Definitief

Onderzoeksrapportage

Wbp / Black Box

Onderzoek en advies aangaande bestandskoppelingen binnen de regels van de Wet bescherming persoonsgegevens

In opdracht van:
Het Ministerie van Sociale Zaken en Werkgelegenheid

Auteurs:
10 2e

nummer	2016
versie	1.0
datum	© HEC en Zenc, 27 januari 2011

Inhoudsopgave

1. Inleiding

1.1 Aanleiding voor het onderzoek

De interventieteams zijn in 2003 opgericht met als doel om door middel van projecten in branches en wijken illegale tewerkstelling en fraude met belastingen en sociale uitkeringen aan te pakken. In de teams werken de Arbeidsinspectie, de Belastingdienst, het UWV, de Sociale verzekeringsbank, de gemeenten, het Openbaar Ministerie en de Politie samen.
Om een selectie van de te controleren ondernemingen en personen te kunnen maken passen deze teams in de voorbereiding van de projecten in de regel bestandskoppelingen toe.
Elke bestandskoppeling wordt vooraf gemeld bij het College bescherming persoonsgegevens (CBP).

Het CBP heeft in september 2006 een nieuw - op de Wet bescherming persoonsgegevens (Wbp) gebaseerd - toetsingskader voor bestandskoppelingen bij fraudebestrijding vastgesteld. Dit toetsingskader hanteert het CBP bij de beoordeling van de rechtmatigheid van bestandskoppelingen. Dit toetsingskader houdt in dat koppeling van bestanden in de controlefase alleen mag plaatsvinden, indien subjecten zijn geselecteerd op basis van een goed onderbouwd selectieprofiel. Alleen de gegevens van personen die aan het selectieprofiel voldoen, mogen worden gekoppeld.

Naar aanleiding hiervan hebben de Landelijke Stuurgroep Interventieteams (LSI) en het CBP in 2007 afgesproken dat zou worden onderzocht of de bestandskoppelingen op de door het CBP voorgeschreven wijze kunnen worden uitgevoerd. De Sociale Inlichtingen en Opsporingsdienst (SIOD) heeft in opdracht van de LSI tussen april 2008 en april 2010 gewerkt aan het zogenoemde ‘Black Box’-project. De ‘Black Box’ is een professionele en beveiligde organisatorische voorziening waarin door middel van speciale software gegevens geanonimiseerd kunnen worden gekoppeld. Alleen de risicopopulatie wordt herleidbaar gemaakt en teruggeleverd aan de opdrachtgever.

In het kader van dit project heeft de SIOD gewerkt aan de ontwikkeling van risicoprofielen om risicovolle personen te selecteren. De uitkomsten van dit project zijn:

a) voor enkelvoudige vormen van Wet werk en bijstand (Wwb)-fraude zijn met toepassing van de Black Box selectieprofielen ontwikkeld waarmee deze bestandskoppelingen overeenkomstig de Wbp kunnen worden uitgevoerd;
b) voor meer complexe situaties waarin selectieprofielen geen rol kunnen spelen (bijvoorbeeld in wijkgerichte interventieteamprojecten), maakt de beveiligde ‘Black Box’-omgeving het mogelijk dat ook zonder deze profielen koppelingen van persoonsgegevens binnen de kaders van de Wbp plaatsvinden.

Naast het ‘Black-Box’-project dat in april 2010 is afgerond is er ook nog steeds het gebruik van de Black Box als een instrument om op basis van hoogwaardige privacy bevorderende technologie en anonimisering opdrachten uit te voeren voor interventieteamprojecten. Deze onderzoeksrapportage gaat in op beide verschijningsvormen van de Black Box. Dat sluit ook

aan op de vragen van het ministerie van SZW. Het ministerie wilde een extern advies dat zich toespitst op de volgende vragen:

a) Is binnen de regels van de Wbp koppeling van persoonsgegevens ten behoeve van fraudebestrijding ook zónder een voorziening als de ‘Black Box’ mogelijk? Zo ja, aan welke voorwaarden moet dan worden voldaan?

b) Indien het antwoord op a) nee is: aan welke voorwaarden moet een voorziening als de ‘Black Box’ voldoen om de gewenste koppelingen van gegevens toch binnen wettelijke regels te kunnen realiseren?

c) Welke consequenties hebben de conclusies van het ambtshalve onderzoek dat door het CBP in 2009 is ingesteld, voor het gebruik van de ‘Black Box’, met name ten aanzien van wijze waarop aan de in de Wbp opgenomen informatieplicht dient te worden voldaan?

Het ministerie heeft voor het onderzoek een begeleidingscommissie ingesteld. Van deze commissie maken ook partners uit de Landelijke Stuurgroep Interventieteams deel uit.

1.2 Onderzoeksvragen

De drie hoofdvragen beantwoorden wij aan de hand van de volgende onderzoeksvragen:

1) *Wat is het juridisch kader voor bestandskoppeling ten behoeve van fraudebestrijding?*

2) *Hoe werken bestandskoppelingen en de “Black-box’ in de praktijk?*

3) *Wat is het resultaat van de confrontatie norm – praktijk?*

4) *Welke oplossingen zijn mogelijk en onder welke condities?*

1.3 Methode van onderzoek

We voerden het onderzoek uit door middel van documentstudie, interviews en validatiesessies. Onze werkvolgorde was als volgt:

1) *Kick-off met de opdrachtgever en de begeleidingscommissie*
   In de kick-off hebben wij de onderzoeksopzet aan de opdrachtgever en de begeleidingscommissie gepresenteerd en besproken.

2) *Desk research*
   De desk research bestond uit onderzoek ten behoeve van het juridisch kader en studie van de documenten die betrekking hebben op de uitvoering van bestandskoppelingen, de 'Black box' en toepassing. De lijst documenten voor de desk research treft u aan in bijlage 1.

3) *Interviews*
   In bijlage 2 treft u de geïnterviewde partijen.

4) *Analyse en concept rapportage*
   De resultaten uit de desk research en de bevindingen uit de interviews zijn geanalyseerd aan de hand van de onderzoeksvragen. Op basis daarvan is een presentatie met voorlopige bevindingen opgesteld.

5) *Toetsing begeleidingscommissie*
   De voorlopige bevindingen zijn 16 december 2010 getoetst in een bijeenkomst met de begeleidingscommissie.

6) *Presentatie voor de LSI*
   Vervolgens zijn op 16 december 2010 de voorlopige bevindingen ook gepresenteerd en besproken in de bijeenkomst van de Landelijke Stuurgroep Interventieteams.

7) *Afronding en oplevering eindrapport*
   De resultaten van de bespreking met de begeleidingscommissie en stuurgroep zijn verwerkt en het eindrapport is vervolgens op 31 januari nog een keer besproken met de begeleidingscommissie en op 3 februari in de LSI, waarna het is opgeleverd aan de opdrachtgever.

1.4 Leeswijzer

Het onderzoeksrapport bestaat uit de volgende onderdelen:

I. Inleiding
II. Bevindingen en aanbevelingen
III. Normen
IV. Praktijk
V. Confrontatie norm-praktijk

2. Bevindingen en aanbevelingen

2.1 Antwoorden op de opdracht

Vraag 1:
Is binnen de regels van de Wbp koppeling van persoonsgegevens ten behoeve van fraudebestrijding ook zonder een voorziening als de ‘Black Box’ mogelijk? Zo ja, aan welke voorwaarden moet dan worden voldaan?

Antwoord vraag 1:
Ja, binnen de Wbp is koppeling van persoonsgegevens mogelijk zonder Black Box, mits er sprake is van een wettelijke grondslag, dan wel een publieke taak en de koppeling noodzakelijk is om de betreffende taak uit te voeren. In dat geval gaat het om een gerichte koppeling. Ongerichte, algemene koppeling mag alleen als er de garantie is dat de betrokkene niet te identificeren is, zoals – op basis van wat wij hebben gehoord, gelezen en gezien - het geval is bij de koppeling in de Black Box en wat daarna het instrument Black Box is gaan heten.

Vraag 2:
Indien het antwoord op a) nee is: aan welke voorwaarden moet een voorziening als de ‘Black Box’ voldoen om de gewenste koppelingen van gegevens toch binnen wettelijke regels te kunnen realiseren?

Antwoord vraag 2:
Voorwaarde voor de Black Box is dat er de garantie moet zijn dat de algemeen gekoppelde personen in de Black Box niet te identificeren zijn, zodat een geselecteerde, risicovolle groep wel geïdentificeerd kan worden in de fase na de Black Box. Daarnaast dient in de hele keten van het Black Box-traject (van aanleveren tot en met verstrekken) de verwerking van persoonsgegevens zorgvuldig, veilig en toetsbaar plaats te vinden. Dit vergt:

1) Anoniem koppelen.

Dit is het geval op basis van de informatie die we gekregen hebben. Via een audit valt te controleren of dit in de praktijk ook zo is. Wat betreft de Wbp betekent dit dat de koppeling in de Black Box in het geval van anonieme koppeling geen verwerking van persoonsgegevens is.

2) Beveiligd aanleveren van gegevens

Beveiligd aanleveren van gegevens aan de Black Box is volgens de procedures het geval. Of dit in de praktijk zo is, zou ook uit een audit moeten blijken. Ons beeld is dat het aanleveren door landelijke organisaties, zoals de SVB en UWV veilig en zorgvuldig verloopt, maar dat nog niet alle gemeenten een uniforme, zorgvuldige werkwijze hebben. Om van een geheel geanonimiseerd traject te kunnen spreken zou het helemaal mooi zijn als ook de aanlevering geanonimiseerd of gepseudonimiseerd zou kunnen plaatsvinden door versleuteling aan de bron door de aanleverende partij. Maar dat is in de praktijk op dit moment een stap te ver. Wat betreft de Wbp betekent dit dat het aanleveren van de persoonsgegevens aan de Black Box

(zowel voor afgeronde project als voor het nog in werking zijnde instrument) wel onder de Wbp valt. En dat geldt ook voor de identificerende gegevens die “naast” de geanonimiseerde koppeling bewaard worden voor de latere koppeling van de hits aan identificerende gegevens.

3) Beveiligd verstrekken van gegevens uit de Black Box.

Het betreft hier de zogenaamde “hits”. Er dient extra aandacht te zijn voor de “no hits” die bewaard blijven gedurende een project. Vandaar het belang van een vernietigingsprotocol waaruit blijkt dat die gegevens niet langer worden bewaard dan noodzakelijk is gelet op het doel waarvoor deze gegevens verkregen zijn. Inmiddels is een vernietigingsprotocol aanwezig.

Conform het eveneens inmiddels verschenen beveiligingsplan is het verstrekken van de “hits”aan de ontvangende projecten voldoende beveiligd. Of dat in de praktijk zo is, kan via een audit bewezen worden. Ook het verstrekken van gegevens gebeurt (nog) niet geanonimiseerd of gepseudonimiseerd, zodat het verstrekken van de “hits” aan de verantwoordelijke(n) voor het betreffende project een verwerking van persoonsgegevens is. De Wbp is daarop dus van toepassing, inclusief de informatieplicht.

4) Functiescheiding

Functiescheiding is voor de veiligheid en zorgvuldigheid bij de verwerking van gegevens via de Black Box van groot belang. Dat is in de huidige praktijk al het geval door scheiding tussen de SIOD en het Inlichtingen Bureau.

5) Audits aan de hand van toetsbare normen en processen

Er heeft (nog) geen audit plaatsgevonden op de Black Box zelf en ook (nog) niet van de gegevensverwerking van het gehele Black Box traject (van aanleveren tot en met verstrekken). Wij raden aan deze audits voor te bereiden en periodiek te laten plaatsvinden. Dat vergt toetsbare normen en processen.

Vraag 3:

Welke consequenties hebben de conclusies van het ambtshalve onderzoek dat door het CBP in 2009 is ingesteld, voor het gebruik van de ‘Black Box’, met name ten aanzien van wijze waarop aan de in de Wbp opgenomen informatieplicht dient te worden voldaan?

Antwoord vraag 3:

Wat betreft de informatieplicht zijn er verschillende fases te onderscheiden:

<u>Fase 1: Aanleveren van persoonsgegevens door de verantwoordelijke (n), gezamenlijk of afzonderlijk aan de Black Box ten behoeve van fraudeonderzoek in het algemeen of voor een speciaal thema</u>.

Er geldt een informatieplicht. Via heldere wet- en regelgeving en/of via (algemene) informatie over mogelijk fraudeonderzoek en mogelijke thema’s kan hier invulling aan worden gegeven.

Op dit moment is (nog) niet helder wie in fase 1 de verantwoordelijke(n) is of zijn. Wij doen bij de aanbevelingen de suggestie om er naar te streven dat de LSI in die positie kan en mag komen. Zolang dat niet geregeld is, is iedere partij afzonderlijk verantwoordelijke voor het geven van (algemene) informatie over de mogelijkheid dat gegevens voor fraudeonderzoek worden gebruikt, dan wel ten behoeve van een speciaal thema.

