gedefinieerd zijn in de overgelegde autorisatiematrix.

Personeelsprofielen
De beheerder van N.SIS II[12] – de NP - heeft geen beschrijving van de profielen met betrekking tot de op N.SIS II aangesloten partijen aan het CBP verstrekt, waarin duidelijk de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om gegevens in te zien, in te voeren, bij te werken, te wissen en te doorzoeken (…) in N.SIS II of de applicaties die daar toegang toe bieden.

3.2.3. Beoordeling

Toegangsrechten tot N.SIS II
De NP dient op grond van de Verordening en het Besluit uitsluitend toegang tot N.SIS II te verlenen aan NP-medewerkers die bevoegd zijn om kennis te nemen van de gegevens van N.SIS II. Daarnaast is de NP ook de centrale verantwoordelijkheid voor N.SIS II en zorgt als zodanig voor de toegang van de bevoegde autoriteiten tot N.SIS II. Op grond van de Wpg dient de NP passende organisatorische maatregelen te nemen om ongeoorloofde toegang tot N.SIS II te voorkomen.
Uit CBP-onderzoek is gebleken dat de autorisatielijst de namen en de toegangsrechten bevat van alle tot N.SIS-II geautoriseerde medewerkers. Dit bestand is vergeleken met de autorisatiematrix. Uit de vergelijking met de autorisatiematrix blijkt dat een aantal toegangsrechten daar niet in voorkomen en/of niet gekoppeld zijn aan een bepaalde rol. Daarnaast constateert het CBP dat de toegangsrechten aan drie actoren zijn toegekend die niet genoemd zijn in de autorisatiematrix. Voorts heeft het CBP met betrekking tot de IND en SIRENE vastgesteld dat op de autorisatielijst medewerkers voorkomen die toegangsrechten hebben die niet gedefinieerd zijn in de overgelegde autorisatiematrix.
Het CBP heeft (kortom) vastgesteld dat niet alle partijen die toegangsrechten hebben tot N.SIS II in de autorisatiematrix staan en dat bij de in de matrix genoemde partijen niet alle typen van toegangsrechten worden vermeld. Nu de NP deze toegangsrechten niet juist heeft geregeld, handelt zij in strijd met artikel 10 lid onder f van de Verordening, artikel 10 lid 1 onder f van het Besluit en artikel 4 lid 3 van de Wpg.

Personeelsprofielen
De NP is een organisatie met toegangsrecht tot N.SIS II. Als beheerder van N.SIS II heeft zij te maken met op N.SIS II aangesloten partijen. De NP dient op grond van de Verordening en het Besluit profielen op te stellen waarin de taken en verantwoordelijkheden worden omschreven van personen (bij de NP en de

[12] Artikel 7 lid 1 van de Verordening en artikel 7 lid 1 van het Besluit.

aangesloten partijen) die bevoegd zijn om gegevens in N.SIS II te zien, in te voeren, bij te werken, te wissen en te doorzoeken. Het CBP heeft aan de NP gevraagd deze profielen te overleggen. De NP heeft dit nagelaten. Nu de NP niet de voren vermelde profielen aan het CBP heeft overgelegd, neemt het CBP aan dat de NP deze profielen niet heeft opgesteld. De NP handelt hierdoor in strijd met artikel 10 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit.

3.3. Toekennen van autorisatie en controle op toegekende autorisaties

3.3.1 Norm

In artikel 13 van de Verordening en artikel 13 van het Besluit is bepaald dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van deze verordening en dit besluit (…). Uit deze artikelen blijkt dat de NP – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

In artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit is bepaald dat degenen die bevoegd zijn een systeem van automatische gegevensverwerking te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft (…).
De NP dient op grond van artikel 13 Wbp en artikel 4 lid 3 van de Wpg een passend beveiligingsniveau te garanderen.
Met betrekking tot autorisaties is in artikel 6 van de Wpg opgenomen dat de NP een systeem van autorisaties onderhoudt dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. In dit artikel is eveneens bepaald dat politiegegevens slechts worden verwerkt door ambtenaren van politie die daartoe door de NP zijn geautoriseerd en voor zover de autorisatie strekt. In artikel 32 lid 1 onder c van de Wpg is bepaald dat de NP zorg draagt voor de schriftelijke vastlegging van de toekenning van de autorisaties.
De toekenning van autorisaties wordt nader uitgewerkt in de NEN-ISO-IEC 27002:2013 (hierna: de NEN-norm). In de NEN-norm worden de internationaal geldende maatregelen voor informatiebeveiliging nader uitgewerkt. De NEN-norm is de Praktijkrichtlijn op het gebied van informatiebeveiliging. De NEN-norm schrijft voor dat toegangsbeveiliging in toegangsbeleid dient te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.[13] Hierin behoort onder meer te zijn voorzien in eisen van formele autorisatie van toegangsverzoeken.[14] Ten behoeve van het beheer van toegangsrechten van gebruikers dienen formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld.[15]
Verder is in artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit bepaald dat de nodige maatregelen worden genomen om ervoor te zorgen dat de voorschriften van de Verordening en het Besluit worden nageleefd. Er dient doorlopend te worden gecontroleerd op het naleven van de beveiligingsmaatregelen. Controle kunnen uitoefenen op toegekende autorisaties impliceert dat deze

[13] NEN-ISO-IEC 27002:2013, 9.1.1, p. 30.
[14] NEN-ISO-IEC 27002:2013, 9.1.2, p. 31.
[15] NEN-ISO-IEC 27002:2013, 9.2.1, p. 32.

toekenningen door de NP vastgelegd moeten zijn. Zonder deze vastlegging kan deze controle immers niet plaatsvinden. Vervolgens dient als gevolg van die controle vastgesteld te kunnen worden of het feitelijk aantal geautoriseerde medewerkers overeenkomt met de vastlegging bij de NP. In de NEN norm is neergelegd dat overbodige gebruikersidentificaties, periodiek moeten worden gecontroleerd (identificeren) en verwijderd.[16]

3.3.2 Definitieve bevindingen

Het CBP heeft bij de NP onderzocht of het proces van toekenning van autorisaties zodanig is ingevuld dat dit voldoende waarborgen biedt om ongeoorloofde toegang tot SIS II gegevens te voorkomen.

Toekennen van autorisaties
De NP heeft toegelicht dat zij in de praktijk alleen verantwoordelijk is voor het toekennen, wijzigen en verwijderen van autorisaties voor de functioneel beheerders van de op N.SIS II aangesloten partijen. Het feitelijk autoriseren van medewerkers bij de aangesloten partijen, valt niet onder de verantwoordelijkheid van de NP. Hier zijn de aangesloten partijen zelf verantwoordelijk voor. Uitzondering hierop vormt de IND, de NP voert wel functioneel beheerstaken voor de medewerkers van de IND uit. De NP heeft geen formeel vastgestelde en gedocumenteerde procedure met betrekking tot de werkwijze toekenning autorisaties voor de functioneel beheerders van de aangesloten partijen[17] aan het CBP overgelegd. Wel heeft de NP een autorisatiemodel voor de NP aan het CBP verstrekt. Deze notitie bevat de uitgangspunten voor de inrichting van autorisaties voor alle gegevensverwerkingen binnen de NP. De status van dit document blijkt niet uit het document.
Voor de feitelijke uitvoering van de autorisatie voor de functioneel beheerders van de aangesloten partijen is de functioneel beheerder van de dienst ICT verantwoordelijk. Voor het autoriseren van medewerkers van de IND, waarvoor de dienst ICT van de NP voor de feitelijke toekenning, wijziging of verwijdering van autorisaties tot N.SIS II verantwoordelijk is, beschikt de NP niet over formeel vastgelegde procedures.

Controle op toegekende autorisaties
Bij de beheerder van N.SIS II - de NP - vinden geen (periodieke) controles plaats op de aan functioneel beheerders van de aangesloten partijen toegekende autorisaties. Op de toegekende autorisaties aan IND-medewerkers vindt eveneens geen (periodieke) controle plaats. De beheerder van N.SIS II heeft voorts geen afspraken gemaakt met de aangesloten partijen ten aanzien van af te leggen verantwoording over intern uitgevoerde controles op het aantal geautoriseerde medewerkers en de hieraan gekoppelde rollen binnen de aangesloten partij.

