



**Correctie van  
persoonsgegevens**

**Organisatieoverstijgende  
aanpak probleemgevallen**

*april 2013*



# Colofon

<b>DATUM</b>	3 april 2013
<b>VERSIE</b>	1.0
<b>PROJECTREFERENTIE</b>	Faciliteren van inzage en correctie door burgers van hun persoonsgegevens
<b>NOVAY REFERENTIE</b>	<a href="https://doc.novay.nl/dsweb/Services/Document-137676">https://doc.novay.nl/dsweb/Services/Document-137676</a>
<b>TOEGANGSRECHTEN</b>	Projectteam en opdrachtgever
<b>STATUS</b>	definitief
<b>EDITOR</b>	dr.ir. Piet Boekhoudt
<b>AUTEURS</b>	<b>Novay:</b> dr.ir. Piet Boekhoudt, dr. Wolfgang Ebbers, dr. Bob Hulsebosch, dr. Joop Kielema, Guido Annokkée
<b>OPDRACHTGEVER</b>	<b>Ministerie van Binnenlandse Zaken en Koninkrijksrelaties</b> <b>Centraal Meld- en informatiepunt Identiteitsfraude en -fouten (CMI):</b> drs. Michel Savelkoul



Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

## Synopsis

Dit rapport beschrijft onderzoek naar de problematiek van het corrigeren van fouten in persoonsgegevens. Daarbij gaat het vooral over de probleemgevallen, de 'schrijnende zaken'. In deze zaken lukt het burgers niet, met medewerking van overheidorganisaties, om hardnekkige fouten in hun persoonsgegevens te laten herstellen. De omvang van deze problematiek is weliswaar beperkt, maar heeft voor de betreffende burgers buitengewoon vervelende en langdurige consequenties. Dit rapport doet (proportionele) aanbevelingen om deze 'schrijnende zaken' te voorkomen en in voorkomende gevallen effectiever op te lossen.

### **Disclaimer**

Dit onderzoek is uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De verantwoordelijkheid voor de inhoud van het onderzoek berust bij de auteurs. De inhoud vormt niet per definitie een weergave van het standpunt van de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

# Inhoudsopgave

<b>MANAGEMENTSAMENVATTING</b>	<b>1</b>
<b>1 INLEIDING</b>	<b>3</b>
1.1 Correctie van persoonsgegevens	3
1.2 Opdrachtoomschrijving	3
1.3 Onderzoeksvragen	4
1.4 Onderzoeksaanpak	5
1.5 Leeswijzer	8
<b>2 PROBLEMATIEK</b>	<b>9</b>
2.1 Beschrijving van de problematiek	9
2.2 Analyse van de Casuïstiek	11
2.3 Inzichten uit interviews	14
2.4 Omvang van de problematiek	17
<b>3 OPLOSSINGSRICHTING</b>	<b>23</b>
3.1 Voorgestelde oplossingsrichting	23
3.2 Waarom deze oplossingsrichting?	24
3.3 Voorgestelde werkwijze en ondersteuning	25
<b>4 AANBEVELINGEN VOOR VERVOLG</b>	<b>29</b>
<b>GERAADPLEEGDE BRONNEN</b>	<b>33</b>
<b>GECONSULTEERDE ORGANISATIES</b>	<b>35</b>
<b>DEELNEMERS INTERVIEWS EN EXPERTSESSIES</b>	<b>36</b>
<b>BIJLAGE: CASUÏSTIEK</b>	<b>37</b>
Casus 1: Een of meer onbekende banen op je conto	38
Casus 2: Van toeslag naar loverboy	39
Casus 3: Niet alle diploma's in mijnoverheid.nl	40
Casus 4: Twee personen versmelten tot één administratieve persoon	41
Casus 5: Persoonsverwisseling: de verplichte cursus alcohol en verkeer	42
Casus 6: Nieuw BSN gekregen	43
Casus 7: Echt paspoort met BSN van een ander	44
Casus 8: Adressering van correspondentie	45
Casus 9: Werkstraf voor vals ID	46
Casus 10: Samenvoegen van adressen	47
Casus 11: De zaak Romet – 1737 auto's op naam	48
<b>BIJLAGE: INTERVIEWPROTOCOL</b>	<b>49</b>



# Managementsamenvatting

Het rapport 'Correctie van persoonsgegevens - Organisatieoverstijgende aanpak probleemgevallen' is het resultaat van onderzoek dat is uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). De **aanleiding** voor het onderzoek komt voort uit de ervaringen van het Centraal Meldpunt Identiteitsfraude en – fouten (CMI) en uit de ambitie van de minister van BZK. De minister heeft aangegeven burgers beter te willen equiperen in het (laten) corrigeren van fouten die zijn ontstaan in overheidbestanden.

Het gebruik van foutieve (persoons)gegevens kan **grote impact op het leven van burgers** hebben. Mensen moeten bijvoorbeeld boetes betalen voor niet gemaakte overtredingen, burgersservicenummers worden zonder medeweten van de burger voor het aanvragen van toeslagen gebruikt, etc. Het is dan voor een burger extra pijnlijk als de overheid niet in staat is de burger te helpen en de burger vastloopt in bureaucratie, waarbij partijen naar elkaar of naar het correct volgen van procedures (ver-)wijzen. Ook de overheid zelf loopt hierdoor reputatieschade op.

Het rapport beschrijft onderzoek naar de problematiek van het corrigeren van fouten in persoonsgegevens. We hanteren daarbij voor het begrip persoonsgegeven de definitie uit de *Wet bescherming persoonsgegevens (Wbp)*:

*Een **persoonsgegeven** is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.*

De **correctieproblematiek van persoonsgegevens** omschrijven we als volgt:

*De **correctieproblematiek van persoonsgegevens** betreft de problemen die burgers ervaren door fouten in hun persoonsgegevens. Het gaat daarbij vooral om de probleemgevallen, de 'schrijnende zaken'. In deze zaken lukt het burgers niet, met medewerking van overheidsorganisaties, om hardnekkige fouten in hun persoonsgegevens te laten herstellen.*

De **doelstelling van dit onderzoek** is om te vast te stellen in hoeverre en op welke wijze overheidsorganisaties burgers nu de mogelijkheid bieden om fouten in hun persoonsgegevens gecorrigeerd te krijgen. Ook in een stadium waarin nog niet helder is of en welke gegevens foutief zijn, maar waar burgers melden dat er 'iets niet klopt'. Het gaat daarbij om:

- de vraag of de overheid effectieve correctie-instrumenten biedt;
- de vraag of de overheid bij ontdekking van foutieve gegevens en verrijkte data juist en volledig corrigeert.

Een subdoel is om, indien mogelijk, een beeld te krijgen van de omvang van de fouten in persoonlijke gegevens in overheidsbestanden die gekoppeld zijn aan het GBA.

In het onderzoek zijn **zowel kwalitatieve als kwantitatieve aspecten** aan bod gekomen, met een sterke **focus op kwalitatieve aspecten** en kwantitatieve onderbouwing waar mogelijk. Daarbij is nadrukkelijk gewerkt met casuïstiek. Cases geven inzicht in de verschillende soorten fouten die in de praktijk worden gemaakt en hoe er mee wordt omgegaan. Deze geven een rijk beeld van de oorzaken van de fouten, welke zich goed laten vertalen naar praktisch

bruikbare adviezen. In een **bijlage** bij het rapport wordt een elftal **casussen** beschreven en nader uitgewerkt.

Centraal in het onderzoek staat het proces van inzage en correctie. In het proces wordt de samenhang tussen de inrichting en uitvoering van het proces, de besturing van het proces en de toegankelijkheid van de informatie onderzocht. De inrichting en uitvoering van het proces wordt verder onderverdeeld in de *constatering* van de foutieve persoonsgegevens, *procedure* voor het corrigeren van fouten en daadwerkelijke *correctie* van gegevens.