Fase 2: Koppelen in de Black Box
Gebeurt anoniem, althans op basis van de informatie die we hebben gekregen. Als het anoniem is, dan is er in deze fase geen verwerking van persoonsgegevens, geen verantwoordelijke en geen sprake van een informatieplicht voor deze koppeling.
Het (tijdelijk) bewaren van de persoonsgegevens valt wel onder de Wbp en betreft de gegevens die al zijn aangeleverd en de informatieplicht die daarbij hoort. Dat zou de LSI dus weer kunnen zijn, zodra dat mag en kan, de afzonderlijke aanleverende organisaties en een variant zou ook nog kunnen zijn dat de Minister van SZW optreedt als verantwoordelijke. Dat is mogelijk, maar raden wij af, omdat de Minister van SZW slechts zeggenschap heeft over de SIOD, maar niet over het IB, laat staan alle andere betrokken partijen.

Fase 3: Het verstrekken van de “hits” en bijbehorende persoonsgegevens
In de praktijk worden die gegevens verstrekt aan de projectleider van een interventieteamproject, die optreedt namens de verantwoordelijken die bij het project betrokken zijn.

Er worden persoonsgegevens verwerkt. Er is dus in beginsel een informatieplicht. Artikel 43 sub b Wbp heeft – mede op grond van de interpretatie die het CBP hieraan heeft gegeven - een opschortende werking in verband met het voorkomen van strafbare feiten. Achteraf moeten de personen over wie persoonsgegevens zijn verwerkt wel worden geïnformeerd door de verantwoordelijke. Eventueel is dit ook – mede – te regelen in heldere wet- en regelgeving.

Wie is hier de verantwoordelijke? Er zijn diverse scenario’s voor de vraag wie verantwoordelijke is:

Scenario 1:
De verstrekkende organisaties en de ontvangende partijen in de LSI en de LSI treedt op als verantwoordelijke zodra dat mag en kan.

Scenario 2:
Zowel de verstrekkende partijen als de ontvangende partijen zijn afzonderlijk verantwoordelijke en moeten de informatieverstrekking achteraf ieder afzonderlijk of in gezamenlijk overleg regelen. Op lokaal niveau kan bijvoorbeeld het College van B&W de verantwoordelijke partij zijn. Bij de Black Box als project was dat ook het geval. Bij de Black Box als instrument zijn er andere (lokale) verantwoordelijken denkbaar.

2.2 Bevindingen

2.2.1 Verantwoordelijke en bewerker

I. Zowel voor de Black Box als project als voor de Black Box als instrument is niet duidelijk wie verantwoordelijke(n) is/zijn en wie (sub)bewerkers zijn (zie 5.1).
II. Het “Convenant tussen de SIOD en het IB”, met als bijlage de “bewerkersovereenkomst tussen beide partijen, gaat er ten onrechte van uit dat de SIOD verantwoordelijke is in de zin van de Wbp en het IB bewerker (zie 5.1).
III. Het LSI is (nog) geen rechtsvorm die het mogelijk maakt om als (gezamenlijke) verantwoordelijke op te treden (zie 5.1).

IV. Een risico is dat als de (gezamenlijke) verantwoordelijke per project wordt bepaald niemand integraal en duurzaam verantwoordelijke is voor de Black Box als zodanig en voor de (te vernietigen) bestanden waar zij naast de geanonimiseerde koppeling gebruik van maken (zie 5.1).

2.2.2 Bestandskoppelingen

I. Niet het hele proces in de keten van de Black Box – van persoonsgegevens leveren aan de Black Box tot en met het verstrekken van de “hits” aan de projecten – verloopt anoniem (5.2)
II. De Black Box is als methode om te anonimiseren en tot een risicomodel te komen vanuit het oogpunt van de Wbp beter dan vele overige praktijken van bestandkoppelingen in het kader van interventieteams (zie 4.1.3)
III. De (clusters van) indicatoren waarmee gekoppeld wordt zijn (nog) niet transparant voor de leden van de LSI en daar buiten. Hoe het precies werkt dient geheim te blijven, maar op hoofdlijnen is meer informatie over de (clusters van) indicatoren gewenst (zie 4.1.2)
IV. Bij de koppeling tussen de “hits”en de identificerende gegevens kan gesteld worden dat informatieverstrekking achteraf volstaat. Van belang is dat ook degenen die wel een “hit” hadden, maar geen fraude blijken te hebben gepleegd hiervan op de hoogte worden gesteld (zie 5.2)

2.2.3 Informatieplicht

I. Bij het door de verantwoordelijke(n) leveren van gegevens aan de Black Box kan zowel bij het project als het instrument worden volstaan met het verstrekken van algemene informatie vooraf over controle op fraude en zodra er themagericht onderzoek wordt gedaan met informatie per thema (zie 5.3)
II. Bij anonieme gegevensverwerkingen is er geen informatieplicht (zie 5.3).
Door in wet- en regelgeving helder te benoemen wie waarvoor en met welk doel verantwoordelijke is kan de plicht om mensen persoonlijk te informeren worden ondervangen (zie 5.3)
III. D**e** landelijke cliëntenraad en de lokale cliëntenraden hebben op dit moment nog geen rol bij de informatieverstrekking.

2.2.4 Meer toezicht

I. Er is nog geen audit gehouden op – de keten van – de Black Box, noch als project, noch als instrument (zie 5.4).
II. Er zijn nog geen toetsbare normen en processen om te auditen (zie 5.4).

2.2.5 Betere communicatie

I. Er leven verschillende beelden over wat de Black Box nu precies is (zie hoofdstuk 4).
II. Het project en de reguliere werkwijze worden door elkaar gehaald.
III. Er is geen gedeeld beeld over de onderzoeken die met behulp van deze techniek zijn uitgevoerd (zie hoofdstuk 4).
IV. Er is niet vastgelegd waarvoor de techniek nu precies geschikt is (zie hoofdstuk 4).
V. Het risicomodel dat in de Black Box als project en instrument wordt gehanteerd staat niet op papier (zie hoofdstuk 4).

2.3 Aanbevelingen

2.3.1 Verantwoordelijke en bewerker

I. Zorg dat er een partij komt die integraal en duurzaam verantwoordelijke is in de zin van de Wbp is voor het Black Box als instrument.
II. Probeer te zorgen dat de LSI als (gezamenlijke) verantwoordelijke kan en mag functioneren namens de deelnemende partijen. Daarmee raden wij het door sommige respondenten ook wel geopperde alternatief om de Minister van SZW de verantwoordelijke voor het Black Box-traject met de interventieteams te laten zijn af. We raden dit af, omdat de minister van SZW heeft geen gezag heeft over het IB (waar de Black Box staat) en ook niet over vrijwel alle andere partijen die betrokken zijn bij het Black Box-traject.

    Uit de feiten en uit de samenwerkingsovereenkomst blijkt dat de LSI feitelijk de opdrachtgever is en de projectvoorstellen toetst. Op dit moment is de LSI in juridische zin echter nog niets (hoewel artikel 43c van de Uitvoeringsregeling Awr er al naar verwijst). Dat leidt tot de navolgende extra aanbevelingen.
III. Probeer van alle deelnemers aan de LSI een volmacht of mandaat te krijgen dat zij in de LSI namens hun organisatie(s) besluiten mogen nemen over de verwerking van persoonsgegevens door de interventieteams met behulp van de Black Box als instrument.
IV. Geef de LSI een juridische status – als verantwoordelijke in de zin van de Wbp - in wet- en regelgeving. Ter inspiratie: kijk in de huidige wetgeving bijvoorbeeld naar artikel 20 Wpg; artikel 43c Uitvoeringsregeling Awr, artikel 62 lid 3 SUWI.
V. Zodra de LSI inderdaad als verantwoordelijke in de zin van de Wbp kan bepalen hoe interventieteams met behulp van de Black Box met persoonsgegevens moeten omgaan, kan de LSI ook een bewerkerscontract afsluiten met de SIOD (of eigenlijk de Minister van SZW) en een subwerkerscontract met het IB (eigenlijk). Bij de anonieme bestandskoppeling worden weliswaar geen persoonsgegevens verwerkt, maar er worden door de SIOD tegelijkertijd wel identificerende gegevens bewaard om later te kunnen koppelen met de ‘hits’ na de geanonimiseerde bestandskoppeling. Alleen al om die reden moet er in ieder geval wel een bewerkerscontract afgesloten worden. Bovendien worden die ‘hits’ met identificerende gegevens vervolgens door

de SIOD verstrekt aan de betreffende projectleider (namens de betreffende – verantwoordelijke – partijen). Ook dat is een verwerking die onder de Wbp valt en instructies van de verantwoordelijke vergt. Idealiter wordt de LSI die verantwoordelijke.

VI. Alternatief is dat alle deelnemers in de LSI ieder afzonderlijk als verantwoordelijke fungeren. In dat geval zal ieder van hen afzonderlijk een (sub)bewerkerscontract met de SIOD / Minister en het IB moeten sluiten.

VII. Wij raden aan het huidige "Convenant tussen de SIOD en het IB" , met als bijlage de "bewerkersovereenkomst tussen beide partijen" te herzien.

VIII. Wij raden aan een onderscheid te maken tussen:

- het (landelijk) aanleveren van gegevens aan de Black Box;
- het landelijk bij de Black Box als instrument geanonimiseerd koppelen van de data;
- het verstrekken van de 'hits' naar het lokale niveau het College van B&W als verantwoordelijke;
- het verstrekken aan een bepaalde branche of andere deelnemer van de interventieteams.

2.3.2 Bestandskoppelingen

I. Gebruik voor de interventieteams de Black Box als instrument om anoniem te kunnen koppelen met een risicomodel. Selectieprofielen zijn daarbij mogelijk, maar niet noodzakelijk.

II. Zorg dat tenminste voor de LSI de (clusters van) indicatoren waarmee gekoppeld Wordt op hoofdlijnen transparant zijn.

2.3.3 Informatieplicht

I. Daar waar mogelijk te anonimiseren, dan is er in beginsel geen informatieplicht.

II. Duidelijk wettelijk te regelen wie verantwoordelijke is voor welk doel bij de bestandskoppelingen (via de Black Box) ten behoeve van de interventieteams. Ook in dat geval is er grosso modo geen informatieplicht, dan heeft de wetgever daar al in voorzien. Hoewel algemene informatie dan nog wel gewenst blijft.

III. De landelijke cliëntenraad en de lokale cliëntenraden een rol geven bij de algemene informatieverstrekking om zich beter in te kunnen leven in de positie van de cliënt en om het noodzakelijke vertrouwen te winnen.

IV. Bij het aanleveren van gegevens aan de Black Box zorgen dat de (gezamenlijke) verantwoordelijke(n) algemene informatie geven, bij de algemene ongerichte koppeling (blijven) zorgen voor anonimisering en bij het verstrekken van de hits met identificerende gegevens zorgen voor informatieverstrekking achteraf aan de onderzochte personen.

2.3.4 Meer toezicht

I. Werken aan toetsbare normen en processen en vervolgens een audit te (laten) doen op Black Box, bijvoorbeeld via de Functionaris Gegevensbescherming van SZW.

II. Ook audit te laten doen bij het IB op het naleven van normen en processen.

2.3.5 Betere communicatie

I. In het algemeen raden we aan meer aandacht te besteden aan de communicatie tussen de partijen die deelnemen aan het Black-Box-traject.
II. Wij ondersteunen voor de nabije toekomst de aanbeveling die de Landelijke Cliënten Raad ons tijdens de interviews gaf om een Gedragscode (eventueel zelfs in de zin van de Wbp) op te stellen waarin op een heldere wijze is vastgelegd hoe de Black Box als instrument op hoofdlijnen werkt en behoort te werken (zonder de geheime operandi modus voor fraudebestrijding prijs te geven.

3. Normen

3.1 Persoonsgegeven

In artikel 10, tweede en derde lid, van de Grondwet is de opdracht neergelegd tot het opstellen van wetgeving ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. In de Wbp zijn de algemene regels voor het verwerken van persoonsgegevens vastgelegd. Verderop in dit hoofdstuk komen ook specifieke sociale zekerheidswetten, de Wet politiegegevens en de Algemene wet rijksbelastingen (Awr) aan de orde.

Het centrale begrip in de Wbp is ‘persoonsgegeven’. Indien sprake is van persoonsgegevens, dan heeft de verantwoordelijke - degene die bepaalt wat er met de persoonsgegevens gebeurt - plichten en mogelijkheden om persoonsgegevens te verwerken op grond van de Wbp. De betrokkene (cliënt) heeft rechten waaraan de verantwoordelijke dient te voldoen. De relevante begrippen worden toegelicht en zo mogelijk wordt bij een begrip aangegeven wat dit concreet betekent voor de Black Box als project en instrument.

Artikel 1, onder a Wbp: Persoonsgegeven
Het begrip ‘persoonsgegeven’ is waar het om draait bij de Wbp. Als er geen sprake is van persoonsgegevens, is de wetgeving niet van toepassing. De Wbp verstaat onder een persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Als de Black Box zodanig technisch en organisatorisch is ingericht dat de koppeling van de gegevens zodanig is geanonimiseerd dat er geen persoonsgegevens worden gekoppeld, dan is de Wbp voor die koppeling niet van toepassing.

Artikel 1, onder b, Wbp: Verwerken van persoonsgegevens
Het begrip verwerken van persoonsgegevens is in artikel 1, onder b, omschreven als: *“elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.”*
Korter gezegd: alles wat met persoonsgegevens wordt gedaan: van verzamelen tot en met vernietigen. Voor de Black Box betekent dit dat zodra er ergens in de keten van het aanleveren van gegevens aan tot en met het verstrekken van gegevens uit de Black Box persoonsgegevens worden gewerkt, de Wbp in beginsel van toepassing is voor de betreffende verwerking.

