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 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

College Bescherming Persoonsgegevens

ONDERZOEK CIOT-BEVRAGINGEN

Onderzoek CIOT
z2010-00168

Rapport definitieve bevindingen
April 2011

DATUM 21 april 2011

INHOUDSOPGAVE

SAMENVATTING EN CONCLUSIES

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is ingesteld bij Besluit verstrekking gegevens telecommunicatie (hierna: het Besluit) van 26 januari 2000. Het CIOT-Informatiesysteem (CIS) stroomlijnt op geautomatiseerde wijze het vragen van informatie (door opsporings- en veiligheidsdiensten) en de beantwoording daarvan (door aanbieders van openbare telecommunicatiediensten en –netwerken) door tussenkomst van het CIOT. Het aantal bevragingen van het CIOT is de afgelopen jaren substantieel toegenomen. Zo is het totale aantal bevragingen toegenomen van 1,7 miljoen in 2007 tot 2,8 miljoen in 2008 en tot ruim 2,9 miljoen in 2009. Een dergelijk massaal gebruik van de bevoegdheid om persoonsgegevens op te vragen in het kader van een (opsporings)onderzoek vraagt dat de wettelijke waarborgen zorgvuldig worden nageleefd. In dit onderzoek is ten aanzien van een aantal waarborgen nagegaan of deze worden nageleefd.

Het College bescherming persoonsgegevens (CBP) heeft in 2010 in het kader van zijn toezichthoudende taak een onderzoek verricht op grond van de Wet bescherming persoonsgegevens (Wbp) en de Wet politiegegevens (Wpg) naar de naleving van de voorschriften in het kader van de CIOT-bevragingen bij het CIOT, het regionaal politiekorps Haaglanden en de Dienst Nationale Recherche (DNR). Onderzocht is:

1. Worden de bevragingen op het CIS alleen door daartoe bevoegden (geautoriseerde ambtenaren) uitgevoerd?
2. Wordt bij no-hit-bevragingen en andere vorderingen die rechtstreeks aan de telecommunicatieaanbieders worden verzonden, gebruik gemaakt van voldoende beveiliging?
3. Worden de CIOT-bevragingen rechtmatig uitgevoerd?

Bij het CIOT heeft het CBP, gezien de taak van het CIOT, alleen de eerste vraag onderzocht.

Het CBP heeft onderzocht of het proces van toekenning en registratie van autorisaties zodanig is ingevuld dat dit voldoende waarborgen biedt om ongeoorloofde toegang tot het CIS te voorkomen, en of er controle plaatsvindt op de toegekende autorisaties. Op grond van de bevindingen van het onderzoek komt het CBP daarbij tot de volgende conclusies.

Ten aanzien van de toegang door medewerkers van het CIOT:

- Medewerkers van het CIOT die beheerstaken uitvoeren hebben toegang tot het CIS. Vanuit deze taak om het beheer van het CIS uit te voeren is de toegang van deze medewerkers tot het CIS in overeenstemming met de vereisten van de NEN-norm op dit punt en met artikel 13 Wbp.
- De toekenning van een autorisatie aan het hoofd Exploitatie en Beheer voor het CIS door de directeur van het CIOT is in overeenstemming met artikel 5 lid 2 Besluit en voldoet op dit punt aan artikel 13 Wbp. Het CBP constateert echter dat de autorisaties van de medewerkers die beheerstaken uitvoeren op het CIS niet voldoen aan artikel 5 lid 2 Besluit en derhalve niet rechtsgeldig zijn afgegeven. Dit is in strijd met artikel 13 Wbp.
- De toegang tot het CIS door de directeur en diens plaatsvervanger voor demonstratiedoeleinden is niet overeenkomstig de NEN-norm, omdat zij niet zijn belast zijn met beheerstaken en bovendien het geven van demonstraties niet onder

beheerstaken worden geschaard. Hiermee wordt in strijd met artikel 13 Wbp gehandeld.

Ten aanzien van de toekenning van autorisaties aan de bevoegde autoriteiten:

- Het CBP constateert dat de autorisaties van de medewerkers van opsporingsdiensten voor toegang tot het CIS niet voldoen aan artikel 5 lid 1 Besluit en derhalve niet rechtsgeldig zijn afgegeven. Dit is in strijd met artikel 13 Wbp.
- Het CBP stelt vast dat formele procedures voor het registreren en afmelden van gebruikers zijn vastgesteld, overeenkomstig de NEN-norm. Hiermee wordt op dit punt voldaan aan de vereisten zoals gesteld in de NEN-norm en wordt in overeenstemming gehandeld met artikel 13 Wbp.

