COLLEGE BESCHERMING PERSOONSGEGEVENS

Rapport van definitieve bevindingen

Onderzoek van het College bescherming persoonsgegevens (CBP) naar

Bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen

z2009-00672
Mei 2010

Inhoud

Samenvatting

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 Wet bescherming persoonsgegevens (Wbp) ambtshalve onderzoek ingesteld naar de werkwijze van de Sociale Inlichtingen en Opsporingsdienst (SIOD) bij bestandskoppelingen en de ontwikkeling van risicoprofielen ten behoeve van fraudebestrijding in de sociale zekerheid.

Uit het onderzoek blijkt dat de werkwijze van de SIOD in strijd is met de artikelen 10, 13 en 34 Wbp.

Beveiliging
De SIOD heeft geen beveiligingsplan opgesteld en de beveiligingsmaatregelen niet aantoonbaar vastgelegd. Ook zijn geen voorzieningen getroffen voor de beveiligde aanlevering van persoonsgegevens. De SIOD voldoet hiermee niet aan de in artikel 13 Wbp voorgeschreven norm dat de verantwoordelijke passende organisatorische en technische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Bewaartermijnen
De persoonsgegevens die niet meer noodzakelijk zijn voor het doel van de verwerking worden niet verwijderd door de SIOD. Daarmee handelt de SIOD in strijd met artikel 10, lid 1, Wbp.

Informatieplicht
De SIOD heeft de betrokkenen niet geïnformeerd over de verwerkingen. De SIOD weet evenmin of de betrokkenen reeds op de hoogte zijn gebracht van de verwerkingen en heeft dit ook niet gecontroleerd. De SIOD handelt hiermee in strijd met de informatieplicht uit artikel 34 Wbp.

1 Inleiding

Bestandskoppeling vormt een belangrijk instrument bij de fraudebestrijding op het beleidsterrein van het Ministerie van Sociale Zaken en Werkgelegenheid[1]. In dit kader is in 2006 de CBP-notitie "Fraudebestrijding door bestandskoppeling"[2] opgesteld. In deze notitie geeft het CBP aan waarop gelet moet worden bij het vinden van een evenwicht tussen fraudebestrijding en respect voor de persoonlijke levenssfeer. Naar aanleiding van een negatief oordeel[3] van het CBP over een bestandskoppeling ten behoeve van bestrijding van uitkeringsfraude in het kader van een 'Waterproof' project, hebben de Landelijke Stuurgroep Interventieteams (LSI) en het CBP op 27 november 2007 overleg gevoerd over de wijze waarop het koppelen van bestanden binnen de kaders van de Wbp kan plaatsvinden[4]. Daarbij is vastgesteld dat koppeling op basis van risicoprofielen dient plaats te vinden. Met de risicoprofielen kan de noodzaak van een koppeling worden onderbouwd, zoals vereist in de Wbp. In dit kader is afgesproken dat de Sociale Inlichtingen en Opsporingsdienst (SIOD) in pilotverband risicoprofielen gaat ontwikkelen waarbij mede gebruik wordt gemaakt van bestandskoppelingen. Voorts is afgesproken dat bij het ontwikkelen van deze risicoprofielen gebruik wordt gemaakt van Privacy Enhancing Technologies (PET). Dit houdt in dat in een beveiligde omgeving (een zogenoemde black box) met behulp van speciale software, geanonimiseerde persoonsgegevens worden gekoppeld en vergeleken. Op basis van deze koppeling en vergelijking komt een risicoprofiel tot stand. Om te controleren of het aldus tot stand gekomen risicoprofiel in de praktijk ook doelmatig is, worden alleen de gegevens van de personen die behoren tot de risicopopulatie (de 'hits') tot individuele natuurlijke personen herleid. Deze personen zullen vervolgens nader worden gecontroleerd, bijvoorbeeld op mogelijke uitkeringsfraude, met gevolgen voor hun uitkering als van fraude daadwerkelijk sprake blijkt te zijn. De resultaten van deze nadere controle (de daadwerkelijke fraudegevallen) zouden worden teruggekoppeld aan de SIOD. Een risicoprofiel kan worden gevalideerd wanneer duidelijk is welke personen wel en welke niet gefraudeerd hebben. De Wbp vereist dat de betrokkenen worden geïnformeerd over de bestandskoppeling.

In april 2008 is de SIOD gestart met het ontwikkelen van de risicoprofielen. Dit ontwikkelingstraject heeft een looptijd van twee jaar, na ommekomst waarvan een evaluatie van het ontwikkelingstraject en de resultaten van het gebruik in de praktijk plaatsvindt.

De SIOD is een directie van het ministerie van Sociale Zaken en Werkgelegenheid (SZW). De SIOD is in 2002 opgericht als bijzondere opsporingsdienst met als doel de strafrechtelijke handhaving van de wet- en regelgeving op het terrein van werk en inkomen. De SIOD werkt bij de bestandskoppelingen en de ontwikkeling van risicoprofielen samen met interventieteams.

