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 www.mijnprivacy.nl

College bescherming persoonsgegevens

Onderzoek beveiliging SIS II bij de Koninklijke Marechaussee (buitengrenspost Schiphol)

z2015-00211

Rapport definitieve bevindingen

(OPENBARE VERSIE)

DATUM 20 november 2015

INHOUDSOPGAVE

SAMENVATTING

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.

SIS II heeft tot doel met behulp van dit systeem 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 is 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 CBP onderzoek richt zich op het gebruik van N.SIS II door de Koninklijke Marechaussee (KMar), district Schiphol, ten behoeve van de grensbewaking van Nederland en het Schengengebied. In het kader van dit onderzoek heeft het CBP de naleving gecontroleerd van de beveiligingsvoorschriften met betrekking tot N.SIS II door de verantwoordelijke autoriteit - de Koninklijke Marechaussee -, district Schiphol. Het CBP heeft tevens de naleving gecontroleerd van de wettelijke vereisten met betrekking tot de opleiding van KMar medewerkers op het gebied van N.SIS II, en de informatieplicht tegenover binnenkomende vreemdelingen.

De volgende vragen staan centraal in het onderzoek:

1. Op welke wijze worden de vereisten met betrekking tot toegang tot N.SIS II (bijvoorbeeld toekennen, wijzigen, verwijderen van autorisaties en controle hiervan) nageleefd?
   a. Worden de bevragingen in N.SIS II alleen door daartoe bevoegden (geautoriseerde medewerkers) uitgevoerd?
   b. Op welke wijze worden de raadplegingen gecontroleerd en wordt er een register bijgehouden van ICT beveiligingsincidenten?
2. Heeft het personeel met toegangsrecht tot N.SIS II een degelijke opleiding gekregen over regels, inzake gegevens beveiliging en bescherming en is het op de hoogte gebracht van ter zake doende strafbare feiten en sancties?

3. Op welke wijze wordt invulling gegeven aan de informatieplicht tegenover binnenkomende vreemdelingen?

Op 21 juli 2015 heeft het CBP het rapport voorlopige bevindingen aan de KMar gezonden. Op 20 augustus 2015 heeft de KMar een schriftelijke reactie gegeven op deze bevindingen. Het CBP heeft de reactie van de KMar beoordeeld. Deze beoordeling is opgenomen in de Bijlage.

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

- *Ten aanzien van toegangsrechten tot N.SIS II en personeelsprofielen*
  De KMar heeft (nog) geen autorisatiematrix opgesteld die specifiek betrekking heeft op N.SIS II. Hierdoor handelt zij in strijd met de NEN-norm en overtreedt de artikelen 4 lid 3 van de Wpg en artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.
  De KMar heeft geen personeelsprofielen opgesteld. Hierdoor overtreedt zij de artikelen 10 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit en handelt zij in strijd met de NEN-norm.
- *Ten aanzien van het toekennen en controleren van autorisaties tot N.SIS II*
  Met betrekking tot het toekennen van autorisaties heeft de KMar geen autorisatieprocedure opgesteld. Hierdoor handelt zij in strijd met de NEN-norm en voldoet het autorisatiesysteem van de KMar niet aan de vereisten van zorgvuldigheid. De KMar heeft onvoldoende gewaarborgd dat uitsluitend KMar-medewerkers die bevoegd zijn om N.SIS II te gebruiken, toegang hebben tot dit systeem. Hierdoor overtreedt de KMar artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit, artikel 13 van de Wbp en de artikelen 4 lid 3 en 6 van de Wpg.
  Met betrekking tot het controleren van autorisaties tot N.SIS II voert de KMar geen doorlopende controles uit ten aanzien van toegekende N.SIS II-autorisaties en heeft zij hiertoe geen procedure opgesteld. Hierdoor overtreedt de KMar artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit en handelt zij in strijd met de NEN-norm.
- *Ten aanzien van een beveiligingsplan met betrekking tot N.SIS II*
  Bij de KMar ontbreekt een beveiligingsplan met betrekking tot N.SIS II. Hierdoor overtreedt de KMar artikel 10 lid 1 van het Besluit. Er is evenmin sprake van het door de KMar (voldoende) ten uitvoer leggen van organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking als bepaald in artikel 13 van de Wbp. Hierdoor overtreedt de KMar eveneens artikel 13 van de Wbp.
- *Ten aanzien van controle gebruik N.SIS II*
  De KMar controleert niet (doorlopend) op het gebruik van N.SIS II. Hierdoor overtreedt zij 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 zij niet in overeenstemming met de NEN-norm.
- *Ten aanzien van beveiligingsincidenten*
  Het CBP heeft niet kunnen vaststellen of (doorlopende) controle op door de KMar verwerkte persoonsgegevens met betrekking tot N.SIS II (op de juiste wijze) plaatsvindt, nu de KMar geen volledig overzicht van

beveiligingsincidenten over het jaar 2014 met betrekking tot N.SIS II aan het CBP heeft overgelegd. De KMar overtreedt hierdoor artikel 10 lid 1 onder d en k van de Verordening en artikel 10 lid 1 onder d en k van het Besluit.

- *Ten aanzien van opleiding van KMar-medewerkers op het gebied van N.SIS II*
  Het personeel van de KMar krijgt geen degelijke opleiding met betrekking tot de regels inzake gegevensbeveiliging en -bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. Hierdoor overtreedt de KMar artikel 14 van de Verordening en artikel 14 van het Besluit.
- *Ten aanzien van informatieplicht tegenover binnenkomende vreemdelingen*
  De KMar informeert personen van derde landen die Nederland binnenkomen en personen van derde landen die Nederland verlaten niet vooraf over de controle die zij in N.SIS II uitvoert en de rechten die deze personen hebben. Hierdoor overtreedt de KMar de artikelen 33 en 34 van de Wbp.

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 [2] 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 (…).[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 is gesignaleerd ter fine van weigering van toegang in het SIS en/of in het nationaal register.[4]
Ook voor verkeer van personen en goederen vanuit het Schengengebied geldt dat er aan bepaalde voorwaarden moet worden voldaan. Voor het verwerken van SIS II-gegevens zijn de Verordening (EG) Nr. 1987/2006[5] en het Besluit 2007/533/JBZ[6] van toepassing. Deze Verordening is met ingang van 9 april 2013 van toepassing op de lidstaten die deelnemen aan SIS I+.[7]
In 2013 is Verordening (EU) (Nr. 1053/2013 van 7 oktober 2013) van kracht geworden.

---

[1] Van de 26 deelnemende landen zijn er ook vier niet EU-landen (IJsland, Liechtenstein, Noorwegen en Zwitserland).
[2] Het SIS II bevat informatie over personen (mogelijke betrokkenheid bij een zwaar misdrijf, personen die geen toegang zouden mogen hebben tot de EU, 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).
[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.

Uit deze verordening blijkt dat lidstaten verplicht zijn de in de Verordening en het Besluit opgenomen bepalingen toe te passen en dat hierop periodiek, zowel door de verantwoordelijke autoriteit, in casu de Koninklijke Marechaussee als door de nationale toezichthouder, het College Bescherming Persoonsgegevens (hierna: het CBP) gecontroleerd dient te worden.
Voorts zijn de nationale bepalingen die zijn neergelegd in het wettelijke kader van toepassing.[8]

Dit onderzoeksrapport betreft de definitieve bevindingen van het door het CBP uitgevoerde onderzoek bij de Koninklijke Marechaussee, district Schiphol.

1.2 Doel, reikwijdte en uitvoering onderzoek

Het CBP is toezichthouder op het Nederlandse (nationale) deel van SIS II (hierna N.SIS II). 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.