Ten aanzien van de registratie van autorisaties:

- Tijdens het onderzoek zijn door het CIOT autorisatieoverzichten overgelegd. Het CBP concludeert dat het CIOT beschikt over een formele registratie van de toegekende autorisaties, zoals voorgeschreven in de NEN-norm. Hiermee wordt op dit punt in overeenstemming gehandeld met de NEN-norm en artikel 13 Wbp.

Ten aanzien van de controle op verleende autorisaties:

- Het CBP heeft de van het CIOT ontvangen autorisatieoverzichten vergeleken met het aantal feitelijk geautoriseerde medewerkers van de onderzochte korpsen en concludeert dat deze overeenkomen. Hiermee wordt op dit punt in overeenstemming met artikel 13 Wbp gehandeld.
- Het CBP stelt vast dat conform de eisen van de NEN-norm een CIS-account onder bepaalde omstandigheden kan worden ingetrokken en dat het CIOT een formele procedure heeft vastgelegd voor het intrekken van een autorisatie. Hiermee wordt op dit punt in overeenstemming gehandeld met de NEN-norm en met artikel 13 Wbp.

1 INLEIDING

1.1 Achtergrond onderzoek

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is ingesteld bij Besluit verstrekking gegevens telecommunicatie (hierna: het Besluit) van 26 januari 2000. Het CIOT valt op grond van artikel 2 van het Besluit onder de verantwoordelijkheid van de minister van Justitie. Het CIOT-Informatiesysteem (CIS) stroomlijnt op geautomatiseerde wijze het vragen van informatie (door opsporings- en veiligheidsdiensten) en de beantwoording daarvan (door aanbieders van openbare telecommunicatiediensten en –netwerken) door tussenkomst van het CIOT. De informatie die gevraagd wordt betreft bijvoorbeeld de naam-, adres- en woonplaatsgegevens behorend bij een telefoonnummer. In geval dat informatie wordt gevraagd over internetaansluitingen gaat het bijvoorbeeld naast naam-, adres- en woonplaatsgegevens ook om gebruikte e-mailadressen.

Het aantal bevragingen van het CIOT is de afgelopen jaren substantieel toegenomen. Zo is het totale aantal bevragingen toegenomen van 1,7 miljoen in 2007 tot 2,8 miljoen in 2008 en tot ruim 2,9 miljoen in 2009. Een dergelijk massaal gebruik van de bevoegdheid om bovengenoemde persoonsgegevens op te vragen in het kader van een (opsporings)onderzoek vraagt dat de wettelijke waarborgen zorgvuldig worden nageleefd. In dit onderzoek is ten aanzien van een aantal waarborgen nagegaan of deze worden nageleefd.

1.2 Doel, reikwijdte en uitvoering van het onderzoek

In het kader van de toezichthoudende taak heeft het College bescherming persoonsgegevens (CBP) een ambtshalve onderzoek verricht conform artikel 60 Wet bescherming persoonsgegevens (Wbp) en artikel 35 Wet politiegegevens (Wpg) naar de naleving van voorschriften in het kader van CIOT-bevragingen bij het CIOT, het regionaal politiekorps Haaglanden en de Dienst Nationale Recherche (DNR).

Het betreft de volgende onderzoeksvragen:

1. Worden de bevragingen op het CIS alleen door daartoe bevoegden (geautoriseerde ambtenaren) uitgevoerd? Voor de beantwoording van deze vraag is onderzocht of de toekenning en registratie van een CIS-autorisatie zowel bij het CIOT zelf als bij de korpsen zodanig is ingevuld dat dit voldoende waarborgen biedt dat ongeoorloofde toegang tot het CIS wordt voorkomen. Voorts is onderzocht of er controle plaatsvindt op de toegekende autorisaties.
2. Wordt bij no-hit-bevragingen en andere vorderingen die rechtstreeks aan de telecommunicatieaanbieders worden verzonden, gebruik gemaakt van voldoende beveiliging? Voor de beantwoording van deze vraag is onderzocht of en zo ja, welke beveiligingsmaatregelen bij rechtstreekse gegevensuitwisseling zijn toegepast.
3. Worden de CIOT-bevragingen rechtmatig uitgevoerd? Voor de beantwoording van deze vraag heeft het CBP onderzocht of de geselecteerde bevragingen op een van de grondslagen van het Wetboek van Strafvordering hebben plaatsgevonden en is door toetsing aan de hand van de vereiste stukken van het dossier het verband tussen de bevraging en het referentienummer waaronder de bevraging heeft plaatsgevonden gecontroleerd.