Omdat de meeste fouten die bij het CMI binnenkomen betrekking hebben op sociale zekerheid, arbeid en auto's heeft het onderzoek zich op deze drie domeinen geconcentreerd.

In de **onderzoeksaanpak** is de volgende **fasering** aangebracht:

- Fase 1: Identificeren en analyseren van de huidige stand van zaken d.m.v. **cases**
- Fase 2: Terugkoppeling van de resultaten in **interviews met experts**
- Fase 3: **Expertsessies** voor het aftasten van draagvlak voor oplossingsrichtingen voor de correctieproblematiek
- Fase 4: Afronding en rapportage

**Hoofdstuk 1** van het rapport gaat nader in op de onderzoeksoopdracht, de onderzoeksvragen en de onderzoeksaanpak.

**Hoofdstuk 2** beschrijft de **problematiek** van burgers die het niet lukt om, met medewerking van overheidorganisaties, hardnekkige fouten in hun persoonsgegevens te laten herstellen. Aan de hand van casuïstiek en de analyse daarvan wordt de aard en de omvang van de problematiek geïllustreerd en nader geduid. Uit het onderzoek komt naar voren dat de (numerieke) omvang van de correctieproblematiek niet groot is. Echter, voor de individuele burger kan het probleem wel degelijk groot zijn met langdurige en ernstige gevolgen voor hemzelf en zijn omgeving. Hoewel overheidsorganisaties zich in het algemeen inzetten om, binnen de eigen procedurele en juridische grenzen, probleemgevallen op te lossen, blijkt het in de praktijk lastig om organisatiegrensoverschrijdende zaken op te lossen. De correctieproblematiek speelt zich af in de ketens.

**Hoofdstuk 3** beschrijft een **oplossingsrichting** voor de correctieproblematiek. Uit zowel de interviews met experts als de analyse van de casuïstiek komt een aantal mogelijkheden naar voren om de correctieproblematiek aan te pakken. Vanwege de omvang van de problematiek, ligt een proportionele oplossingsrichting voor de hand. Proportioneel betekent dat er geen maatregelen worden voorgesteld die een onevenredig zware belasting voor (ketens van) overheidorganisaties betekenen in termen van procedures, werkwijzen en kosten. Een deel van de oplossingsrichting is van preventieve aard, een ander deel heeft te maken met de effectieve behandeling van (schrijnende) probleemgevallen. Het betreffende hoofdstuk gaat vooral in op de effectieve behandeling van schrijnende zaken in termen van meer samenwerking in ketens. Hiervoor reikt het rapport een zestal instrumenten aan om bij het oplossen van probleemgevallen binnen de ketens (beter) te kunnen samenwerken.

**Hoofdstuk 4**, tenslotte, doet in aansluiting op de voorgestelde en met experts getoetste oplossingsrichtingen een achttal **aanbevelingen voor vervolg**. De rol die het CMI hierbij kan spelen wordt in de aanbevelingen verder uitgewerkt.



# 1 Inleiding

## 1.1 CORRECTIE VAN PERSOONSGEGEVENS

Het gebruik van foutieve (persoons)gegevens kan grote impact op het leven van burgers hebben. Mensen moeten bijvoorbeeld boetes betalen voor niet gemaakte overtredingen, burgersservicenummers worden zonder medeweten van de burger voor het aanvragen van toeslagen gebruikt, etc. Het is dan voor een burger extra pijnlijk als de overheid niet in staat is de burger te helpen en de burger vastloopt in bureaucratie, waarbij partijen naar elkaar of naar het correct volgen van procedures (ver-)wijzen. Ook de overheid zelf loopt hierdoor reputatieschade op. Het is niet goed als blijkt dat tussenkomst van de media nodig is om fouten te herstellen. Het vertrouwen van burgers in de overheid daalt hierdoor, met alle problemen van dien.

Wanneer een fout bij de overheid aan het licht komt, blijkt het voor burgers in de praktijk niet altijd eenvoudig om de fout(en) te herstellen. Het lijkt erop dat de burger hierin beter gefaciliteerd kan worden. Zeker ook als het gaat om correctie van basis persoonsgegevens (NAW-gegevens, BSN-nummer, etc.) in combinatie met verrijkte gegevens die door verschillende organisaties in ketens worden gebruikt en gedeeld. Daarnaast is correctie met terugwerkende kracht vaak zeer ingewikkeld of niet mogelijk.

Het aanbieden van een correctievoorziening creëert ook risico's. Kwaadwillenden kunnen misbruik maken van de voorziening. Om de burger gegevens te laten corrigeren is het noodzakelijk zijn/haar identiteit vast te stellen met een betrouwbaar authenticatiemiddel, ook online. Daarnaast moet duidelijk zijn welke gegevens de burger zelf kan corrigeren en welke gegevens slechts door geautoriseerde partijen aangepast mogen worden. Het veranderen van het nummer van een mobiele telefoon is iets dat de burger zelf zou kunnen doen; het veranderen van een geboortedatum daarentegen niet.

BZK streeft ernaar, dat burgers hun persoonsgegevens bij de overheid kunnen inzien via MijnOverheid. Daar kunnen ze zelf controleren of de overheid beschikt over correcte gegevens. Inzage en correctie via MijnOverheid dekt echter niet volledig de behoefte af, om de volgende redenen:

- nog niet alle informatie is te zien op MijnOverheid;
- niet alle (verrijkte) informatie over personen en goederen zit in dossiers en is geschikt of bedoeld om via MijnOverheid zichtbaar te maken;
- corrigeren van fouten kan een zaak zijn van informatieketens en niet alleen van individuele organisaties;
- burgers weten vaak niet dat er foutieve gegevens zijn geregistreerd, maar maken bezwaar tegen een besluit. De wet voorziet dan wel in klacht-, bezwaar- en beroepsmogelijkheden en in correctiemogelijkheden, maar het kan desondanks onduidelijk zijn of / en welke procedures er zijn om fouten te herstellen..

Om deze redenen is aanvullend onderzoek nodig naar andere inzage- en correctieprocedures.

## 1.2 OPDRACHTOMSCHRIJVING

Dit rapport is het resultaat van een onderzoek dat is uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

De aanleiding voor het onderzoek komt voort uit de ervaringen van het Centraal Meldpunt Identiteitsfraude en – fouten (CMI) en uit de ambitie van de minister van BZK. De minister heeft aangegeven burgers beter te willen equiperen in het (laten) corrigeren van fouten die zijn ontstaan in overheidbestanden. Aanleiding is tevens het verder willen verhogen van de kwaliteit van de Gemeentelijke Basisadministratie (GBA).

De doelstelling van dit onderzoek is om te vast te stellen in hoeverre en op welke wijze overheidsorganisaties burgers nu de mogelijkheid bieden om fouten in hun persoonsgegevens gecorrigeerd te krijgen. Ook in een stadium waarin nog niet helder is of en welke gegevens foutief zijn, maar waar burgers melden dat er 'iets niet klopt'. Het gaat daarbij om:

- de vraag of de overheid effectieve correctie-instrumenten biedt;
- de vraag of de overheid bij ontdekking van foutieve gegevens en verrijkte data juist en volledig corrigeert.

Voor het begrip persoonsgegeven hanteren we in dit rapport de definitie uit de *Wet bescherming persoonsgegevens (Wbp)*:

*Een **persoonsgegeven** is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.*

Een subdoel is om, indien mogelijk, een beeld te krijgen van de omvang van de fouten in persoonlijke gegevens in overheidbestanden die gekoppeld zijn aan het GBA en zicht te krijgen op de correctie-instrumenten en hun gebruikersvriendelijkheid. Het begrip overheid moet hierbij ruim worden geïnterpreteerd. Onder fouten wordt hier verstaan fouten die nadelig uitwerken voor burgers en/of overheid. Het gaat niet om procedures rond privacy. Het onderzoek richt zich op correctieprocedures van persoonsgegevens en verrijkte data met partijen die gegevens halen uit het GBA.

