BIJLAGE

In deze bijlage beoordeelt het CBP de schriftelijke reacties van de NP d.d. 22 juli 2015 (zienswijze) en d.d. 25 augustus 2015 (aanvullende zienswijze) op het rapport voorlopige bevindingen van het CBP van 1 juli 2015.

Interpretatie van de geldende wet- en regelgeving

Zienswijze

De NP geeft aan dat artikel 10 lid van de Verordening ruimte laat voor interpretatie. Het CBP legt deze bepaling uit als een verplichting tot het hebben van een specifiek voor N.SIS II opgesteld beveiligingsplan. De NP hanteert een risico gebaseerde aanpak van de informatiebeveiliging gericht op de bescherming van de informatie en de processen. Dit resulteert in één beleid, één kader en jaarplannen op strategisch, tactisch en operationeel niveau. Deze aanpak is in lijn met het bepaalde in artikel 10 lid 1 van de Verordening, omdat verwezen wordt naar de vaststelling van een veiligheidsplan. De door de NP opgestelde plannen zijn ook van toepassing op N.SIS II, maar niet exclusief op N.SIS II.
De NP is van mening dat een specifiek beveiligingsbeleid voor N.SIS II in materiële zin geen verschil zal maken en leidt tot sub-optimalisatie in de informatievoorziening. Een generiek beleid over de hele informatievoorziening is in de optiek van de NP de enige manier om grip te houden op de politieprocessen en daarmee de vereiste waarborgen aan te brengen voor de bescherming van de integriteit van gegevens en de privacy van burgers.
De NP heeft de voren vermelde zienswijze gebaseerd op IV-strategie van de NP, zoals vastgelegd in het Bestemmingsplan, de vernieuwingsstrategie en de IV-portfolio. Ook de werkwijze en eisen bij aanbestedingen en bij convenanten zijn gebaseerd op deze beleidslijn. Verwezen wordt naar verschillende bijlagen.

Reactie CBP

Het CBP begrijpt uit de zienswijze van de NP dat zij het oneens is met de uitleg die het CBP geeft aan het begrip - beveiligingsplan - als bedoeld in artikel 10 lid 1 van het Besluit. Het CBP gaat hierop derhalve in bij de beoordeling van het beveiligingsplan.

Beveiligingsplan

Zienswijze

De NP geeft aan dat op alle verwerkingen van de politie wet- en regelgeving van toepassing is en dat is expliciet vastgelegd in het boekwerk privacy by design. De NP heeft een volledig herzien stelsel voor informatiebeveiliging. Het stelsel is volledig afgestemd met het Ministerie van V & J en behandeld in het Combi-MT. Verwezen wordt naar een document waarin de beleidskaders voor informatiebeveiliging bij de NP worden beschreven. Voorts verwijst de NP naar een globaal uitgevoerde beveiligingsanalyse op basis waarvan twee uitvoeringsregelingen zijn opgesteld waaraan de eigen diensten van de NP moeten voldoen. Deze betreffen een beveiligingsniveau “standaard” en “hoog”. Op N.SIS II is voor de ICT dienstverlening het standaardbeveiligingsniveau van toepassing, welke maatregelen in het

rekencentrum zijn doorgevoerd. Dit laat onverlet dat lijnmanagers conform het beleid en kader eigenstandig beveiligingsanalyses uitvoeren en keuzes maken welke risico's acceptabel zijn en welke niet.
De dienst ICT heeft een volledig functionerend stelsel van fysieke beveiliging. Deze is in lijn met het fysieke beveiligingsbeleid 2015 en het BHV-beleid, welke momenteel beide in consultatie zijn. Het beleid fysieke beveiliging is een samenbundeling van de gangbare praktijk binnen de politie en is grotendeels geïmplementeerd. De fysieke beveiligingsnormen in het informatiebeveiligingskader worden toegepast. Onderdeel daarvan is het directe toezicht van het sectorhoofd op de fysieke en logische toegangsbeveiliging van zijn medewerkers. Verwezen wordt naar twee bijlagen waarin richtlijnen hiervoor zijn uitgewerkt. De NP geeft voorts aan dat er geen usb-sticks of laptops worden gebruikt voor N.SIS II. De hardware componenten worden vernietigd door een externe leverancier waarmee en contract is afgesloten en procedures zijn afgesproken.
De dienst ICT van de NP heeft werkplekcontroles en clear deskpolicy, welke inzicht geven in mate van toezicht op de werkplek. Deze controles kunnen worden overlegd.
De NP wijst verder op de voortgangs- en verantwoordingsrapportages. In de kwartaalrapportages wordt informatiebeveiliging in generieke zin meegenomen. Op die wijze is informatiebeveiliging en de voortgang daarop onderdeel van de normale managementcyclus. Ten slotte merkt de NP op dat er geen voortgangsrapportages zijn aangereikt, omdat in geen enkele daarvan op N.SIS II wordt ingegaan.