Bij het CIOT heeft het CBP, gezien de taak van het CIOT, alleen de eerste vraag onderzocht. Bij DNR en het korps Haaglanden zijn alle drie de vragen onderzocht. Per onderzochte dienst is een rapport opgesteld. Dit rapport betreft de resultaten van het onderzoek bij het CIOT.

Het CBP heeft het CIOT bezocht op 25 en 26 februari 2010. Tijdens het onderzoek ter plaatse zijn voor de eerste onderzoeksvraag interviews gehouden en heeft het CBP kennis genomen van de werking van het CIOT-Informatiesysteem.
Op grond van het bepaalde in artikel 60 lid 2 Wbp is het rapport van voorlopige bevindingen op 16 december 2010 aan de minister van Veiligheid en Justitie toegezonden en is hij in de gelegenheid gesteld zijn zienswijze kenbaar te maken.
Bij brief van 25 februari 2011 heeft de minister zijn schriftelijke reactie gegeven op de voorlopige bevindingen. Dit heeft geleid tot een aanpassing van de tekst onder 3.1.1, 3.1.2, 3.2.1 en 3.2.2 ten aanzien van de aldaar besproken mandatering en heeft op dit punt geleid tot een wijziging in de conclusies van het onderzoek. Voor het overige heeft de reactie niet geleid tot wijziging van de bevindingen en conclusies.

1.3 Wettelijk kader

De bevindingen in dit onderzoek zijn getoetst aan artikel 5 leden 1 en 2 Besluit verstrekking gegevens telecommunicatie en artikel 13 Wet bescherming persoonsgegevens (Wbp).

2 ORGANISATIE CIOT

Het CIOT is onderdeel van het ministerie van Justitie en valt onder de Directie Instrumentatiebeleid, Rechtspleging en Rechtshandhaving van dit ministerie. Het CIOT faciliteert de bevragingen door (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten, geeft uitvoering aan het Besluit verstrekking gegevens telecommunicatie, houdt toezicht op de uitvoering van het vraag- en antwoordproces en rapporteert ten slotte over het gebruik van het CIS en verstrekt auditinformatie. Deze taken heeft het CIOT organisatorisch in drie taakgroepen ondergebracht: Bedrijfsvoering, Project- en productmanagement en Exploitatie en beheer. De taakgroep Bedrijfsvoering zorgt voor de uitvoering van de administratieve taken ten aanzien van de aansluiting en verplichtingen van de telecommunicatieaanbieders via Service Level Agreements (SLA's). Binnen het CIOT is Bedrijfsvoering verantwoordelijk voor de interne organisatie van het CIOT. De taakgroep Exploitatie en beheer is verantwoordelijk voor het technisch beheer van het CIOT-systeem en het bieden van technische ondersteuning aan de telecommunicatieaanbieders en de korpsen. Hieronder vallen onder meer het toewijzen van een account voor het CIS aan bevoegde medewerkers van korpsen en het faciliteren van de telecommunicatie-aanbieders en korpsen ten aanzien van de aansluiting op het CIS. De taakgroep Project- en productmanagement is verantwoordelijk voor de innovatie van het CIS, voor het relatiebeheer en voor de systeemontwikkeling.

3 TOEGANG TOT HET CIS

Het CBP heeft bij het CIOT onderzocht of het proces van toekenning en registratie van autorisaties zodanig is ingevuld dat dit voldoende waarborgen biedt om ongeoorloofde toegang tot het CIS te voorkomen.

3.1 Toegang tot het CIS bij het CIOT

3.1.1 Norm

A. *Toegang door medewerkers van het CIOT*

Artikel 13 Wbp legt aan de verantwoordelijke de verplichting op om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen. Door zorg te dragen voor het ontwikkelen en onderhouden van een systeem van autorisaties dat voldoet aan de geldende (internationale) standaarden geeft de verantwoordelijke voor wat betreft dit onderdeel invulling aan zijn verplichting tot het tenuitvoerleggen van passende maatregelen. Deze toegangsbeveiliging door middel van autorisaties is nader uitgewerkt in het Besluit. Artikel 5 lid 2 Besluit regelt dat de technische voorzieningen met betrekking tot het CIS alleen toegankelijk zijn voor personen die door de minister van Justitie zijn geautoriseerd.

Nu er in het Besluit en in de Wbp slechts is voorzien in een algemene regeling voor informatiebeveiliging en in het Besluit slechts in algemene zin iets is opgenomen over autorisaties, 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 onderdelen van de Code voor informatiebeveiliging, de NEN-ISO/IEC 27002:2007-norm (hierna: de NEN-norm)[1]. De NEN-norm is een gezaghebbende norm voor informatiebeveiliging en 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 13 Wbp. Dit sluit niet uit dat het CIOT eventueel ook op andere wijze kan aantonen dat wordt voldaan aan artikel 13 Wbp.