Het CBP onderzoek richt zich op het gebruik van N.SIS II door de Koninklijke Marechaussee, district Schiphol ten behoeve van de grensbewaking van Nederland en het Schengengebied. In het kader van dit onderzoek heeft het CBP de naleving gecontroleerd van de beveiligingsvoorschriften met betrekking tot N.SIS II door de verantwoordelijke autoriteit - de Koninklijke Marechaussee -, district Schiphol. Het CBP heeft tevens de naleving gecontroleerd van de wettelijke vereisten met betrekking tot de opleiding van KMar medewerkers op het gebied van N.SIS II, en de informatieplicht tegenover binnenkomende vreemdelingen.

De volgende vragen staan centraal in het onderzoek:

1. Op welke wijze worden de vereisten met betrekking tot toegang tot N.SIS II (bijvoorbeeld toekennen, wijzigen, verwijderen van autorisaties en controle hiervan) nageleefd?
   a. Worden de bevragingen in N.SIS II alleen door daartoe bevoegden (geautoriseerde medewerkers) uitgevoerd?
   b. Op welke wijze worden de raadplegingen gecontroleerd en wordt er een register bijgehouden van ICT beveiligingsincidenten?
2. Heeft het personeel met toegangsrecht tot N.SIS II een degelijke opleiding gekregen over regels, inzake gegevens beveiliging en bescherming en is het op de hoogte gebracht van ter zake doende strafbare feiten en sancties?
3. Op welke wijze wordt invulling gegeven aan de informatieplicht tegenover binnenkomende vreemdelingen?

Bij brief van 30 maart 2015 heeft het CBP bij de KMar, district Schiphol het onderzoek aangekondigd en de relevante schriftelijke stukken opgevraagd (o.a. het beveiligingsplan N.SIS II, autorisatieprocedures, een overzicht van geautoriseerde medewerkers).
De KMar heeft bij brief van 22 april 2015 geantwoord en een korte toelichting gegeven op de gestelde vragen. Op 13 mei 2015 heeft het CBP het onderzoek ter plaatse

[8] Wet bescherming persoonsgegevens, hoofdstuk 9 Toezicht, paragraaf 1, artikelen 51-61.

schriftelijk aangekondigd. Op 19 en 26 mei 2015 heeft het CBP onderzoeken ter plaatse bij de KMar uitgevoerd en ter plaatse de relevante documentatie opgevraagd. Het CBP heeft op 21 juli 2015 het rapport voorlopige bevindingen vastgesteld.
Op 20 augustus 2015 heeft de Minister van Defensie haar schriftelijke reactie (hierna: zienswijze) op deze bevindingen aan het CBP doen toekomen.

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

- Artikelen 1, 4, derde lid, 6 en 32 Wet politiegegevens[9]
- Artikel 13, 33 en 34 Wet bescherming persoonsgegevens[10]
- Artikelen 7, 10, 13, 31, 42 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 KONINKLIJKE MARECHAUSSEE

De Koninklijke Marechaussee (KMar) is een politiekorps met militaire status. De KMar werkt voor de Nederlandse Staat en haar werk bestaat uit meerdere taken, o.a. militaire politietaak; grenspolitie; bewaken en beveiligen; bijstand openbare orde en veiligheid; recherche; politiewerk Caribisch gebied; politiemissies en ceremoniële taken. De taken en bevoegdheden van de KMar zijn vastgelegd in artikel 4, Politiewet 2012 en artikel 5, Veiligheidswet BES.

Als grenspolitie controleert de KMar het grensverkeer van personen en bestrijdt zij grensoverschrijdende criminaliteit, zowel in Nederland als aan de buitengrenzen van de EU. Op grond van de Verordening en het Besluit heeft de KMar een wettelijke taak

[9] Uit de MvT van de Wpg, nr. 30327, Regels inzake de verwerking van politiegegevens (wet politiegegevens), p. 9 (gepubliceerd op 24 oktober 2005) blijkt dat de Wpg op de KMar van toepassing is. Het betreft - op grond van artikel 6 lid 1 onder c van de Politiewet - de uitvoering van de politietaak door de KMar op de luchthaven Schiphol.
[10] Overweging 15 van de Verordening luidt " Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([10]), is van toepassing op de verwerking van persoonsgegevens overeenkomstig deze verordening." Nu de voren vermelde richtlijn is geïmplementeerd in de Wbp, is deze wet eveneens van toepassing op het verwerken van persoonsgegevens door de KMar.

om controle uit te oefenen op inkomende en uitgaande personen en goederen in het Schengen gebied. De KMar verwerkt sinds 2013 voor dit doel persoonsgegevens en gegevens over goederen die het Schengengebied inkomen of hieruit reizen in N.SIS II, waarin informatie over gesignaleerde personen of goederen zijn opgenomen.

De KMar werkt in vijf districten, waaronder district Schiphol. De KMar, district Schiphol is o.a. verantwoordelijk voor de bewaking van de buitengrenspost Luchthaven Schiphol.

2.1 Verantwoordelijke

De Koninklijke Marechaussee valt onder de verantwoordelijkheid van het Ministerie van Defensie.[11] In het kader van dit onderzoek is de Minister van Defensie de verantwoordelijke in de zin van artikel 1, aanhef en onder d, Wbp en artikel 1, aanhef en onder f, 3e van de Wpg.

3. DEFINITIEVE BEVINDINGEN ONDERZOEK

3.1. Toegangsrechten tot N.SIS II en Personeelsprofielen

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 KMar – 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 medewerkers van de KMar 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 uitgewerkt in onderstaande nationale wet- en regelgeving.

In artikel 13 van de Wet bescherming persoonsgegevens (hierna: Wbp) is bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. 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 die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

[11] Het Ministerie van Defensie bestaat uit 7 organisatiedelen. Een van die delen is de KMar. Dit blijkt uit het organogram van het Ministerie van Defensie, www.defensie.nl/overdefensie/inhoud/organogram

Artikel 4 lid 3 van de Wet politiegegevens (hierna: Wpg) legt aan de KMar 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.

Met betrekking tot autorisaties is in artikel 6 van de Wpg opgenomen dat de KMar 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 KMar zijn geautoriseerd en voor zover de autorisatie strekt.

In de NEN-ISO-IEC 27002:2013 (hierna: 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 wordt algemeen aanvaard en erkend daar waar het beveiliging van informatie betreft. Als een organisatie voldoet aan de NEN-norm, gaat het CBP ervan uit dat ook wordt voldaan aan artikel 4 lid 3 van de Wpg.
Nu er in de Verordening, het Besluit en de Wpg slechts is voorzien in een algemene regeling voor informatiebeveiliging sluit het CBP voor de beoordeling of sprake is van passende technische en organisatorische beveiligingsmaatregelen aan bij de nadere invulling die daaraan wordt gegeven in de NEN-norm. Het onderhouden van een systeem van autorisaties voor toegangsbevoegdheden als onderdeel van het treffen van beveiligingsmaatregelen volgt uit de NEN-norm. De toekenning van autorisaties wordt hierin nader uitgewerkt. Er dienen autorisatieprocedures vastgesteld te worden.[12] Een medewerker van de KMar krijgt alleen toegang tot de informatie die hij nodig heeft voor het uitvoeren van zijn taken. Hierdoor ontstaan er verschillende rollen/toegangsprofielen.[13] Voorts krijgt een medewerker alleen toegang tot de informatie verwerkende faciliteiten (IT-apparatuur, -toepassingen, -procedures, en –ruimten) die hij nodig heeft om zijn taak/functie uit te voeren.[14] Regels voor toegangsbeveiliging behoren te worden ondersteund door formele procedures en gedefinieerde verantwoordelijkheden. Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.[15] Deze procedure omvat onder andere het aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en het onmiddellijk verwijderen of blokkeren van toegangsrechten van gebruikers die de organisatie hebben verlaten.[16]

[12] NEN-ISO-IEC 27002:2013,9.1.2, p. 31.
[13] NEN-ISO-IEC 27002:2013, 9.1.1 overige informatie onder d sub a need to know, p. 31
[14] NEN-ISO-IEC 27002:2013, 9.1.1 overige informatie, onder d, sub b need to use, p. 31.
[15] NEN-ISO-IEC 27002:2013, 9.2.2 gebruikers toegang verlenen, beheersmaatregel, p. 32-33.
[16] NEN-ISO-IEC 27002:2013, 9.2.2 onder e, p. 32-33.