Definitieve bevindingen

De NP heef bij de (aanvullende) zienswijze diverse documenten overgelegd.
Het CBP heeft deze documenten beoordeeld.

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 geeft aan dat zij geen specifiek voor N.SIS II opgesteld beveiligingsplan heeft, maar dat zij desondanks handelt in overeenstemming met artikel 10 lid 1 van de Verordening, omdat de door de NP opgestelde plannen ook van toepassing zijn op N.SIS II. De NP verwijst hiertoe naar de overgelegde documenten.
Het CBP is van oordeel dat er eveneens sprake is van een beveiligingsplan in de zin van artikel 10 lid 1 van het Besluit, indien uit de door de NP overgelegde documenten en het gestelde in de (aanvullende) zienswijze een beveiligingsplan met betrekking tot N.SIS II kan worden afgeleid. Dat is het geval indien er voldoende aanknopingspunten zijn die het CBP gezamenlijk kunnen doen concluderen tot een beveiligingsplan met betrekking tot N.SIS II. Hiertoe dient in die documenten voldoende te worden beschreven welke concrete technische en organisatorische maatregelen er *met betrekking tot N.SIS II* ten uitvoer worden gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking en op welke wijze de doelmatigheid van de getroffen beveiligingsmaatregelen (doorlopend) worden gecontroleerd.

Uit de overgelegde documenten en het gestelde in de (aanvullende) zienswijze blijkt niet welke concrete technische en organisatorische maatregelen er *met betrekking tot N.SIS II* door de NP ten uitvoer zijn gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Het betreft immers slechts documenten die generiek van aard zijn, dan wel vallen buiten de scope van het onderzoek, dan wel geen duidelijkheid bieden hoe N.SIS II is ingebed in het geheel.

Nu uit de overgelegde documenten en het gestelde in de (aanvullende) zienswijze niet een beveiligingsplan in de zin van artikel 10 van het Besluit kan worden afgeleid, overtreedt de NP artikel 10 lid 1 van het Besluit.

Toegangsrechten N.SIS II en personeelsprofielen

Zienswijze

Naar aanleiding van de door het CBP getrokken conclusie dat de NP de toegangsrechten tot N.SIS II niet correct heeft ingeregeld, wijst de NP erop dat de autorisatielijst de werkelijk toegekende rechten en rollen bevat; dat de autorisatieprocedures nog decentraal zijn ingeregeld (gebaseerd op de voormalige korpsen), waarbij iedere procedure de noodzakelijke waarborgen biedt en in materiële zin rechten worden toegekend aan medewerkers die daadwerkelijk toegang dienen te verkrijgen tot de informatie en dat het centraliseren van de autorisatieprocedures en de daarbij behorende tooling een ingrijpende operatie is die de NP in het komende jaar verwacht af te ronden. Voorts geeft de NP aan dat de ketenpartners elk op grond van hun wettelijke taak toegang hebben tot het N.SIS II-register. In de geldende Nederlandse verhoudingen wordt deze verleend op basis van het vertrouwen dat de ketenpartners elk hun eigen beheerregime op orde hebben en houden. De NP controleert de autorisatie van individuele collega's bij de ketenpartners niet. De NP erkent dat het CBP terecht heeft vastgesteld dat de NP in het door mandateren van het uitgeven van toegangsrechten aan ketenpartners onvoldoende zicht houdt op de daar geldende autorisatieprocedures. Ten slotte wijst de NP op het "project autoriseren". De in het kader van dit project opgestelde personeelsprofielen kunnen aan het CBP ter beschikking worden gesteld.