3.2 Verantwoordelijke

Als er persoonsgegevens worden verwerkt in - de keten van - het Black Box-project of de Black Box als instrument dan zijn er ook verantwoordelijke(n) in de zin van de Wbp. Wanneer is dat het geval en wat betekent dat?

Artikel 1, onder d, Verantwoordelijke
In de Wbp gelden alle verplichtingen voor de verantwoordelijke, terwijl eveneens de betrokkene (hier: de cliënt) zijn rechten kan vorderen jegens de verantwoordelijke. Met andere woorden: alle bepalingen (ook de bepaling betreffende de informatieplicht) in de Wbp richten zich op de verantwoordelijke.
Het begrip verantwoordelijke wordt in artikel 1, onder d, Wbp omschreven als de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Oftewel degene die macht kan uitoefenen over de persoonsgegevens.

Hoe meer organisaties gezamenlijk verantwoordelijke zijn, hoe complexer de verantwoordelijkheidsvraag zal worden.

De bepalingen uit de Wbp kunnen voor verantwoordelijke(n) worden samengevat in zeven beginselen. Bij ieder beginsel wordt aangegeven wat dit concreet voor de Black Box kan betekenen.

1. Transparantie
Het gaat hierbij om het principe dat de cliënt door de verantwoordelijke op de hoogte gesteld hoort te zijn van het feit dat gegevens over hem worden verwerkt en voor welk doel. Alleen als de cliënt op de hoogte is dat gegevens over hem worden verwerkt, is deze in staat om desgewenst van zijn rechten gebruik te maken.

Concreet vloeit uit het transparantiebeginsel in administratieve zin de plicht voort om verwerkingsprocessen te melden bij het CBP, tenzij zij zijn vrijgesteld[1]. Zowel bij het aanleveren van gegevens aan de Black Box, als de verwerkingen in de Black Box als bij het verstrekken van gegevens uit de Black Box aan een project is het de vraag of er een verantwoordelijke is die een melding moet doen bij het CBP.

Daarnaast vloeit uit het transparantiebeginsel bijvoorbeeld voort dat de cliënten op de hoogte gebracht moeten worden van het feit dat zijn/haar persoonsgegevens ten behoeve van fraudeonderzoek worden verwerkt. In hoeverre op grond van de feiten de informatieplicht geldt in de verschillende fasen van de Black Box als project en als instrument komt later aan de orde. Binnen het Black Box traject kunnen er verschillende verantwoordelijken zijn.

[1] Via www.cbpweb.nl is een meldingsformulier te downloaden.

2. Doelbinding
Het doelbindingsbeginsel vereist dat de persoonsgegevens slechts worden verzameld voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden (geen blanco cheque, of vage doelen), dat niet meer gegevens worden verwerkt dan voor die doeleinden noodzakelijk zijn en dat deze gegevens niet worden gebruikt voor doeleinden die daarmee niet verenigbaar zijn. Bovendien mogen de gegevens, op grond van artikel 10 Wbp, ook niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor de gegevens worden verwerkt. Indien voor de Black Box (tijdelijk) persoonsgegevens worden bijgehouden, naast de al dan niet geanonimiseerde koppeling – dienen deze vernietigd te worden zodra zij niet meer noodzakelijk zijn gelet op het doel waarvoor de werden verkregen. Er zal dus een vernietigingsprotocol moeten zijn. Het bepalen van wat een noodzakelijk termijn is, dient de verantwoordelijke(n) zelf vast te stellen op basis van goede argumenten. Zij kunnen daarvoor eventueel te rade bij de betrokken professionals. De centrale vraag is dan “hoe lang persoonsgegevens bewaard dienen te worden in een vorm die het mogelijk maakt de betrokkene te identificeren gelet op wat noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt”, in de zin van artikel 10, eerste lid, Wbp.

3. Rechtmatige grondslag
Er is een rechtmatige grondslag voor de verwerking van cliëntgegevens indien minimaal aan één van de volgende grondslagen is voldaan:

1. Toestemming van de cliënt
Bij toestemming gaat het steeds om een vrije gerichte toestemming die op toereikende informatie berust. Toestemming van de cliënt als grondslag is bij de Black Box-projecten niet erg waarschijnlijk.

2. De uitvoering van een overeenkomst waarbij de cliënt partij is
Ook niet echt waarschijnlijk bij de Black Box als project of instrument.

3. De nakoming van een wettelijke verplichting
Als er een wettelijke grondslag is. Voor veel bestandkoppelingen bestaat er een wettelijke grondslag, zoals we nog zullen zien, maar voor het afgeronde Black Box-project en de bestaande praktijk van de Black Box als instrument bestaat er (nog) geen specifieke wettelijke grondslag.

4. Een vitaal belang (calamiteiten, nood breekt wet)
Deze rechtvaardigingsgrond mag echter niet aangewend worden voor structurele gegevensverwerkingen. Deze rechtvaardigingsgrond zal daarom in beginsel niet van toepassing zijn op de Black Box.

5. Noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door een bestuursorgaan
Zie de gemaakte opmerkingen bij het nakomen van een wettelijke verplichting..

6. Een gerechtvaardigd belang van degene die verantwoordelijk is voor de gegevensverwerking, terwijl het belang van de cliënt niet wordt geschaad.
Deze laatste bepaling is een zogenaamde “restbepaling”, die alleen gehanteerd mag worden als alle andere mogelijkheden zijn uitgeput en dan alleen nog voor goed beargumenteerbare uitzonderingsgevallen.

4. Kwaliteit van gegevens
De gegevens moeten toereikend, ter zake dienend en niet overmatig zijn in relatie tot het doel waarvoor ze worden verwerkt. De gegevens dienen ook nauwkeurig te zijn en zonodig te worden bijgewerkt. In dit verband dienen alle redelijke maatregelen te worden getroffen om tekortkomingen te herstellen. Bij samenwerkingsverbanden gaat het bij de kwaliteit van de gegevens vaak om de vraag in hoeverre de kwaliteit van gegevens te beheersen is en of de gegevens inderdaad juist zijn.

5. Beveiliging
Op grond van artikel 13 Wbp geldt er voor de verantwoordelijke een beveiligingsplicht. De verantwoordelijke zal voor passende organisatorische en technische maatregelen moeten zorgen tegen verlies van gegevens en tegen iedere vorm van onrechtmatige verwerking. Ook zullen er inspanningen dienen te worden verricht om te zorgen dat er zo min mogelijk persoonsgegevens worden verwerkt. Privacybevorderende technieken kunnen daarbij behulpzaam zijn. Denkbaar is bijvoorbeeld dat met pseudoniemen gewerkt wordt. In de studie nr. 23 Beveiliging van persoonsgegevens heeft het CBP (eigenlijk nog de Registratiekamer, 2001) de algemene beveiligingsplicht enigszins concretere invulling gegeven aan de hand van risicoklassen. Gegevens van wettelijk geregelde geheimhouders (politie, belasting, etc.) zitten in de hoogste risicoklassen.

6. Rechten van de cliënt
De Wbp geeft de cliënt de volgende rechten ten opzichte van de verantwoordelijke:

a) Het recht op inzage: de wettelijke termijn om hieraan te voldoen bedraagt vier weken. Bij het Black Box-project en instrument kan er in een bepaalde fase in de keten ook sprake zijn van een inzagerecht. Het recht op inzage is niet absoluut, op goede gronden kan er vanaf geweken worden.
b) Het recht op correctie: onjuiste of onvolledige gegevens moeten op verzoek worden gecorrigeerd. Hiervoor geldt bij de Black Box hetzelfde als bij de inzage.
c) Het recht op verwijdering: door de cliënt kan gevraagd kan worden bepaalde gegevens of alle gegevens betreffende zichzelf te laten verwijderen. Idem als bij inzage en correctie.
d) Het recht op afscherming: idem.
e) Het recht op verzet: de betrokkene kan verzoeken bepaalde gegevens of alle gegevens betreffende zichzelf niet meer te verwerken, idem.
f) Naast al deze rechten heeft de cliënt bij verschillende deelnemers het recht op geheimhouding, bijvoorbeeld als belastingbetaler op grond van artikel 67, eerste lid, van de Awr. Dit betekent dat gegevens die de Belastingdienst heeft verzameld geheimgehouden dienen te worden. In de ‘Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994’ is in artikel 43c echter een bepaling opgenomen die de geheimhoudingsverplichting doorbreekt. Ook geheimhouding is dus niet absoluut geregeld.

Het inwilligen van de verzoeken om cliëntenrechten gehonoreerd te krijgen moet controleerbaar zijn.
De genoemde rechten zijn relatief. Met goede argumenten mag hiervan afgeweken worden. Of de argumenten goed zijn kan eerst het CBP bepalen en uiteindelijk de rechter.

7. Bijzondere gegevens

Verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden, tenzij de wetgever daarvoor een ontheffing heeft verleend in de artikelen 17 tot en met 23 Wbp. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag.

3.3 Bewerker

Artikel 1, onder e, Bewerker
Overeenkomstig artikel 1, onder e, Wbp is een bewerker degene die voor de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag onderworpen te zijn. Bewerker is degene die voor de verantwoordelijke persoonsgegevens verwerkt, zonder dat hij diens ondergeschikte is.
De bewerker verwerkt gegevens voor de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid.
De verantwoordelijke die gegevens buiten zijn rechtstreeks gezag verwerkt wil hebben is op grond van artikel 14, tweede lid, Wbp verplicht een overeenkomst met de bewerker aan te gaan, het zogenaamde bewerkerscontract.

Of er een bewerker is in de keten van de Black Box als project of instrument moet uit de feiten blijken. Eerst dient duidelijk te zijn wie er verantwoordelijke(n) voor de gegevensverwerkingen zijn in de eventueel verschillende fases in de keten. Vervolgens kan bepaald worden of die verantwoordelijken gebruik maken van (sub)bewerkers die volledig op basis van de instructies van de verantwoordelijke(n) hun werkzaamheden uitvoeren op basis van een bewerkerscontract.

3.4 "Niets"

Als er geen enkele macht over de persoonsgegevens kan worden uitgeoefend is de Wbp niet van toepassing.[2]
Vanuit dit perspectief zou idealiter de hele gegevensverwerking van de Black Box (van het aanleveren van de gegevens tot en met het verstrekken van de treffers op basis van een "hit") zo kunnen worden ingericht dat geen enkele feitelijke macht uitgeoefend kan worden over de persoonsgegevens.

3.5 Juridisch kader bestandskoppelingen

De Memorie van Toelichting (MvT) van de Wbp stelt op p.93/94 over bestandskoppelingen in relatie tot de Wbp het volgende:
" In het algemeen zal gelet op de toepasselijkheid van de eis van verenigbaar gebruik vooral gezocht moeten worden naar zodanige vormen van verwerking dat de mogelijk vast te stellen gegevens niet buiten de kring van personen bekend worden dan ten behoeve van wie de koppeling heeft plaatsgevonden. Zo is denkbaar dat twee bestanden van twee verschillende verantwoordelijken tegen elkaar moeten worden afgedraaid om te zien of er dubbelen inzitten, zonder dat één van de verantwoordelijke daarmee komt te beschikken over alle gegevens van de ander. Technisch kan de vergelijking van de gegevens als het ware in een ***"black box"*** *plaatsvinden, waarbij mogelijke treffers aan één van beide verantwoordelijken worden meegedeeld.*

Een voorbeeld is de vergelijking van het gedetineerdenbestand en het bestand van de ontvangers van een sociale uitkering. Wanneer geen aanspraak bestaat op een uitkering in geval van detentie, kunnen beide bestanden worden vergeleken met als resultaat dat eventuele treffers worden bekend gemaakt aan het desbetreffende uitvoeringsorgaan van de sociale zekerheid. Het is daartoe niet nodig dat penitentiaire inrichtingen kennis nemen van het bestand van uitkeringsgerechtigden of de uitvoeringsorganen van de sociale zekerheid kennis nemen van de gehele gedetineerdenadministratie. Dit dient dan door technische en organisatorische maatregelen te worden voorkomen. De verstrekking van treffers aan het desbetreffende uitvoeringsorgaan vindt in dat geval zijn rechtvaardiging in de opdracht de criteria voor de toekenning van een uitkering toe te passen. In dit geval vertoont het doel van de koppeling een zodanig nauwe verwantschap met het oorspronkelijke doel waarvoor het uitvoeringsorgaan de gegevens heeft verkregen dat – mede gelet op de voorzieningen die zijn getroffen om de verspreiding van de gegevens te beperken tot het noodzakelijke minimum – sprake is van verenigbaar gebruik. Anders ligt de situatie wanneer gekoppeld wordt voor een doel dat relatief ver verwijderd ligt van het doel waarvoor de gegevens zijn vergaard. In dat geval zal – los van de koppelingen die hun grondslag kunnen vinden in artikel 43 – veel eerder sprake zijn van onverenigbaar gebruik.

---

2 Zie de toelichting bij artikel 1, onder b, Wbp over 'handelingen met persoonsgegevens', in: Theo Hooghiemstra en Sjaak Nouwt, Tekst en toelichting Wet bescherming persoonsgegevens' derde herziene druk, 2007, Sdu uitgevers, p. 36.

Tot zover wat er in de MvT van de Wbp al over een “Black Box” in relatie tot bestandskoppelingen is gesteld voordat de Black Box bestond waar deze onderzoeksrapportage over gaat.