Het onderhouden van een systeem van autorisaties voor speciale bevoegdheden als onderdeel van het treffen van beveiligingsmaatregelen volgt uit de NEN-norm. Ten aanzien van toegang geldt op basis van de NEN-norm dat alleen functies die noodzakelijkerwijs toegang moeten hebben tot het informatiesysteem hiervoor geautoriseerd mogen worden. In het kader van beheer en onderhoud van het CIS kan aan medewerkers van het CIOT toegang worden verleend tot de technische voorzieningen daarvan.

[1] NEN-ISO/IEC 27002:2007, 11.2.2 Beheer van speciale bevoegdheden , p. 71.

B. Autorisatie door de minister van Justitie

De technische voorzieningen die de uitwisseling van informatie mogelijk maken zijn alleen toegankelijk voor personen die door de minister van Justitie zijn geautoriseerd. Het belang hiervan ligt in de omstandigheid dat de gegevens die het betreft van gevoelige aard (kunnen) zijn, zodat toegang daartoe gestructureerd en bovendien niet door willekeurige personen plaats moet kunnen vinden. De omstandigheid dat de autorisatie wordt toegekend door de minister van Justitie benadrukt het gewicht van de maatregel. Het autoriseren door de minister van Justitie van personen voor de toegang tot het CIS maakt daarmee onderdeel uit van de eerdergenoemde uit artikel 13 Wbp volgende maatregelen. Dit autorisatievereiste is nader geregeld in artikel 5 lid 2 Besluit.

Het toekennen van autorisaties kan de minister van Justitie ingevolge artikel 10:12 Algemene wet bestuursrecht (Awb) door middel van een mandaatbesluit overdragen aan personen die werkzaam zijn onder zijn verantwoordelijkheid. Een algemeen mandaat van deze strekking dient ingevolge artikel 10:5 Awb schriftelijk te worden verleend. Ingevolge artikel 10:9 Awb kan de mandaatgever toestaan dat ondermandaat verleend wordt.

3.1.2 Bevindingen toegang medewerkers van het CIOT tot het CIS

A. Toegang door medewerkers van het CIOT

Het CIOT is verantwoordelijk voor de goede werking van het CIS en heeft tot taak het beheer te voeren over het systeem. In het kader hiervan dient het CIOT het systeem centraal beschikbaar te stellen en te onderhouden. Systeembeheerders en applicatiebeheerders van het CIOT moeten het CIS zodanig inrichten en beheren dat telecommunicatieaanbieders hun gegevens geautomatiseerd beschikbaar kunnen stellen en bevoegde autoriteiten geautomatiseerd bevragingen op deze gegevens kunnen uitvoeren. Tevens moeten zij in geval van storingen of calamiteiten het CIS kunnen testen en aanpassen om het proces van bevragingen optimaal te ondersteunen.
Voor de uitvoering van het beheer van het CIS beschikt het CIOT over een aantal pc's die via een webclient voor beheertaken toegang geven tot het CIS. De vijf medewerkers van de taakgroep Exploitatie en Beheer hebben toegang tot het systeem voor het uitvoeren van de beheertaken, de onderhoudstaken en de technische ondersteuning aan de telecommunicatieaanbieders alsmede aan de bevoegde autoriteiten die CIOT-bevragingen uitvoeren. Voor de beheerders van het CIOT die gebruik maken van het CIS dient aan het uitvoeren van een bevraging een incidentmelding of technisch probleem ten grondslag te liggen.

Voor de directeur en de plaatsvervangend directeur van het CIOT geldt dat zij ook beschikken over een eigen webclient met toegang tot het CIS. Deze webclients zijn geïnstalleerd met de beveiligingseisen die aan de pc's van de opsporingsdiensten worden gesteld. Zij hebben rechtstreekse toegang tot de gegevens van het CIS met het oog op het geven van demonstraties van het systeem. De plaatsvervangend directeur heeft verklaard dat voor zijn toegang en de toegang van de directeur tot het CIS voor het geven van demonstraties door het openbaar ministerie toestemming is gegeven. Afgesproken is dat de directeur en de plaatsvervangend directeur de toegang tot het CIS slechts gebruiken in het kader van een demonstratie, waarbij zij alleen hun persoonlijke gegevens raadplegen. De bevragingen die ten behoeve van een

demonstratie worden uitgevoerd volgen de weg van de reguliere bevragingen van bevoegde autoriteiten, van elke bevraging wordt een rapport opgesteld waarin wordt vastgelegd welke actie, voor wie en wanneer op het CIS is uitgevoerd. Deze rapportages zijn beschikbaar ten behoeve van de auditor. Alle handelingen in het CIS, ook die door CIOT-medewerkers zijn uitgevoerd, worden gelogd.