Interventieteams zijn multidisciplinaire teams waarvan de deelnemende organisaties samen werken aan de bestrijding van fraude op het terrein van de sociale zekerheid, de fiscaliteit en de illegale tewerkstelling. Daarnaast richten interventieteams zich, in de zogenaamde 'wijkgerichte aanpak', ook op het signaleren van de behoefte aan - en aanbieden van - maatschappelijke ondersteuning. Binnen interventieteams wordt samengewerkt tussen onder andere de Belastingdienst, het Uitvoeringsinstituut werknemersverzekeringen (UWV), de Arbeidsinspectie (AI), de gemeenten, de Sociale Verzekeringsbank (SVb) , het Openbaar Ministerie (OM) en de

---

[1] *Convenant tussen de Sociale Inlichtingen- en Opsporingsdienst en de Stichting Inlichtingenbureau*, 28 december 2008, Staatscourant 19 januari 2009/11.
[2] *Notitie Fraudebestrijding door Bestandskoppeling*, College bescherming persoonsgegevens, september 2006.
[3] 29 mei 2007, z2006-00476.
[4] Brief van de Staatssecretaris van Sociale Zaken en Werkgelegenheid aan de Tweede kamer, 19 december 2007; UB/A/2007/41263.

SIOD. De afgevaardigden van deze instanties vormen samen de LSI. De LSI neemt besluiten ten aanzien van de interventieteamprojecten en wijst de projectverantwoordelijke partij aan.

Het CBP heeft op grond van artikel 60 Wet bescherming persoonsgegevens (Wbp) een onderzoek ingesteld naar de huidige werkwijze van de SIOD bij het ontwikkelen van risicoprofielen in het kader van de bestrijding van sociale zekerheidsfraude.

2 Procedure

Op 29 mei 2009 heeft de SIOD het CBP de notitie doen toekomen over de voortgang met betrekking tot de bestandskoppelingen en de ontwikkeling van risicoprofielen[5]. Op 25 augustus 2009 heeft het CBP inlichtingen ingewonnen door een onderzoek ter plaatse te verrichten bij de SIOD in Den Haag.

Tijdens het onderzoek ter plaatse heeft het CBP gesproken met technische en leidinggevende medewerkers, waarbij nadere inlichtingen zijn ingewonnen en stukken zijn opgevraagd, die later zijn ontvangen.[6] Na ontvangst van de gevraagde inlichtingen heeft het CBP een analyse uitgevoerd om te bezien of aanvullend onderzoek noodzakelijk was.

Op 2 februari 2010 heeft het CBP de SIOD geïnformeerd over het feit dat het ambtshalve onderzoek heeft ingesteld naar de gegevensverwerkingen die de SIOD uitvoert in het kader van de ontwikkeling van risicoprofielen.

Op 16 februari 2010 heeft het CBP een aanvullend verzoek om inlichtingen aan de SIOD verstuurd. De SIOD heeft de gegevens geleverd op 23 februari 2010.

Op 13 maart 2010 is het rapport van voorlopige bevindingen gestuurd aan de minister van Sociale Zaken en Werkgelegenheid.

Bij brief van 7 april 2010 heeft de minister van Sociale Zaken en Werkgelegenheid een zienswijze gegeven op het rapport van voorlopige bevindingen. De zienswijze heeft op een aantal punten geleid tot het aanpassen van de bevindingen. De conclusie is echter ongewijzigd gebleven.

3 Feiten

3.1 Achtergrond

De SIOD heeft een omgeving ingericht die door de SIOD wordt aangeduid als de 'black box'.[7] In deze black box voert de SIOD in opdracht en ten behoeve van de regionale interventieteams bestandskoppelingen uit en ontwikkelt risicoprofielen met behulp van deze bestandkoppelingen.[8] Een risicoprofiel is een profiel dat een verhoogde kans geeft op bepaalde gedragingen of problematiek (bijvoorbeeld fraude of overlast) op basis van een aantal specifieke indicatoren. Dit gaat als volgt. In een risicomodel worden door een interventieteam specifieke risicofactoren benoemd. Deze factoren vormen tezamen het risicoprofiel. In het model wordt

==========

[5] Sociale Inlichtingen en Opsporingsdienst; Notitie: *Black Box en de ontwikkeling van risicoprofielen*, 27 mei 2009.
[6] E-mails van 10, 11 en 21 september 2009.
[7] Sociale Inlichtingen en Opsporingsdienst; Notitie: *Black Box en de ontwikkeling van risicoprofielen*, 27 mei 2009.
[8] Sociale Inlichtingen en Opsporingsdienst; Notitie: *Black Box en de ontwikkeling van risicoprofielen*, 27 mei 2009.

aangegeven welke persoonsgegevens nodig zijn om de risicofactoren in kaart te brengen en wat de bron is van deze persoonsgegevens (bijvoorbeeld de gemeente, de belastingsdienst etc.).

Vervolgens vraagt de SIOD aan de hand van het risicomodel de benodigde gegevensbestanden op bij de verschillende bronnen en voert daarmee bestandskoppelingen uit. Uit de bestandskoppeling komt een groep personen met een verhoogd risico op fraude naar voren. Dit is de risicopopulatie, oftewel de 'hits'. De gegevens van deze personen c.q. adressen worden aan de deelnemende interventieteams geleverd. In de praktijk zijn dat de betreffende gemeenten. De gemeenten voeren vervolgens nadere controles uit, bijvoorbeeld in de vorm van een huisbezoek, om na te gaan in hoeverre sprake is van daadwerkelijke fraude of overlast bij de personen met een hit. Het is de bedoeling dat het resultaat van deze controle wordt teruggekoppeld aan de SIOD met het oogmerk de risicoprofielen te kunnen valideren. Met de controleresultaten kunnen de onderzoekers van de SIOD het risicoprofiel aanscherpen. Uit een notitie van de SIOD is gebleken dat de resultaten van deze controles echter (nog) niet of nauwelijks aan de SIOD worden geleverd. [9]

In de 2008 en 2009 heeft de SIOD de verschillende interventieteams ondersteund met bestandskoppeling bij in totaal 25 interventieteamprojecten.[10] Het betreft hierbij drie zogenoemde fenomeen projecten, vijftien branchegerichte projecten en zeven zogenoemde wijkgerichte projecten. De drie genoemde typen projecten worden hieronder kort toegelicht.