Op grond van artikel 10 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit dient de KMar 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 (…).

Ten slotte 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 toekenningen door de KMar 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 KMar. In de NEN norm is neergelegd dat toegangsrechten van KMar-medewerkers regelmatig dienen te worden beoordeeld en gecontroleerd[17] en dat overbodige gebruikersidentificaties, periodiek moeten worden gecontroleerd en verwijderd. [18] Hiertoe dient de KMar gebruik te maken van een formele procedure.[19]

3.1.2 Definitieve Bevindingen

A. Toegangsrechten en personeelsprofielen

Bij brief van 30 maart 2015 heeft het CBP de KMar schriftelijk verzocht om een actueel overzicht van toegekende autorisaties die van toepassing zijn voor toegang tot N.SIS II. Het CBP heeft van de KMar een autorisatielijst ontvangen met namen van alle geautoriseerde medewerkers, hun functie, inlog en rol. Om zicht te krijgen op concrete toegangsrechten is een vergelijking gemaakt met de autorisatielijst die verkregen is via de Nationale Politie in de hoedanigheid van de beheerder van N.SIS II. Bij e-mailbericht van 6 juli 2015 gaf de KMar toestemming voor het gebruik van deze lijst. Beide autorisatielijsten zijn met elkaar vergeleken.
De Kmar heeft tijdens de interviews aangegeven dat er geen autorisatiematrix beschikbaar is, waarin de relatie tussen verschillende rollen toegekend aan medewerkers en de benodigde toegangsrechten wordt omschreven. De KMar heeft verklaard dat er aan een autorisatiematrix wordt gewerkt.

De KMar heeft geen profielen opgesteld waarin de taken en verantwoordelijkheden worden omschreven van de KMar-medewerkers die bevoegd zijn om – met betrekking tot N.SIS II - gegevens in te zien, op te nemen, bij te werken, te wissen en te doorzoeken.

B. Toekennen en controleren van autorisaties tot N.SIS II

De KMar heeft aangegeven dat de beoordeling van het toekennen, wijzigen en verwijderen van autorisaties van medewerkers van de KMar plaatsvindt op basis van

[17] NEN-ISO-IEC 27002:2013, 9.2.5, p. 35.
[18] NEN-ISO-IEC 27002:2013, 9.2.1, p. 32.
[19] NEN-ISO-IEC 27002:2013, 9.1.1, overige informatie, onder d.

het functieprofiel van de medewerker. De teamleider van de medewerker beoordeelt of de betreffende medewerker de toegang (nog) nodig heeft. Deze teamleider doet het verzoek tot toekenning, wijziging of verwijdering aan de IV-afdeling van het district waartoe de brigade behoort. De KMar heeft verklaard dat deze beoordeling "handmatig" plaatsvindt. De KMar heeft geen autorisatieprocedure met betrekking tot het toekennen, wijzigen en beëindigen van toegang tot N.SIS II.

De KMar heeft tevens aangegeven dat de tot N.SIS II toegekende autorisaties niet worden gecontroleerd. Er is geen procedure opgesteld voor het controleren van de genoemde autorisaties. Toegangsrechten worden automatisch ingetrokken nadat er 30 achter een volgende dagen geen gebruik is gemaakt van het account. De KMar is bezig met het opzetten van steekproeven die betrekking hebben op het controleren van de toegekende autorisaties.

Het CBP heeft de door de KMar overgelegde autorisatielijst gecontroleerd, en vervolgens vragen gesteld over de toegekende autorisaties in bepaalde functies.
Het CBP constateerde dat een P&O-adviseur van de KMar toegangsrechten (via een account) had om mutaties in N.SIS II uit te voeren, terwijl deze autorisatie niet noodzakelijk is voor het uitvoeren van P&O-taken. De overige functies waren geautoriseerd om N.SIS II te bevragen. De KMar heeft op 1 juni 2015 per e-mail verklaard dat "er een check heeft plaatsgevonden, en dat betrokkenen (medewerkers in bepaalde functies) geen functionaliteiten meer binnen het SIS hebben." De toegangsrechten zijn inmiddels ingetrokken.

3.1.3. Beoordeling

A. Toegangsrechten en personeelsprofielen

Desgevraagd heeft de KMar aan het CBP meegedeeld dat er (nog) geen autorisatiematrix, waarin de relatie tussen de rol van een medewerker en de benodigde autorisaties wordt omschreven, door de KMar is opgesteld.
In artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit is bepaald dat medewerkers die bevoegd zijn een systeem voor automatische gegevensverwerking te gebruiken uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft en in artikel 4 lid 3 van de Wpg is bepaald dat ongeoorloofde toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via direct geautomatiseerde toegang omvat, voorkomen dient te worden.
Uit de NEN-norm blijkt dat regels voor toegangsbeveiliging behoren te worden ondersteund door formele procedures en gedefinieerde verantwoordelijkheden. Een medewerker van de KMar krijgt alleen toegang tot de informatie die hij nodig heeft voor het uitvoeren van zijn taken. Hierdoor ontstaan er verschillende rollen/toegangsprofielen.[20] In een autorisatiematrix dient neergelegd te worden welke rollen er gekoppeld zijn aan welke rechten. Aangezien de KMar (nog) geen autorisatiematrix heeft opgesteld, kan het voorkomen, zoals blijkt uit de bevindingen (paragraaf 3.1.2 – Toekennen en controleren van autorisaties tot N.SIS II), dat een

[20] NEN-ISO-IEC 27002:2013, 9.1.1 overige informatie onder d sub a, p. 31.

P&O-medewerker van de KMar toegang heeft tot N.SIS II om mutaties door te voeren, terwijl hij daartoe niet gerechtigd hoort te zijn.
Nu de KMar (nog) geen autorisatiematrix en autorisatieprocedure heeft opgesteld die betrekking hebben op N.SIS II handelt zij in strijd met de NEN-norm en overtreedt hierdoor de artikelen 4 lid 3 van de Wpg en artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.

Op grond van artikel 10 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit dient de KMar profielen op te stellen waarin de taken en verantwoordelijkheden worden omschreven van KMar-medewerkers die bevoegd zijn om – met betrekking tot N.SIS II - gegevens in te zien, in te voeren, bij te werken, te wissen en te doorzoeken (…) en op grond van de NEN-norm krijgt een medewerker van de KMar, op basis van toegangsprofielen, alleen toegang tot de informatie die hij nodig heeft voor het uitvoeren van zijn taken.[21]
De KMar heeft geen profielen opgesteld die aan de voren vermelde criteria voldoen. Hierdoor overtreedt zij de artikelen 10 lid 1 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit en handelt zij in strijd met de NEN-norm.

B. Toekennen en controleren van autorisaties tot N.SIS II

De teamleider bij de de KMar beoordeelt of KMar-medewerkers geautoriseerd mogen worden tot N.SIS II. Deze beoordeling vindt plaats zonder vastgestelde autorisatieprocedure. De KMar heeft geen autorisatieprocedure met betrekking tot het toekennen, wijzigen en beëindigen van toegang tot N.SIS II.

In artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit is bepaald dat uitsluitend KMar-medewerkers die bevoegd zijn om N.SIS II te gebruiken toegang mogen hebben tot dit systeem. In artikel 13 van de Wbp en artikel 4 lid 3 van de Wpg is bepaald dat de KMar voor een passend beveiligingsniveau dient zorg te dragen en in artikel 6 van de Wpg is bepaald dat de KMar een systeem van autorisaties onderhoudt dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Gegevens mogen slechts worden verwerkt door KMar-medewerkers voor zover zij daartoe door de KMar zijn geautoriseerd en voor zover de autorisatie strekt. Uit de NEN-norm blijkt dat de KMar het autoriseren van toegangsverzoeken formeel dient te regelen. Regels voor toegangsbeveiliging behoren te worden ondersteund door formele procedures en gedefinieerde verantwoordelijkheden. Door de KMar behoort een formele gebruikerstoegangsverleningsprocedure te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.[22] Deze procedure omvat onder andere het aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en het onmiddellijk verwijderen of blokkeren van toegangsrechten van gebruikers die de organisatie hebben verlaten.[23]
Nu de KMar geen autorisatieprocedure heeft opgesteld, handelt zij in strijd met de NEN-norm waarin is neergelegd dat er een formele gebruikerstoegangsverleningsprocedure dient te zijn opgesteld. Hierdoor heeft de KMar geen passend beveiligingsniveau en voldoet het autorisatiesysteem van de

[21] NEN-ISO-IEC 27002:2013, 9.1.1 overige informatie onder d sub a need to know, p. 31
[22] NEN-ISO-IEC 27002:2013, 9.2.2 gebruikers toegang verlenen, beheersmaatregel, p. 32-33.
[23] NEN-ISO-IEC 27002:2013, 9.2.2 onder e, p. 32-33.

KMar niet aan de vereisten van zorgvuldigheid. De KMar heeft onvoldoende gewaarborgd dat uitsluitend KMar-medewerkers die bevoegd zijn om N.SIS II te gebruiken, toegang hebben tot dit systeem.[24] Hierdoor overtreedt de KMar artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit, artikel 13 van de Wbp en de artikelen 4 lid 3 en 6 van de Wpg.

Het CBP is nagegaan of de KMar de tot N.SIS II toegekende autorisaties controleert en of zij hiertoe gebruik maakt van een opgestelde procedure. De KMar heeft aangegeven dat de tot N.SIS II toegekende autorisaties niet worden gecontroleerd en dat er geen procedure is opgesteld.
In artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit is bepaald dat de nodige maatregelen worden genomen om ervoor te zorgen dat de voorschriften van de Verordening en het Besluit worden nageleefd. Er dient door de KMar doorlopend te worden gecontroleerd op het naleven van de beveiligingsmaatregelen. In de NEN norm is neergelegd dat de toegangsrechten van KMar-medewerkers regelmatig door de KMar worden beoordeeld en gecontroleerd[25] en dat periodiek moeten worden gecontroleerd op overbodige gebruikersidentificaties en dat deze worden verwijderd.[26] Hiertoe dient de KMar gebruik te maken van een formele procedure.[27]
Nu de KMar geen doorlopende controles uitvoert ten aanzien van toegekende N.SIS II-autorisaties en hiertoe geen procedure heeft opgesteld, overtreedt zij artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit en handelt zij in strijd met de NEN-norm.

3.2. Beveiligingsaspecten N.SIS II

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 KMar – een organisatie met toegangsrecht tot SIS II-gegevens - dient te voldoen aan de in de Verordening en het Besluit vermelde artikelen.

A. Beveiligingsplan

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.
In artikel 13 van de Wbp is bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen

[24] Uit de bevindingen, par. 3.1.2 onder B blijkt immers dat een P & O-adviseur van de KMar ten onrechte toegangsrechten (via een account) had om mutaties in N.SIS II uit te voeren.
[25] NEN-ISO-IEC 27002:2013, 9.2.5, p. 35.
[26] NEN-ISO-IEC 27002:2013, 9.2.1, p. 32.
[27] NEN-ISO-IEC 27002:2013, 9.1.1, overige informatie, onder d.

tegen verlies of tegen enige vorm van onrechtmatige verwerking. 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 die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

B. Controle gebruik N.SIS II

In artikel 10 lid 1 onder i van de Verordening en artikel 10 lid onder i van het Besluit is bepaald dat de KMar 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.[28]

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.

C. Beveiligingsincidenten

In artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit is bepaald dat de KMar passende maatregelen neemt ter voorkoming van onbevoegde gegevensopslag in het geheugen, alsmede onbevoegde kennisneming, wijziging of verwijdering van in N.SIS II opgeslagen persoonsgegevens en artikel 10 lid 1 onder k van het Besluit is bepaald dat er door de KMar (doorlopend) controles moeten plaatsvinden met betrekking tot het naleven van de in lid 1 genoemde beveiligingsmaatregelen. Indien een medewerker van de KMar bijvoorbeeld onbevoegd heeft kennisgenomen van opgeslagen persoonsgegevens, dan is er sprake van een informatiebeveiligingsincident. 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.[29]

[28] NEN-ISO-IEC 27002:2013, 12.4.1, p. 58.
[29] NEN-ISO-IEC 27002:2013,16.1.1, p. 86.

3.2.2 Definitieve Bevindingen

A. Beveiligingsplan

Er is geen beveiligingsplan specifiek gericht op N.SIS II of ander beleidsdocument dat expliciet ingaat op de organisatorische en technische maatregelen die de KMar treft om verwerkte persoonsgegevens te beveiligen.
De KMar heeft twee documenten aan het CBP overgelegd die betrekking hebben op ICT beveiliging. Het eerste document betreft een generieke procedure voor afhandeling van cyberincidenten bij het Ministerie van Defensie. Het tweede stuk is een risicoanalyse ten aanzien van een koppeling tussen twee applicaties. In dit stuk worden de implementatiestatus van de (interne defensie) normen en het risiconiveau beschreven.

B. Controle gebruik N.SIS II

Het gebruik van N.SIS II door de KMar wordt centraal gelogd door de Nationale Politie.[30] Daarnaast vindt bij de KMar een decentrale logging plaats ten aanzien van het biometrisch station.
De centrale logging betreft applicaties die toegang tot N.SIS II bieden. Tijdens het onderzoek ter plaatse op 19 mei 2015 heeft de KMar verklaard dat het gebruik van N.SIS II alleen wordt gecontroleerd in het kader van integriteitsonderzoeken. Deze worden ingesteld naar aanleiding van interne en/of externe signalen over medewerkers. Voorts worden geen doorlopende controles uitgevoerd met betrekking tot het gebruik van N.SIS II door KMar-medewerkers.
Op 29 mei 2015 heeft het CBP een logbestand over het biometrisch station ontvangen (periode 9 t/m 23 februari 2015). Het biometrisch station is een systeem waarmee de KMar bij de grenscontrole vingerafdrukken en gezichtskenmerken kan afnemen voor visumcontrole. Door middel van het biometrisch station wordt tevens een bevraging gedaan in een lokale kopie van de SIS II-database. Het overgelegde bestand bevat de logging van het gebruik van de biometrische stations.
De KMar geeft in het e-mailbericht van 6 juli 2015 aan dat de logging meerdere doelen dient. Hierbij worden de volgende doelen genoemd: "audittrail, management info, systeemcontrole, en controle werking systemen."
Met betrekking tot het gebruik van de lokale kopie van N.SIS II vindt er geen (doorlopende) controle plaats.