Beoordeling
Medewerkers van het CIOT die beheerstaken uitvoeren hebben toegang tot het CIS. Vanuit deze taak om het beheer van het CIS uit te voeren is de toegang van deze medewerkers tot het CIS in overeenstemming met de vereisten van de NEN-norm op dit punt[2] en met artikel 13 Wbp.
De toegang tot het CIS door de directeur en diens plaatsvervanger is niet overeenkomstig de NEN-norm. Het geven van demonstraties kan niet onder beheerstaken worden geschaard en zij zijn niet belast met beheerstaken. De toegang van de directeur en diens plaatsvervanger tot het CIS voor het geven van demonstraties is daarom in strijd met artikel 13 Wbp. De door het openbaar ministerie gegeven toestemming doet hieraan niet af.

B. *Autorisatie door de minister van Justitie*
Teneinde toegang tot de technische voorzieningen van het CIS te krijgen dient een autorisatie voor medewerkers van het CIOT ingevolge artikel 5 lid 2 Besluit door de minister van Justitie te zijn verleend. De minister van Justitie kan dit mandateren aan een onder zijn verantwoordelijkheid werkende medewerker, mogelijk de directeur, van het CIOT. Deze verleent vervolgens de autorisaties aan medewerkers van het CIOT die toegang tot de technische voorzieningen van het CIS moeten hebben om de onderhoud- en beheerstaken uit te kunnen voeren. Tijdens het onderzoek heeft de directeur van het CIOT verklaard[3] dat een dergelijk mandaat niet is verstrekt, terwijl de minister van Justitie evenmin zelf autorisaties aan medewerkers van het CIOT heeft toegekend.
In reactie op de voorlopige bevindingen heeft de minister van Veiligheid en Justitie alsnog een Mandaatbesluit Centraal Informatiepunt Onderzoek Telecommunicatie 2000, gedateerd 22 juni 2000, overgelegd. Dit besluit is bij brief van 22 juni 2000 namens de minster van Justitie door de directeur Opsporingsbeleid toegezonden aan de directeur van het CIOT en geeft laatstgenoemde de bevoegdheid om namens de minister besluiten te nemen ten aanzien van – kort gezegd – het beheer. Uit het onderzoek is gebleken dat de directeur van het CIOT aan het hoofd Exploitatie en Beheer een autorisatie heeft verleend tot het CIS. Voorts is gebleken dat het hoofd Exploitatie en Beheer autorisaties heeft verleend aan medewerkers Exploitatie en Beheer voor het uitvoeren van de beheertaken op het CIS.

Beoordeling
Uit het door de minister alsnog overgelegde Mandaatbesluit CIOT 2000 blijkt dat is voorzien in een rechtsgeldig mandaat waarmee de directeur van het CIOT namens de minister van Justitie autorisaties tot het CIS kan verlenen aan medewerkers van het CIOT. Hiermee is de autorisatie aan het hoofd van afdeling Exploitatie en Beheer tot het CIS door de directeur van het CIOT in overeenstemming met artikel 5 lid 2 Besluit en voldoet op dit punt aan artikel 13 Wbp. Uit het onderzoek blijkt voorts dat de

[2] NEN-ISO/IEC 27002:2007, 11.2.2 Beheer van speciale bevoegdheden , p. 71.
[3] E-mail d.d. 27 juli 2010.

medewerkers van afdeling Exploitatie en Beheer door het hoofd Exploitatie en Beheer zijn geautoriseerd. Het mandaatbesluit CIOT 2000 voorziet echter niet in de mogelijkheid van ondermandaat, nog daargelaten dat er feitelijk geen ondermandaat is verleend aan het hoofd Expoitatie en Beheer. Autorisaties kunnen dus enkel door de directeur kunnen worden toegekend. Het CBP stelt vast dat nu de autorisaties van de medewerkers van afdeling Exploitatie en Beheer niet door de directeur zijn toegekend deze niet rechtsgeldig overeenkomstig artikel 5 lid 2 Besluit zijn afgegeven. Hiermee wordt in strijd met artikel 13 Wbp gehandeld.

3.2 Toekenning van autorisaties door het CIOT aan bevoegde autoriteiten

3.2.1 Norm

Artikel 13 Wbp legt aan de verantwoordelijke de verplichting op om passende technische en organisatorische maatregelen te nemen om gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze verplichting tot het nemen van passende maatregelen wordt enerzijds nader ingevuld door artikel 5 lid 1 Besluit, met specifieke eisen ten aanzien van het CIS, en anderzijds door de in de NEN-norm gestelde vereisten.