3.3.3 Beoordeling

Toekennen van autorisaties
Uit de Verordening en het Besluit blijkt dat de NP uitsluitend degenen die bevoegd zijn toegangsrechten N.SIS II kan verlenen en uit de Wpg blijkt dat de NP voor de schriftelijke vastlegging van de toekenning van autorisaties dient zorg te dragen.

[16] NEN-ISO-IEC 27002:2013, 9.2.1, p. 32.
[17] Zie voor de deelnemers: Official Journal C208 of the European Union, volume 58, 24 june 2015.

Daarnaast is de NP ook de centrale verantwoordelijkheid voor N.SIS II en zorgt als zodanig voor de toegang van de bevoegde autoriteiten tot N.SIS II. De NP heeft een autorisatiemodel aan het CBP overgelegd. Deze notitie bevat slechts de uitgangspunten voor de inrichting van autorisaties voor alle gegevensverwerkingen binnen de NP en is dus niet toegespitst op N.SIS II. De NP heeft geen formeel vastgestelde en gedocumenteerde procedure met betrekking tot de werkwijze toekenning autorisaties voor de functioneel beheerders van de aangesloten partijen voor N.SIS II aan het CBP overgelegd. Voor het autoriseren van medewerkers van de IND voor N.SIS II beschikt de NP evenmin over formeel vastgelegde procedures. Het CBP stelt daarmee vast dat van de schriftelijke vastlegging van de procedure ten behoeve van N.SIS II bij de NP en de IND geen sprake is. Nu de NP geen specifieke schriftelijke procedure heeft vastgelegd ten behoeve van het autoriseren van functioneel beheerders tot N.SIS II en dit evenmin het geval is ten aanzien van de medewerkers van de IND handelt zij niet in overeenstemming met de NEN-norm en overtreedt zij hierdoor artikel 32 lid 1 onder c van de Wpg. Voorts handelt de NP niet in overeenstemming met artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.

Controle op toegekende autorisaties

Uit de Verordening en het Besluit blijkt dat de NP de in de Verordening en het Besluit neergelegde beveiligingsmaatregelen met betrekking tot N.SIS II doorlopend dient te controleren. Uit de bevindingen blijkt dat er bij de beheerder van N.SIS II - de NP - geen (periodieke) controles plaatsvinden op de aan de functioneel beheerders van de aangesloten partijen toegekende autorisaties. Op de toegekende autorisaties aan IND-medewerkers vindt eveneens geen (periodieke) controle plaats. Voorts blijkt dat er geen afspraken zijn vastgelegd tussen de Landelijke Eenheid en de regionale eenheden voor de verantwoording over de regionaal toegekende autorisaties. De NP is eindverantwoordelijk voor alle op N.SIS II toegekende autorisaties. Bij deze verantwoordelijkheid hoort ook dat de NP controle uitoefent op de decentraal toegekende autorisaties. Indien de NP niet zelf deze controles uitoefent zouden er afspraken met betrekking tot de door regionale eenheden af te leggen verantwoording gemaakt moeten worden, zodat kan worden vastgesteld dat alleen daar bevoegde medewerkers toegang tot SIS II-gegevens hebben.
Nu er geen (doorlopende) controles plaatsvinden op de aan functioneel beheerders en IND-medewerkers toegekende autorisaties en er geen afspraken zijn gemaakt met de regionale eenheden over de af te leggen verantwoording, overtreedt de NP artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit.

3.4. Beveiligingsincidenten

3.4.1. Norm

In artikel 13 van de Verordening en artikel 13 van het Besluit is bepaald dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van deze verordening en dit besluit (…). Uit deze artikelen blijkt dat de NP – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

In artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit is bepaald dat onbevoegde gegevensopslag in het geheugen, alsmede onbevoegde kennisneming, wijziging of verwijdering van opgeslagen persoonsgegevens dient te worden voorkomen. Indien een medewerker van de NP bijvoorbeeld onbevoegd heeft kennisgenomen van opgeslagen persoonsgegevens, dan is er sprake van een informatiebeveiligingsincident. In artikel 3 lid 2 onder f van de Regeling informatiebeveiliging politie is opgenomen dat in een beleidsdocument bij de NP behoort te worden neergelegd de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door politieambtenaren worden gemeld, de politieambtenaar bij wie deze inbreuken worden gemeld en de wijze waarop deze worden afgehandeld. In de NEN-norm wordt aangegeven dat een consistente en doeltreffende aanpak dient te worden bewerkstelligd van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. Hiertoe dienen procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.[18]