Mogelijkheden om bestanden te mogen koppelen

Ten eerste zijn er geen belemmeringen als bestandskoppeling louter is bedoeld voor het opstellen van een risico-analyse op basis van anonieme, statistische gegevens. In hoeverre dit het geval is bij de Black Box als project en instrument gaan we aan de hand van de feiten onderzoeken.

Ten tweede mogen gegevensuitwisselingen tussen overheidsinstanties als bij wet is geregeld en noodzakelijk is om de betreffende wetten uit te voeren. Dit is bijvoorbeeld het geval bij:

- artikel 64 en 67 van de Wet Werk en Bijstand (WWB) en de artikelen 54 en 57 van de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). De gegevens van de andere partij zijn dan noodzakelijk om de eigen wet goed te kunnen uitvoeren in de zin van artikel 8, onder e, Wbp.
- artikel 20 Wet politiegegevens
- artikel 43c Uitvoeringsregeling Awr.

Ten derde is gegevensuitwisseling zonder een wettelijke regeling nog mogelijk als de gegevensuitwisseling kan worden gegrond op de interpretatie van artikel 9 Wbp (doelbinding).

Ten vierde is er een Kabinetsstandpunt over het advies van de Commissie Brouwer-Korf, waarin wordt aangegeven dat de gegevensuitwisseling in het kader van samenwerking van inspectiediensten in de Awb wordt geregeld in 2011, waarbij inspectiediensten gegevens mogen uitwisselen ten behoeve van elkaars toezichtsactiviteiten (zie Kamerstukken 31 051, nr. 5: zie ook het verslag van het AO op 15 maart over deze onderwerpen: 31051, nr. 7.

Ten vijfde hebben bestandskoppelingen met private partners geen wettelijke basis en zijn dus niet toegestaan, tenzij er in een specifiek geval wel een wettelijke basis aanwezig is, bijvoorbeeld in de WWB. Structurele bestandskoppelingen tussen overheidsorganen en private partijen moeten bij wet worden geregeld. Hiervoor moet een deugdelijke onderbouwing worden geleverd:

- Welk belang rechtvaardigt de inbreuk?;
- Kan de informatie niet op andere wijze worden verkregen?;
- Staat de inbreuk in verhouding tot het doel?

Ten zesde heeft de Centrale Raad van Beroep op 27 april 2010 (08/6125 WWB, RSV:2010,171) – in tegenstelling tot het CBP – bepaald dat bestandskoppeling mag tussen adressen van uitkeringsgerechtigden met een zeer hoog of zeer laag watergebruik welke door het waterbedrijf door middel van een bestandkoppeling zijn verstrekt. Deze inlichtingen kunnen volgens de Centrale Raad worden aangemerkt als inlichtingen welke noodzakelijk zijn voor de uitvoering van de WWB in de zin van artikel 64, eerste lid, aanhef en onder m, van de WWB.
Gelet op het gegeven dat de omvang van het waterverbruik op een adres van belang is voor de beantwoording van de vraag of – en zo ja hoeveel – personen op dat adres woonachtig zijn, merkt de Raad dit doel aan als het behartigen van het belang van het economisch welzijn van Nederland als bedoeld in artikel 8, tweede lid, van het EVRM, nu daaronder mede

begrepen moet worden geacht het tegengaan en bestrijden van misbruik en fraude van sociale uitkeringen.

De hierboven geschetste mogelijkheden kennen enkele begrenzingen, zoals het vereiste dat niet meer persoonsgegevens verwerkt mogen worden dan noodzakelijk is om de fraude daadwerkelijk te bestrijden. In 2006 heeft het CBP een belangwekkend toetsingskader opgesteld waarin staat waar rekening mee gehouden dient te worden bij het vinden van een evenwicht tussen fraudebestrijding en respect voor de persoonlijke levenssfeer. De betreffende notitie gaat in het bijzonder in op de positie van gemeenten die misbruik van sociale voorzieningen en uitkeringen aan willen pakken.

Toetsingskader CBP

Ten behoeve van onderhavig onderzoek sommen we de meest relevante onderdelen van de CBP-nota Fraudebestrijding door bestandskoppeling op met soms een noot van de auteurs van deze onderzoeksrapportage er bij:

1. De vraag die moet worden beantwoord is wanneer een gegevensverwerking ‘noodzakelijk’ is en wanneer deze ‘niet noodzakelijk’ is. De algemene wetenschap dat er fraude met uitkeringen bestaat, maakt het niet zonder meer noodzakelijk bestanden te koppelen waardoor de hele populatie uitkeringsontvangers op persoonsniveau wordt gecontroleerd (NB. Via de Black Box kan dit worden voorkomen, noot van de auteurs).
2. De WWB maakt koppelingen mogelijk van bestanden genoemd in artikel 64 WWB indien dit noodzakelijk is voor de uitvoering van de WWB.
3. De verantwoordelijke – het College van burgemeester en wethouders – (NB. Het CBP geeft hier aan dat B&W de verantwoordelijke is! Mogelijk van belang voor de vraag naar de verantwoordelijke, noot van de auteurs) dient af te wegen of de voorgenomen bestandkoppeling in verhouding staat tot het te bereiken doel en of hetzelfde doel niet op minder ingrijpende wijze bereikt kan worden.
4. Bij koppeling aan bestanden met persoonsgegevens van organisaties die niet in artikel 64 WWB zijn genoemd geldt bovendien de verenigbaarheidstoets uit artikel 9, tweede lid van de Wbp.
5. Het CBP onderscheidt 3 niveaus van controle in de sociale zekerheid: 1. Afhandeling van een aanvraag of uitkering; 2. Nadere controle in het kader van handhavingsbeleid; 3. Fraudeopsporing en vervolging.
6. Bij de Black Box gaat het zowel bij het project als het instrument met name om de tweede fase. Daarover zegt het CBP: Indien bijvoorbeeld op basis van statistisch materiaal, besloten wordt extra controles uit te voeren op bepaalde categorieën uitkeringsontvangers, dan zou, mits de themacontrole openlijk is aangekondigd, koppeling van bestanden mogelijk kunnen zijn. Bij een redelijk vermoeden van schuld bij de cliënt kunnen meer en ingrijpender controlemogelijkheden worden benut. (NB, Het CBP lijkt in dit toetsingskader de Black Box-aanpak, mits algemene informatie vooraf wordt gegeven over het thema, mogelijk te maken. noot van de auteurs)
7. Nadat de risicogroep voor de daadwerkelijke controle in algemene zin is geïnformeerd over de themacontrole (bijvoorbeeld in het informatieblad van de sociale dienst) kan bij koppelingen op persoonsniveau (NB. Het gaat dan dus niet om de anonieme koppeling!, noot van de auteurs) niet worden volstaan met informatie vooraf dat de gegevens van de uitkeringsvrager misschien door middel van bestandkoppeling gecontroleerd kunnen worden. Dan zal iedere keer als een uitkeringsvrager op persoonsniveau is gekoppeld, de verantwoordelijke aan de betrokkene achteraf moeten laten weten met welke bestanden is gematcht.

8. Tijdens de opsporing en vervolging heeft de betrokkene 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.

Gerichte koppelingen - met name als het koppelingen tussen overheidsorganisaties en toezichthouders betreft - zijn in beginsel geen probleem mits de noodzaak kan worden aangetoond , algemene informatie vooraf wordt gegeven en de betrokkene achteraf weet met welke bestanden hij is gematcht. Maar ongerichte, algemene bestandkoppeling mag in beginsel slechts anoniem en niet op persoonsniveau om tot profielen te komen. Dat is de Black-Box-methodiek die in het volgende hoofdstuk over de feiten verder wordt uitgewerkt. In het navolgende gaan we dieper in op de vraag in hoeverre er – als er gekoppeld mag worden – een informatieplicht is.

3.6 Informatieplicht

De vraag of en zo ja in hoeverre de verantwoordelijke(n) een informatieplicht heeft bij het afgeronde Black Box-project en bij het gebruik van de Black Box als instrument bij interventieteamprojecten hangt af van:

- de vraag of het om persoonsgegevens gaat;
- of het om gerichte of ongerichte koppeling gaat (dat stellen we straks vast aan de hand van de feiten);
- of het gaat om het vooraf of achteraf informeren van de betrokkene;
  of het – uitgaande van een gerechtvaardigde bestandkoppeling -, een onevenredige inspanning vergt;
- of dat de betreffende verantwoordelijke de bestanden koppelt op grond van een heldere wettelijke grondslag, in dat geval heeft de wetgever de burger in beginsel al geïnformeerd.

Met andere woorden is in juridische zin een uitzondering op de informatieplicht voor de verantwoordelijke(n) eventueel mogelijk op grond van:

- Artikel 43, sub b, Wbp in het kader van het voorkomen van strafbare feiten. Het betreft een uitzonderingsbepaling, is niet bedoeld voor structurele bestandkoppelingen en vereist dat er achteraf nog wel wordt geïnformeerd;
- Artikel 34 lid 4 Wbp als er sprake is van een onevenredige inspanning. Ook dan dienen er wel passende waarborgen getroffen te worden, zoals achteraf informeren;
- Anoniem koppelen, geen macht kunnen uitoefenen over de persoonsgegevens, Wbp (voor dat deel) niet van toepassing;
- Duidelijke wettelijke bepalingen waaruit blijkt dat de verantwoordelijke de betreffende bestandskoppeling uitvoert samen met de beschreven andere (overheids)organisatie(s). In dat geval heeft de wetgever de informatie al aan de burger gegeven en kan voor de zorgvuldigheid nog extra aan algemene informatieverstrekking gedaan worden.

3.7 Toezicht

Adequaat toezicht vergt toetsbare normen en processen op basis waarvan audits mogelijk zijn. De verantwoordelijke(n) doen er goed aan zo nodig zichzelf en anders de bewerker(s) periodiek te (laten) auditen. Bij politiegegevens in de zin van de Wet politiegegevens (Wpg) en trouwens ook bij de GBA is zo'n periodieke audit zelfs al verplicht.

Daarnaast is er de wettelijke bevoegdheid van het CBP – mogelijk in samenspraak met IWI (ook al is hun samenwerkingsconvenant inmiddels verlopen) om toezicht uit te oefenen op verantwoordelijke(n) en hun bewerkers. Het departement van SZW en grote uitvoeringsorganisaties hebben ook nog een Functionaris Gegevensbescherming (FG) in de zin van artikel 62 Wbp die toezicht kan uitoefenen.

3.8 Convenanten en overeenkomsten

Samenwerkingsovereenkomst

De samenwerkingsovereenkomst voor interventieteams regelt sinds 2003 de samenwerking tussen interventieteams op het terrein van fraudebestrijding tussen de:

- Belastingdienst;
- Arbeidsinspectie;
- UWV;
- Gemeente;
- SVB;
- OM;
- Departement Financiën;
- Departement SZW;
- Politie (sinds 2007).

De samenwerkingsovereenkomst regelt: voorwaarden voor samenwerking; de landelijke stuurgroep; de analysefunctie; regionale platforms, interventieteams; instrumenten van onderzoek; afhandeling van geconstateerde fraude en illegaliteit; aard/inhoud eindrapport van een interventieteam; communicatie/ *woordvoerderslijn* ten aanzien van interventieteams en gegevensuitwisseling en privacy.

Convenant tussen SIOD en het IB

Het “Convenant tussen de SIOD en het IB”, met als bijlage de “bewerkersovereenkomst tussen beide partijen” en in het verlengde daarvan het CBP (gelet op het verslag van de hoorzitting met de SIOD) in recente uitspraken gaan er volgens ons echter ten onrechte van uit dat de SIOD verantwoordelijke is in de zin van de Wbp en het IB bewerker. Als grondslag om verantwoordelijke te mogen zijn (en dus macht uit te mogen oefenen over de persoonsgegevens) wordt in het convenant artikel 85 lid 2 Wet SUWI aangehaald. Dat artikel creëert een bevoegdheid voor bijzondere opsporingsambtenaren om strafbaar gestelde feiten op te sporen. Dat is niet de rol van de Black Box, noch als afgerond project om tot profielen te komen, noch als instrument op een hoogwaardige, privacyvriendelijke wijze gegevensbestanden te koppelen.

3.9 Ethische aspecten

Bij het “normen” gaat het niet alleen om juridische normen. Ook ethische normen spelen een rol. Vanuit ethisch perspectief kunnen (clusters) van risico-indicatoren stigmatiserend werken.

Ook is het vanuit ethisch perspectief gewenst dat informatie achteraf te corrigeren valt en dat degenen die onderzocht zijn zonder dat fraude is vastgesteld daar geen hinder van kunnen ondervinden en op de hoogte worden gesteld.

4. Praktijk

In dit hoofdstuk bespreken we de organisatie en werkwijze van de interventieteams. We beschrijven het proces van start tot en met afronding van een project: globaal op het niveau van de Landelijke Stuurgroep Interventieteams (LSI) en meer in detail op het uitvoeringsniveau van de teams. Vervolgens gaan wij in het proces van gegevensverwerking waaronder de processen met de Black Box. We belichten in deze beschrijving vooral de rollen van de partners in de verschillende processen en de verantwoordelijkheden en we kijken naar de documenten waarin in organisatie en werkwijzen zijn vastgelegd en de status van deze documenten.