Fenomeen projecten bestaan in de praktijk uit twee soorten projecten: 'Kadastercheck' en 'Waterproof'. Bij het project Kadastercheck[11] heeft een koppeling plaatsgevonden tussen bestanden van uitkeringsgerechtigden afkomstig van de gemeentelijke sociale diensten en bestanden van het Kadaster. Het doel van deze koppeling is de detectie van vermogensfraude (het niet opgeven van het bezit van onroerend goed door uitkeringsgerechtigden). Bij het project Waterproof [12]zijn gegevens van uitkeringsgerechtigden gekoppeld aan gegevens van waterleidingbedrijven. Doel van deze koppeling is het in kaart brengen van personen die een dusdanig laag waterverbruik hebben dat mogelijk sprake is van woonfraude (iemand heeft een woonadres opgegeven bij de uitkerende instantie maar woont daar waarschijnlijk niet).

De branchegerichte projecten zijn gericht op ondernemingen en alle mogelijk daarbij horende vormen van overtredingen en fraude (vergunningen, tewerkstelling van illegalen, premieafdracht etc.). De nadruk ligt op bepaalde risicosectoren zoals de tuinbouw-, horeca- en schoonmaaksector. Deze projecten zijn primair gericht zijn op ondernemingen en niet op burgers en daarom leveren deze projecten in beginsel weinig risico op voor de privacy van de burgers. Ze blijven daarom verder buiten beschouwing.

Wijkgerichte projecten zijn gericht op uiteenlopende problematiek van overlast, fraude en achterstanden in probleemwijken. De SIOD heeft een risicoprofiel opgesteld voor een zogenaamde 'wijkgerichte aanpak'. Bij een dergelijk wijkgericht project is sprake van een 'integrale aanpak', hetgeen inhoudt dat het doel, naast bestrijding van uitkeringsfraude, ook het bieden van maatschappelijke ondersteuning en het tegengaan van overlast en criminaliteit is. Dat betekent dat naast indicatoren die betrekking hebben op fraude, overlast en criminaliteit ook indicatoren die betrekking hebben op maatschappelijke ondersteuning worden verwerkt.[13] Zo heeft de SIOD bijvoorbeeld bij de leerplichtambtenaar verzuimmeldingen opgevraagd en verwerkt van kinderen in de betreffende wijk.[14] De SIOD heeft ook de gegevens verwerkt van

==========

[9] Sociale Inlichtingen en Opsporingsdienst; Notitie: *Black Box en de ontwikkeling van risicoprofielen*, 27 mei 2009.
[10] Email 10 september 2009.
[11] RCF Noord, LSI Projectvoorstel 6 maart 2008.
[12] Uitgevoerd in Noord Holland en Oost Brabant.
[13] Bijlage bij de email van de SIOD, 23 februari 2010.
[14] Idem.

volwassenen die ouder zijn dan 30 jaar en die na hun 25e weer bij hun ouder(s) zijn gaan wonen. Ook deze verwerking heeft als doel de behoefte aan maatschappelijke ondersteuning in kaart te brengen.
Het oorspronkelijke doel van de (ontwikkeling van de) risicoprofielen was fraudebestrijding in de sociale zekerheid.[15] Door persoonsgegevens te verwerken ten behoeve van maatschappelijke ondersteuning is de doelstelling, en daarmee ook de omvang, van de bestandskoppelingen aanzienlijk verruimd.[16]

De persoonsgegevens die door de SIOD worden verzameld en verwerkt, hebben een gevoelig karakter. Het gaat vaak om uitkeringsontvangers; dit zijn personen die zich in een afhankelijke positie van de overheid bevinden. Daarnaast gaat het in bepaalde gevallen ook om gegevens die verbonden worden aan een vermoeden van uitkeringsfraude, wat een uitgesproken negatieve lading heeft. Onbehoorlijke of onzorgvuldige verwerking van dergelijke persoonsgegevens kan zeer negatieve sociale of maatschappelijke gevolgen hebben voor de personen in kwestie.

3.2 De beveiliging

De door de SIOD als 'black box' aangeduide omgeving is een specifieke digitale omgeving die door technische en organisatorische maatregelen is afgeschermd en die uitsluitend toegankelijk is voor een beperkt aantal functionarissen. In deze omgeving vinden de bestandskoppelingen plaats. Deze black box bevindt zich bij het Inlichtingenbureau in Utrecht. De SIOD en het Inlichtingenbureau[17] hebben op 23 december 2008 een samenwerkingsconvenant[18] ondertekend waarin het Inlichtingenbureau als bewerker in de zin van artikel 1, lid 1, onder e, Wbp wordt benoemd en de SIOD als verantwoordelijke wordt benoemd in de zin van artikel 1, lid 1, onder d, Wbp.

Tijdens onderzoek ter plaatse heeft de SIOD verklaard dat de SIOD geen beveiligingsplan heeft voor de black box en dat over beveiliging nog niets op papier staat, maar dat wel enkele beveiligingsmaatregelen zijn getroffen, bestaande uit een firewall op de servers en toegangscontrole op de servers door middel van een password.