In artikel 5 lid 1 Besluit is vastgelegd dat een bevoegde autoriteit, zoals een opsporingsambtenaar die daartoe is aangewezen door de korpsbeheerder, alleen dan verzoeken in het CIS kan invoeren indien deze daartoe door de minister van Justitie is geautoriseerd en daarbij gebruik maakt van een hem toegekende toegangscode.
Het toekennen van autorisaties kan de minister van Justitie ingevolge artikel 10:12 Awb door middel van een mandaatbesluit overdragen aan personen die werkzaam zijn onder zijn verantwoordelijkheid. Een algemeen mandaat van deze strekking dient ingevolge artikel 10:5 Awb schriftelijk te worden verleend. Ingevolge artikel 10:9 Awb kan de mandaatgever toestaan dat ondermandaat verleend wordt.

De NEN-norm schrijft voor dat toegangsbeveiliging in toegangsbeleid dient te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang. Hierin behoort onder meer te zijn voorzien in eisen voor formele autorisatie van toegangsverzoeken.[4] Ten behoeve van het beheer van toegangsrechten van gebruikers dienen formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld.[5]

3.2.2 Bevindingen

Het CIOT heeft in de procedure CIS-accounts[6] een aantal uitgangspunten voor het toekennen van toegang tot het CIS door een bevoegde autoriteit formeel vastgelegd. Teneinde een bevoegde autoriteit, zijnde een door de beheerder van het korps aangewezen opsporingsambtenaar, toegang te kunnen verlenen tot het CIS houdt het CIOT de CIS-procedure aan, waarin dit specifieke proces van accounttoekenning is vastgelegd. De medewerker van een opsporingsdienst ontvangt op deze manier onder

[4] NEN-ISO-IEC 27002:2007, 11.1.1 toegangsbeleid, p.69;

[5] NEN-ISO-IEC 27002:2007, 11.2.1 registratie van gebruikers, p.70.

[6] Procedure CIS-accounts CIOT informatiesysteem versie 3.1, ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie, versie 2.0, 11 mei 2007.

meer de toegangscode die hij nodig heeft om een verzoek in het CIS te kunnen invoeren ingevolge artikel 5 lid 1 Besluit. De bevoegde autoriteit dient op grond van dit artikel bovendien geautoriseerd te zijn door de minister van Justitie. De minister van Justitie kan dit mandateren aan een medewerker van het CIOT die volgens de CIS-procedure de bevoegde autoriteit autoriseert tot het CIS. Van de zijde van het CIOT is echter tijdens het onderzoek verklaard dat dergelijke mandaten niet zijn verstrekt, terwijl de minister van Justitie evenmin zelf autorisaties aan bevoegde autoriteiten heeft toegekend.
In reactie op de voorlopige bevindingen heeft de minister van Veiligheid en Justitie alsnog een Mandaatbesluit Centraal Informatiepunt Onderzoek Telecommunicatie 2000, gedateerd 22 juni 2000, overgelegd. Dit besluit is bij brief van 22 juni 2000 namens de minster van Justitie door de directeur Opsporingsbeleid toegezonden aan de directeur van het CIOT en geeft laatstgenoemde de bevoegdheid om namens de minister besluiten te nemen ten aanzien van – kort gezegd – het beheer. Uit het onderzoek is gebleken dat de toekenning van autorisaties aan medewerkers van de bevoegde autoriteiten plaatsvindt door medewerkers van afdeling Exploitatie en Beheer

Beoordeling
Uit het door de minister alsnog overgelegde Mandaatbesluit CIOT 2000 blijkt dat is voorzien in een rechtsgeldig mandaat waarmee de directeur van het CIOT namens de minister van Justitie autorisaties tot het CIS kan verlenen aan de bevoegde autoriteiten. Het mandaatbesluit CIOT 2000 voorziet niet in de mogelijkheid van ondermandaat zodat autorisaties enkel door de directeur kunnen worden toegekend. Het CBP stelt vast dat nu de autorisaties van de bevoegde autoriteiten niet door de directeur zijn toegekend deze niet rechtsgeldig overeenkomstig artikel 5 lid 1 Besluit zijn afgegeven. Hiermee wordt in strijd met artikel 13 Wbp gehandeld

Het CBP constateert dat de NEN-norm, die vereist dat in een vastgesteld toegangsbeleid dient te zijn voorzien in eisen voor formele autorisatie van toegangsverzoeken, waartoe formele procedures voor het registreren en afmelden van gebruikers dienen te zijn vastgesteld,[7] door het CIOT is ingevuld door middel van de formeel vastgestelde procedure CIS-accounts. Deze procedure wordt gehanteerd om de door de korpsbeheerder aangewezen opsporingsambtenaar de door het Besluit vereiste toegangscode voor het CIS te geven. Hiermee wordt op dit punt voldaan aan de vereisten zoals gesteld in de NEN-norm en in overeenstemming gehandeld met artikel 13 Wbp.