4.1 Interventieteams: organisatie en werkwijze

De samenwerking in de vorm van de interventieteams en de daarbij behorende afspraken liggen vast in de Samenwerkingsovereenkomst van 8 oktober 2003, getekend door de deelnemende partijen.[3][4] Hierin zijn onder meer de structuur, organisatie, aansturing, taken, bevoegdheden en verantwoordelijkheden aangegeven. Op basis van deze Overeenkomst zijn formats ontwikkeld om het operationele werk van de teams te stroomlijnen en standaardiseren. Zo zijn er formats voor onder andere het projectvoorstel, het projectplan en het draaiboek voor het project, het data-inwinplan, de opvraag gegevens en de melding Wbp. De formats zijn voortdurend onderwerp van actualisatie en bijstelling. De formats worden per project ingevuld en toegespitst op het specifieke project. De praktijk van aansturing van en uitvoering door de interventieteams is op deze manier gestandaardiseerd, gestroomlijnd en documentair onderbouwd.

4.1.1 Organisatie

Doel Interventieteams
Het ministerie van Sociale Zaken en Werkgelegenheid heeft in 2003 een landelijk dekkend netwerk van interventieteams opgezet. Hierin werken verschillende controle- en handhavingsdiensten samen. Het doel van de teams is het voorkomen en terugdringen van zwart werk, illegale arbeid, uitbuiting, sociale zekerheids– en fiscale fraude en de daarmee samenhangende misstanden en het verbeteren van naleving van regelgeving.

De kracht van deze aanpak is gelegen in de brede, interdisciplinaire benadering. Iedere discipline brengt zijn eigen informatie en expertise in. Door informatie te combineren wint de informatie aan diepgang en kunnen samenhangen en inconsistenties aan het licht komen.

---

[3] Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2003). Samenwerkingsovereenkomst voor interventieteams.
[4] Ministerie van Sociale Zaken en Werkgelegenheid (2003). Interventieteams Multidisciplinaire samenwerking. Afsprakendocument tussen partijen

Hierdoor kunnen controleactiviteiten beter worden gericht en effectiever worden uitgevoerd. Vervolgens kan door de inzet van verschillende disciplines een situatie meer integraal worden aangepakt. Om snel en flexibel op alle plaatsen in het land te kunnen opereren, is gekozen voor een structuur met teams die projectmatig werken, met een concrete doelstelling, gerichte taakverdeling, een vastgestelde tijdsplanning en vastgesteld budget.[5][6]

De interventieteamstructuur bestaat uit een Landelijke Stuurgroep Interventieteams (LSI), de interventieteams (IT's), de analysefunctie en de regionale platforms.

Betrokken organisaties
De partijen die deelnemen aan de Interventieteamstructuur zijn:
- De Belastingdienst (BD),
- De Arbeidsinspectie (AI),
- Het Uitvoeringsinstituut Werknemers Verzekeringen (UWV),
- De Sociale Verzekeringsbank (SVB),
- Gemeenten,
- De Sociale Inlichtingen – en Opsporingsdienst (SIOD) van het Ministerie van SZW,
- Het Openbaar Ministerie,
- De Politie.

De eerder genoemde Samenwerkingsovereenkomst is door deze partners ondertekend. Daarbij moet het volgende worden opgemerkt. Er hebben 7 gemeenten (portefeuillehouders) ondertekend. Deze gemeenten vertegenwoordigen niet dé gemeenten. Datzelfde geldt voor de politie; ondertekenaar is een vertegenwoordiger van de Raad van Hoofdcommissarissen, maar deze vertegenwoordigt niet de afzonderlijke korpsen.

Onder "de gemeenten" als deelnemer in de teams kunnen diverse gemeentelijke onderdelen vallen. Allereerst de onderdelen die met handhaving van de sociale zekerheidswetten te maken hebben, zoals de Sociale Dienst en de Sociale Recherche. Daarnaast kan het gaan om betrokkenheid van afdelingen Burgerzaken in verband met de GBA en afdelingen die zich met vergunningen en handhaving daarvan bezig houden, maar ook bijvoorbeeld leerplicht. Organisaties die geen deel uitmaken van de teams zelf maar wel een rol spelen voor de teams zijn de SIOD en de RCF's.

Analysefunctie SIOD
De Sociale Inlichtingen – en Opsporingsdienst (SIOD) van het Ministerie van SZW vervult de analysefunctie en voert voor de teams risicoanalyses uit. Van belang is hier op te merken dat dit een van de rollen van de SIOD is. De SIOD heeft in de eerste plaats zelfstandige controle- en opsporingstaken. Daarnaast kan zij in opdracht van gemeenten of andere organisaties risicoanalyses uitvoeren.[7]

---

[5] Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2009). Jaarplan 2010
[6] P. Castenmiller, Y. Bommeljé, A. Azouz, L. van der Meulen (2007). *Impuls voor de Interventieteams.* Zenc, Kennisland.
[7] Ministerie van Sociale Zaken en Werkgelegenheid. (10 juli 2009): Verzamelbrief Handhaving. Brief aan de TK.

Regionale platforms Fraude bestrijding (RPF) en RCF-Kenniscentra Handhaving
Bij de instelling van de interventieteams is ook de instelling van 9 regionale platforms geregeld. Dit is een bestuurlijk overleg tussen gemeenten, UWV, SVB, AI, Belastingdienst en OM. De gemeente is verantwoordelijk voor de platforms. De platforms hebben tot doel de regionale contacten en expertise te waarborgen en concrete projectvoorstellen te formuleren. Deze worden door de gemeentelijke vertegenwoordiger bij de Landelijke Stuurgroep Interventieteams ingediend.
Elk bestuurlijk platform wordt ondersteund door een RCF – Kenniscentrum Handhaving. De 9 RCF's vormen tezamen een landelijk dekkend kennisnet voor handhavende instanties op het terrein van werk, inkomen, zorg en fiscaliteit. De RCF's leggen verbindingen tussen gemeenten onderling en tussen gemeenten en hun ketenpartners. Zij vervullen daarvoor de rol van linking pin tussen interventieteams en de betrokken gemeentelijke onderdelen. In de tweede plaats helpen zij, los van de interventieteams, gemeenten bij het realiseren van programmatisch handhaven en faciliteren zij gemeenten bij handhavingsprojecten in het domein werk en inkomen.[8]

Landelijke Stuurgroep Interventieteams (LSI)
De LSI is verantwoordelijk voor het functioneren van de Interventieteams. De LSI wordt ondersteund door een secretariaat van het min. SZW.
De LSI maakt een Jaarplan waarin projecten worden opgenomen die zijn aangedragen door de deelnemende organisaties. De LSI toetst deze projecten vooraf aan het jaarplan en monitort de uitvoering aan de hand van voortgangsverslagen. Tenslotte beoordeelt de LSI de evaluatie van ieder project. De opzet van het Jaarplan, dat ook het overige ontwikkelwerk bevat dat randvoorwaardelijk is voor het functioneren van de Interventieteams, is afgestemd met de Handhavingsprogramma's van het Ministerie van SZW.

In de LSI zijn de organisaties vertegenwoordigd die aan de interventieteams deelnemen plus de betrokken departementen. De gemeenten worden vertegenwoordigd door een bestuurlijk vertegenwoordiger (VNG) tevens voorzitter van een RPF, en een vertegenwoordiger van Divosa. De politie wordt vertegenwoordigd door de Raad van Hoofdcommissarissen

De LSI is verantwoordelijk voor de interventieteams en is opdrachtgever. De operationele verantwoordelijkheid voor een specifiek team is gedelegeerd aan een van de leden van de LSI, de landelijke projectleider.
De LSI benoemt de projectleiders van de teams voor de dagelijkse leiding en mandateert hen voor de noodzakelijke zaken bij de uitvoering van projecten. De verantwoordelijkheden staan beschreven in de Overeenkomst en worden in ieder projectplan geconcretiseerd.

Typen projecten
De interventieteams onderscheiden gebiedsgerichte, branche- en sectorgerichte en fenomeengerichte projecten.
Gebiedsgerichte projecten richten zich op het verbeteren van het leefklimaat in wijken. Voorbeelden van wijkprojecten zijn: Ede, Tilburg en Zaltbommel.
Branche- en sectorgerichte projecten richten zich op branches of sectoren. Voorbeelden

---

[8] Brochure RCF Kenniscentra Handhaving; www.rcf.nl

zijn controles van de kassen in Westland, wokrestaurants, exportveilingen.
Bij fenomeengerichte projecten gaat het om controle op bepaalde typen fraude of misstanden, zoals controle op verzwegen samenwoning en huisvesting van migranten.

De teams
De samenstelling van een team is afhankelijk van het specifieke project; soms nemen alle partners deel soms niet. Als daar aanleiding toe is participeren daarnaast ook wel andere organisaties zoals de Voedsel en Warenautoriteit, nutsbedrijven ed.
Ook in wijkprojecten wordt vaak samengewerkt met partijen die niet zijn opgenomen in de Overeenkomst. Bijvoorbeeld met het (voormalige) ministerie van VROM/WWI en woningcorporaties.

De projectleider
De teams hebben een projectleider (PL) die de operationele leiding heeft. De organisatie die het project heeft ingebracht levert doorgaans de projectleider. De PL onderhoudt de kontakten met de landelijk projectleider uit de LSI, met de SIOD, met de betrokken organisaties. Hij doet tevens de Wbp-melding en hij regelt de communicatie met burgers en bedrijven op basis van afspraken die daarvoor in LSI-verband zijn gemaakt.
In de Overeenkomst is geregeld dat de projectleider erop toe ziet dat de gegevens conform de Wbp en de van toepassing zijnde bijzondere wetten verwerkt worden en dat maatregelen genomen worden tegen onbevoegde raadpleging van de gegevens, zowel binnen het interventieteam als door derden, evenals een adequate beveiliging getroffen is voor de vastlegging, raadpleging en verzending van gegevens volgens de minimum beveiligingseisen vastgesteld door de LSI.

Leercirkels
Voortdurende kwaliteitsverbetering is de rode draad in de jaarplannen van de LSI. Daarvoor zijn onder andere de leercirkels in het leven geroepen: werkgroepen die bepaalde onderwerpen uitwerken. De leercirkel Privacy houdt zich bezig met het verbeteren van de kennis over privacyaspecten en het borgen van privacybeschermende maatregelen in het uitvoeringsproces. De leercirkel Informatieproces Risicoanalyse werkt aan het verbeteren van het proces gegevensaanlevering en –verwerking.

4.1.2 Werkwijze LSI

Opstellen Jaarplan
De stuurgroep bepaalt haar beleid in een Jaarplan. Hierin wordt teruggekeken op het afgelopen jaar, op de resultaten en ervaringen van de teams. Vervolgens wordt tegen de achtergrond van de maatschappelijke ontwikkelingen, beleidsontwikkelingen en het meerjaren handhavingsprogramma van het ministerie gekeken wat de koers is voor de interventieteams en waar het zwaartepunt van de projecten moet liggen. Verder wordt de capaciteit die door iedere partij ter beschikking wordt gesteld voor de teams in beeld gebracht en worden de in dat jaar uit te voeren projecten ingepland.

Opdrachtverstrekking projecten
De betrokken organisaties dragen hun ideeën voor projecten aan bij de LSI. Gemeentelijke projectvoorstellen kunnen worden geïnitieerd door de RCF’s, die vervolgens via de RPF’s bij de betreffende gemeenten politiek-bestuurlijk draagvlak

proberen te verkrijgen.
De organisaties dienen volgens een vast format het projectvoorstel in.[9] Hierin staat het doel omschreven, in het kort de te volgen werkwijze en of er een risicoanalyse door de SIOD nodig is. Als er geen risicoanalyse nodig is, dan moet dit in het voorstel met argumenten worden onderbouwd.
De LSI beoordeelt het voorstel tegen de achtergrond van de in het Jaarplan benoemde speerpunten en de beschikbare capaciteit.

Gedelegeerde verantwoordelijkheid landelijk projectleider
De LSI wijst de LSI-partner aan die verantwoordelijk is voor het team. Dit is het lid dat de organisatie vertegenwoordigt die het voorstel heeft ingebracht. Het LSI-lid benoemt een projectleider, normaliter een projectleider afkomstig uit de betreffende organisatie.

Vervolgens werkt de organisatie die het voorstel heeft ingediend, het voorstel uit in een gedetailleerd projectplan. Voor dit projectplan bestaat een format om de noodzakelijke informatie op schrift te krijgen.[10] Hierin staat onder andere uitvoerig beschreven welke rol iedere partner heeft, hoe de gegevensuitwisseling en bewerking is geregeld, hoe de communicatie binnen het team en naar buiten verloopt. De projectleider legt het plan ter kennisname voor aan de LSI.

De landelijk projectleider onderhoudt het contact met de projectleider van het interventieteam. De landelijk projectleider kan aan de hand van het plan toetsen of het team zich houdt aan de afgesproken werkwijze en randvoorwaarden.

Dechargeproces
De LSI monitort de voortgang op basis van voortgangsrapportages en evalueert het project aan de hand van de eindrapportage. De LSI besluit over de daadwerkelijke beëindiging van een project.

4.1.3 Werkwijze interventieteams

Voorbereiding projectplan
De projectleider bereidt het project voor door het projectplan in detail uit te werken op basis van het format. Dit gebeurt in de zogenaamde vooronderzoeksfase. Tegelijkertijd werkt hij aan draaiboek, waarvoor ook een format is.[11]

---

[9] Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (actueel). Format Projectvoorstel.
[10] Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (actueel). Format Projectplan.
[11] Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (actueel). Format Draaiboek.