C. Beveiligingsincidenten

Tijdens de interviews op 19 en 26 mei 2015 heeft de KMar aangegeven dat beveiligingsincidenten ten aanzien van N.SIS II door de Nationale Politie worden bijgehouden. Bij het Ministerie van Defensie worden alle beveiligingsincidenten door DefCERT[31] geregistreerd. DefCERT houdt een logboek bij voor alle ICT-beveiligingsincidenten en zorgt voor de afhandeling van deze incidenten. De incidenten worden verder niet teruggekoppeld naar de KMar. Het CBP heeft tijdens de twee onderzoeken ter plaatse het overzicht van beveiligingsincidenten N.SIS II met

[30] De Nationale Politie is als beheerder van N.SIS II verantwoordelijk voor het beheer en onderhoud van het systeem.
[31] DefCERT: Defensie Computer Emergency Response Team.

betrekking tot het jaar 2014 opgevraagd. De KMar zou hiervoor zorgdragen. Daarnaast heeft het CBP de KMar op 27 mei 2015 per e-mail verzocht om een "*kopie van het logboek ICT beveiligingsincidenten 2014 die (direct of indirect) betrekking hebben op N.SIS II*" toe te sturen.
Het CBP heeft van de KMar geen overzicht van beveiligingsincidenten over 2014 ontvangen. De KMar heeft twee documenten over beveiligingsincidenten aan het CBP overgelegd. Het eerste document is een procedure voor de afhandeling van cyberincidenten, waarin de werkwijze van afhandeling van cyberincidenten en de taken van alle betrokken partijen worden beschreven. In het tweede document worden o.a. ICT-beveiligingsincidenten vermeld zoals datalekken vastgesteld naar aanleiding van integriteitsonderzoeken. Deze onderzoeken worden, zoals eerder verklaard, ingesteld naar aanleiding van interne en/of externe signalen over medewerkers. In 2014 waren er 12 incidenten geclassificeerd als "*het lekken van informatie uit politiesystemen*" en 3 incidenten van "het raadplegen van gegevens uit nieuwsgierigheid" geclassificeerd als "*wangedrag*".
Bij de in het tweede document vermelde incidenten worden geen systemen of applicaties genoemd waarop deze incidenten betrekking hadden.

3.2.3 Beoordeling

A. Beveiligingsplan

In artikel 10 van het Besluit is bepaald dat de KMar een beveiligingsplan dient vast te stellen en in artikel 13 van de Wbp is neergelegd dat de KMar passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
De KMar heeft desgevraagd twee documenten aan het CBP overgelegd die betrekking hebben op ICT beveiliging. Het eerste document betreft een generieke procedure voor afhandeling van cyberincidenten bij het Ministerie van Defensie en het tweede document een risicoanalyse ten aanzien van een koppeling tussen twee applicaties. In deze documenten wordt niet expliciet ingegaan op de organisatorische en technische maatregelen die de KMar behoort te treffen om verwerkte persoonsgegevens met betrekking tot N.SIS II te beveiligen. Van een beveiligingsplan met betrekking tot dit systeem is derhalve geen sprake.

Nu een beveiligingsplan met betrekking tot N.SIS II ontbreekt, overtreedt de KMar artikel 10 lid 1 van het Besluit. Er is evenmin sprake van het door de KMar (voldoende) ten uitvoer leggen van organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking als bepaald in artikel 13 van de Wbp. Tot deze organisatorische maatregelen behoort immers ook een door de KMar opgesteld beveiligingsplan met betrekking tot N.SIS II. Hierdoor overtreedt de KMar eveneens artikel 13 van de Wbp.

B. Controle gebruik N.SIS II

In artikel 10 lid 1 onder i van de Verordening en artikel 10 lid 1 onder i van het Besluit is bepaald dat de KMar naderhand moet kunnen nagaan en vaststellen welke persoonsgegevens door wie en voor welk doel in N.SIS II zijn opgenomen en uit de NEN-norm blijkt dat logbestanden regelmatig door de KMar moeten worden beoordeeld. In artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k

van het Besluit is bepaald dat (doorlopend) interne controle door de KMar dient plaats te vinden om ervoor te zorgen dat de voorschriften van deze verordening worden nageleefd. Bij de KMar is er geen sprake van (doorlopende) controles ten aanzien van het gebruik van N.SIS II. De KMar heeft immers tijdens het onderzoek ter plaatse op 19 mei 2015 verklaard dat het gebruik van N.SIS II alleen wordt gecontroleerd in het kader van integriteitsonderzoeken en dat er geen (doorlopende) controles worden uitgevoerd met betrekking tot het gebruik van N.SIS II, door middel van de applicaties die KMar-medewerkers gebruiken. Voorts blijkt dat er door middel van het biometrisch station (tevens) een bevraging door de KMar-medewerkers wordt gedaan in een lokale kopie van de SIS II-database en dat er ten aanzien van het gebruik van deze lokale kopie geen (doorlopende) controle door de KMar plaatsvindt. Nu de KMar niet (doorlopend) controleert op het gebruik van N.SIS II overtreedt zij 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 zij niet in overeenstemming met de NEN-norm.

C. Beveiligingsincidenten

In artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit is bepaald dat controle op door de KMar opgeslagen persoonsgegevens met betrekking tot N.SIS II dient plaats te vinden, en uit de NEN-norm blijkt dat een consistente en doeltreffende aanpak dient te worden bewerkstelligd van het beheer van informatiebeveiligingsincidenten, en dat er door de KMar gecommuniceerd moet worden over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
Het CBP heeft aan de KMar gevraagd om overzichten van beveiligingsincidenten met betrekking tot N.SIS II over het jaar 2014 aan haar te leveren. De KMar heeft twee documenten aan het CBP geleverd. Deze documenten geven geen overzicht van alle beveiligingsincidenten met betrekking tot N.SI S II. Het CBP heeft hierdoor niet kunnen vaststellen of controle op door de KMar verwerkte persoonsgegevens met betrekking tot N.SIS II (op de juiste wijze) plaatsvindt. De KMar overtreedt hierdoor artikel 10 lid 1 onder d en k van de Verordening en artikel 10 lid 1 onder d en k van het Besluit.

3.3. Opleiding medewerkers op het gebied van N.SIS II

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 KMar – 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 KMar, 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.

3.3.2. Definitieve Bevindingen

Het CBP heeft op tijdens het onderzoek ter plaatse op 19 mei 2015 aan de KMar 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 geïnterviewde KMar medewerkers hebben verklaard dat het personeel een basisopleiding en training krijgt over de systemen die bij grenscontrole worden toegepast. Het KMar personeel heeft tevens toegang tot een (intranet) informatiesysteem waarin de beschrijving van werkprocessen (o.a. afhandeling signaleringen) en achtergrond informatie staan vermeld. Via intranet kunnen ook wetsartikelen geraadpleegd worden die betrekking hebben op SIS II. Een update van alle relevante wetgeving wordt verzorgd via het Centrum Opleidingen.
Afgesproken is dat de KMar de programma's van de beide opleidingen aan het CBP zou overleggen, samen met *printscreens* van intranet die betrekking hebben op de voor het personeel toegankelijke informatiebronnen ten aanzien van de wettelijke regels SIS II.

Op 29 mei 2015 heeft het CBP een digitale versie van het document over de opleiding ontvangen. Het document bevat een beschrijving van de leerdoelen van de opleiding m.b.t. gebruik van systemen waarin signaleringen voorkomen en afhandeling van verschillende typen signaleringen. In het document staat geen informatie vermeld met betrekking tot gegevensbeveiliging en –bescherming in de context van N.SIS II (of de applicaties die toegang tot N.SIS II bieden). Op 1 juni 2015 heeft het CBP per e-mail *printscreens* van intranet gekregen. Op de overgelegde *printscreens* zijn de wetsartikelen zichtbaar die betrekking hebben op SIS II.