3.4.2. Definitieve bevindingen

In het document met betrekking tot informatiebeveiligingsbeleid is opgenomen dat NP deskundigen er op toezien dat informatiebeveiligingsincidenten zo spoedig mogelijk correct afgehandeld worden en dat zij streven naar het identificeren en oplossen van weeffouten op organisatieniveau in het mechanisme van informatiebeveiliging.
In het document met betrekking tot informatiebeveiliging is opgenomen dat de CISO toeziet op de werking van incidentenprocedures in de bestaande structuren en zorgt voor de beschrijving van procedures voor de dienst ICT overstijgende incidenten, alsmede de CISO regelmatig de werking van de incidentenafhandeling evalueert, analyseert en regie voert richting de korpsleiding rondom high impact incidenten en dat de CISO de bestuurlijke coördinatie van de dienst ICT overstijgende incidenten verzorgt. Desgevraagd is verklaard dat voor informatiebeveiligingsincidenten de CISO[19] eindverantwoordelijk is voor de afhandeling van informatiebeveiligingsincidenten. Bij sommige incidenten wordt samengewerkt met andere afdelingen binnen de NP. Dit betreft veelal integriteitsincidenten en fraudeonderzoeken.
De NP beschikt niet over procedures voor het beheer van informatiebeveiligingsincidenten met betrekking tot N.SIS II. Het CBP heeft op 12 mei 2015 een document betreffende de afhandeling van beveiligingsincidenten van de NP ontvangen. Dit document betreft sheets van een op 9 maart 2015 gehouden presentatie. In deze presentatie is een sheet opgenomen met een stroomschema voor de sturing en informatievoorziening in geval van incidenten. Voorts is een sheet opgenomen met incidenten (drempelwaarden) waarbij de CISO altijd moet worden geïnformeerd.
Desgevraagd is op 12 mei 2015 door de CISO verklaard dat er voor kleine technische incidenten/problemen op de servers bij de Dienst ICT een incidentenregister wordt bijgehouden en dat er geen beveiligingsincidenten (zoals virusbesmettingen) zijn geweest op de systemen die gebruikt worden om bevragingen op te doen. Voorts is

[18] NEN-ISO-IEC 27002:2013,16.1.1, p. 86.
[19] CISO: Chief Information Security Officer.

verklaard dat incidenten in samenwerking met andere afdelingen binnen de NP worden onderzocht en afgehandeld. Dit betreffen interne fraude en integriteitsonderzoeken.
Alleen "grote" informatiebeveiligingsincidenten worden opgeschaald naar de CISO. Er zouden zich in 2014-2015 geen informatiebeveiligingsincidenten hebben voorgedaan die direct of indirect de internationale informatiesystemen (waaronder N.SIS II) hebben geraakt. Er zijn derhalve volgens de CISO geen informatiebeveiligingsincidenten in het incidentenregister opgenomen.

3.4.3. Beoordeling

Uit artikel 3 lid 2 van de Regeling Informatiebeveiliging politie blijkt dat de NP in een beleidsdocument neer moet leggen op welke wijze informatiebeveiligingsincidenten door politieambtenaren moeten worden gemeld en uit de NEN-norm blijkt dat de NP procedures moet vaststellen om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. Het CBP heeft beoordeeld of het document informatiebeveiligingsbeleid en de sheets van de op 9 mei 2015 gehouden presentatie voldoen aan de voren vermelde eisen. Uit deze documenten blijkt onder andere dat bij de NP deskundigen erop moeten toezien dat informatiebeveiligingsincidenten zo spoedig mogelijk correct worden afgehandeld. Uit deze documenten is niet gebleken dat de NP een op N.SIS II toegesneden procedure heeft ten aanzien van het beheer van informatiebeveiligingsincidenten. Voorts merkt het CBP op dat de door de NP uitgevoerde onderzoeken geen onderzoeken naar informatiebeveiligingsincidenten betreffen maar interne fraude- en -integriteitsonderzoeken.
Van een snelle, doeltreffende en ordelijke respons op een N.SIS II beveiligingsincident, neergelegd in een N.SIS II-procedure, is derhalve geen sprake. Hierdoor handelt de NP niet in overeenstemming met de NEN-norm en overtreedt zij hiermee artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit.