### 1.3 ONDERZOEKSVRAGEN

Opdrachtgever heeft in zijn opdracht de volgende onderzoeksvragen geformuleerd:

1. Hoe vaak ontdekt een overheidsorganisatie dat er wordt gewerkt met foutieve persoonsgegevens en verrijkte data?
  - a. Hoe heeft de organisatie dit gemerkt?
  - b. Of/en hoe heeft de betreffende burger:
    - i. dit gemerkt;
    - ii. dit aangekaart.
2. In hoeverre heeft de organisatie zelf een inzage en/of correctieprocedure?
  - a. In hoeverre is deze er voor burgers?
  - b. Is een correctieverzoek ook mogelijk via internet (met uitzondering van correcties die mogelijk zijn via mijnoverheid.nl)?
3. Hoe heeft de burger de foutieve persoonsgegevens en/of verrijkte data gecorrigeerd/laten corrigeren?
4. Hoe heeft de overheidsorganisatie de foutieve persoonsgegevens en/of verrijkte data gecorrigeerd?
  - a. Binnen de organisatie;

- b. Buiten de organisatie (bij gekoppelde gegevens).
5. Welke mogelijkheden tot correctie missen:
- a. De overheidsorganisatie;
  - b. De burger.

Uit de onderzoeksvragen blijkt dat het probleemveld complex, maatschappelijk gevoelig en onvoldoende verkend is. Het betreft vraagstukken over maatschappelijk en bestuurlijk draagvlak, organisatorische processen en procedures, wetgeving en technologie. In de beantwoording van de vraagstelling is dan ook, naast de letterlijke vragen, een systematiek toegepast die er voor zorgt dat alle relevante aspecten de revue passeren. De aanpak daarvoor is uitgewerkt in de volgende paragraaf.

#### **1.4 ONDERZOEKSAANPAK**

In het onderzoek zijn zowel kwalitatieve als kwantitatieve aspecten aan bod gekomen, met een sterke focus op kwalitatieve aspecten en kwantitatieve onderbouwing waar mogelijk. Daarbij is nadrukkelijk gewerkt met casuïstiek. Cases geven inzicht in de verschillende soorten fouten die in de praktijk worden gemaakt en hoe er mee wordt omgegaan. Deze geven een rijk beeld van de oorzaken van de fouten, welke zich goed laten vertalen naar praktisch bruikbare adviezen.

Nadrukkelijk wordt dit onderzoek vanuit een *multi-stakeholder* perspectief uitgevoerd. Denk hierbij aan uitvoeringsorganisaties, gemeenten, ketenpartijen (zoals brokers), meldpunten en natuurlijk de burger zelf. Centraal staat het functioneren van het netwerk. Kenmerkend voor een netwerk is dat *stakeholders* niet alleen verschillende visies op een probleem hebben, maar ook verschillende belangen, voortkomend uit de verschillende rollen en taken die een *stakeholder* in het netwerk vervult. Mogelijke oplossingen zullen hier rekening mee moeten houden.

In het onderzoek wordt ook meegenomen hoe fouten verder kunnen worden voorkomen. Het doel is ook om de kwaliteit van het GBA verder te vergroten. Het inbouwen van nieuwe of extra controlemechanismen kan mogelijk de kwaliteit van de gegevens verbeteren. En daardoor de kans op fouten verkleinen. De beste maatregelen tegen fouten in persoonsgegevens zijn maatregelen om ze te voorkomen, hoewel 100% foutvrij natuurlijk niet haalbaar is en er een oplossing moet zijn voor uitzonderlijke gevallen.

Centraal in het onderzoek staat het proces van inzage en correctie. In het proces wordt de samenhang tussen de volgende elementen onderzocht, te weten:

1. De inrichting en uitvoering van het proces, in termen van triggers van proces (wie constateert de fout, overheid of burger) duidelijkheid, overdrachtsmomenten, communicatie en toegankelijkheid voor burgers;
2. Hoe is de besturing (governance) van dit proces, in termen van taakverdeling, verantwoordelijkheden, duidelijkheid in rolverdeling tussen actoren;
3. De toegankelijkheid van de informatie, in termen van beschikbaarheid en vindbaarheid, maar ook in termen van (semantische) bruikbaarheid van gegevens.

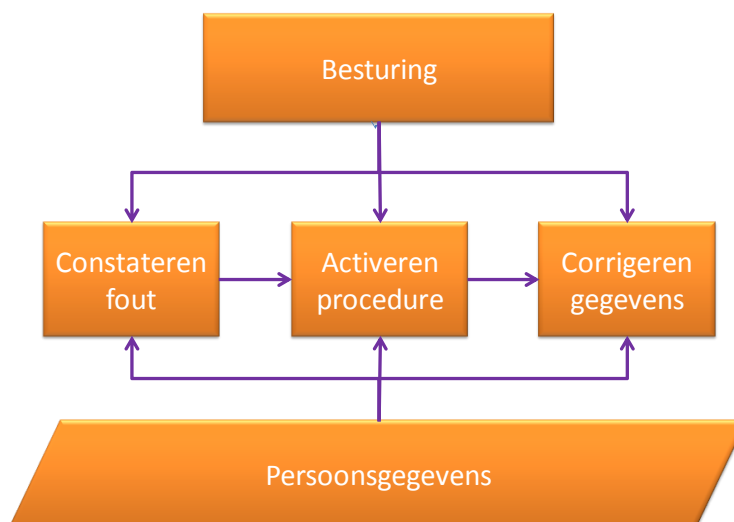
Deze drie aspecten worden in samenhang onderzocht. Verbeteringen zijn alleen te bereiken door maatregelen te nemen die deze samenhang bevorderen. Procedures werken bijvoorbeeld alleen als er voldoende doorzettingsmacht in een netwerk is om de procedure daadwerkelijk uit te voeren en de betrokken partijen over

een gedeelde informatiepositie beschikken.

De inrichting en uitvoering van het proces wordt verder onderverdeeld in de volgende stappen:

1. Constatering: hoe en door wie wordt geconstateerd dat gewerkt wordt met foutieve gegevens? Dit aspect heeft te maken met de mogelijkheden die burgers hebben om persoonsgegevens in te zien en de uitbreidingen die worden gezocht in mijnoverheid.nl. Maar het heeft heel nadrukkelijk ook te maken met de mogelijkheden die burgers wordt geboden om niet-elektronische gegevens in te zien, zoals gegevens in (eventueel papieren) dossiers. Overheden moeten burgers faciliteren om van hun recht op inzage gebruik te maken. In de fase van constatering speelt de overheid een actieve rol. Zij zal moeten constateren of van een beslissing mag worden aangenomen dat zij op juiste (persoons)gegevens is gebaseerd. Geautomatiseerde beslissingen zijn niet altijd juiste beslissingen, controle blijft daarom belangrijk. Een aantal (extreme) gevallen van misbruik laten zien dat de overheid hier al in een vroeg stadium had kunnen constateren dat er iets niet klopte.
2. Procedure: zijn er procedures om fouten te corrigeren en hoe zien ze er uit? De procedures zijn opgesteld om fouten binnen afzonderlijke organisaties te herstellen. In de iOverheid waarin informatie op veel plaatsen in een netwerk wordt hergebruikt, is het wijzigen van gegevens een proces dat ergens in een netwerk plaatsvindt en niet meer bij de afzonderlijke organisaties. Hier speelt ook de vraag welke wettelijke kaders er zijn en of die wettelijke kaders vertaald zijn naar interne procedures.
3. Correctie van gegevens (uitvoering): hoe worden deze procedures in de praktijk gebruikt, door zowel overheden als burgers? Dit is het aspect dat het meest uitgebreid in kaart zal worden gebracht. Aspecten die hier spelen zijn onder andere , ketensamenwerking, gedrag van afzonderlijke ambtenaren, technische voorzieningen, kwaliteit van gegevensbeheer, juridische kaders.