3.3.3. Beoordeling

Het CBP is nagegaan of het personeel van de KMar een degelijke opleiding krijgt met betrekking tot N.SIS II zoals is bepaald in artikel 14 van de Verordening en artikel 14 van het Besluit.
Het CBP heeft van de KMar vernomen dat het KMar-personeel een basisopleiding en training krijgt over de systemen die bij de grenscontrole worden toegepast. Het CBP heeft deze opleiding en training beoordeeld aan de hand van een handleiding. Uit deze handleiding blijkt dat er slechts sprake is van een beschrijving van de leerdoelen van de opleiding met betrekking tot het gebruik van de systemen waarin signaleringen voorkomen en afhandeling van verschillende typen signaleringen. In deze handleiding staat geen informatie vermeld met betrekking tot gegevensbeveiliging en –bescherming in de context van N.SIS II. Hierdoor is er geen sprake van een degelijke opleiding met betrekking tot N.SIS II.
De KMar heeft aangegeven dat het personeel (tevens) toegang heeft tot het intranet. Volgens de KMar worden in dit systeem werkprocessen beschreven, kunnen wetsartikelen met betrekking tot N.SIS II worden geraadpleegd en staat er achtergrondinformatie in vermeld. Het CBP heeft de ontvangen *printscreens* beoordeeld. Uit deze *printscreens* blijkt slechts dat door het KMar-personeel wetsartikelen met betrekking tot SIS II kunnen worden geraadpleegd. Hierdoor is het intranet informatiesysteem evenmin aan te merken als een degelijke N.SIS II-opleiding.

Nu het KMar-personeel geen degelijke opleiding met betrekking tot N.SIS II krijgt overtreedt de KMar artikel 14 van de Verordening en artikel 14 van het Besluit.

3.4. Informatieplicht tegenover binnenkomende vreemdelingen

3.4.1 Norm

In artikel 33 van de Wbp is bepaald dat indien persoonsgegevens worden verkregen bij de betrokkene, de verantwoordelijke de betrokkene vóór het verkrijgen informeert over zijn identiteit en de doeleinden van de verwerking van de gegevens, tenzij de betrokkene daarvan reeds op de hoogte is. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder waar onder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
In artikel 34 van de Wbp is bepaald dat indien persoonsgegevens op een andere wijze worden verkregen dan bedoeld in artikel 33, de verantwoordelijke de betrokkene vóór het verkrijgen informeert over zijn identiteit en de doeleinden van de verwerking van de gegevens, tenzij de betrokkene daarvan reeds op de hoogte is. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

3.4.2 Definitieve Bevindingen

Tijdens het onderzoek ter plaatse op 19 mei 2015 heeft het CBP vragen gesteld over de naleving van de informatieplicht door de KMar met betrekking tot gegevensverwerkingen in N.SIS II. De KMar medewerkers hebben verklaard dat binnenkomende en uitgaande reizigers - onderdanen van derde landen - niet (op een individueel niveau) worden geïnformeerd over controle van hun persoonsgegevens via N.SIS II. Op de luchthaven liggen er regelmatig flyers die informatie over het visum bevatten. De KMar heeft een flyer getiteld *'Informatieblad kort verblijf voor visumvrije vreemdelingen'* aan het CBP overgelegd. De flyer is opgesteld in het Nederlands en bestemd voor '*visumvrije vreemdelingen*'. Hij bevat voornamelijk praktische informatie over toegang tot en verblijf in Nederland. In de flyer staat geen informatie vermeld over controle van persoonsgegevens in N.SIS II en de rechten van de betrokkene.

3.4.3 Beoordeling

Op grond van de artikelen 33 en 34 van de Wbp moeten onderdanen van derde landen (niet EU-onderdanen) die Nederland binnenkomen en onderdanen van derde landen die Nederland verlaten door de KMar worden geïnformeerd over de controle die de KMar uitvoert ten aanzien van hun persoonsgegevens in N.SIS II. Voorts dient de KMar aan te geven welke rechten zij hebben. Het informeren dient plaats te vinden *voordat* de KMar de controle via het informatiesysteem N.SIS II uitvoert.
De KMar heeft aan het CBP een flyer overgelegd getiteld: *'Informatieblad kort verblijf voor visumvrije vreemdelingen'.* Het CBP merkt op dat deze flyer, nu deze in het Nederlands is opgesteld, slechts toegankelijk is voor een beperkte groep. Bovendien

wordt in de flyer in het geheel geen informatie verstrekt over de controle van persoonsgegevens in N.SIS II en welke rechten onderdanen van derde landen hebben. Voorts merkt het CBP op dat de KMar geen informatie heeft overgelegd waaruit blijkt dat onderdanen van derde landen op andere wijze worden geïnformeerd over de controle in N.SIS II en welke rechten zij hebben.
Nu de KMar personen van derde landen die Nederland binnenkomen en personen van derde landen die Nederland verlaten niet vooraf informeert over de controle die zij in N.SIS II uitvoert en de rechten die deze onderdanen hebben, overtreedt de KMar de artikelen 33 en 34 van de Wbp.[32]

4 Conclusies

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

- *Ten aanzien van toegangsrechten tot N.SIS II en personeelsprofielen*
  De KMar heeft (nog) geen autorisatiematrix opgesteld die specifiek betrekking heeft op N.SIS II. Hierdoor handelt zij in strijd met de NEN-norm en overtreedt de artikelen 4 lid 3 van de Wpg en artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.
  De KMar heeft geen personeelsprofielen opgesteld. Hierdoor overtreedt zij de artikelen 10 lid 1 lid 1 onder g van de Verordening en artikel 10 lid 1 onder g van het Besluit en handelt zij in strijd met de NEN-norm.
- *Ten aanzien van het toekennen en controleren van autorisaties t ot N.SIS II*
  Met betrekking tot het toekennen van autorisaties heeft de KMar geen autorisatieprocedure opgesteld. Hierdoor handelt zij in strijd met de NEN-norm en voldoet het autorisatiesysteem van de KMar niet aan de vereisten van zorgvuldigheid. De KMar heeft onvoldoende gewaarborgd dat uitsluitend KMar-medewerkers die bevoegd zijn om N.SIS II te gebruiken, toegang hebben tot dit systeem.[33] Hierdoor overtreedt de KMar artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit, artikel 13 van de Wbp en de artikelen 4 lid 3 en 6 van de Wpg.
  Met betrekking tot het controleren van autorisaties tot N.SIS II voert de KMar geen doorlopende controles uit ten aanzien van toegekende N.SIS II-autorisaties en heeft zij hiertoe geen procedure opgesteld. Hierdoor overtreedt de KMar artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit en handelt zij in strijd met de NEN-norm.
- *Ten aanzien van een beveiligingsplan met betrekking tot N.SIS II*
  Bij de KMar ontbreekt een beveiligingsplan met betrekking tot N.SIS II. Hierdoor overtreedt de KMar artikel 10 lid 1 van het Besluit. Er is evenmin sprake van het door de KMar (voldoende) ten uitvoer leggen van organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies

[32] Ten overvloede merkt het CBP nog op dat het informeren van onderdanen van derde landen eenvoudig kan plaatsvinden door bijvoorbeeld een bord in de ruimte te plaatsen waar de controle plaatsvindt en hierop de informatie te plaatsen. Evident is dat de tekst door de onderdanen van derde landen gelezen moet kunnen worden voordat de controle wordt uitgevoerd.

[33] Uit de bevindingen, par. 3.1.2 onder B blijkt immers dat een P&O-adviseur van de KMar ten onrechte toegangsrechten (via een account) had om mutaties in N.SIS II uit te voeren.

of tegen enige vorm van onrechtmatige verwerking als bepaald in artikel 13 van de Wbp. Hierdoor overtreedt de KMar eveneens artikel 13 van de Wbp.