Volgens een notitie van de SIOD zijn met de dataleveranciers afspraken gemaakt om de gegevens op een beveiligde manier aan te leveren.[19] Tijdens het onderzoek ter plaatse verklaarde de SIOD dat er per dataleverancier afspraken vastgelegd worden in een afsprakendocument en dat dit document wordt opgesteld door de SIOD. De SIOD verklaarde tevens tijdens het onderzoek ter plaatse dat de SIOD aanbiedingsbrieven opstelt. In deze aanbiedingsbrieven zouden volgens SIOD ook de beveiligingsafspraken zijn vastgelegd.

==========

[15] Brief van de Staatssecretaris van Sociale Zaken en Werkgelegenheid aan de Tweede kamer, 19 december 2007; UB/A/2007/41263.
[16] Een toetsing van de grondslagen van de verwerkingen die geen fraudebestrijding ten doel hebben doch zien op afgeleide c.q. andere doelen aan artikel 8 Wbp valt buiten de scope van dit onderzoek. Er is dan ook niet onderzocht of er voor de verwerkingen met andere doelen dan fraudebestrijding in de sociale zekerheid een rechtmatige grondslag is.
[17] Stichting Inlichtingenbureau is een met kennis en faciliteiten ondersteunende organisatie voor de regionale interventieteams.
[18] *Convenant tussen de Sociale Inlichtingen- en Opsporingsdienst en de Stichting Inlichtingenbureau*, Staatscourant 19 januari 2009/11. Zie: https://zoek.officielebekendmakingen.nl/stcrt-2009-791.html?zoekcriteria=%3Fzkt%3DEenvoudig%26vrt%3Dstcrt%2B2009%2B11&resultIndex=0&sorttype=1&sortorder=4
[19] Sociale Inlichtingen en Opsporingsdienst; Notitie: *Black Box en de ontwikkeling van risicoprofielen*, 27 mei 2009, pagina 3.

Voorbeelden van beide documenten zijn door de SIOD aan het CBP verstrekt.[20] De documenten bevatten – in tegenstelling tot de verklaring van de SIOD – geen afspraken over het beveiligd aanleveren van gegevens, noch andere beveiligingsafspraken.

3.3 Het bewaren van persoonsgegevens

Tijdens het onderzoek ter plaatse heeft de SIOD verklaard dat alle gebruikte persoonsgegevens bewaard blijven, ook de persoonsgegevens die niet meer noodzakelijk zijn. Dit geldt zowel voor de persoonsgegevens van de personen die tot de risicopopulatie behoren (de 'hits') als voor de persoonsgegevens van personen die niet behoren tot de risicopopulatie (de 'no hits') . Deze gegevens worden derhalve feitelijk niet verwijderd, noch is met betrekking tot het verwijderen van niet-noodzakelijke gegevens schriftelijk iets vastgelegd.

3.4 De informatieplicht

Tijdens het onderzoek ter plaatse heeft de SIOD verklaard dat de SIOD betrokkenen niet informeert over de verwerking van persoonsgegevens en dat het informeren van betrokkenen wordt overgelaten aan de projectleiders van het betreffende interventieteam. Het CBP heeft tijdens het onderzoek geen documenten of aanwijzingen aangetroffen waaruit blijkt dat afspraken zijn gemaakt over het informeren van betrokkenen, noch over een controle op de naleving van de informatieplicht. Er zijn geen waarborgen aangetroffen waaruit blijkt dat betrokkenen worden geïnformeerd. De SIOD verklaarde tijdens het onderzoek ter plaatse over het koppelproject 'Kadastercheck' dat dit project in de krant had gestaan en dat hierdoor betrokkenen over het project geïnformeerd waren.

4 Beoordeling

4.1 De verantwoordelijke

Artikel 1, onder d, Wbp definieert de verantwoordelijke als "de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt."

De SIOD is een directie van het ministerie van Sociale Zaken en Werkgelegenheid. In de publieke sector geldt het bij of krachtens het geldende bestuursrecht bevoegde bestuursorgaan formeel als 'verantwoordelijke' in de zin van de Wbp. Omdat de SIOD als directie onderdeel is van het ministerie van Sociale Zaken en Werkgelegenheid is de minister van Sociale Zaken en Werkgelegenheid formeel de verantwoordelijke voor de gegevensverwerking in de zin van artikel 1, onder d, Wbp.[21]

Het onderzoek richt zich specifiek op de activiteiten van het organisatieonderdeel 'SIOD'. De SIOD bepaalt de doeleinden en de middelen van de verschillende verwerkingen in de black box en maakt afspraken met derde partijen over de verwerking van de persoonsgegevens (koppelprojecten). Bovendien wordt in het convenant[22] tussen de SIOD en het Inlichtingenbureau, de SIOD aangeduid als verantwoordelijke in de zin van artikel 1, lid 1, onder d van de Wbp. Dit convenant is namens de staatssecretaris van Sociale Zaken en Werkgelegenheid ondertekend door , directeur van de SIOD. Het CBP merkt daarom in dit onderzoeksrapport de SIOD aan als de organisatie die, ten aanzien van de verschillende

[20] Afspraken analyse ondersteuning Ede-Veldhuizen, 13 januari 2009 en het uitvraagformulier wijkgerichte aanpak
[21] Memorie van Toelichting bij de Wbp, Kamerstukken II 1997/98, 25.892, nr. 3; pagina 57.
[22] Staatscourant, 19 januari 2009, 2009/11.

verwerkingen in de black box, namens de minister van Sociale Zaken en Werkgelegenheid, in de dagelijkse praktijk verantwoordelijk is voor de naleving van de Wbp. Overigens doet dit niets af aan de verantwoordelijkheid van de interventieteams c.q. de deelnemers aan die interventieteams ten aanzien van de gegevensverwerkingen die in het kader van de interventieteams plaatsvinden. Er is hierbij vaak sprake van een gezamenlijke verantwoordelijkheid voor de verwerking van persoonsgegevens. Dit onderzoek richt zich echter uitsluitend op de rol van de SIOD; interventieteams zijn in dit onderzoek verder niet onderzocht.