3.5. Controle gebruik N.SIS II : logging

3.5.1. Norm

In artikel 13 van de Verordening en artikel 13 van het Besluit is bepaald dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van deze verordening en dit besluit (…). Uit deze artikelen blijkt dat de NP – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

In artikel 10 lid 1 onder i van de Verordening en artikel 10 lid onder i van het Besluit is bepaald dat de NP naderhand moet kunnen nagaan en vaststellen welke persoonsgegevens door wie en voor welk doel in een geautomatiseerd gegevensverwerkingssysteem zijn opgenomen. Uit de NEN-norm blijkt dat logbestanden worden gemaakt van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, en dat deze worden bewaard en regelmatig worden beoordeeld.[20]

[20] NEN-ISO-IEC 27002:2013, 12.4.1, p. 58.

In artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit is bepaald dat de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen doorlopend worden gecontroleerd en met betrekking tot deze interne controle de nodige organisatorische maatregelen worden genomen om ervoor te zorgen dat de voorschriften van deze verordening worden nageleefd.

3.5.2. Definitieve bevindingen

Op 26 mei 2015 is van de beheerder van N.SIS II - de NP - een logbestand ontvangen. Desgevraagd is op 12 mei 2015 verklaard dat mutaties in autorisaties niet worden gelogd. Logfiles worden alleen gecontroleerd in geval van veiligheidssignalen, integriteitsonderzoeken, klachten of een technische verstoring. Deze controles worden door andere afdelingen van de NP of in samenwerking hiermee uitgevoerd.
De CISO van de NP heeft verklaard dat logfiles niet doorlopend worden gecontroleerd. In de brief van 9 april 2015 heeft de NP voorts verklaard dat het niet mogelijk is om op eenvoudige wijze de mutaties van de autorisaties inzichtelijk te maken en dat dit in de applicaties niet wordt gelogd. Theoretisch is het mogelijk, zij het met forse inspanning, om twee back-up's met elkaar te vergelijken en daaruit handmatig de wijzigingen af te leiden.

3.5.3. Beoordeling

De beheerder van N.SIS II - de NP - heeft verklaard dat de logfiles niet voortdurend worden gecontroleerd en wijzigingen en verwijderingen van autorisaties in applicaties (lees ook N.SIS II) niet worden gelogd. Daarnaast is gebleken dat logfiles alleen worden gecontroleerd bij vermoeden van veiligheidssignalen, integriteitsonderzoeken, klachten of een technische verstoring.
Hieruit blijkt dat werkzaamheden door functioneel beheerders ten behoeve van veranderingen in autorisaties tot N.SIS II niet worden gelogd. De logging van het gebruik van N.SIS II is onvolledig omdat niet alle accounts met toegangsrechten tot N.SIS II worden gelogd en controle op toegekende of gewijzigde autorisaties niet kan plaatsvinden. De NP overtreedt hierdoor de artikelen 10 lid 1 onder i en k van de Verordening en artikel 10 lid 1 onder i en k van het Besluit en handelt niet in overeenstemming met de NEN-norm.

3.6. <u>Opleiding personeel</u>

3.6.1. Norm

In artikel 13 van de Verordening en artikel 13 van het Besluit is bepaald dat de lidstaten ervoor zorgen dat elke instantie met toegangsrecht tot SIS II-gegevens de nodige maatregelen treft met het oog op de naleving van deze verordening en dit besluit (…). Uit deze artikelen blijkt dat de NP – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

In artikel 14 van de Verordening en artikel 14 van het Besluit is bepaald dat het personeel van de NP, alvorens toestemming te krijgen om in N.SIS II opgeslagen gegevens te verwerken, een degelijke opleiding krijgt over regels inzake

gegevensbeveiliging en – bescherming en dat het op de hoogte wordt gebracht van ter zake doende strafbare feiten en sancties.