Definitieve bevindingen

Toegangsrechten N.SIS II
De NP benoemt dat de autorisatieprocedures thans decentraal zijn geregeld en dat iedere procedure de noodzakelijke waarborgen biedt. De NP heeft het CBP evenwel geen documenten ter beschikking gesteld, waaruit blijkt dat de procedures zijn omgeven met waarborgen. Voor het wijzigen van rechten van bestaande accounts wordt eveneens verwezen naar de werkinstructies. Deze werkinstructies zijn niet door de NP aan het CBP overgelegd.
In de eerder door de NP verstrekte autorisatiematrix staat niet nader gespecificeerd welke politiemedewerkers deze rechten toegewezen mogen krijgen.
Verder besteedt de NP aandacht aan de operatie betreffende centralisering van de autorisatieprocedures. Een aantal van de door de NP overgelegde documenten zien op de toekomstige situatie.

Personeelsprofielen
In de zienswijze verwijst de NP naar het 'project autoriseren' en geeft zij aan dat de in het kader van dit project opgestelde personeelsprofielen ter beschikking kunnen worden gesteld. Het CBP gaat er van uit dat de NP hiermee doelt op het thans nog niet afgeronde project van centraliseren van autorisatieprocedures en dat de in het kader van dit project opgestelde personeelsprofielen gedurende de onderzoeksperiode niet werden en ook thans nog niet worden gebruikt. In de zienswijze van de NP wordt verder niet aangegeven dat de in het kader van het project opgestelde personeelsprofielen zien op de omschrijving van taken en verantwoordelijkheden van (alle) personen met bevoegdheden met betrekking tot N.SIS II.

Beoordeling

Toegangsrechten 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 heeft 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.

Het CBP heeft 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.

De NP merkt in haar zienswijze op dat de autorisatielijst de werkelijk toegekende rechten en rollen bevat. Het CBP merkt hierover op dat de NP nalaat deze stelling te onderbouwen. Voorts geeft de NP aan dat de autorisatieprocedures (thans) nog decentraal zijn geregeld en dat iedere procedure de noodzakelijke waarborgen biedt. Het CBP stelt vast dat uit de door de NP overgelegde documenten niet blijkt dat de decentraal geregelde autorisatieprocedures met waarborgen zijn omkleed. Ook blijkt dat een aantal door de NP overgelegde documenten nog niet zijn geïmplementeerd en dus (nog) niet van kracht zijn. Ten slotte wordt opgemerkt dat de NP erkent dat zij de autorisaties van medewerkers bij de ketenpartners niet controleert en dat zij onvoldoende zicht houdt op de geldende autorisaties bij de ketenpartners.

Het CBP is van oordeel dat de NP in haar zienswijze niet heeft aangetoond dat alle partijen die toegangsrechten hebben tot N.SIS II in de autorisatiematrix staan en dat bij de in de matrix genoemde partijen alle typen van toegangsrechten worden vermeld. Het CBP handhaaft het standpunt dat deze toegangsrechten niet juist zijn geregeld. Hierdoor handelt de NP 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 aangesloten partijen) die bevoegd zijn om gegevens in N.SIS II te zien, in te voeren, bij

te werken, te wissen en te doorzoeken. Deze profielen dienen door de NP thans in de praktijk te worden toegepast. Het CBP heeft aan de NP gevraagd deze profielen te overleggen. De NP heeft hieraan, ook in de zienswijzeprocedure, geen gehoor gegeven. De in het kader van het "project autoriseren" aangeboden personeelsprofielen zijn nog niet van kracht. Het betreft immers een nog niet afgerond project. Nu de NP de thans van toepassing zijnde profielen niet alsnog aan het CBP heeft overgelegd, neemt het CBP aan dat de NP deze profielen niet heeft. 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.