Het schema in Figuur 1 geeft een overzicht van deze elementen van het onderzoek.



**Figuur 1 Correctieproces**

Omdat de meeste fouten die bij het CMI binnenkomen betrekking hebben op sociale zekerheid, arbeid en auto's heeft het onderzoek zich op deze drie domeinen geconcentreerd.

Daarbij is in de onderzoeksaanpak de volgende fasering aangebracht:

- Fase 1: Identificeren en analyseren van de huidige stand van zaken d.m.v. cases
- Fase 2: Terugkoppeling van de resultaten in interviews
- Fase 3: Expertsessies (draagvlak)
- Fase 4: Afronding en rapportage

De fasen worden hieronder elk kort beschreven.

### **Fase 1: Identificeren en analyseren van de huidige stand van zaken d.m.v. cases**

De eerste fase van het onderzoek richt zich op het maken van een aantal, maar wel diverse, cases. Het doel is om een aantal rijke beschrijvingen van voorbeelden te maken. Dit biedt de mogelijkheid om de problematiek in de diepte te onderzoeken en om alle (mogelijk) relevante aspecten te identificeren. Het in Figuur 1 geschetste model is hiervoor het uitgangspunt. De analyses hebben tot doel om de relatie tussen structuur en proces te onderzoeken.

In de aanpak is er in eerste instantie voor gekozen om de cases te zoeken bij een aantal grote uitvoeringsorganisaties en hiervoor een aantal interviews te plannen bij deze organisaties. Tijdens de uitvoering van het onderzoek is echter gebleken dat organisaties hieraan moeilijk medewerking konden verlenen. De organisaties die in dit onderzoek benaderd zijn, worden vermeld in de Bijlage: Geconsulteerde organisaties. De belangrijkste reden hiervoor is, dat is gebleken dat organisaties van mening zijn dat zij het probleem binnen de eigen mogelijkheden en procedures oplossen. Het probleem voor de burger hoeft daarmee echter niet opgelost te zijn, omdat het probleem op een andere plaats in de keten kan blijven bestaan of kan opduiken. Vandaar dat in de aanpak in tweede instantie is gekozen voor cases die zijn aangedragen door het CMI en de Nationale Ombudsman. In deze cases komt inderdaad de ketenproblematiek duidelijk naar voren.

### **Fase 2: Terugkoppeling van de resultaten in interviews**

Om diepte aan de uitwerking van de cases te geven hebben interviews met deskundigen plaatsgevonden. Deze interviews toetsen de inzichten uit de cases en zijn bedoeld om o.a. meer inzicht te bieden in de volgende zaken:

- omvang van de problematiek;
- triggers van het proces, verzoeken tot wijzigen of fouten in beslissingen;
- aanwezigheid van procedures;
- soorten procedures en werkprocessen;
- escalatiemogelijkheden;
- complexiteit van het (informatie)netwerk waarin de fout zich heeft voorgedaan;
- mogelijkheden en verantwoordelijkheden die organisaties hebben om correcties te maken (rol in de besturing);
- de toegankelijkheid van informatie.

Naast interviews met deskundigen bij uitvoeringsorganisaties is ook gesproken met deskundigen die goed zicht hebben op de informatieketen waar deze organisaties mee te maken hebben. In het bijzonder is binnen het domein van sociale zekerheid gesproken met BKWI (Bureau Keteninformatisering Werk & Inkomen), omdat BKWI zich in een unieke positie bevindt om te monitoren welke partij welke gegevens gebruikt en/of aanlevert in de SUWI-keten en op een efficiënte manier actie kan ondernemen indien fouten geconstateerd zijn in de gegevens.

### **Fase 3: Expertsessies (draagvlak)**

Naar aanleiding van de inzichten uit deskresearch, analyse van het casemateriaal en interviews met deskundigen ontstaat een beeld van mogelijke oplossingsrichtingen. In expertsessies worden de voorlopige inzichten en oplossingsrichtingen gepresenteerd. Er zal nadrukkelijk gezocht worden naar terugkoppeling op de resultaten en getoetst worden of er draagvlak is voor de voorgestelde oplossingsrichting. Zonder overigens van de betrokkenen commitment namens hun organisatie te vragen. Voor de expertsessies zijn vertegenwoordigers van de belangrijkste partijen uit de drie eerder genoemde domeinen uitgenodigd. Van de expertsessies zijn schriftelijke verslagen gemaakt, die aan de deelnemers ter aanvulling en correctie zijn voorgelegd.

### **Fase 4: Afronding en rapportage**

De uitkomsten uit de vorige fases zijn in deze fase geanalyseerd en gerapporteerd in de onderhavige rapportage. Hierin worden ook handreikingen gegeven aan de opdrachtgever en overheidsorganisaties voor betere correctiemogelijkheden en –procedures. De bevindingen zullen worden gepresenteerd aan de opdrachtgever en de begeleidingscommissie bij dit onderzoek.

## **1.5 LEESWIJZER**

Dit rapport is als volgt opgebouwd:

- **Hoofdstuk 2** beschrijft de problematiek van burgers die het niet lukt om, met medewerking van overheidorganisaties, hardnekkige fouten in hun persoonsgegevens te laten herstellen. Aan de hand van casuïstiek en de analyse daarvan wordt de aard en de omvang van problematiek geïllustreerd en nader geduid.
- **Hoofdstuk 3** gaat in op de voorgestelde oplossingsrichting. Deze oplossingsrichting gaat over proportionele maatregelen, zowel voor wat betreft preventie als effectieve behandeling van schrijnende zaken.
- **Hoofdstuk 4** doet naar aanleiding van de bevindingen uit het onderzoek een aantal aanbevelingen. De rol die de opdrachtgever, het CMI, hierbij kan spelen wordt in de aanbevelingen verder uitgewerkt.
- In de **bijlage** bij dit rapport zijn illustratieve casussen opgenomen die een rijk beeld geven van de correctieproblematiek.

# 2 Problematiek

## 2.1 BESCHRIJVING VAN DE PROBLEMATIEK

In essentie draait het in dit onderzoek om de problematiek van burgers die door fouten in hun persoonsgegevens vastlopen bij overheden en niet in staat zijn om de foutieve persoonsgegevens gewijzigd te krijgen. Alvorens een preciezere beschrijving te geven van de problematiek, herhalen we de definitie van het begrip persoonsgegeven uit de *Wet bescherming persoonsgegevens (Wbp)*:

*Een **persoonsgegeven** is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.*

Gegevens zijn dus persoonsgegevens als de gegevens informatie bevatten over een natuurlijke persoon en die persoon identificeerbaar is.