- *Ten aanzien van controle gebruik N.SIS II*
  De KMar controleert niet (doorlopend) op het gebruik van N.SIS II. Hierdoor overtreedt zij 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 zij niet in overeenstemming met de NEN-norm.
- *Ten aanzien van beveiligingsincidenten*
  Het CBP heeft niet kunnen vaststellen of (doorlopende) controle op door de KMar verwerkte persoonsgegevens met betrekking tot N.SIS II (op de juiste wijze) plaatsvindt, nu de KMar geen volledig overzicht van beveiligingsincidenten over het jaar 2014 met betrekking tot N.SIS II aan het CBP heeft overgelegd. De KMar overtreedt hierdoor artikel 10 lid 1 onder d en k van de Verordening en artikel 10 lid 1 onder d en k van het Besluit.
- *Ten aanzien van opleiding van KMar-medewerkers op het gebied van N.SIS II*
  Het personeel van de KMar krijgt geen degelijke opleiding met betrekking tot de regels inzake gegevensbeveiliging en -bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. Hierdoor overtreedt de KMar artikel 14 van de Verordening en artikel 14 van het Besluit.
- *Ten aanzien van informatieplicht tegenover binnenkomende vreemdelingen*
  De KMar informeert onderdanen van derde landen die Nederland binnenkomen en onderdanen van derde landen die Nederland verlaten niet vooraf over de controle die zij in N.SIS II uitvoert en de rechten die deze onderdanen hebben. Hierdoor overtreedt de KMar de artikelen 33 en 34 van de Wbp.

Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Collegelid

BIJLAGE

In deze bijlage beoordeelt het CBP de schriftelijke reactie van de KMar d.d. 20 augustus 2015 (zienswijze) op het rapport voorlopige bevindingen van het CBP van 21 juli 2015.

Verantwoordelijke

De KMar geeft in haar *zienswijze* aan dat de Minister van Defensie de verantwoordelijke is voor de gegevensverwerking op grond van de Wpg en niet van de Wbp.

Het CBP merkt hierover op dat in het kader van dit onderzoek de Minister van Defensie de verantwoordelijke is in de zin van en artikel 1, aanhef en onder f, 3e van de Wpg en artikel 1, aanhef en onder d, van de Wbp.[34]

Toegangsrechten tot N.SIS II en Personeelsprofielen

Autorisatiematrix

In haar *zienswijze* geeft de KMar aan dat de constateringen van het CBP ten aanzien van het ontbreken van een autorisatiematrix en het daarmee kunnen automatiseren van controle op de toegangsrechten juist zijn. Er wordt gewerkt aan een autorisatiematrix om het proces van toekennen, wijzigen en verwijderen van autorisaties te kunnen automatiseren.

In artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit is bepaald dat medewerkers die bevoegd zijn een systeem voor automatische gegevensverwerking te gebruiken uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft en in artikel 4 lid 3 van de Wpg is bepaald dat ongeoorloofde toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via direct geautomatiseerde toegang omvat, voorkomen dient te worden.
Uit de NEN-norm blijkt dat regels voor toegangsbeveiliging behoren te worden ondersteund door formele procedures en gedefinieerde verantwoordelijkheden. Een medewerker van de KMar krijgt alleen toegang tot de informatie die hij nodig heeft voor het uitvoeren van zijn taken. Hierdoor ontstaan er verschillende rollen/toegangsprofielen.[35] In een autorisatiematrix dient neergelegd te worden welke rollen er gekoppeld zijn aan welke rechten. Aangezien de KMar (nog) geen autorisatiematrix heeft opgesteld, kan het voorkomen, zoals blijkt uit de bevindingen

[34] Overweging 15 van de Verordening luidt " Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([34]), is van toepassing op de verwerking van persoonsgegevens overeenkomstig deze verordening." Nu de voren vermelde richtlijn is geïmplementeerd in de Wbp, is deze wet eveneens van toepassing op het verwerken van persoonsgegevens door de KMar.

[35] NEN-ISO-IEC 27002:2013, 9.1.1 overige informatie onder d sub a, p. 31.

(paragraaf 3.1.2 – Toekennen en controleren van autorisaties tot N.SIS II), dat een P&O-medewerker van de KMar toegang heeft tot N.SIS II om mutaties door te voeren, terwijl hij daartoe niet gerechtigd hoort te zijn.
Het CBP stelt vast dat nu de KMar (nog) geen autorisatiematrix en autorisatieprocedure heeft opgesteld die betrekking hebben op N.SIS II zij in strijd handelt met de NEN-norm. Hierdoor overtreedt de KMar de artikelen 4 lid 3 van de Wpg en artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit.

Toekennen en controleren van autorisaties tot N.SIS II

De KMar geeft in haar *zienswijze* aan dat er een procedure is en dat het een handmatige beoordeling betreft. De teamleider bij de de KMar beoordeelt of KMar-medewerkers geautoriseerd mogen worden tot N.SIS II.

Het CBP heeft aan de KMar gevraagd schriftelijke procedures te overleggen (tijdens de onderzoeken ter plaatse bij de KMar hebben plaatsgevonden). De KMar heeft hieraan met betrekking tot de autorisatieprocedure geen gevolg gegeven. Ook bij de zienswijze ontbreekt deze procedure.
Gelet op het vorenstaande gaat het CBP er vanuit dat de KMar geen autorisatieprocedure heeft met betrekking tot het toekennen, wijzingen en beëindigen van toegang tot N.SIS II.

In artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit is bepaald dat uitsluitend KMar-medewerkers die bevoegd zijn om N.SIS II te gebruiken toegang mogen hebben tot dit systeem. In artikel 13 van de Wbp en artikel 4 lid 3 van de Wpg is bepaald dat de KMar voor een passend beveiligingsniveau dient zorg te dragen en in artikel 6 van de Wpg is bepaald dat de KMar een systeem van autorisaties onderhoudt dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Gegevens mogen slechts worden verwerkt door KMar-medewerkers voor zover zij daartoe door de KMar zijn geautoriseerd en voor zover de autorisatie strekt. Uit de NEN-norm blijkt dat de KMar het autoriseren van toegangsverzoeken formeel dient te regelen. Regels voor toegangsbeveiliging behoren te worden ondersteund door formele procedures en gedefinieerde verantwoordelijkheden. Door de KMar behoort een formele gebruikerstoegangsverleningsprocedure te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.[36] Deze procedure omvat onder andere het aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en het onmiddellijk verwijderen of blokkeren van toegangsrechten van gebruikers die de organisatie hebben verlaten.[37]
Nu de KMar geen autorisatieprocedure heeft opgesteld, handelt zij in strijd met de NEN-norm waarin is neergelegd dat er een formele gebruikerstoegangsverleningsprocedure dient te zijn opgesteld. Hierdoor heeft de KMar geen passend beveiligingsniveau en voldoet het autorisatiesysteem van de KMar niet aan de vereisten van zorgvuldigheid. De KMar heeft onvoldoende gewaarborgd dat uitsluitend KMar-medewerkers die bevoegd zijn om N.SIS II te

[36] NEN-ISO-IEC 27002:2013, 9.2.2 gebruikers toegang verlenen, beheersmaatregel, p. 32-33.
[37] NEN-ISO-IEC 27002:2013, 9.2.2 onder e, p. 32-33.

gebruiken, toegang hebben tot dit systeem.[38] Hierdoor overtreedt de KMar artikel 10 lid 1 onder f van de Verordening en artikel 10 lid 1 onder f van het Besluit, artikel 13 van de Wbp en de artikelen 4 lid 3 en 6 van de Wpg.