3.3 Controle op toegekende autorisaties

Controle kunnen uitoefenen op toegekende autorisaties impliceert dat deze toekenningen vastgelegd moeten zijn. Zonder deze vastlegging kan controle immers niet plaatsvinden. Vervolgens dient als gevolg van die controle vastgesteld te kunnen worden of het feitelijke aantal geautoriseerden overeenkomt met de vastlegging bij het CIOT.

[7] NEN-ISO-IEC 27002:2007 11.1.1 toegangsbeleid, p.69; 11.2.1 registratie gebruikers, p.70.

3.3.1 Norm

A. Registratie van autorisaties
Artikel 13 Wbp legt aan de verantwoordelijke de verplichting op om passende technische en organisatorische maatregelen te nemen om gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Een van de organisatorische maatregelen die dienen te worden getroffen is het vastleggen van de toegekende autorisaties. De eerder genoemde NEN-norm vereist in dit verband dat er een formele registratie wordt bijgehouden van alle personen die geregistreerd zijn als gebruikers van de dienst [8].

B. Controle op verleende autorisaties
Voornoemde verplichting de toekenning van autorisaties vast te leggen biedt, zoals gezegd, aan de verantwoordelijke de mogelijkheid de toekenning van autorisaties te controleren. Om vast te stellen of de controle hierop door het CIOT voldoende wordt uitgeoefend, sluit het CBP ook hier aan bij de NEN-norm waarin is voorgeschreven dat een formele procedure dient te zijn vastgelegd voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen, in welke procedure alle fasen in de levenscyclus van gebruikerstoegang tot de betreffende informatiesystemen zijn opgenomen[9]. Deze procedure moet ook voorzien in het onmiddellijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd of de organisatie hebben verlaten[10]. De doelstelling hiervan is de toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen, zoals ook volgt uit het vereiste van artikel 13 Wbp om passende technische en organisatorische maatregelen te treffen om gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

3.3.2 Bevindingen

A. Registratie van autorisaties
Tijdens het onderzoek ter plaatse bij het CIOT heeft het CBP autorisatieoverzichten ontvangen van de geregistreerde gebruikers bij het korps Haaglanden en de DNR. Uit de interviews blijkt voorts dat alle aanvragen voor een autorisatie tot het CIS bij het CIOT (afdeling Exploitatie en Beheer) worden uitgeprint, geregistreerd en in een kluis bewaard.

Beoordeling
Tijdens het onderzoek zijn door het CIOT autorisatieoverzichten overgelegd. Het CBP concludeert dat het CIOT beschikt over een formele registratie van de toegekende autorisaties zoals voorgeschreven in de NEN-norm[11]. Hiermee wordt op dit punt in overeenstemming met de NEN-norm en artikel 13 Wbp gehandeld.

B. Controle op verleende autorisaties
Zoals bovenvermeld heeft het CBP tijdens het onderzoek ter plaatse bij het CIOT autorisatieoverzichten ontvangen van de geregistreerde gebruikers bij het korps

[8] NEN-ISO-IEC 27002:2007, 11.2.1 registratie gebruikers, p.70.

[9] NEN-ISO-IEC 27002:2007, 11.2. beheer van toegangsrechten van gebruikers, p.70.

[10] NEN-ISO-IEC 27002:2007, 11.2.1 registratie gebruikers, p.70.

[11] NEN-ISO-IEC 27002:2007, 11.2.1 registratie gebruikers, p.70.

Haaglanden en de DNR. Hieruit blijkt dat bij het korps Haaglanden 44 medewerkers en bij de DNR landelijk 39 medewerkers over toegang tot het CIS beschikken. Het CBP heeft deze overzichten gecontroleerd aan de hand van in interviews bij het korps Haaglanden en de DNR ontvangen informatie ten aanzien van de respectieve aantallen feitelijk geautoriseerde medewerkers.
Uit het onderzoek blijkt voorts dat een autorisatie om verschillende redenen kan worden ingetrokken. Ten eerste is een certificaat maximaal één jaar geldig. Het CIOT verplicht de bevoegde autoriteiten jaarlijks opnieuw een certificaat aan te vragen. Daarnaast kan een autorisatie worden ingetrokken bij uitdiensttreding of wijziging van een functie van een medewerker of vermoedens van fraude.
Het CIOT vereist dat de lokale beheerder van het korps, indien een medewerker de organisatie verlaat, van functie wijzigt of de autorisatie niet meer gebruikt, de autorisatie direct blokkeert en dit schriftelijk aan het CIOT meldt. Na controle wordt het account door het CIOT ingetrokken en wordt via de lokale beheerder de medewerker hiervan schriftelijk op de hoogte gesteld. Het CIOT heeft deze werkwijze voor het intrekken of blokkeren van een account in een formele procedure vastgelegd, als de procedure intrekken CIS-autorisatie[12].