Dit rapport beschrijft onderzoek naar de problematiek van het corrigeren van fouten in persoonsgegevens. We omschrijven de correctieproblematiek van persoonsgegevens als volgt

*De **correctieproblematiek van persoonsgegevens** betreft de problemen die burgers ervaren door fouten in hun persoonsgegevens. Het gaat daarbij vooral om de probleemgevallen, de ‘schrijnende zaken’. In deze zaken lukt het burgers niet, met medewerking van overheidsorganisaties, om hardnekkige fouten in hun persoonsgegevens te laten herstellen.*

Een illustratief voorbeeld van de correctieproblematiek, staat beschreven in de volgende casus:

*Mevrouw V. heeft vijf Chinese restaurants als werkgever op haar naam staan, terwijl ze daar niet heeft gewerkt. Er blijkt een, verder onbekende, man op een vervalst paspoort met haar BSN te hebben gewerkt. Een lijdensweg langs Belastingdienst en UWV volgt, en beide partijen wijzen naar elkaar. Niemand wil of kan deze gegevens wissen, want er zijn pensioenrechten opgebouwd, premies betaald. Er wordt een halve oplossing bedacht: de Belastingdienst zal de signalen van het UWV over de betreffende banen handmatig negeren, zodat er geen belastingboetes ontstaan. De structurele oplossing voor compleet fouterstel is er nog niet. De man met het vervalste paspoort heeft onlangs nog in Zeeland gewerkt, maar is weer spoorloos.*

Dat burgers vastlopen wil geenszins zeggen dat de betrokken overheidsorganisaties en ketenpartners zich niet inzetten om deze problematiek op te lossen en te voorkomen. Figuur 2 visualiseert enkele aspecten van deze problematiek. Men loopt in de praktijk echter tegen barrières aan die een effectieve afhandeling verhinderen. De belangrijkste barrières die effectieve correctie bemoeilijken zijn:

- wetgeving, bijvoorbeeld om met terugwerkende kracht te corrigeren;
- beperkte mogelijkheden om de onjuistheid van gegevens vast te stellen;

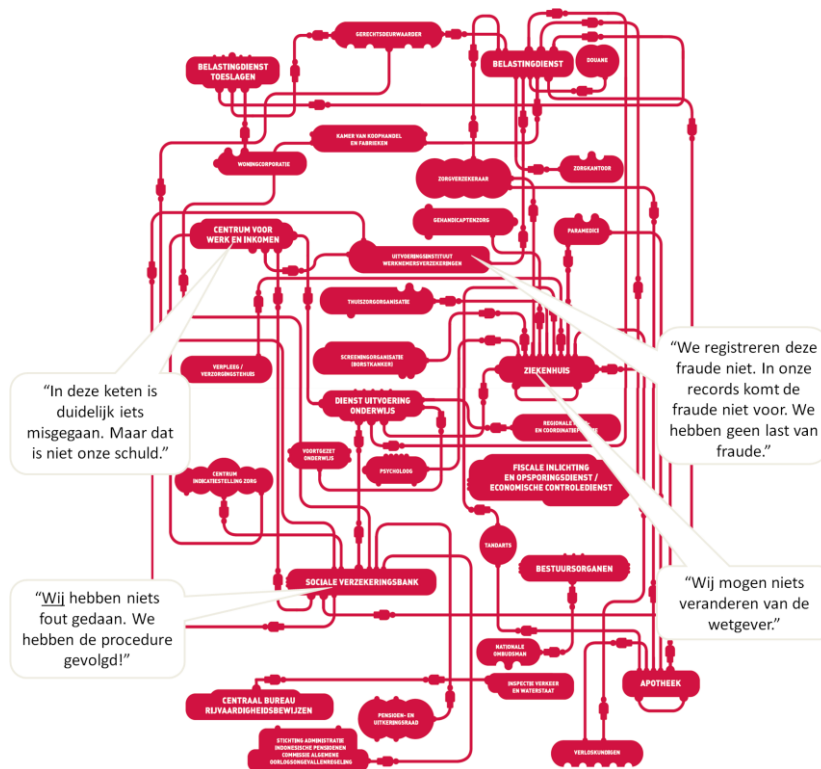
- de- en hercontextualiseren van gegevens;
- vernetwerking van de informatievoorziening;
- verkokering en onvoldoende gezamenlijk handelen binnen ketens.

Wetgeving kan zorgen voor een bepaalde mate van complexiteit, waardoor correctie moeilijk of onmogelijk lijkt en men in voorkomende gevallen de mogelijkheden voor een effectieve correctie niet voldoende (her)kent en benut. Een voorbeeld daarvan is te vinden in de loonaangifteketen: daar is wettelijk geregeld dat alles dat wordt aangeleverd, ook geregistreerd moet worden. Dat mag dan ook niet meer verwijderd worden. Alleen de zogenaamde inhoudingsplichtige (werkgever) of de Inspecteur van de Belastingdienst mag de 'werkgeschiedenis rechtzetten'. In het geval een bedrijf failliet gegaan is en niet meer te bereiken is, mag de Inspecteur van de Belastingdienst feiten veranderen. Een ander voorbeeld gaat over het gebruik van een verkeerde naam in een vonnis. Indien daar een verkeerde naam staat is het niet meer mogelijk om deze te verwijderen. Alleen via een herziening bij de Hoge Raad kan iemands naam gezuiverd worden. Ook wanneer deze naam dus vanaf het begin van het strafproces ten onrechte boven een vonnis heeft gestaan. Een derde voorbeeld komt uit de wet strafvordering justitiële gegevens. De strafrechtsketennummer (SKN) is de linking pin waar een zaak aan opgehangen wordt. Hier hangen de naam onder, de biometrische gegevens, de zaak zelf, etc. Maar de naam die bij deze SKN hoort kan juridisch gezien niet worden gewijzigd. Het SKN is namelijk geen gegeven van het Openbaar Ministerie dus het OM kan hierin geen wijzigingen maken. Binnen de overheid zijn meer van dit soort constructies van 'gespleten' wetgeving.

Daarnaast is het voor overheidsorganisaties soms moeilijk om vast te stellen of gegevens daadwerkelijk onjuist zijn. Het kan bijvoorbeeld lastig zijn om uit de polisadministratie vast te stellen of er sprake is van een incompleet of onjuist arbeidsverleden. Eventueel bewijs kan moeilijk geverifieerd worden, bijvoorbeeld omdat een werkgever failliet is gegaan.

Het risico dat fouten in persoonsgegevens grote gevolgen heeft voor burgers is de afgelopen jaren groter geworden. De informatie-uitwisseling vindt steeds meer geautomatiseerd plaats in ketens en netwerken; incorrecte gegevens verspreiden zich dan snel over meerdere partijen en menselijk toezicht op de correctheid van de gegevens neemt af. De WRR wijst op het gevaar van het de- en hercontextualiseren van gegevens en de grote mate van vernetwerking binnen de overheid. Hierdoor is vooral de besturing een punt dat aandacht verdient. De procedures voor de correctie zijn binnen de afzonderlijke organisaties belegd. Van deze organisaties wordt vervolgens, door een burger, verwacht dat zij in staat is om een genomen besluit aan te passen door gegevens te corrigeren. Als deze gegevens van een andere organisatie afkomstig zijn dan moet duidelijk zijn waar de gegevens gewijzigd kunnen worden en wie daartoe bevoegd is. In de praktijk blijkt dit een lastig proces. Het gaat er niet alleen om dat het proces formeel goed georganiseerd is, maar ook of in de praktijk het proces werkt. Door de sterke vernetwerking van de informatievoorziening wordt het steeds moeilijker om te achterhalen waar de fouten gemaakt zijn, wie ze moet herstellen en ook of het herstellen op een plaats ook tot effect heeft dat de fout in het hele netwerk is hersteld. Aandacht voor kwaliteit van persoonsgegevens gaat verder dan het volgen van procedures. Betrokkenheid bij de burger, goede onderlinge communicatie en leren van fouten zijn minstens zo belangrijk.





**Figuur 2 Gegevensstromen tussen (overheids)instanties gefaciliteerd door BSN**

(bron: WRR-rapport *iOverheid* (2011); iBC2013, Identiteitsfraude in ketens, M. Savelkoul)

In het proces van correctie moet naar voren komen welke foute gegevens van een burger tot een verkeerde beslissing hebben geleid. Hierin kunnen ook juridische aspecten een rol spelen. Bijvoorbeeld doordat bepaalde interpretaties of gebruik van bepaalde gegevens in de ene context correct zijn en in andere niet. Er kunnen immers semantische verschillen (verschillen in betekenis) in persoonsinformatie zijn. Zo zijn er verschillen in de manier waarop de Belastingwetgeving en de wet GBA het begrip woonadres definiëren, waardoor een persoon twee, correcte woonadressen kan hebben. Een basisregistratie heeft een bepaalde context als uitgangspunt. Veelal is deze context een wettelijke context. In andere wettelijke contexten kennen begrippen uit de basisregistraties, een net iets andere betekenis. Hergebruik van gegevens vraagt om een zorgvuldige afweging om te zien of en hoe de gegevens wel in een andere context gebruikt kunnen worden.