Toekennen van autorisaties en controle op toegekende autorisaties

Zienswijze

De NP verwijst kortheidshalve naar de reactie onder 3.2. Verder geeft de NP aan dat zij profielen heeft voor de rechten van ketenpartners welke overeenkomen met de geldende wettelijke taken van die organisaties. Voor het autoriseren van medewerkers schrijft de Verordening procedures voor, waaronder functioneel beheerders. De bij de NP bestaande procedures hebben ook hun werking voor N.SIS II.

Definitieve bevindingen

Toekennen van autorisaties
Voor het toekennen van autorisaties en de controle op toegekende autorisaties verwijst de NP naar de in de zienswijze onder 3.2. gegeven inhoudelijke reactie en daarmee naar de door de NP verstrekte documenten. In deze documenten wordt onder meer verwezen naar werkinstructies voor het toekennen van autorisaties en wordt beschreven hoe de toekomstige (wenselijke) situatie er uit moet gaan zien en hoe dit in 2015 zal worden uitgevoerd. Alhoewel er in de documenten voorts richtlijnen worden gegeven en voor de concrete uitwerking wordt verwezen naar procedures en werkinstructies, heeft de NP deze niet aan het CBP overgelegd.

Controle op toegekende autorisaties
Het CBP constateert dat de NP bij haar zienswijze een document heeft overgelegd waarin controle op toegekende autorisaties aan de orde komt. Het betreft een document dat richtlijnen bevat voor het autoriseren van medewerkers en richtlijnen voor de controle van toegekende toegangsrechten. Voor de controle op toegekende autorisaties is in het document opgenomen dat er eenmaal per kwartaal een controle uitgevoerd moet worden op verleende autorisaties en de daadwerkelijke toegang tot informatie, applicaties, systemen en netwerken. In dit document worden richtlijnen gegeven en voor de concrete uitwerking wordt verwezen naar procedures.

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.

Daarnaast heeft 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.

Uit de door de NP bij de zienswijze overgelegde documenten blijkt niet dat de NP een procedure heeft ten behoeve van het autoriseren van functioneel beheerders tot N.SIS II en dit evenmin het geval is ten aanzien van medewerkers van de IND.
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 handhaaft het CBP het standpunt dat de NP niet in overeenstemming handelt met de NEN-norm en dat de NP hierdoor artikel 32 lid 1 onder c van de Wpg overtreedt. 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 het door de NP tijdens de zienswijzeprocedure overgelegde document blijkt dat er in dit document richtlijnen worden gegeven voor het autoriseren van medewerkers en voor de controle van toegekende toegangsrechten. Voor de concrete uitwerking wordt in deze richtlijnen verwezen naar procedures en werkinstructies. Nu de NP deze procedures en werkinstructies niet aan het CBP heeft overgelegd, heeft de NP niet aangetoond dat er (doorlopende) controles plaatsvinden op de aan functioneel beheerders en IND-medewerkers toegekende autorisaties en dat er afspraken zijn 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.

Beveiligingsincidenten

Zienswijze

De NP heeft de aanpak van incidenten en verstoringen ingeregeld. Dat betreft eveneens N.SIS II, zonder dat daaraan in de betreffende procedures wordt gerefereerd. Incidenten en verstoringen met een internationaal aspect vallen onder de regie van de CISO. In de gevraagde periode zijn er geen verstoringen met betrekking tot N.SIS II geweest. Is er bijvoorbeeld sprake van een stroomstoring, dan is ook de bevraging van N.SIS II verstoord. In dat geval maakt de NP gebruik van vervangende werkwijzen. Operationele incidenten zoals het geblokkeerd raken van een account en het uitvallen van een server worden geregistreerd en adequaat geadresseerd binnen de beheersstructuren van de dienst ICT en de dienst IM. Bij overschrijden van vooraf gestelde drempelwaarden wordt de CISO geïnformeerd. In het informatiebeveiligingskader politie is vastgesteld hoe met incidenten moet worden omgegaan. De NP kent, per eenheid, richtlijnen voor het melden van incidenten. Alle incidenten worden door de politie beoordeeld, waarbij wordt gezocht naar oorzaak, gevolg en kans op herhaling.
Voorts wordt erop gewezen dat de NP een procedure heeft voor het afhandelen van beveiligingsincidenten. Deze treden in werking afhankelijk van de ernst en omvang van het incident.