Beoordeling
Het CBP constateert dat de op de autorisatieoverzichten van het CIOT vermelde aantallen geautoriseerde medewerkers bij het korps Haaglanden en de DNR overeenkomen met het aantal feitelijk bij die korpsen geautoriseerde medewerkers. Het CBP stelt vervolgens vast dat conform de eisen van de NEN-norm[13] een CIS-account onder bepaalde omstandigheden kan worden ingetrokken en dat het CIOT een formele procedure kent voor het intrekken van een autorisatie. Hiermee wordt op dit punt in overeenstemming met de NEN-norm en artikel 13 Wbp gehandeld.

4 CONCLUSIE

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

Ten aanzien van de toegang door medewerkers van het CIOT:

- Medewerkers van het CIOT die beheerstaken uitvoeren hebben toegang tot het CIS. Vanuit deze taak om het beheer van het CIS uit te voeren is de toegang van deze medewerkers tot het CIS in overeenstemming met de vereisten van de NEN-norm op dit punt en met artikel 13 Wbp.
- De toekenning van een autorisatie aan het hoofd Exploitatie en Beheer voor het CIS door de directeur van het CIOT is in overeenstemming met artikel 5 lid 2 Besluit en voldoet op dit punt aan artikel 13 Wbp. Het CBP constateert echter dat de autorisaties van de medewerkers die beheerstaken uitvoeren op het CIS niet voldoen aan artikel 5 lid 2 Besluit en derhalve niet rechtsgeldig zijn afgegeven. Dit is in strijd met artikel 13 Wbp.
- De toegang tot het CIS door de directeur en diens plaatsvervanger voor demonstratiedoeleinden is niet overeenkomstig de NEN-norm, omdat zij niet zijn belast zijn met beheerstaken en bovendien het geven van demonstraties

[12] Procedure CIS-accounts CIOT informatiesysteem versie 3.1, ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie, versie 2.0, 11 mei 2007.

[13] NEN-ISO-IEC 27002:2007, 11.2.1 registratie gebruikers, p.70.

niet onder beheerstaken worden geschaard. Hiermee wordt in strijd met artikel 13 Wbp gehandeld.

Ten aanzien van de toekenning van autorisaties aan de bevoegde autoriteiten:

- Het CBP constateert dat de autorisaties van de medewerkers van opsporingsdiensten voor toegang tot het CIS niet voldoen aan artikel 5 lid 1 Besluit en derhalve niet rechtsgeldig zijn afgegeven. Dit is in strijd met artikel 13 Wbp.
- Het CBP stelt vast dat formele procedures voor het registreren en afmelden van gebruikers zijn vastgesteld, overeenkomstig de NEN-norm. Hiermee wordt op dit punt voldaan aan de vereisten zoals gesteld in de NEN-norm en wordt in overeenstemming gehandeld met artikel 13 Wbp.

Ten aanzien van de registratie van autorisaties:

- Tijdens het onderzoek zijn door het CIOT autorisatieoverzichten overgelegd. Het CBP concludeert dat het CIOT beschikt over een formele registratie van de toegekende autorisaties, zoals voorgeschreven in de NEN-norm. Hiermee wordt op dit punt in overeenstemming gehandeld met de NEN-norm en artikel 13 Wbp.

Ten aanzien van de controle op verleende autorisaties:

- Het CBP heeft de van het CIOT ontvangen autorisatieoverzichten vergeleken met het aantal feitelijk geautoriseerde medewerkers van de onderzochte korpsen en concludeert dat deze overeenkomen. Hiermee wordt op dit punt in overeenstemming met artikel 13 Wbp gehandeld.
- Het CBP stelt vast dat conform de eisen van de NEN-norm een CIS-account onder bepaalde omstandigheden kan worden ingetrokken en dat het CIOT een formele procedure heeft vastgelegd voor het intrekken van een autorisatie. Hiermee wordt op dit punt in overeenstemming gehandeld met de NEN-norm en met artikel 13 Wbp.

Deze definitieve bevindingen zijn aldus vastgesteld op 21 april 2011.

Voor het College bescherming persoonsgegevens,

mw.mr.dr. J. Beuving
collegelid

** ** **