4.2 De beveiliging

Artikel 13 Wbp schrijft voor 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. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van de gegevensverwerking.[23] Dit wil zeggen dat deze verplichting niet alleen de black box betreft, maar ook de eisen die de SIOD stelt aan het transport van de gegevens. Dit betekent dat er onder meer afspraken dienen te worden gemaakt over het beveiligd transporteren van de gegevens.

De SIOD heeft enkele beveiligingsmaatregelen ten uitvoer gelegd, bestaande uit een firewall op de servers en toegangscontrole op de servers door middel van een password. In de beoordeling of de beveiligingsmaatregelen zijn aan te merken als 'passend' zijn het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (hierna: VIR)[24] en de Code voor Informatiebeveiliging[25] van belang. Het VIR is van belang omdat dit het beveiligingsvoorschrift voor de rijksoverheid is; het geldt voor alle ministeries en hetgeen daaronder valt, dus ook de SIOD. De Code voor Informatiebeveiliging is van belang omdat dit in de IT sector een algemeen erkend professioneel normenkader is.

Het VIR richt zich op het feitelijk *aantoonbare* niveau van informatiebeveiliging. Het VIR vereist hierbij onder meer dat op basis van een expliciete risicoafweging betrouwbaarheidseisen voor informatiesystemen vastgesteld worden en dat maatregelen getroffen worden, gebaseerd op deze betrouwbaarheidseisen. Voorts dient te worden vastgesteld dat de getroffen maatregelen *aantoonbaar* overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd.[26]

Het VIR sluit aan[27]op de Code voor Informatiebeveiliging[28]. Deze Code stelt dat een 'beleidsdocument voor informatiebeveiliging' behoort tot een van de beheersmaatregelen die worden beschouwd als gebruikelijke praktijk voor informatiebeveiliging.[29]

In het begrip 'passende' uit artikel 13 Wbp ligt onder meer besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip 'passende' duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naar mate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze

==========

[23] Memorie van Toelichting bij de Wbp, Kamerstukken II, 1997-1998, 25 892, nr. 3, pagina 98.
[24] Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007), http://wetten.overheid.nl.
[25] Code voor Informatiebeveiliging, NEN-ISO/IEC 27002:2007 nl.
[26] Artikel 4 van het Besluit voorschrift informatiebeveiliging rijksdienst 2007.
[27] Toelichting op het Besluit voorschrift informatiebeveiliging rijksdienst 2007.
[28] Code voor informatiebeveiliging, NEN-ISO/IEC 27002:2007
[29] Idem, pagina 8 en 15.

worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer met zich brengen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens.[30]

Om de risico's en de bijbehorende eisen aan de beveiliging in het onderhavige onderzoek te bepalen is het van belang dat het koppelen van bestanden door de SIOD *omvangrijke* verwerkingen van persoonsgegevens met een gevoelige aard betreft. Het gaat vaak om personen met een uitkering. Daarnaast gaat het in bepaalde gevallen ook om indicaties van uitkeringsfraude, wat een zeer negatieve lading heeft. Verlies, onbehoorlijke of onzorgvuldige verwerking van dergelijke persoonsgegevens kunnen voor de betrokkenen zeer negatieve sociale of maatschappelijke gevolgen hebben. De context van de gegevensverwerkingen is eveneens gevoelig. Het gaat vaak om een grote groep personen die voor zijn inkomen afhankelijk is van de overheid. Het koppelen van bestanden door de SIOD dient derhalve te worden beschouwd als verwerkingen met een groot risico .

Gelet op het grote risico dat samenhangt met de gegevensverwerkingen, de aard van de gegevens en de context waarbinnen de gegevens verwerkt worden, is een minimale eis om in het kader van de onderzochte gegevensverwerking te voldoen aan het criterium 'passende technische en organisatorische maatregelen' dat er een uitgewerkt beveiligingsplan is opgesteld. Dit volgt uit artikel 13 Wbp, uit het VIR alsmede uit de Code voor informatiebeveiliging.

Het CBP heeft vastgesteld dat bij bestandskoppelingen bij de SIOD sprake is van de volgende tekortkomingen: de SIOD beschikt niet over een uitgewerkt beveiligingsplan en er zijn geen afspraken gemaakt over de beveiligde aanlevering van gegevens. De SIOD voldoet hiermee niet aan de norm in artikel 13 Wbp dat de verantwoordelijke passende organisatorische en technische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

4.3 Het bewaren van persoonsgegevens

Artikel 10, lid 1, Wbp schrijft voor dat persoonsgegevens niet langer bewaard worden in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

De persoonsgegevens die niet meer noodzakelijk zijn worden niet verwijderd door de SIOD. Daarmee handelt de SIOD in strijd met artikel 10, lid 1, Wbp.

4.4 De informatieplicht

In hoofdstuk 5 van de Wbp wordt de informatieplicht beschreven (artikel 33 en 34 Wbp). Deze bepalingen vormen een uitwerking van het transparantiebeginsel en van het in artikel 6 Wbp neergelegde beginsel van 'fair processing': behoudens uitzonderingen is de gegevensverwerking slechts 'behoorlijk' in de zin van artikel 6 Wbp, indien de betrokkene daarvan overeenkomstig de regels van de artikelen 33 of 34 Wbp op de hoogte wordt gebracht. De verplichting van de verantwoordelijke om op eigen initiatief de betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking is een belangrijk instrument om de gegevensverwerking transparant te maken.