Beveiligingsaspecten N.SIS II

Beveiligingsplan

In haar *zienswijze* geeft de KMar aan dat het beheer van N.SIS II in handen is van het nationale Bureau Sirene en is ondergebracht bij de politie. Bureau Sirene draagt zorg voor het beveiligingsplan. De minister van Defensie draagt verantwoordelijkheid voor de beveiliging van haar eigen applicaties die de informatie tot N.SIS II ontsluiten. De KMar heeft daartoe aan het CBP een beveiligingsplan overgelegd.

Het CBP merkt hierover op dat in artikel 10 van het Besluit is bepaald dat de KMar een beveiligingsplan dient vast te stellen en in artikel 13 van de Wbp is neergelegd dat de KMar passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
De KMar geeft in haar zienswijze aan dat zij een beveiligingsplan aan het CBP heeft overgelegd. Zij heeft in het kader van het onderzoek desgevraagd twee documenten aan het CBP overgelegd die betrekking hebben op ICT beveiliging. Het eerste document betreft een generieke procedure voor afhandeling van cyberincidenten bij het Ministerie van Defensie betreft en het tweede document een risicoanalyse ten aanzien van een koppeling tussen twee applicaties die toegang bieden tot SIS II. In deze documenten wordt niet expliciet ingegaan op de organisatorische en technische maatregelen die de KMar behoort te treffen om verwerkte persoonsgegevens met betrekking tot N.SIS II te beveiligen. Van een beveiligingsplan met betrekking tot dit systeem is derhalve geen sprake.
Nu een beveiligingsplan met betrekking tot N.SIS II ontbreekt, overtreedt de KMar artikel 10 lid 1 van het Besluit. Er is evenmin sprake van het door de KMar (voldoende) ten uitvoer leggen van organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking als bepaald in artikel 13 van de Wbp. Tot deze organisatorische maatregelen behoort immers ook een door de KMar opgesteld beveiligingsplan met betrekking tot N.SIS II. Hierdoor overtreedt de KMar eveneens artikel 13 van de Wbp.

Controle gebruik N.SIS II

De KMar geeft in haar *zienswijze* aan dat zij alsnog voor een doorlopende controle op het gebruik van N.SIS II zal zorgdragen.

In artikel 10 lid 1 onder i van de Verordening en artikel 10 lid 1 onder i van het Besluit is bepaald dat de KMar naderhand moet kunnen nagaan en vaststellen welke persoonsgegevens door wie en voor welk doel in N.SIS II zijn opgenomen en uit de NEN-norm blijkt dat logbestanden regelmatig door de KMar moeten worden

[38] Uit de bevindingen, par. 3.1.2 onder B blijkt immers dat een P & O-adviseur van de KMar ten onrechte toegangsrechten (via een account) had om mutaties in N.SIS II uit te voeren.

beoordeeld. In artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit is bepaald dat (doorlopend) interne controle door de KMar dient plaats te vinden om ervoor te zorgen dat de voorschriften van deze verordening worden nageleefd.
Het CBP merkt op dat de KMar niet aangeeft op welke wijze zij alsnog voor een doorlopende controle op het gebruik van N.SIS II zal zorgdragen en met ingang van welke datum. Van het beëindigen van de overtreding is derhalve (nog) geen sprake. Nu de KMar niet (doorlopend) controleert op het gebruik van N.SIS II overtreedt zij 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 zij niet in overeenstemming met de NEN-norm.

Beveiligingsincidenten

De KMar geeft in haar *zienswijze* aan dat beveiligingsincidenten specifiek met betrekking tot N.SIS II niet apart worden geregistreerd.
In artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit is bepaald dat de KMar passende maatregelen neemt ter voorkoming van onbevoegde gegevensopslag in het geheugen, alsmede onbevoegde kennisneming, wijziging of verwijdering van in N.SIS II opgeslagen persoonsgegevens en in artikel 10 lid 1 onder k van de Verordening en artikel 10 lid 1 onder k van het Besluit is bepaald dat er door de KMar (doorlopend) controles moeten plaatsvinden met betrekking tot het naleven van de in lid 1 genoemde beveiligingsmaatregelen. Uit de NEN-norm blijkt dat een consistente en doeltreffende aanpak dient te worden bewerkstelligd van het beheer van informatiebeveiligingsincidenten, en dat er door de KMar gecommuniceerd moet worden over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
Het CBP heeft tijdens de onderzoeken ter plaatse op 19 en 26 mei 2015 aan de KMar gevraagd om overzichten van beveiligingsincidenten met betrekking tot N.SIS II over het jaar 2014 aan haar te leveren. De KMar heeft twee documenten aan het CBP geleverd. Deze documenten geven geen overzicht van alle beveiligingsincidenten met betrekking tot N.SIS II. Het CBP verlangt van de KMar een volledig overzicht van beveiligingsincidenten in het jaar 2014 met betrekking tot N.SIS II. Ook in de zienswijzeprocedure heeft de KMar geen documenten overgelegd waarin alle beveiligingsincidenten met betrekking tot N.SIS II overzichtelijk worden weergegeven. De geconstateerde beveiligingsincidenten waarover de KMar het CBP nader wil informeren, hebben slechts betrekking op integriteitsonderzoeken naar personeelsleden. Het overzicht van beveiligingsincidenten dient ook andere soorten incidenten (bijv. inbreuken door externe factoren) te bevatten.

Het CBP heeft hierdoor niet kunnen vaststellen of controle op door de KMar verwerkte persoonsgegevens met betrekking tot N.SIS II (op de juiste wijze) plaatsvindt. De KMar overtreedt hierdoor artikel 10 lid 1 onder d en k van de Verordening en artikel 10 lid 1 onder d en k van het Besluit.

Opleiding medewerkers op het gebied van N.SIS II

De KMar geeft in haar *zienswijze* aan dat het executieve personeel gegevens verwerkt volgens het regime van de Wpg. Zij krijgen in de opleiding onderwijs in gegevensverwerking en de regels omtrent beveiliging en bescherming zoals omschreven in de Wpg. Voor de operationele medewerkers is deze opleiding, in combinatie met de basisopleiding voldoende om aan de eisen te voldoen van artikel 14 van de Verordening.

Het CBP is nagegaan of het personeel van de KMar een degelijke opleiding krijgt met betrekking tot N.SIS II zoals is bepaald in artikel 14 van de Verordening en artikel 14 van het Besluit.

Het CBP wijst op de beoordeling in het rapport (paragraaf 3.3.3) waarin ook de basisopleiding is betrokken. Het CBP stelt vast dat door de KMar geen nieuwe gezichtspunten worden aangedragen. Het CBP handhaaft derhalve haar standpunt dat het KMar-personeel geen degelijke opleiding krijgt met betrekking tot N.SIS II en de KMar hierdoor artikel 14 van de Verordening en artikel 14 van het Besluit overtreedt.

Informatieplicht tegenover binnenkomende vreemdelingen

De Kmar geeft in haar *zienswijze* aan dat in de Wpg geen verplichting is opgenomen om betrokkenen over wie de politiegegevens verwerkt actief te informeren over deze gegevensverwerking.

Het CBP wijst op overweging 15 in de Verordening waarin het volgende is neergelegd. " Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([39]), is van toepassing op de verwerking van persoonsgegevens overeenkomstig deze verordening." Het CBP merkt hierover op dat de voren vermelde richtlijn is geïmplementeerd in de Wbp. Dat impliceert dat naast de Wpg ook de Wbp en daarmee de artikelen 33 en 34 uit deze wet op de KMar van toepassing zijn. Nu de KMar onderdanen van derde landen die Nederland binnenkomen en onderdanen van derde landen die Nederland verlaten niet vooraf informeert over de controle die zij in N.SIS II uitvoert en de rechten die deze onderdanen hebben, overtreedt de KMar de artikelen 33 en 34 van de Wbp.

[39] PB L 281 van 23.11.1995, blz. 31.