## 2.2 ANALYSE VAN DE CASUÏSTIEK

Een aantal illustratieve cases is bestudeerd om de problematiek in de diepte te onderzoeken en om alle mogelijk relevante aspecten te identificeren. De cases zijn uitgewerkt aan de hand van de onderzoeksvragen die beschreven staan in sectie 1.3:

- Fase 1: constateren van de fout
  - Door wie?
  - Soort fout?
  - Soort gegevens?
- Fase 2: procedure

- Bij welke partij?
- Aanwezig?
- Beschrijving
- Fase 3: uitvoering correctieproces
  - Acties door burger
  - Acties door overheid of andere organisaties
  - Mogelijkheden en beperkingen in uitvoering, zoals techniek, organisatie (bevoegdheden, interne werkprocessen), wetgeving, etc.
  - Resultaat
- Besturing
  - Conclusies t.a.v. besturingsmogelijkheden in correctieproces.

De uitgewerkte 11 cases zijn te vinden in de Bijlage: casuïstiek. Hier valt een aantal algemene zaken op:

- Het duurt over het algemeen erg lang voordat een case wordt opgelost. De aanpak is vaak weinig efficiënt en vergt veel inspanning van het slachtoffer zelf. Dit heeft te maken met het feit dat het in de beginfase van veel cases vaak onduidelijk is dat er sprake is van een probleem; pas in een ver gevorderd stadium wordt duidelijk dat het een probleemgeval betreft.
- Er zijn in veel gevallen meerdere partijen betrokken bij het probleem. Het slachtoffer wordt hierdoor regelmatig van het “kastje naar de muur” gestuurd. Daarnaast wordt het probleem pas echt opgelost als alle betrokken partijen hier werk van maken. Het gebrek aan afstemming resulteert in een betrokkenheid van het CMI en/of de Nationale Ombudsman. Deze twee partijen fungeren dan als een breekijzer of smeermiddel om tot een oplossing te komen.

Kijkend naar de specifieke processtappen, valt op dat de burger (het slachtoffer) in de meeste gevallen zelf de fout constateert en dit aankaart. De oorzaak van de fout is niet eenduidig te bepalen waardoor bijna iedere case op zichzelf staand is. Wel duidelijk is dat fouten voortkomen uit **fraude** (bewust kwaadwillende handelingen) van personen of uit **onvolkomenheden in het verwerkingsproces** van persoonsgegevens. Bij de eerste categorie is sprake van identiteitsfraude waarbij een kwaadwillend persoon de identiteit van iemand anders aanneemt. Deze persoon is dan vaak de dupe van de handelingen van de fraudeur die misbruikt maakt van voornamelijk NAW gegevens of het BSN. Een gestolen, verloren of vervalst identiteitsbewijs ligt hier vaak aan ten grondslag. Bij de tweede categorie is regelmatig sprake van persoonsvermenging. Dit kan komen door onzorgvuldige verificatie van identiteitsgegevens of door het onjuist koppelen van verschillende digitale identiteiten uit verschillende domeinen/organisaties. Dergelijke koppelingen worden vaak gebaseerd op verschillende sets aan persoonsgegevensbestanden die deels wel en deels niet overlappen of gebaseerd zijn op verschillende identificerende nummers (burgerservicenummer vs. strafrechtkenummer). Een bijkomend gevolg van persoonsvermenging is dat de dossiers over de betreffende persoon ook overgedragen worden naar het slachtoffer. Andere onvolkomenheden in het verwerkingsproces met persoonsgegevens betreffen tikfouten (in het BSN, naam, geboortejaar), onoplettendheid (bij twee burgers met grotendeels identieke persoonsgegevens, doorvoeren van onjuiste mutaties), onvolledige dossiervorming (het ontbreken van delen van het werkverleden of behaalde diploma's) of simpelweg het ontbreken van goede faciliteiten om de identiteit van de burger te verifiëren (de echtheid van een identiteitsbewijs kunnen controleren).

Aan de proceskant valt op dat het slachtoffer over het algemeen weet bij welke partij melding van de fout of het probleem te maken. Deze partij maakt hier in veel gevallen ook werk van. Soms gebeurt dit via goed omschreven processtappen, soms gebeurt dit op een bijna creatieve of ad hoc manier. De betrokkenheid van de uitvoerende ambtenaar speelt daarbij een belangrijke rol in een succesvolle afronding van het herstelproces. Echter, bij de uitvoering van het correctieproces lopen deze ambtenaren vaak tegen verschillende beperkingen aan zoals het gemis van kennis om een probleemgeval te herkennen en vervolgens aan te pakken of het ontbreken van mandaat om onjuiste gegevens te corrigeren, door bijvoorbeeld vigerende wetgeving of omdat dit door een andere partij dient te gebeuren.

De echte problemen beginnen vaak als het correctiespoor dood loopt binnen de eigen organisatie wat vervolgens uitmondt in het doorverwijzen van het slachtoffer naar een andere organisatie. Partijen blijven dan naar elkaar wijzen voor de oplossing. In een aantal gevallen volgt daarna een escalatietraject via het CMI of de Nationale Ombudsman. Dergelijke trajecten zijn over het algemeen moeizaam maar succesvol.

Uit de cases en de gekozen aanpak om tot een oplossing te komen kunnen een aantal conclusies getrokken worden ter verbetering van het correctieproces:

- Voorkomen is beter dan genezen. Relatief veel probleemgevallen ontstaan door onvoldoende verificatie van de echtheid van identiteitsbewijzen. Een betere controle hierop zou kunnen bijdragen aan het reduceren van identiteitsfraude en persoonsvermenging door fouten in persoonsgegevens.
- Hetzelfde geldt voor het kunnen controleren van digitale persoonsgegevens. Ook hier ontbreken vaak de mogelijkheden om dit te doen. Het koppelen van bestanden zou kunnen helpen om meer zekerheid te krijgen over de betrouwbaarheid van de persoonsgegevens.
- De verzameling persoonsgegevens is soms niet groot genoeg om een persoon uniek te kunnen identificeren. Het uitbreiden van de set van persoonsgegevens bij het uitvragen van GBA kan voor unieke identificatie zorgen.
- Oplettendheid is geboden bij het aan elkaar koppelen van verschillende digitale identiteiten en daarbij behorende persoonsgegevens. Volledige zekerheid of deze digitale identiteiten bij dezelfde persoon behoren is vereist alvorens over te gaan tot koppelen. Het zelfde geldt voor het koppelen van een digitaal dossier aan een digitale identiteit.
- Meer bewustzijn is vereist op het herkennen van (mogelijke) probleem- of fraudegevallen. Indicatoren hiervoor in de systemen zijn wenselijk maar ontbreken vaak.
- Het is voor partijen vaak onduidelijk hoe om te gaan met situaties waarin sprake is van persoonsverwisseling. Richtlijnen hiervoor ontbreken.
- Domein- of organisatieoverstijgende correctieprocedures ontbreken. Als de betreffende partij er niet uit komt volgt doorverwijzing naar een andere partij met daarbij een grote kans op 'van kastje naar de muur'-situaties voor het slachtoffer.

Het met terugwerkende kracht corrigeren van de gevolgen van incorrecte persoonsgegevens of persoonsvermenging bij meerdere organisaties is niet triviaal. Soms moeten bij verschillende partijen, bijna tegelijkertijd corrigerende acties plaatsvinden. Een gezamenlijke inspanning is dan noodzakelijk. De inzet van het CMI zou kunnen helpen om een dergelijke inspanning te coördineren en tot een succes af te ronden.