Artikel 34 Wbp regelt de situatie waarbij de gegevens buiten de betrokkene om, hetzij bij derden of door eigen waarneming van de verantwoordelijke, worden verkregen. Bij bestandskoppelingen worden persoonsgegevens buiten de betrokkene om verkregen. De in artikel 34 Wbp opgenomen informatieplicht is derhalve op bestandskoppelingen van toepassing.

[30] Memorie van Toelichting bij de Wbp, Kamerstukken II, 1997-1998, 25 892, nr. 3, pagina 99.

Artikel 34 Wbp schrijft voor dat de betrokkenen geïnformeerd dienen te worden over de gegevensverwerking, tenzij zij daarvan reeds op de hoogte zijn. De verantwoordelijke zal zich pas ontslagen mogen achten van zijn informatieplicht als hij weet dat de betrokkene op de hoogte is.[31]

Artikel 1, onder f, Wbp definieert het begrip 'betrokkene' als degene op wie een persoonsgegeven betrekking heeft. Het begrip 'betrokkene' omvat in dezen alle personen die tot de risicopopulatie (de 'hits') behoren, i.e. zowel de personen bij wie door nader onderzoek fraude wordt geconstateerd, als de personen waarbij - al dan niet door nader onderzoek - verder niets wordt geconstateerd dat tot nadere maatregelen leidt.
Dit betekent dat alle personen die tot de risicopopulatie behoren ingevolge artikel 34 Wbp geïnformeerd dienen te worden over de identiteit van de verantwoordelijke en de doeleinden van de verwerking, tenzij zij reeds op de hoogte zijn. Bij koppelingen op persoonsniveau kan niet worden volstaan met informatie vooraf dat de gegevens van een uitkeringsontvanger misschien door middel van bestandskoppeling gecontroleerd zullen worden. Iedere keer als een uitkeringsontvanger op persoonsniveau gekoppeld is, zal de verantwoordelijke de betrokkene achteraf moeten laten weten met welke bestanden is gekoppeld.[32]

Indien wordt overgegaan tot nader onderzoek door de sociale recherche dient de betrokkene, wanneer het onderzoeksbelang dit toelaat, geïnformeerd te worden over de activiteiten die daartoe hebben geleid. Tijdens het onderzoek door de sociale recherche heeft hij recht op informatie over het onderzoek en over zijn rechten als verdachte. In het belang van het onderzoek kan de informatieplicht met een beroep op artikel 43, sub b, Wbp opgeschort worden. Per geval zal moeten worden afgewogen of en hoe lang een beroep op deze uitzonderingsgrond gerechtvaardigd is.[33]

Uitgangspunt is dat de verantwoordelijke de informatie zodanig moet verstrekken dat vaststaat dat de informatie de betrokkene zal bereiken.[34] Advertenties in landelijke of plaatselijke dagbladen zijn niet toereikend om aan te kunnen nemen dat de [alle] betrokkenen zijn geïnformeerd. De context van deze vorm van informatieverspreiding is niet specifiek genoeg om van de betrokkene te verwachten dat hij erop attent is dat voor hem relevante informatie wordt overgedragen. Alhoewel de betrokkene bij eventuele naspeuringen in dergelijke gevallen zou kunnen weten dat mogelijk over hem informatie wordt verwerkt, is de ratio van de bepaling dat hij een dergelijke onderzoeksplicht juist niet heeft .[35]

De SIOD heeft verklaard dat de SIOD de betrokkenen niet informeert, maar dat het informeren wordt overgelaten aan de projectleiders van het betreffende interventieteam. Tijdens het onderzoek van het CBP is niet gebleken dat over dit aspect afspraken zijn gemaakt of dat door de SIOD wordt gecontroleerd of de betrokkenen daadwerkelijk worden geïnformeerd.

De SIOD heeft de betrokkenen niet geïnformeerd. De SIOD weet evenmin of de betrokkenen reeds op de hoogte zijn gebracht van de verwerkingen en heeft dit ook niet gecontroleerd. De SIOD handelt hiermee in strijd met de informatieplicht uit artikel 34 Wbp.

==========

[31] Memorie van Toelichting bij de Wbp, Kamerstukken II, 1997-1998, 25 892, nr. 3, pagina 150.
[32] College bescherming persoonsgegevens, Notitie: *Fraudebestrijding door bestandskoppeling*, september 2006, pagina 6.
[33] idem.
[34] Memorie van Toelichting bij de Wbp, Kamerstukken II, 1997-1998, 25 892, nr. 3, pagina 153.
[35] idem.

5. Zienswijze verantwoordelijke

De inspecteur-generaal heeft op 7 april 2010 namens de minister van Sociale Zaken en Werkgelegenheid schriftelijk een zienswijze gegeven op het rapport van voorlopige bevindingen 'Bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen'. De zienswijze behandelt respectievelijk de beveiliging, het bewaren van persoonsgegevens en de informatieplicht.