Intake SIOD
De projectleider neemt voor het uitvoeren van de risicoanalyse contact op met een analist van de SIOD. Het project wordt doorgesproken en de analist stelt in overleg met de projectleider vast welke gegevens door de deelnemende organisaties moeten worden aangeleverd. Tevens stellen zij een planning op voor de aanlevering en uitvoering van de analyse. De SIOD maakt van dit gesprek volgens een vast format een Intakeverslag dat de basis is voor de uitvoering van de SIOD-activiteiten[12]. In dit intakeverslag staan de rollen en verantwoordelijkheden van de actoren benoemd, wordt de analyseopdracht geformuleerd, de werkwijze en de op te leveren producten. Er staat in aangegeven dat de projectleider van het team verantwoordelijk is voor de aanlevering van de gegevens, er is een passage opgenomen over vernietiging van gegevens en over de informatieplicht Wbp die berust bij de partners van het project.
Het Intakeverslag wordt door de SIOD en de projectleider geaccordeerd.

Instemming projectplan LSI
De projectleider legt via de landelijk projectleider het Projectplan voor instemming voor aan de LSI. Het plan bevat een analyseparagraaf. Het projectplan is opvraagbaar in het kader van de Wet openbaarheid van bestuur.

Gegevensopvraag en levering
De daadwerkelijke gegevensopvraag bij de deelnemende partijen mag niet dan nadat de LSI goedkeuring aan het projectvoorstel heeft gegeven.
De projectleider verzoekt na goedkeuring van het projectvoorstel door de LSI, de vertegenwoordigers van de deelnemende organisaties om de met de SIOD afgesproken gegevens te leveren. De levering is geregeld in de Overeenkomst. Als er niet-LSIpartners aan het project deelnemen, dan wordt een aparte overeenkomst voor de gegevenslevering van die partij opgesteld.
Voor de wijze waarop de gegevens moeten worden aangeleverd zijn formats ontwikkeld, het Data-inwinplan en de bijlage met de technische specificaties.[13] In de ontwikkelde standaardbrief voor opvraag van de gegevens door de projectleider bij de organisaties staat de rechtsgrond, de levertermijn en de wijze van levering in verband met beveiliging. De levering gebeurt door de bronhouder direct aan de bewerker SIOD zonder tussenkomst van de projectleider. Indien van de Black Box-methode gebruik wordt gemaakt, dan leveren bronhouders direct aan het Inlichtingenbureau.

Melding CBP
De projectleider meldt de gegevensverwerking aan het CBP volgens het format dat daarvoor tussen LSI en CBP is afgesproken.[14]

---

[12] Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (actueel). Format Intake.
[13] Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (actueel). Format Data-inwinplan.
[14] Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2004). Instructie voor het op basis van de modelmelding concretiseren van de melding van interventieteams.
Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams/CBP (2004). Melding privacy.

Analyse SIOD
De SIOD voert zijn analyse uit en levert de uitkomsten op die voldoen aan de normen gesteld door de projectleider. De uitkomsten zijn lijsten met namen van personen, bedrijven en adressen met verhoogd risico op normovertreding en die voldoen aan de scorerange die door de projectleider is bepaald.
Als de SIOD gebruik maakt van de Black Box-methodiek worden voorafgaand aan de analyse bewerkingen uitgevoerd door het Inlichtingenbureau. Hiervoor hebben SIOD en het Inlichtingenbureau een convenant afgesloten, zoals we in hoofdstuk 3 al zagen.

Bespreking resultaten en afspreken precieze interventies
De analyseresultaten van de SIOD worden besproken in het interventieteam. De deelnemers kunnen nog aanvullende eigen informatie over de hoge risico objecten en subjecten inbrengen en uitwisselen. Op basis hiervan wordt een definitieve lijst gemaakt en de detailaanpak van de interventies besproken. Dit wordt verder vastgelegd in het draaiboek.

Informatieverstrekking aan doelpopulatie
Voorlichting aan derden is de taak van de voorlichter van de organisatie die trekker is van het project. De voorlichter zorgt kort voor aanvang van het project voor een persbericht waarin het doel van het IT wordt uitgelegd. Dit dient tevens als vooraankondiging van de activiteiten van de Belastingdienst in het project. Voor branche en fenomeen gerichte onderzoeken wordt verzocht het persbericht te plaatsen in vakbladen en periodieken. Bij wijkgerichte projecten wordt dit geplaatst in huis- aan – huisbladen en verspreid via andere communicatiekanalen van de gemeente.
De wijze van communicatie (het communicatieplan) is vastgelegd in het projectplan van het team.

Uitvoeren Interventies
De voorgenomen interventies worden door de organisaties uitgevoerd. Bij de uitvoering worden door de organisaties formulieren gehanteerd waarop de bevindingen worden aangetekend.
De interventies worden afgesloten met een dagevaluatie waarin een korte samenvatting wordt gegevens van de voorlopige resultaten, de opbrengsten voor elke organisatie, ervaringen en verbeterpunten.

Informatieverstrekking tijdens en achteraf
De wijze van informatieverstrekking aan de te bezoeken personen, bedrijven en adressen is afhankelijk van het type project en de risico's. Normaliter wordt ter plekke een brief verstrekt met een toelichting op en de rechtsgronden voor de controle.

Na afloop van het project stelt de persvoorlichter een persbericht op met de resultaten van het project. In sommige gevallen wordt achteraf een persconferentie gegeven.

Verwerken onderzoeksgegevens IVT-systeem
De onderzoeksgegevens en onderzoeksresultaten worden door de projectleider verwerkt in het Interventie Team (IVT)-systeem, het systeem dat speciaal voor de interventieteams is opgezet. We gaan hier later verder op in.

Tussenrapportages en eindrapport
De projectleider meldt de voortgang aan de LSI in verslagen en stelt een eindrapport op.

Afsluiting onderzoek
Pas na goedkeuring van het eindrapport door de LSI kan de projectleider tot afsluiting van het onderzoek worden overgegaan. Onderdeel daarvan is het laten vernietigen van basisgegevens en onderzoeksgegevens en het opvragen van vernietigingsrapporten aan de SIOD en het BKWI, de beheerder van het IVT-systeem. De projectleider bericht de SIOD en het BKWI de datum van beëindiging van het project.

4.2 Gegevensverwerking

In deze paragraaf bespreken we de gegevensstroom en de verwerking van de gegevens die voor een interventieproject nodig zijn. Om gericht en binnen het kader van de Wbp te kunnen werken hebben de teams een lijst nodig met objecten en subjecten met een verhoogd risico op normovertreding. Voor de uitvoering van een risicoanalyse die een dergelijke lijst moet opleveren wordt normaliter de SIOD ingeschakeld. De SIOD voert de risicoanalyse uit door het koppelen van gegevens van objecten en subjecten uit de verschillende bronnen aan een (gevalideerd) risicomodel. Het risicomodel bevat indicatoren die (in samenhang) een verhoogd risico aangeven. Koppeling van objecten en subjecten aan het model genereert een lijst met scores voor het risico.
Uiteindelijk stelt het team een definitieve lijst op met een selectie van de subjecten en objecten die tijdens de interventie gecontroleerd worden.

Voor het toewerken naar deze definitieve werk-lijst zijn de volgende routes te onderscheiden:
1. Reguliere gegevensverwerking met inzet van een SIOD-analyse.
2. Gegevensverwerking met inzet van een SIOD-analyse met gebruikmaking van de Black box.
3. Gegevensverwerking zonder inzet van een SIOD-analyse.

Van belang is hier op te merken dat uit het onderzoek (documenten en gesprekken) niet helemaal helder is geworden wie nu precies beslist en op basis waarvan voor welke van de 3 varianten gekozen moet worden. In het projectplan dat wordt voorgelegd aan de LSI is een analyseparagraaf is opgenomen. In deze analyseparagraaf moet worden aangegeven of de SIOD een risicoanalyse uitvoert. Indien wordt afgezien van een SIOD-analyse moet de projectleider dat motiveren. De analyseparagraaf is nog niet aangepast op inzet van de methodiek Black Box van de SIOD. Dat wil zeggen dat nog niet standaard wordt aangegeven of wel/niet van deze methodiek gebruik wordt gemaakt en op grond van welke overwegingen wel of niet. Uit de gesprekken is dan ook gebleken dat lang niet bij alle leden van de LSI en projectleiders duidelijk is welke projecten wel en niet met behulp van deze methodiek tot nu toe zijn uitgevoerd.

Het blijkt dat tot dusver alleen een aantal wijkgerichte aanpak-projecten met behulp van de Black Box-methodiek zijn uitgevoerd. De achterliggende reden is dat tot dusverre alleen voor deze aanpakken risicomodellen zijn ontwikkeld.

We beschrijven allereerst de hoofdroute van de gegevensstromen en gegevensbewerking en welke beslissingen hierin worden genomen. Daarna gaan we in op de methodiek Black Box.

4.2.1 Hoofdroute gegevensverwerking

Bepalen wel of geen analyse SIOD
De projectleider bepaalt of een risicoanalyse van de SIOD nodig is. Zoals gezegd is de reguliere werkwijze dat de SIOD een risicoanalyse uitvoert. Het kan zijn dat van te voren bij de deelnemende partijen al groepen subjecten of objecten met verhoogd risico op een andere wijze zijn geïdentificeerd. In dat geval moet de projectleider in het Projectplan voor de LSI motiveren waarom wordt afgezien van een SIOD-analyse.

Bepalen gegevensopvraag en analyse projectleider en SIOD
De projectleider neemt contact op met de SIOD over de inzet van de SIOD. In dit gesprek, in SIOD-terminologie de Intake, wordt het project (doel, doelpopulatie, aanpak, deelnemende partijen) besproken. Verder bespreken zij de analysevraag. Bepaald wordt of er een (getoetst) risicomodel voorhanden is dat toegepast kan worden in de analyse, dan wel dat er risico-indicatoren voorhanden zijn. De indicatoren zijn werkendeweg in de loop van de tijd ontwikkeld door de teams in samenspraak met de SIOD. De modellen zijn onder meer ontwikkeld in het project Black Box. Indien er geen modellen of indicatoren voorhanden zijn, kunnen de analist van de SIOD en projectleider besluiten een expertmeeting te houden om risico-indicatoren te benoemen.

Gezamenlijk wordt bepaald welke gegevens bij welke bronhouder opgevraagd moeten worden. Op basis daarvan wordt conform het format het Data-inwinplan opgesteld. In dit plan staan per bron de gegevens die opgevraagd moeten worden, bij welke contactpersoon van de deelnemende organisaties, de termijnen, de wijze van aanlevering en hoe die beveiligd kan plaatsvinden, het aanleveradres en technische specificaties.

Opvraag gegevens bij bronhouder door projectleider
De projectleider vraagt per brief/mail aan de deelnemende organisaties om de benodigde gegevens aan te leveren. Hiervoor is een standaardbrief waarin staan: de rechtsgrond voor de datalevering, levertermijn, wijze van aanlevering, de technische specificaties. Voor niet- interventieteam-organisaties die deelnemen of waarvan gegevens worden opgevraagd wordt een aparte Overeenkomst gesloten.
De leden van het IT en reguliere leveranciers (bijvoorbeeld Rijks Dienst Wegverkeer, Kamer van Koophandel) hebben op dit moment vaste contactpersonen die voor de gegevensopvraag worden benaderd, de zogenaamde informatiemakelaars. Voor WWB-gegevens van gemeenten vervult het Inlichtingenbureau die functie. Voor het opvragen van gemeentelijke gegevens die uit andere bron komen (bijvoorbeeld vergunningen, belastingen ed.) vervult het RCF vaak een bemiddelende rol.

De politie levert in dit stadium nog geen gegevens; de politiegegevens volgen ook een andere route. De gegevens van de politie zijn géén persoonsgegevens, maar gegevens over adressen waar gedurende een bepaald jaar incidenten hebben plaatsgevonden. De politie levert de gegevens aan in een vast format in een beveiligd bestand aan de analist.

Ze worden in een later stadium aan de output van de analist toegevoegd.

Ontvangst gegevens door bewerker[15]
De gegevens moeten conform de vastgelegde afspraken direct naar de bewerker worden verstuurd op een beveiligde wijze. De SIOD constateert in dit proces een aantal knelpunten. In de eerste plaats is de aanlevering door gemeenten lastig, omdat er geen landelijke standaarden zijn. Bovendien gaat het om data uit verschillende gemeentelijke bestanden die niet, zoals bij de landelijke organisaties het geval is, volgens een afgesproken kanaal en format worden aangeleverd. In de praktijk bestaan de risico's uit onbeveiligde aanlevering en onbetrouwbare en niet-valide data. Gemeentelijke data vereisen daardoor een extra bewerkingsslag om op te schonen en in het juiste technische formaat te zetten (het zogenaamde normaliseren).

Uitvoeren risico-analyse
De SIOD voert de risico-analyse uit. De data worden gekoppeld aan het gekozen risicomodel of de risico-indicatoren. De output is een lijst met scores op personen en objecten. In samenspraak met de projectleider wordt aangegeven welke scorerange nader door de SIOD wordt geanalyseerd. In deze laatste bewerking worden de geselecteerde subjecten en objecten en hun netwerken geanalyseerd. De output zijn netwerkdiagrammen op naam.