## 2.3 INZICHTEN UIT INTERVIEWS

Om de aard en de omvang van de problematiek in kaart te brengen zijn interviews gehouden met experts. Voor deze interviews is gebruik gemaakt van een interviewprotocol (zie Bijlage: interviewprotocol). De interviews geven een rijk beeld van de correctieproblematiek, dat in hoofdlijn antwoorden geeft op de volgende vragen:

- hoe en door wie wordt een fout vastgesteld?
- hoe worden fouten gecorrigeerd?
- hoe groot is de correctieproblematiek?
- welke verbetermogelijkheden zijn er nodig?

### Hoe en door wie wordt een fout vastgesteld?

Fouten worden vastgesteld bij de **behandeling van zaken**, waarbij medewerkers tegen inconsistenties in gegevens kunnen aanlopen. Wanneer het gaat om fouten in het GBA, dan zou een terugmelding moeten worden gedaan, maar dat blijkt in de praktijk een weerbarstige regel te zijn. Een respondent merkte op dat professionals alleen een terugmelding zullen doen als het hun aangaat. Ze hebben het te druk om ook onderzoeken te kunnen doen. Er zal eerst 'gerede twijfel' moeten zijn. Daarnaast kan het heel goed voorkomen dat gegevens bij bijvoorbeeld UWV verschillen van de gegevens in de GBA, zoals adresgegevens. Dat hoeft niet te betekenen dat de gegevens fout zijn. Verder komt het voor dat de geboortedatum van iemand niet bekend is. In de GBA is het mogelijk om iemand als geboortedatum 00-00-52 te geven. Dit zou gewoon overgenomen moeten worden, maar de Belastingdienst kan dit niet gebruiken in hun systemen en maakt er dan bijvoorbeeld 01-01-52, 01-07-52 of 31-12-51 van. De semantiek van de gegevens en de context waarin het gebruikt wordt speelt dus een belangrijke rol bij het vaststellen of een gegeven juist is of niet. Wat is een adres? Welk adres moet/mag je gebruiken om een dossier naar toe te sturen? Mensen krijgen bijvoorbeeld geen uitkering als hun GBA-adres afwijkt; GBA hanteert het adres als daar waar iemand minimaal drie dagen in de week woont. Gegevens zijn niet noodzakelijk fout: het netto bedrag wordt aangeleverd door UWV terwijl de gemeente bruto nodig heeft.

Fouten kunnen ook ontstaan doordat aan gegevens een **verkeerde interpretatie** wordt gegeven. Wanneer iemand verhuisd is zonder een nieuwe bestemming op te geven, wordt dit vaak in de GBA in onderzoek gezet. Volgens een respondent komt het voor dat andere organisaties dan klakkeloos aan dat deze persoon vertrokken is zonder nieuwe bestemming, terwijl dat dus nog uitgezocht dient te worden.

Vaak worden fouten worden pas ontdekt wanneer de **burger** er mee bezig gaat, bijvoorbeeld tijdens het aanvragen van een uitkering. Een respondent merkte op dat correctieverzoeken bij UWV vaak vooruit lopen op wat in GBA staat. UWV weet eerder van adreswijzingen dan GBA, omdat mensen bang zijn om hun uitkering niet te ontvangen.

Verder maken overheidsorganisaties steeds vaker gebruik van **bestandsvergelijkingen** om mogelijke fouten te ontdekken en fraude te voorkomen. Er zijn burgers met schulden bij de overheid die zich uitschrijven bij een gemeente, maar zich niet bij een andere gemeente inschrijven. Deze mensen krijgen in GBA de status 'Vertrokken Onbekend Waarheen' (VOW-ers). Vaak zijn zij wel bij de politie bekend. Van ongeveer 55.000 mensen is bekend dat ze zijn vertrokken van hun oude adres, zonder dat hun nieuwe adres bekend is. Sommige mensen proberen daarmee schuldeisers en deurwaarders te ontlopen door hun nieuwe adres niet op te geven;

per jaar gaat het om 15.000 personen met uitstaande rekeningen van naar schatting zo'n 25 miljoen euro.

Koppeling van bestanden (GBA en Politie) zou kunnen helpen om deze bewuste ontlopers te vinden. Diverse respondenten vinden dat voorzichtigheid met het trekken van conclusies bij bestandsvergelijkingen wel geboden is. Bij een bestandvergelijking van UWV en de gemeente Amsterdam leek het erop dat er 8500 'spookburgers' waren die niet bij de gemeente Amsterdam geregistreerd staan en gemeentelijke belasting ontduiken, maar wel een uitkering van het UWV krijgen. Hoewel het onderzoek nog niet is afgerond, lijkt het er nu op dat er na 'afpellen' veel minder valt te kwalificeren als 'verdachte gevallen' dan aanvankelijk door de gemeente gedacht.

### **Hoe worden fouten gecorrigeerd?**

Correcties in de **GBA** zijn, als het gaat om niet-fraudegerelateerde fouten, volgens Agentschap BPR (Basisadministratie Persoonsgegevens en Reisdocumenten) eenvoudig uit te voeren. Via de desbetreffende gemeente kan - met een brondocument als bewijs - een fout worden gecorrigeerd. Geautoriseerde instanties zoals de Belastingdienst, het UWV en de SVB krijgen automatisch bericht van mutaties in de GBA om daarmee hun (schaduw)administratie bij te werken. Identiteitsfraude maakt correctie van persoonsgegevens een stuk lastiger. Om de juiste identiteit van de fraudeur, maar ook gedupeerde vast stellen, is onderzoek nodig.

BKWI heeft drie jaar geleden besloten om een correctiedienst in te bouwen in hun **Suwinet Inkijk**-dienst. Dergelijke functionaliteit is ook te vinden op [www.werk.nl](http://www.werk.nl). Bij Suwinet kan de burger correctieverzoeken indienen bij gemeenten, UWV en GBA. Van deze drie bronhouders worden de daar bekende gegevens getoond. Een burger kan bijvoorbeeld melden dat zijn werkervaring of telefoonnummer niet klopt en kan een ander telefoonnummer / aantal werkjaren intoetsen. Er gaat dan een mail naar de desbetreffende locatie waar de persoon geregistreerd is, typisch is dit het gemeentehuis in de plaats waar de persoon woont. Vervolgens wordt dit door de behandelend ambtenaar in de bron aangepast. Daarna moet op Suwinet Inkijk aangevinkt worden dat dit afgehandeld is. De burger ziet dan de status van zijn verzoek. Andere professionals zien dit ook. Bij twijfel zal de ambtenaar gaan bellen met de klant voor tekst en uitleg of zal vragen of hij naar het gemeentehuis wil komen. Voor correctie van bijvoorbeeld het geboortejaar zal dit laatste zeker het geval zijn; de klant moet zich met een paspoort melden bij het gemeenteloket. De bronhouder bepaalt of gegevens worden gecorrigeerd. Hiervoor moeten vaak dus schriftelijk bewijzen aangeleverd worden. De eigenaar van de gegevens, de bronhouder, is altijd bekend, door wetgeving vastgelegd. Discussies over wie de gegevens moet corrigeren zijn er dus niet. Voor bronhouders is het belangrijk dat zij hun gegevens op orde hebben.