5.1 De beveiliging

De namens de minister van Sociale Zaken en Werkgelegenheid ingediende zienswijze stelt dat uit artikel 13 Wbp of uit de Memorie van Toelichting bij dit artikel, niet blijkt dat er een schriftelijk beveiligingsplan aanwezig moet zijn. De ingediende zienswijze geeft daarbij aan dat volgens de Memorie van Toelichting bij de WBP sprake moet zijn van een 'adequate beveiliging'. Volgens de zienswijze is de door de SIOD in 2009 ontwikkelde black box een met veiligheidsmaatregelen omkleed systeem waarin bestanden anoniem worden gekoppeld en waaruit uitsluitend herkenbare resultaten aan de opdrachtgever worden teruggeleverd. De SIOD heeft volgens de zienswijze voldaan aan de wettelijke eis om persoonsgegevens te beveiligen. Tot slot wordt in de zienswijze aangegeven dat uit het oogpunt van transparantie de SIOD evenwel de beveiligingsmaatregelen die bij de black box zijn toegepast, op korte termijn zal beschrijven.

5.2 Het bewaren van persoonsgegevens

De namens de minister ingediende zienswijze bevat een verklaring dat, in tegenstelling tot de eerdere verklaring van de SIOD tijdens het onderzoek ter plaatse, de gegevens worden verzameld en verwerkt in het kader van het 'black box' project, en dat dit project nog niet is afgerond. Dit is de reden waarom de reeds verzamelde gegevens nog worden bewaard. Nadat het project is afgerond zal de SIOD de gebruikte persoonsgegevens verwijderen, aldus de namens de minister ingediende zienswijze.

5.3 De informatieplicht

Ten aanzien van de informatieplicht wordt in de zienswijze bestreden dat de SIOD de verantwoordelijke is voor de verwerkingen. Ter ondersteuning van deze stelling draagt de minister aan dat op grond van de feitelijke situatie, waarin de SIOD ten behoeve van de LSI voor het ontwikkelen van risicoprofielen bestandskoppelingen en risicoanalyses uitvoert, niet kan worden volgehouden dat de SIOD de verantwoordelijke is in de zin van artikel 1, onder d, Wbp. Voorts geeft zienswijze aan dat de SIOD eventueel een afspraak zou kunnen maken met de opdrachtgever over het informeren van betrokkenen. Hierbij wordt aangegeven dat de SIOD niet de bevoegdheid heeft om het informeren van betrokkenen af te dwingen of te controleren.

6. Reactie CBP op zienswijze

6.1 De beveiliging

Artikel 13 Wbp schrijft voor 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. De beveiligingsverplichting strekt zich uit tot

alle onderdelen van het proces van de gegevensverwerking.[36] Dit wil zeggen dat deze verplichting niet alleen de black box betreft, maar ook de eisen die de SIOD stelt aan het transport van de gegevens. Dit betekent dat er onder meer afspraken dienen te worden gemaakt over het beveiligd transporteren van de gegevens.

De Wbp is het algemene wettelijke kader voor de verwerking van persoonsgegevens. Artikel 13 Wbp bevat de norm inzake technische en organisatorische maatregelen. Artikel 13 Wbp kan nader ingevuld worden door sectorale wetgeving. Het in het rapport van bevindingen aangehaalde besluit Voorschrift Informatiebeveiliging Rijksoverheid 2007 (VIR) is te beschouwen als een uitwerking van de, in algemene termen geformuleerde, (informatie)beveiligingsmaatregelen voor de Rijksoverheid en is een voor de Rijksoverheid bindende uitwerking van de norm uit artikel 13 Wbp dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen. Op grond van het VIR dient een rijksoverheidsorganisatie een keuze te maken voor te treffen beveiligingsmaatregelen en dient een rijksoverheidsorganisatie deze maatregelen aantoonbaar vast te leggen en te implementeren.[37] Voorts heeft het CBP reeds in 2001 aangegeven in het rapport 'Beveiliging van persoonsgegevens' dat er een beveiligingsplan moet zijn opgesteld voordat met de verwerking van persoonsgegevens kan worden aangevangen.[38]

De SIOD heeft geen beveiligingsplan en de SIOD heeft evenmin de beveiligingsmaatregelen aantoonbaar vastgelegd. De SIOD heeft enkele beveiligingsmaatregelen ten uitvoer gelegd, bestaande uit een firewall op de servers en toegangscontrole op de servers door middel van een password. Artikel 13 Wbp vereist echter dat de verantwoordelijke passende technische en organisatorische maatregelen neemt, waarbij tevens de gevoeligheid van de gegevens in aanmerking moet worden genomen. Gelet op de tekst van artikel 13 Wbp en de uitwerking daarvan in het VIR, alsmede het voornoemde CBP- rapport 'Beveiliging van persoonsgegevens' uit 2001 kunnen deze maatregelen niet als 'passend' gelden.

De namens de minister ingediende zienswijze stelt dat de beveiligingsmaatregelen uit het oogpunt van transparantie op korte termijn zullen worden beschreven, maar noemt echter geen duidelijke termijn waarbinnen de beveiligingsmaatregelen beschreven zullen zijn.

De zienswijze bevat evenmin een reactie op de bevinding van het CBP dat er geen afspraken zijn gemaakt over het beveiligd leveren van persoonsgegevens aan en door de SIOD. De SIOD handelt hiermee in strijd met artikel 13 Wbp.[39]

6.2 Het bewaren van persoonsgegevens

Het project is opgedeeld in verschillende koppelprojecten. Het is niet noodzakelijk om binnen deze verschillende koppelprojecten persoonsgegevens te bewaren als deze persoonsgegevens bij koppeling geen resultaat in de vorm van een 'hit' hebben opgeleverd.[40] De SIOD heeft tijdens het onderzoek ter plaatse verklaard dat alle gebruikte persoonsgegevens bewaard blijven, ook de persoonsgegevens die niet meer noodzakelijk zijn. De stelling dat de gebruikte persoonsgegevens niet zijn verwijderd omdat deze gegevens worden verzameld en verwerkt in het kader van het black box project dat nog niet is afgerond, is mede in het licht hiervan niet begrijpelijk.