Verrijking data in team, definitieve selectie
De analyseresultaten van de SIOD worden in het team besproken. Ook wanneer er geen gebruik wordt gemaakt van de SIOD analyses vindt hier de bespreking op persoons- of objectniveau plaats. Elke deelnemer van het team kan aanvullende informatie leveren. In dit stadium kan de SIOD indien gewenst de politiegegevens over adressen inbrengen. In deze bespreking stelt de projectleider de definitieve werk-lijst op die op de interventiedag gebruikt wordt. De politie kan in verband met de concrete interventie nagaan of er meer relevante politie-informatie bekend is over de geselecteerde objecten en personen.

Opslag onderzoeksgegevens en resultaten
Voor de opslag van alle relevante informatie en gegevens is in opdracht van het ministerie door het BKWI een applicatie ontwikkeld, het zogenaamde IVT-systeem. BKWI beheert dit systeem op basis van een convenant tussen BKWI en het ministerie.
Het BKWI autoriseert de projectleider voor toegang tot het systeem. De projectleider kan het BKWI verzoeken deelnemers aan het team voor delen van het systeem te autoriseren. Op deze manier kan informatie worden gedeeld. De projectleider is verantwoordelijk voor het toevoegen van de onderzoeksresultaten.

Dataopslag, beheer en vernietiging
De gegevens die SIOD bewerkt en analyseert zijn onderworpen aan de informatiebeleid regels van de SIOD. Na het door de projectleider aangegeven datum beëindiging van een project vernietigt de SIOD de gegevens.

---

[15] Het begrip bewerker wordt hier overgenomen zoals dat in het draaiboek van de interventieteams staat en ook door het SIOD wordt gebruikt. De wijze waarop het begrip in het draaiboek en door de SIOD gebruikt wordt komt niet geheel overeen met de betekenis van het begrip bewerker in de Wbp.

Er is een aparte procedure voor het vernietigen van bestanden.[16]
Het IVT-systeem is onderworpen aan de reguliere procedures die voor het beheer door het BKWI gelden, onder andere het normenkader voor privacy en beveiliging en de daarop uit te voeren audits. De projectleider meldt de datum beëindiging aan het BKWI. Dit is de datum waarop de LSI het project als beëindigt beschouwt. Vervolgens gaat volgens het protocol dat het BKWI daarvoor hanteert de procedure voor vernietiging van data in werking, waarvan schriftelijk melding wordt gemaakt aan de projectleider. Er is overigens geen audit op het proces.

Terugkoppeling onderzoeksresultaten voor aanscherping risicomodellen
De SIOD werkt met risicomodellen die zij wil toetsen op validiteit. Daarvoor zijn de uitkomsten van de interventieonderzoeken noodzakelijk. De SIOD constateert dat de terugkoppeling van resultaten aan de SIOD nog niet is gerealiseerd. Het risico dat daardoor ontstaat is dat de modellen die voor de analyse worden gebruikt, niet valide zijn en dus hun voorspellende waarde verliezen.

Wij hebben een procedure terugkoppeling en validatie ook in documenten niet terug kunnen vinden.

4.2.2 Black Box

Aanleiding
Het CBP heeft in september 2006 een - op de Wet bescherming persoonsgegevens (Wbp) gebaseerd - toetsingskader voor bestandskoppelingen bij fraudebestrijding vastgesteld. Dit toetsingskader hanteert het CBP bij de beoordeling van de rechtmatigheid van bestandskoppelingen. Dit toetsingskader houdt in dat koppeling van niet-openbare bestanden in de controlefase alleen mag plaatsvinden, indien subjecten zijn geselecteerd op basis van een goed onderbouwd selectieprofiel. Alleen de gegevens van personen die aan het selectieprofiel voldoen, dus waarvan de noodzaak tot koppeling is aangetoond, mogen worden gekoppeld aan externe bestanden.

Naar aanleiding van dit toetsingskader heeft de LSI met het CBP afgesproken te onderzoeken of bestandskoppelingen op de door het CBP gewenste manier, kunnen worden uitgevoerd. De LSI heeft de SIOD hiervoor opdracht gegeven. Dit is uitgevoerd in het project Black Box, dat is uitgevoerd van 2008 tot april 2010. De opzet daarvan is met het CBP afgestemd.

Selectieprofielen en risicomodellen[17]
Het project heeft in de eerste plaats een aantal gevalideerde selectieprofielen voor WWB-fraude opgeleverd. Het gaat zowel om generieke profielen als om specifieke vormen van WWB- fraude, zoals leefvorm. De profielen bestaan uit kenmerken die in het kader van de

[16] Ministerie van Sociale Zaken en Werkgelegenheid SIOD (2010). Procedure vernietiging IT bestanden.
[17] Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (april 2010). Black Box en selectieprofielen.

uitkeringsverstrekking zijn verzameld, dus gegevens die uit interne bestanden worden gehaald. Subjecten die aan deze profielen voldoen kunnen volgens de voorwaarden door het CBP gesteld, worden gekoppeld aan externe bestanden.

Daarnaast zijn enkele bestaande risicomodellen WWB herijkt. Risicomodellen bevatten indicatoren die in samenhang een verhoogd risico (in dit geval) op WWB-fraude voorspellen. De indicatoren hebben betrekking op interne en externe bestanden. De risicomodellen worden gebruikt bij de externe bestandskoppelingen.

Black Box: beveiligde omgeving
In het project is verder de “Black Box” ontwikkeld. Dit is de technische infrastructuur en de procedures waarmee in een beveiligde omgeving op een zorgvuldige manier data kunnen worden gekoppeld.

Convenant SIOD – Inlichtingenbureau, reglementering
De SIOD is voor de opzet van en de uitvoering van de bestandskoppelingen in de Black Box een samenwerkingsverband aan gegaan met Stichting het Inlichtingenbureau (IB). Hiervoor is een Convenant tussen de SIOD en het IB afgesloten. In dit convenant is de SIOD als verantwoordelijke in zin van de WBP aangegeven, het IB als bewerker en de leden van de IT’s als opdrachtgevers. Als bijlage is een Bewerkersovereenkomst opgenomen. In hoofdstuk 2 hebben we al kanttekeningen geplaatst bij deze Bewerkersovereenkomst.
Daarnaast gelden het reguliere Informatiebeveiligingsbeleid van het IB en is er voor de Black Box en annex opgesteld, waarin oa. de vernietigingsprocedure is opgenomen.
Voor de werkwijze met de Black Box is een Procedurebeschrijving opgesteld.

Werkwijze Black Box
In de werkwijze van de Black Box zijn de volgende fasen te onderscheiden.
Fase 1: bestandsopschoning en anonimisering
Fase 2: koppeling en genereren scorelijst
Fase 3: genereren genonimiseerde analyseset voor de SIOD

De SIOD is opdrachtgever van het IB en onderhoudt voor de projecten het contact met het IB, onder andere op basis van het data-inwinplan. Hiervoor gaven we aan dat de projectleider een verzoek tot gegevenslevering verstuurt aan de deelnemende organisaties. Deze organisaties leveren in dit geval hun bestanden aan het IB.
Het IB voert een technische controle uit. Indien nodig worden bestanden “genormaliseerd”, dat wil zeggen geschoond en in het goed technische formaat gezet. Doorgaans geldt dit zoals eerder vermeld, voor data die door gemeenten worden aangeleverd.

In de volgende stap worden de bestanden geanonimiseerd. De oorspronkelijke data worden opgeslagen in de zogenaamde red-box omgeving.
Vervolgens wordt in een aparte omgeving verder gewerkt met de geanonimiseerde bestanden (greenbox). Hier vindt de koppeling plaats met het risicomodel. Dit risicomodel is ontwikkeld in een sessie met experts van de interventieteams. De output van de koppeling is een lijst met scores die wordt overgedragen aan de SIOD.
De projectleider en de SIOD bepalen in overleg welke range van scores zal worden gebruikt voor verdere analyse door de SIOD.

De selectie die voldoet aan de aangegeven range scores wordt vervolgens door het IB genonimiseerd, dat wil zeggen voorzien van identificeerbare kenmerken. Dit is, samen met de anonieme data, het analysebestand voor de SIOD. De SIOD gebruikt dit bestand voor haar netwerkanalyse. Gerelateerde subjecten die anoniem in het netwerk van geselecteerde subjecten en op basis van actuele risico's tevoorschijn komen volgens de interpretatie van de analist, kunnen in tweede instantie worden voorzien van identificeerbare kenmerken. De SIOD doet daartoe een verzoek bij het IB.

Onderzoeken uitgevoerd met behulp van Black Box
Met behulp van de Black Box zijn tot nu toe alleen wijkgerichte projecten uitgevoerd, namelijk:

- Middengebied, Vlissingen
- Kanaleneiland, Utrecht
- De Riet, Almelo
- De Vergt, Zaltbommel
- Merwestein, Nieuwegein
- Heerlen
- Weert
- Roermond

In kringen van de LSI en de IT's is deze tot de wijkgerichte aanpakken beperkte inzet niet bekend. De Black Box-methodiek is een gestandaardiseerd proces dat de SIOD speciaal heeft ontwikkeld voor complexe koppelingen en meerdere verschijningsvormen van normovertredend gedrag, waar bij de wijkgerichte aanpak sprake van is. Verdere ontwikkeling van de methodiek zou volgens de SIOD gericht moeten zijn op het genereren van profielen en modellen voor bedrijven en fraude met andere regelingen dan de WWB. De SIOD is recent gestart met het ontwikkelen van modellen voor bedrijven. Voor WAO- en WW-fraude zijn er al profielen ontwikkeld[18]; deze kunnen volgens de SIOD worden doorontwikkeld in de context van de Black Box-methodiek. Daarvoor moet de SIOD opdracht krijgen van de LSI.

[18] SEOR (2010). Eindrapportage selectieprofielen WWB en UWV. Onderzoek voor SIOD/SZW. Rotterdam, SEOR

5. Confrontatie norm – praktijk

5.1 Verantwoordelijke en bewerker

Onduidelijk is wie verantwoordelijke(n) en/of bewerker in de zin van de Wbp zijn bij het aanleveren van gegevens aan de Black Box, bij de verwerkingen in de Black Box zelf en bij het verstrekken van de “hits” aan de interventieteams.
Volgens het Convenant SIOD – IB zou de SIOD verantwoordelijke zijn in de zin van de Wbp. In de Pleitnotitie voor CBP in verband met de hoorzitting eind 2010 stelt de SIOD zelf dat het een bewerker is en dat tijdens het Black Box-project de gemeente de verantwoordelijke was bij het beperkte aantal projecten die in de gemeenten in het kader van het project tot april 2010 zijn uitgevoerd. Met de gemeente wordt in juridische zin het College van B&W bedoeld en dat komt overeen met het toetsingskader van het CBP in 2006. Desalniettemin volgt het CBP in de hoorzitting (zie het verslag) vooralsnog de papieren werkelijkheid en stelt dat de SIOD verantwoordelijke is. Volgens ons is dat niet juist.

De Overeenkomst LSI van 2003 laat zien dat er vele partijen zijn die aan te merken zouden kunnen zijn als gezamenlijke verantwoordelijke. De LSI is (nog) geen rechtsvorm en ook projectleider en een RCF zijn juridisch (nog) niets.

Sommige geïnterviewden pleiten er voor dat de Minister van SZW de verantwoordelijke is. Dat zou voor de SIOD het geval kunnen zijn, maar over veel van de partijen die bij de interventieteams en de keten van de Black Box als project en instrument betrokken waren en zijn heeft de Minister van SZW geen zeggenschap. Het lost dus niet in één keer de vraag naar de verantwoordelijke op. Landelijk zou de LSI als opdrachtgever een goede kandidaat zijn om als verantwoordelijke te fungeren, maar dan moet zij daar ook een grondslag voor hebben. Bijvoorbeeld doordat alle leden van de LSI daartoe ge(vol)machtigd zijn. Bij de gemeenten en de politie is dat op dit moment nog enigszins problematisch om te realiseren, hoewel er nationale politie op komst is, dus wie weet. In ieder geval zou het bij benadering een goede verantwoordelijke kunnen zijn. Dat moet dan dus nog wel worden geregeld.

Op lokaal niveau is college van B&W een goede kandidaat zoals we zagen. Maar kan een afzonderlijk college van B&W ook de verantwoordelijkheid dragen voor de landelijke Black Box?

Verder kan vastgesteld worden dat er nog geen bewerkerscontracten zijn, anders dan die tussen SIOD en IB en die laatste klopt volgens ons niet.

5.2 Bestandskoppelingen

Voor de Black Box als project liep tot april 2010 slechts een heel beperkt deel van de bestandkoppelingen via de Black Box.
De Black Box wordt nog wel als instrument voor de interventieteams gebruikt en vanaf dit jaar met name ook voor branches.

Wat betreft de algemene koppeling van bijvoorbeeld alle uitkeringsgerechtigden in een wijk gebeurt dit bij de Black Box in de red box op een anonieme wijze ten behoeve van selectieprofielen, “hits”. Er van uitgaande dat het echt anoniem gekoppeld wordt (een audit zou dat uit moeten wijzen) is er vanuit de Wbp geen bezwaar, want op dat deel van het proces is de Wbp dan niet van toepassing.