Ten slotte merkt de NP op dat incidenten worden afgehandeld, dat er in de onderzoeksperiode geen incidenten met N.SIS II zijn geweest en dat in het geval van datalekken en andere relevante incidenten altijd het ministerie wordt geïnformeerd.

Definitieve bevindingen

De NP stelt – kort gezegd – dat de afhandeling van informatiebeveiligingsincidenten adequaat plaatsvindt en verwijst naar verschillende beleidsplannen en procedures die hier op zien. Ten eerste wijst de NP op het informatiebeveiligingskader politie, waarin zou zijn vastgelegd hoe met incidenten omgegaan dient te worden. Ten tweede verwijst de NP naar richtlijnen voor het melden van incidenten per eenheid. Het CBP heeft geconstateerd dat in het informatiebeveiligingskader slechts kaders worden gesteld ten aanzien van de omgang met beveiligingsincidenten. Uit het informatiebeveiligingskader en de opmerkingen van de NP aangaande de richtlijnen per eenheid, zou derhalve kunnen worden afgeleid dat er nadere procedures gelden aangaande informatiebeveiligingsincidenten. Deze documenten zijn, ondanks daartoe strekkende verzoeken van het CBP, evenwel niet door de NP verstrekt. Het CBP meent dat het op de weg van de NP had gelegen om deze documenten aan het CBP te verstrekken indien deze relevant zijn voor het onderzoek van het CBP. Ten vierde verwijst de NP naar overgelegde documenten. Deze documenten gaan niet in op beveiligingsincidenten waarop het onderzoek van het CBP gericht is, zoals onbevoegde gegevensopslag of - kennisname. Alle documenten zijn verder concepten en bevatten geen verdere concrete uitwerking van deze beleidsuitgangspunten.

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 nogmaals beoordeeld of uit de door de NP gegeven informatie en verstrekte documenten kan worden afgeleid dat aan de voren vermelde eisen wordt voldaan.

Het CBP heeft vastgesteld dat in het overgelegde document slechts kaders worden gesteld ten aanzien van de omgang met beveiligingsincidenten. Uit de opmerkingen van de NP aangaande de richtlijnen per eenheid zou kunnen worden afgeleid dat er nadere procedures gelden aangaande beveiligingsincidenten. Deze procedures zijn echter niet aan het CBP overgelegd. Op basis van het voorgaande komt het CBP tot de conclusie dat de NP niet heeft aangetoond dat zij beschikt over procedures om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten die N.SIS II (mede) raken te bewerkstelligen. Hierdoor handelt de NP niet in overeenstemming met de NEN-norm en overtreedt zij artikel 10 lid 1 onder d van de Verordening en artikel 10 lid 1 onder d van het Besluit.

Controle gebruik N.SIS II: logging

Zienswijze

De NP geeft in haar zienswijze aan dat het CBP artikel 10 lid 1 onder i en k van de Verordening en artikel 10 lid 1 onder i en k van het Besluit interpreteert als de verplichting tot het enerzijds volledig loggen van alle applicaties en anderzijds het (doorlopend) controleren daarvan. De NP is van mening dat aldaar voorgeschreven wordt dat controle van de opneming van gegevens mogelijk is en er een adequaat mechanisme is van interne controle en toezicht. Systeemlogging is één vorm – maar niet de enige - waarmee aan de verplichting in artikel 10 lid 1 onder i en k van de Verordening en artikel 10 lid 1 onder i en k van het Besluit kan worden voldaan.
De NP verwijst naar de schermprints van applicaties die toegang geven tot N.SIS II die reeds aan het CBP zijn verstrekt.
De NP hanteert het volgende mechanisme passend binnen het informatiebeveiligingskader van de politie. Bij de opname van gegevens in N.SIS II wordt in het systeem zelf vastgelegd wie de betreffende registratie opvoert of de contactpersoon daarvan is. Het Bureau SIRENE houdt steekproefsgewijs toezicht op de registraties in N.SIS II en of deze passen binnen de doelstelling van het systeem.
Voorts wijst de NP erop dat:

1. zij een klachtenprocedure en privacyrichtlijnen heeft waarmee een geregistreerde zijn wettelijke rechten kan uitoefenen;
2. de NP privacyfunctionarissen in dienst heeft met een toezichthoudende taak op de naleving van de relevante privacywetgeving;
3. de NP informatiebeveiligingsfunctionarissen in dienst heeft die preventief en correctief adviseren over de beveiliging en zo nodig de CISO informeren;
4. de afdeling korpsaudit via een jaarkalender onderdelen van de informatieverwerking van de politie onderzoekt en informatiebeveiliging onderdeel daarvan uitmaakt;
5. op regelmatige basis, onder andere voor de jaarrekeningcontrole, externe audits worden uitgevoerd binnen de NP;
6. het toekennen van autorisaties verloopt via gestandaardiseerde processen;
7. de CISO een toezichthoudende taak heeft op het totale systeem van informatiebeveiliging en gevraagd en ongevraagd delen van de beveiliging kan toetsen;
8. er controles uitgevoerd worden op integriteitsschending en daartoe ook logging gebruikt en afwijkend gedrag monitort, zowel binnen als buiten de organisatie.

De NP verwijst naar enkele documenten en geeft aan dat deze documenten ter inzage beschikbaar zijn voor het CBP.
Ten slotte geeft de NP aan dat in SIS II application controls (geprogrammeerde controles) aanwezig zijn in de componenten en dat de politie in al haar applicaties geprogrammeerde controles realiseert. In alle componenten van SIS II zijn geprogrammeerde controles aanwezig die betrekking hebben op invoer- en verwerkingscontroles.

Definitieve bevindingen

De NP geeft in haar zienswijze aan dat bureau SIRENE steekproefsgewijs toezicht houdt op de registraties in N.SIS II en of deze passen binnen de doelstelling van het systeem. De NP voert evenwel niet aan dat het controle op de logfiles betreft, zodat de relevantie voor (in ieder geval dit gedeelte van) het onderzoek van het CBP ontbreekt. Overigens heeft het CBP van deze steekproefsgewijze controles, hoewel hierom is verzocht, geen achterliggende documenten ontvangen van de NP, zodat het CBP niet kan vaststellen dat deze controles plaatsvinden. Ten aanzien van de door de NP genoemde onderdelen, van het controlemechanisme van de NP merkt het CBP op dat deze niet zien op een (doorlopende) controle van logfiles. De door de NP genoemde controles kunnen naar het oordeel van het CBP niet worden beschouwd als doorlopende controle van de logging als bedoeld in artikel 10 lid 1 onder k van de Verordening en het Besluit. Immers, uit de zienswijze van de NP blijkt dat er slechts in geval van (niet willekeurige) controles op integriteitsschending onder meer op logging wordt gecontroleerd. Uit de zienswijze van de NP blijkt verder niet dat er (doorlopend) op logging wordt gecontroleerd. De NP voert tenslotte aan dat er in SIS II geprogrammeerde controles aanwezig zijn die betrekking hebben op invoer- en verwerkingscontroles. Het CBP stelt vast dat dit controles op de juistheid- en volledigheid van de invoer van gegevens in SIS II betreffen. Het is voor het CBP op basis van de verkregen aanvullende informatie niet mogelijk om vast te stellen dat er doorlopend controles van de logfiles plaatsvindt. Het CBP heeft de NP uitdrukkelijk verzocht procedures en rapportages te verstrekken van uitgevoerde controles op de logfiles. Vooralsnog heeft de NP deze niet aan het CBP verstrekt. Wel zou het CBP documenten bij de NP kunnen inzien. De NP is niet overgegaan tot het verstrekken van deze documenten, hoewel dit op de weg van de NP had gelegen indien de genoemde documenten van relevantie zijn voor het onderzoek van het CBP, en heeft daarnaast in de zienswijze niet uiteengezet in hoeverre deze documenten relevant zijn. Het CBP zal met de genoemde documenten dan ook geen rekening kunnen houden.

Beoordeling

Het CBP heeft beoordeeld of uit de zienswijze van de NP blijkt dat met betrekking tot N.SIS II de logfiles door de NP (doorlopend) worden gecontroleerd. Voorts is het CBP nagegaan of uit de zienswijze van de NP blijkt dat de mutaties in toegangsrechten in N. SIS II worden gelogd en hierdoor controle door de NP op de werkzaamheden van functioneel beheerders en IND-medewerkers mogelijk is.