==========

[36] Memorie van Toelichting bij de Wbp, Kamerstukken II, 1997-1998, 25 892, nr. 3, pagina 98.
[37] Toelichting bij het besluit Voorschrift Informatiebeveiliging Rijksoverheid 2007 (VIR), pagina 7.
[38] G. W. van Blarkom en drs. J. J. Borking, *Beveiliging van persoonsgegevens*, Achtergrondstudies en Verkenningen nr. 23, Registratiekamer april 2001, pagina 15.
[39] Volgens de zienswijze zal de SIOD de beveiligingsmaatregelen die bij de black box zijn toegepast, op korte termijn beschrijven. Deze maatregel kan de strijdigheid met artikel 13 Wbp opheffen indien deze beschrijving materieel passend is.
[40] Zie ook: *ANPR Rotterdam- Rijnmond, Onderzoek naar de verwerking van no-hits bij de inzet van Automatic Numberplate Recognition*, College bescherming persoonsgegevens, januari 2010.

De namens de minister ingediende zienswijze geeft geen verklaring waarom het noodzakelijk is om, voor de *gehele* duur (twee jaar) van het totale project, alle binnen dit project gebruikte persoonsgegevens te bewaren. De zienswijze geeft evenmin een (aannemelijke) reden waarom het bewaren van de persoonsgegevens noodzakelijk zou zijn.

Gelet op het gevoelig karakter van de gegevens en de context waarbinnen de gegevens verwerkt worden, is het van groot belang dat de verwerkte persoonsgegevens niet langer te bewaren dan nodig is voor de verwezenlijking van de doeleinden mede ter voorkoming van misbruik c.q. onrechtmatig hergebruik. Misbruik c.q. onrechtmatig hergebruik van dergelijke persoonsgegevens kan immers, gelet op de gevoelige aard van de gegevens, zeer negatieve sociale of maatschappelijke gevolgen hebben voor de personen in kwestie.

Vast staat dat de SIOD persoonsgegevens die niet meer noodzakelijk zijn, niet verwijderd. De SIOD handelt daarmee in strijd met artikel 10 Wbp. [41]

6.3 De informatieplicht

De namens de minister ingediende zienswijze bestrijdt dat de SIOD verantwoordelijke in de zin van de Wbp is maar geeft niet aan welke partij dan wel beschouwd dient te worden als verantwoordelijke. De zienswijze geeft evenmin aan welke partij uitvoering dient te geven aan de informatieplicht (artikel 34 Wbp).

Vast staat dat de SIOD tezamen met anderen de doeleinden (risicoprofielen) en de middelen (bestandskoppelingen in de black box) van de verschillende verwerkingen bepaalt. Bovendien wordt in het samenwerkingsconvenant[42] en de daarin opgenomen bewerkersovereenkomst tussen de SIOD en het Inlichtingenbureau, de SIOD aangeduid als verantwoordelijke in de zin van artikel 1, lid 1, onder d, Wbp. De SIOD is daarmee in praktische zin de verantwoordelijke voor de verwerkingen.

De namens de minister ingediende zienswijze geeft geen aanleiding de bevindingen op dit punt te wijzigen.

Voor wat betreft het in de bevindingen gestelde over de nakoming van de informatieplicht bevat de zienswijze geen reactie op de geconstateerde overtreding van de informatieplicht. Omdat de SIOD de betrokkenen niet geïnformeerd heeft en evenmin weet of de betrokkenen reeds op de hoogte zijn gebracht van de verwerkingen en dit ook niet heeft gecontroleerd, handelt de SIOD in strijd met de informatieplicht uit artikel 34 Wbp.

7. Conclusie

Uit het onderzoek blijkt dat de werkwijze van SIOD in strijd is met de artikelen 10, 13 en 34 Wbp.

Beveiliging
De SIOD heeft geen beveiligingsplan opgesteld en de beveiligingsmaatregelen niet aantoonbaar vastgelegd. Ook zijn geen voorzieningen getroffen voor de beveiligde aanlevering van

[41] Deze strijdigheid wordt opgeheven op het moment dat de gebruikte persoonsgegevens zijn verwijderd. Volgens de zienswijze zal de SIOD de gebruikte persoonsgegevens na afloop van het project verwijderen. Volgens planning zou het project inmiddels afgelopen moeten zijn. De gebruikte persoonsgegevens zouden dientengevolge moeten zijn verwijderd. Dit is niet vastgesteld of onderzocht door het CBP.
[42] Staatscourant, 19 januari 2009, 2009/11.

persoonsgegevens. De SIOD voldoet hiermee niet aan de in artikel 13 Wbp voorgeschreven norm dat de verantwoordelijke passende organisatorische en technische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Bewaartermijnen
De persoonsgegevens die niet meer noodzakelijk zijn voor het doel van de verwerking worden niet verwijderd door de SIOD. Daarmee handelt de SIOD in strijd met artikel 10, lid 1, Wbp.

Informatieplicht
De SIOD heeft de betrokkenen niet geïnformeerd over de verwerkingen. De SIOD weet evenmin of de betrokkenen reeds op de hoogte zijn gebracht van de verwerkingen en heeft dit ook niet gecontroleerd. De SIOD handelt hiermee in strijd met de informatieplicht uit artikel 34 Wbp.