Zodra de geselecteerde hits gekoppeld worden aan de identificerende gegevens is de Wbp uiteraard wel van toepassing. Dat gaat om veel kleinere aantallen personen. Die koppeling dient gericht te zijn en er moet een wettelijke grondslag voor zijn, zoals in hoofdstuk 2 uiteen is gezet.

Hoewel niet het hele proces in de keten van de Black Box – van persoonsgegevens aanleveren, via anoniem koppelen, een kleine selectie persoonsgegevens verstrekken aan interventieteams – anoniem verloopt, is de Black Box als methode wel vele malen beter dan vele overige praktijken van bestandkoppelingen in het kader van interventieteams.

De (clusters van) indicatoren waarmee gekoppeld wordt zijn (nog) niet transparant.

5.3 Informatieplicht

Conform het toetsingskader van het CBP zijn in de fase van nadere controle bij verschillende projecten (persberichten met) algemene informatie verstrekt. Soms zijn er ook zowel vooraf als achteraf brieven verstrekt.

Ten behoeve van de bestandkoppeling om – geanonimiseerd – tot selectieprofielen te komen is geen persoonlijke informatie aan alle betrokkenen vooraf verstrekt. Dat hoefde volgens ons ook niet, omdat die koppeling anoniem plaats heeft gevonden en bijbehorende identifcerende gegevens vernietigd zijn. Mocht de anonimiteit ter discussie worden gesteld (een audit kan uitsluitsel geven), dan zou eventueel betoogd kunnen worden dat het verstrekken van persoonlijke informatie aan alle betrokkenen die op basis van een bepaalt vooraf gecommuniceerd thema gekoppeld worden om tot algemene selectieprofielen te komen een onevenredige inspanning vergt. Of het echt onevenredig is, is bediscussieerbaar. Vanuit de norm en de praktijk geredeneerd is volgens ons beter om in te zetten op anonimiteit en inzet van privacy bevorderende technologie. In de fase van structurele, algemene koppeling om bijvoorbeeld tot selectieprofielen te komen is een beroep op 43 sub b Wbp volgens ons niet kansrijk, omdat dit artikel is bedoeld voor uitzonderingsgevallen en in het geval er een mogelijke verdachte is opschortende werking te bieden voor wat betreft de informatieplicht. Artikel 43 sub b Wbp kan dus wel in de laatste fase van de keten, maar niet bij de algemene koppeling ingeroepen worden. Daar is anonimiteit de beste waarborg. Eventueel aangevuld met wet- of regelgeving waarin een en ander helder is vastgelegd. Dat is niet alleen van belang voor de persoonlijke levenssfeer, maar ook om bijvoorbeeld de financiële en andere zakelijke aspecten rond de Black Box goed te regelen.
.

5.4 Toezicht

Er is nog geen audit bescherming persoonsgegevens geweest op de Black Box voor het project en ook nog niet op het instrument als zodanig dat nog steeds gebruikt wordt.
De Functionaris Gegevensbescherming is de laatste jaren nauwelijks betrokken bij de Black Box.

Een audit vergt ook toetsbare normen en processen. Hoewel er veel procedures zijn, zal een audit nog wel wat voorbereidingen vergen.

Om toezicht te kunnen houden zal ook inzicht noodzakelijk zijn in de indicatoren voor het risicomodel. Tot op heden is dat nog onduidelijk.

Cliëntenorganisaties zijn (nog) niet betrokken bij het toezicht.

5.5 Overeenkomsten en convenanten

Niet alle organisaties die betrokken zijn bij interventieteams - bijvoorbeeld de Voedsel – en Warenautoriteit (VWA) – hebben de samenwerkingsovereenkomst ondertekend. Dat kan relevant zijn voor het gebruik van de Black Box als instrument bij interventieteamprojecten.

Het Convenant tussen de SIOD en de IB moet worden herzien, zowel vanuit normatief als feitelijk perspectief.

5.6 Ethische aspecten

Wat betreft de mogelijke stigmatiserende werking van clusters) van risico-indicatoren valt het ook voor de LSI-leden niet te controleren of er sprake is van een stigmatiserende werking.

Wat betreft het achteraf informeren van degenen die onderzocht zijn, hebben we gezien dat in een aantal gemeenten degenen die onderzocht worden persoonlijk een brief krijgen als zij worden onderzocht en later ook te horen krijgen als geen fraude is vastgesteld.

Bijlage 1: Relevante documentatie

G. van den Berg, Th. Hooghiemstra, O. Kinkhorst e.a.(2009). Langs elkaar heen, over geïntegreerde dienstverlening in het publieke domein, papernote 27, HEC.

P. Castenmiller, Y. Bommeljé, A. Azouz, L. van der Meulen (2007). *Impuls voor de Interventieteams.* Zenc, Kennisland.

CBP (26 mei 2010): Rapport van definitieve bevindingen. Onderzoek van het CBP naar bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen.

CBP (22 juni 2010): Persbericht: Overtredingen van de wet bij bestandskoppeling.

CBP (november 2009): Bevindingen heimelijke waarneming, naleving informatieplicht door gemeenten.

CBP (25 november 2009): Persbericht: Naleving informatieplicht door sociale diensten nog steeds onvoldoende; 17 van 20 onderzochte sociale diensten informeren betrokkenen niet over heimelijke waarneming.

CBP (20 december 2007): Fraudebestrijding door bestandskoppeling. Brief aan de staatssecretaris van Sociale Zaken en Werkgelegenheid.

CBP (29 mei 2007): Ambtshalve onderzoek Waterproof. Brief aan de minister van Sociale Zaken en Werkgelegenheid.

CBP (2007): Informatieblad: Informatie delen in samenwerkingsverbanden.

CBP (12 juli 2006): Besluit voorafgaand onderzoek beëindigd, Koppeling Diftar.

CBP (2006): Informatieblad: Verstrekken van persoonsgegevens.

CBP (2006): Procesbeschrijving Interventieteams. Brief aan het ministerie van Sociale Zaken en Werkgelegenheid.

CBP (2006): Notitie bescherming persoonsgegevens door bestandskoppelingen.

Centrale Raad voor Beroep (27 april 2010). Uitspraak in hoger beroep n.a.v. Waterproof. LJN BM3881, Centrale Raad van Beroep, 08/6125 WWB.

T.F.M. Hooghiemstra en S. Nouwt, Tekst en toelichting Wet bescherming persoonsgegevens, SDU, derde druk, 2007.

R. Koorn et al. (2004). Privacy Enhancing Technologies. Witboek voor beslissers. Den Haag, Ministeriebzk.

Ministerie van Justitie (2009). Gewoon doen. Beschermen van veiligheid en persoonlijke levenssfeer. Den Haag, Ministerie van Justitie.

Ministerie Justitie en Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (3 november 2009). Evaluatie Wet bescherming persoonsgegevens. Brief van de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties aan de Voorzitter van de Tweede Kamer der Staten-Generaal. Den Haag, Ministerie Justitie.

Ministerie van Justitie, WODC (2008). Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk.

Ministerie van Justitie (2002): Handleiding voor de verwerker van persoonsgegevens

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (december 2010). Memo aan de leden, Consequenties uitspraak CRB van 15 december 2010

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (actueel). Format Projectvoorstel, Format Projectplan, Format Draaiboek.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (september 2010). Interventieteamprojecten vanaf 2004

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (7 april 2010). Zienswijze naar aanleiding van uw onderzoek, brief aan het CBP.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (maart 2010). Informatieproces risicoanalyse, eindrapportage werkgroep leercirkels.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2009). Jaarplan 2010.

Ministerie van Sociale Zaken en Werkgelegenheid Landelijke Stuurgroep Interventieteams (12 juli 2007). Memo aan de leden, Bestandskoppeling.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2007). Folder voor Interventieteams.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2004). Instructie voor het op basis van de modelmelding concretiseren van de melding van interventieteams.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams/CBP (2004). Melding privacy.

Ministerie van Sociale Zaken en Werkgelegenheid, Landelijke Stuurgroep Interventieteams (2003). Samenwerkingsovereenkomst voor interventieteams.

Ministerie van Sociale Zaken en Werkgelegenheid (2003). Interventieteams Multidisciplinaire samenwerking. Afsprakendocument tussen partijen.

Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (actueel). Format Intake. Format Data-inwinplan.

Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (week 46 2010). SIOD weekbericht: Hoorzitting bij CBP over Black Box project.

Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (2010). Pleitnotitie ten behoeve van het College bescherming persoonsgegevens (CBP) betreffende de hoorzitting over de Black Box.

Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (7 april 2010). Zienswijze naar aanleiding van uw onderzoek, brief aan het CBP.

Ministerie van Sociale Zaken en Werkgelegenheid, SIOD (april 2010). Black Box en selectieprofielen.

Ministerie van Sociale Zaken en Werkgelegenheid SIOD (2010). Procedure vernietiging IT bestanden.
Ministerie van Sociale Zaken en Werkgelegenheid SIOD en Stichting Inlichtingenbureau. Convenant 23 december 2008.

Ministerie van Sociale Zaken en Werkgelegenheid. (2010): Integrale Rapportage Handhaving 2009.

Ministerie van Sociale Zaken en Werkgelegenheid. (2010): Integrale Rapportage Handhaving 2009. Brief aan de TK.

Ministerie van Sociale Zaken en Werkgelegenheid. (2010): Controle door een interventieteam. Brochure.

Ministerie van Sociale Zaken en Werkgelegenheid. (10 juli 2009): Verzamelbrief Handhaving. Brief aan de TK.

Ministerie van Sociale Zaken en Werkgelegenheid. (zd): Instructie voor het op basis van de modelmelding concretiseren van de melding van interventieteams.

Ministerie van Sociale Zaken en Werkgelegenheid. (15 maart 2007): Fraude door bestandskoppeling. Brief aan het RCF Noord-Holland.

Ministerie van Sociale Zaken en Werkgelegenheid. (29 december 2007): Bestandskoppeling. Brief aan de voorz. van de TK.

Ministerie van Sociale Zaken en Werkgelegenheid. (23 mei 2003): Besluitvorming

Interventieteams. Brief aan de TK.

Ministerie van Sociale Zaken en Werkgelegenheid, IWI (oktober 2009). Signalering van fraude. Verkennende studie.

Ministerie van Sociale Zaken en Werkgelegenheid, IWI (juni 2008). Bestandskoppelingen. Een verkennende studie naar het gebruik van bestandskoppelingen in het kader van fraudebestrijding.

Regionaal Coordinatiepunt Fraudebestrijding Zuidoost Nederland (14 april 2010): Projectvoorstel Gebiedsgericht aanpak Donderberg Roermond. Brief aan de Landelijke Stuurgroep Interventieteams.

Regionaal Platform Fraudebestrijding Noord (april 2010): Projectvoorstel De Warme Bakker. Brief aan de Landelijk Stuurgroep Interventieteams.

Regionaal Coordinatiepunt Fraudebestrijding Noord-Holland (februari 2007): Brief aan Ministerie van SZW, Voorzitter LSI, Opschorting project Waterproof.

Regionaal Coordinatiepunt Fraudebestrijding Noord-Holland (februari 2007): Brief aan de minister van SZW, Standpunt CBP en bestandskoppelingen.

SEOR (2010). Eindrapportage selectieprofielen WWB en UWV. Onderzoek voor SIOD/SZW. Rotterdam, SEOR.

Stichting Inlichtingenbureau (16 november 2010): Black box procedurebeschrijving.

Stichting Inlichtingenbureau (8 november 2010): Informatiebeveiligingsbeleid 2010/2011, Addendum Dienstverlening SIOD (Black Box), v 1.1.

Stichting Inlichtingenbureau (16 februari 2010): Informatiebeveiligingsbeleid 2009/2010.

E. Schreuders (2001). Datamining, de toetsing van beslisregels en privacy. Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen.

VNG (juni 2005): Fraudebestrijding via interventieteams. Brief aan de leden.

VNG (2005): Landelijke Platforms Fraudebestrijding. Bijlage bij ledenbrief.

Nationale Ombudsman (2009): Rapportnummer 2009/0210 In het kader van de actie "Aanpak Illegale Hotels".

Nationale Ombudsman (2009): Rapportnummer 2009/0095 In het kader van een huisbezoek Amsterdam, project 3W.

Nationale Ombudsman (2009): Rapportnummer 2009/030 - 2008/259 Interventieteam Zeist schendt huisrecht.

Ombudsman van Rotterdam (2007): Baas in eigen huis, Tja we komen eigenlijk voor alles.

Websites

Minszw/onderwerpen/fraudebestrijding
Minszw/ informatie voor gemeenten/dossiers/Handhaving
http://www.rcf.nl/
http://www.ngfg.nl/
http://www.bijstandsbond.org/

Bijlage 2: Lijst met geïnterviewden

RCF – Kenniscentra Handhaving:	10 2e
Sociale Verzekerings Bank	10 2e
UWV	10 2e
Arbeidsinspectie	10 2e
Belastingdienst	10 2e
Politie	10 2e
Minszw - SIOD	10 2e
Min. SZW - IWI	10 2e
Min. SZW	10 2e
Belastingdienst - FIOD	10 2e
Min. Veiligheid en Justitie	10 2e
Stichting Inlichtingenbureau	10 2e
Landelijke Clientenraad	10 2e
BKWI	10 2e
Externe expert	10 2e

Bijlage 3: Schema

Gegevensverwerking zonder en met Black Box