3.6.2. Definitieve bevindingen

Het CBP heef aan de NP gevraagd of personeel met toegangsrecht tot N.SIS II een degelijke opleiding krijgt over regels inzake gegevensbeveiliging en –bescherming en of zij op de hoogte worden gebracht van ter zake doende strafbare feiten en sancties. De NP heeft verklaard dat er geen opleiding wordt gegeven die specifiek betrekking heeft op SIS II en ook niet op andere wijze.

3.6.3. Beoordeling

Het personeel van de NP krijgt geen specifieke opleiding met betrekking tot de regels inzake gegevensbeveiliging en-bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. In de reguliere opleiding(en) van de NP wordt eveneens geen aandacht besteed aan N.SIS II. Van een degelijke opleiding is derhalve geen sprake. Hierdoor handelt de NP in strijd met artikel 14 van de Verordening en artikel 14 van het Besluit.

4. Conclusies

- *Ten aanzien van een beveiligingsplan*
  De NP heeft geen beveiligingsplan vastgesteld met betrekking tot N.SIS II. Hierdoor overtreedt de NP artikel 10 lid 1 van het Besluit en handelt zij niet in overeenstemming met de NEN-norm.
- *Ten aanzien van toegangsrechten tot N.SIS II en personeelsprofielen*
  Niet alle partijen die toegangsrechten hebben tot N.SIS II staan in de autorisatiematrix en bij de in de matrix genoemde partijen worden niet alle typen van toegangsrechten vermeld. Nu de NP deze toegangsrechten niet juist heeft geregeld, handelt zij in strijd met artikel 10 lid onder f van de Verordening, artikel 10 lid 1 onder f van het Besluit en artikel 4 lid 3 van de Wpg.
  De NP heeft geen personeelsprofielen aan het CBP overgelegd. Het CBP neemt derhalve aan dat de NP deze profielen niet heeft opgesteld. De NP handelt hierdoor in strijd met artikel 10 lid 1 onder g van de Verordening en artikel 10 lid onder g van het Besluit.
- *Ten aanzien van het toekennen van autorisaties en controle op toegekende autorisaties*
  Met betrekking tot het toekennen van autorisaties heeft de NP geen specifieke schriftelijke procedure vastgelegd ten behoeve van het autoriseren van functioneel beheerders tot N.SIS II en dat is evenmin het geval ten aanzien van de medewerkers van de IND. Hierdoor overtreedt de NP artikel 32 lid 1 onder c van de Wpg en handelt zij niet in overeenstemming met artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.
  Met betrekking tot controle op toegekende autorisaties vinden er bij de NP geen (doorlopende) controles plaats op de aan functioneel beheerders en IND-medewerkers toegekende autorisaties en zijn er geen afspraken gemaakt met de regionale eenheden over de af te leggen verantwoording. Hierdoor

overtreedt de NP artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit.

- *Ten aanzien van beveiligingsincidenten*
  Er is geen snelle, doeltreffende en ordelijke respons op een N.SIS II informatiebeveiligingsincident en neergelegd in een N.SIS II-procedure. De NP handelt hierdoor niet in overeenstemming met de NEN-norm en overtreedt hiermee artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit.
- *Ten aanzien van controle gebruik N.SIS II-logging*
  De logfiles worden door de NP niet (doorlopend) gecontroleerd en niet alle applicaties worden gelogd. Door het niet loggen van de mutaties in toegangsrechten in N.SIS II is controle op de werkzaamheden van functioneel beheerders en IND-medewerkers niet mogelijk. Hierdoor overtreedt de NP artikel 10 lid 1 onder i en k van de Verordening en artikel 10 lid 1 onder i en k van het Besluit en handelt niet in overeenstemming met de NEN-norm.
- *Ten aanzien van opleiding personeel*
  Het personeel van de NP krijgt geen specifieke en degelijke opleiding met betrekking tot de regels inzake gegevensbeveiliging en -bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. In de algemene opleiding wordt eveneens geen aandacht besteed aan N.SIS II. Hierdoor overtreedt de NP artikel 14 van de Verordening en artikel 14 van het Besluit.

Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Collegelid