De door bureau SIRENE toegepaste steekproeven op de registraties van N.SIS II betreft niet de controle op de logfiles en is bovendien niet door de NP onderbouwd, nu de NP hiertoe geen documenten heeft overgelegd. De door de NP geduide onderdelen zien evenmin op een (doorlopende) controle op de logfiles. De controles van de NP zien slechts op integriteitschending en de NP controleert niet doorlopend op logging. Voorts merkt het CBP op dat de in SIS II geprogrammeerde controles slechts betrekking hebben op de juistheid van de invoer- en verwerkingscontroles. Het CBP heeft herhaald aan de NP verzocht procedures en rapportages te overleggen van door de NP uitgevoerde controles op de logfiles. De NP heeft nagelaten deze aan het CBP te verstrekken. Zij heeft slechts aangeboden dat het CBP documenten kan inzien, terwijl het CBP meermaals heeft verzocht *alle* documenten te overleggen. Ook heeft de NP nagelaten de relevantie van deze documenten te vermelden.

Ten slotte merkt het CBP op dat mutaties in toegangsrechten in N SIS II niet door de NP worden gelogd en hierdoor controle door de NP op de werkzaamheden van functioneel beheerders en ten behoeve van de IND-medewerkers niet mogelijk is.

Het CBP stelt vast dat de NP niet heeft aangetoond dat zij (alsnog) voldoet aan het bepaalde in de artikelen 10 lid 1 onder i en k van de Verordening en artikel 10 lid 1 onder i en k van het Besluit. De NP blijft deze artikelen derhalve overtreden. Hierdoor handelt de NP evenmin in overeenstemming met de NEN-norm.

Opleiding personeel

Zienswijze

De NP geeft aan dat politieagenten een opleiding volgen waarin specifiek aandacht wordt besteed aan gegevensverwerking en beveiliging en waarin de eigen rol bij informatiebeveiliging wordt benadrukt. Er worden opleidingselementen aangeboden op het gebied van informatiebeveiliging en gebruik. Deze zijn verweven in de leerstof en kennen daarmee een werking op informatieverwerking naar en uit N.SIS II.

Definitieve bevindingen

De NP voert aan dat in de reguliere opleiding van medewerkers op regelmatige basis aandacht wordt besteed aan gegevensverwerking en de beveiliging en waarin de eigen rol van medewerkers bij informatiebeveiliging wordt benadrukt.
Het CBP heeft echter geen bescheiden ontvangen waaruit blijkt dat er in de reguliere opleiding van medewerkers in algemene zin aandacht wordt besteed aan gegevensverwerking en beveiliging en de eigen rol van medewerkers hierin. Daarnaast constateert het CBP dat uit de reactie van de NP in ieder geval niet blijkt dat er in de algemene opleiding aandacht wordt besteed aan N.SIS II. Voorts blijkt niet dat personeel op de hoogte wordt gebracht van ter zake doende strafbare feiten en sancties.

Beoordeling

Het CBP is nagegaan of uit de zienswijze blijkt dat het personeel van de NP 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.

De NP heeft in haar zienswijze niet aangetoond dat in de reguliere opleiding van medewerkers in algemene zin aandacht wordt besteed aan gegevensverwerking en beveiliging en de eigen rol van medewerkers hierin. Nu eveneens niet is gebleken dat in de algemene opleiding van medewerkers aandacht wordt besteed aan N.SIS II, stelt het CBP vast dat van een degelijke opleiding met betrekking tot N.SIS II geen sprake is. Gelet hierop ziet het CBP geen aanleiding zijn conclusie te wijzigen.

Het CBP handhaaft derhalve haar standpunt dat het personeel van de NP geen specifieke en degelijke opleiding krijgt met betrekking tot de regels inzake gegevensbeveiliging en –bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. De NP overtreedt hierdoor artikel 14 van de Verordening en artikel 14 van het Besluit.

Conclusies
Het CBP ziet geen aanleiding de conclusies te wijzigen.