UWV heeft destijds besloten niet aan Suwinet Inkijk mee te doen omdat de hoogte van de uitkering lastig te corrigeren is (dit zijn bewerkte gegevens en geen feitelijke gegevens). CWI (nu UWV werkbedrijf) wilde wel meedoen met de correctievoorziening. Het betrof dan vooral 'gemakkelijke' gegevens waarvan de burger kan aangeven dat er iets niet goed is. Er kwamen echter maar weinig verzoeken binnen zodat al heel snel de procedures werden vergeten bij de lokale UWV Werkbedrijven. Op dit moment gaat UWV over op het centraal afhandelen van correctieverzoeken via het **klantcontactcentrum**. Slechts enkele gemeenten hebben Suwinet Inkijk ook ingeregeld. Het aantal meldingen dat gemiddeld bij deze gemeenten binnenkomt bedraagt ongeveer 5 per jaar. Bij het UWV werkbedrijf gaat het landelijk om 800-900 verzoeken per maand. In het sociale domein gaan volgens een respondent organisaties heel verschillend om met terugmeld- en correctievoorzieningen: sommigen

varen blind op GBA, slechts een klein gedeelte van de gemeenten maakt gebruik van de Suwinet Inkijk, anderen wachten weer op de komst van Digimelding dat het centrale punt voor het gestandaardiseerd melden van onjuistheden aan basisregistraties gaat worden. Een respondent denkt overigens dat als bijvoorbeeld het UWV echt alle inconsistenties gaat melden bij de gemeenten, deze onder zullen sneeuwen

### **Hoe groot is de correctieproblematiek?**

Uit de gesprekken met experts komt over het algemeen naar voren dat het aantal probleemgevallen i.v.m. de onjuiste persoonsgegevens niet groot is als je het afzet tegen klant- en transactievolumes. Precieze aantallen kunnen vaak niet genoemd worden. De experts kunnen wel een beperkt inzicht geven in de omvang van fouten in persoonsgegevens. Deze omvang van fouten geeft een indicatie voor de omvang van de correctieproblematiek. Anders gezegd: het is aannemelijk dat naarmate het aantal fouten in persoonsgegevens toeneemt, de omvang van de correctieproblematiek groter wordt.

In de strafrechtketen gaat het bijvoorbeeld om aanzienlijke aantallen fouten, zoals uit een intern onderzoek in het Progis-programma blijkt. Daarin is vastgesteld dat 7% van de zaken in de strafrechtketen fouten bevat. Deze fouten kunnen zitten in beschrijvingen, culturele perspectieven of fonetische fouten. Wel gaat het hier om fouten die bewust door verdachten worden gecreëerd; fraude leidt altijd tot fouten. Met opzet worden bijvoorbeeld valse namen gegeven om de kans op vervolging te verkleinen. Het gaat hier echter om daders, niet om slachtoffers waar het in het onderhavige onderzoek om draait.

Onderzoek<sup>1</sup> in het Verenigd Koninkrijk stelt dat op dit moment 65% van alle fraudegevallen gerelateerd is aan het misbruik van persoonsgegevens. Dit onderzoek maakt duidelijk dat *“the age of data enabled fraud is here to stay”*.

Het is aannemelijk dat er in de toekomst meer fouten boven water komen door de vorming van de Nationale Politie, als de bedrijfsproductiesystemen van de 26 voormalige politiekorpsen aan elkaar gekoppeld worden. Bovendien komen er steeds meer intelligente systemen waarmee onregelmatigheden en inconsistenties opgespoord kunnen worden. Een voorbeeld daarvan is het Fraude Registratie en Informatie Systeem (FRIS), waarmee allerlei analyses kunnen worden uitgevoerd (bijvoorbeeld door informatie van sociale media, de TNT Verhuisservice en markplaats.nl te combineren). Bovendien zal de problematiek steeds meer zichtbaar worden, omdat er meer biometrische gegevens beschikbaar komen, bijvoorbeeld vingerafdrukken (HAVANK) en DNA.

Het CMI merkt dat er een toename is van het aantal zaken dat in behandeling is (30% per jaar). Sommige zaken lopen al jaren, sommige zaken komen ook weer terug. Oorzaken voor de toename zijn o.a. meer bekendheid van het CMI en een mogelijke toename van identiteitsfraude.

De omvang van de problematiek komt volgens de experts niet volledig boven water, omdat burgers hun zaak opgeven. Bijvoorbeeld omdat ze opzien tegen een zware procesgang of omdat zij de kosten te groot vinden (bijvoorbeeld griffierechtkosten). Een ander voorbeeld waardoor de omvang van de problematiek onvolledig in

---

<sup>1</sup> *Fraudescape - Depicting the UK's fraud landscape (2013)*

beeld komt, heeft te maken van slachtoffers van bestellingen op naam bij internetbedrijven. Op meldingen hiervan worden specialisten gezet, die onderzoek doen. Probleem hierbij is, volgens geïnterviewden, dat banken hieraan niet willen meewerken, omdat ze i.v.m. hun imago fraudegevallen buiten de deur willen houden. Banken kiezen er voor om slachtoffers schadeloos te stellen, waarmee de zaak voor het slachtoffer in eerste instantie is opgelost.

In paragraaf 2.4 gaan we dieper in op de omvang van de problematiek zoals die uit deskresearch naar voren komt.

### **Welke verbetermogelijkheden zijn er nodig?**

In de eerste interviewronde die met experts is gehouden, komt een divers beeld naar voren van wat men nodig vindt. Een respondent van de politie stelt bijvoorbeeld dat de processen, besturing en verantwoordelijkheden aangaande de correctie van foutieve persoonsgegevens helder zijn en dat de dienstverlening naar de (gedupeerde) burger goed geregeld is. Hij ziet geen aanleiding om in deze procedures verbeteringen aan te brengen.

Anderen stellen dat er meer gebruik gemaakt moet gaan worden van **bestandsvergelijkingen**, ook al wijst men op de eerder genoemde terughoudendheid in het trekken van voorbarige conclusies. Onlangs is bijvoorbeeld een project gestart i.v.m. spoorloze debiteuren: hiervoor is men met een 15-tal organisaties bij elkaar gaan zitten en heeft men nagedacht over hoe dit op te lossen. Het koppelen van de bestanden van UWV en DUO zou hierbij kunnen helpen, maar men loopt dan wel tegen de Wet Bescherming Persoonsgegevens (WBP) aan. Daarom was ont koppeling van gegevens nodig, waarvoor een *trusted third party* is ingeschakeld (in dat geval het Inlichtingenbureau).

Vaak wordt door respondenten genoemd dat er meer werk moet worden gemaakt van **preventie**, bijvoorbeeld GBA terugmeldingen ter voorkoming van fouten in persoonsgegevens, verificatie van de echtheid van identiteitsbewijzen en het beter herkennen van (mogelijke) probleem- of fraudegevallen. In de praktijk van het uitschrijven van een bekeuring (in de zin van de Wet Mulder een bestuurlijke boete) zou volgens een respondent bij twijfel een controle moeten plaatsvinden op het bureau om de juiste identiteit vast te stellen. Eigenlijk zou, volgens de respondent, “de vingerafdruk naar de straat gebracht moeten worden” om die controle ter plaatse te kunnen uitvoeren.

Volgens een respondent ligt de focus soms wat teveel op het voorkomen van misbruik door allerlei middelen. Dat kost veel geld voor een relatief kleine doelgroep: op zoek naar 3500 uitkeringen ter waarde van hooguit enkele miljoenen is niets op de miljoenen transacties en het totale uitkeringsgeld (dat in de miljarden ligt). Ook worden er miljoenen geïnvesteerd in opsporen. De pijn zit bij burger, die geholpen moet worden. Dezelfde respondent merkt op dat er wel een spanning is tussen de politieke realiteit en de uitvoeringsrealiteit. Politiek gezien scoort het goed om te voorkomen dat voortvluchtigen een uitkering hebben. In de uitvoering zijn dit 400 mensen op de 1.2 miljoen. De vraag is dus: waar leg je de prioriteiten?

## **2.4 OMVANG VAN DE PROBLEMATIEK**

In de deskresearch is onderzocht wat de omvang is van fouten die nadelig uitwerken voor burger en/of overheid.

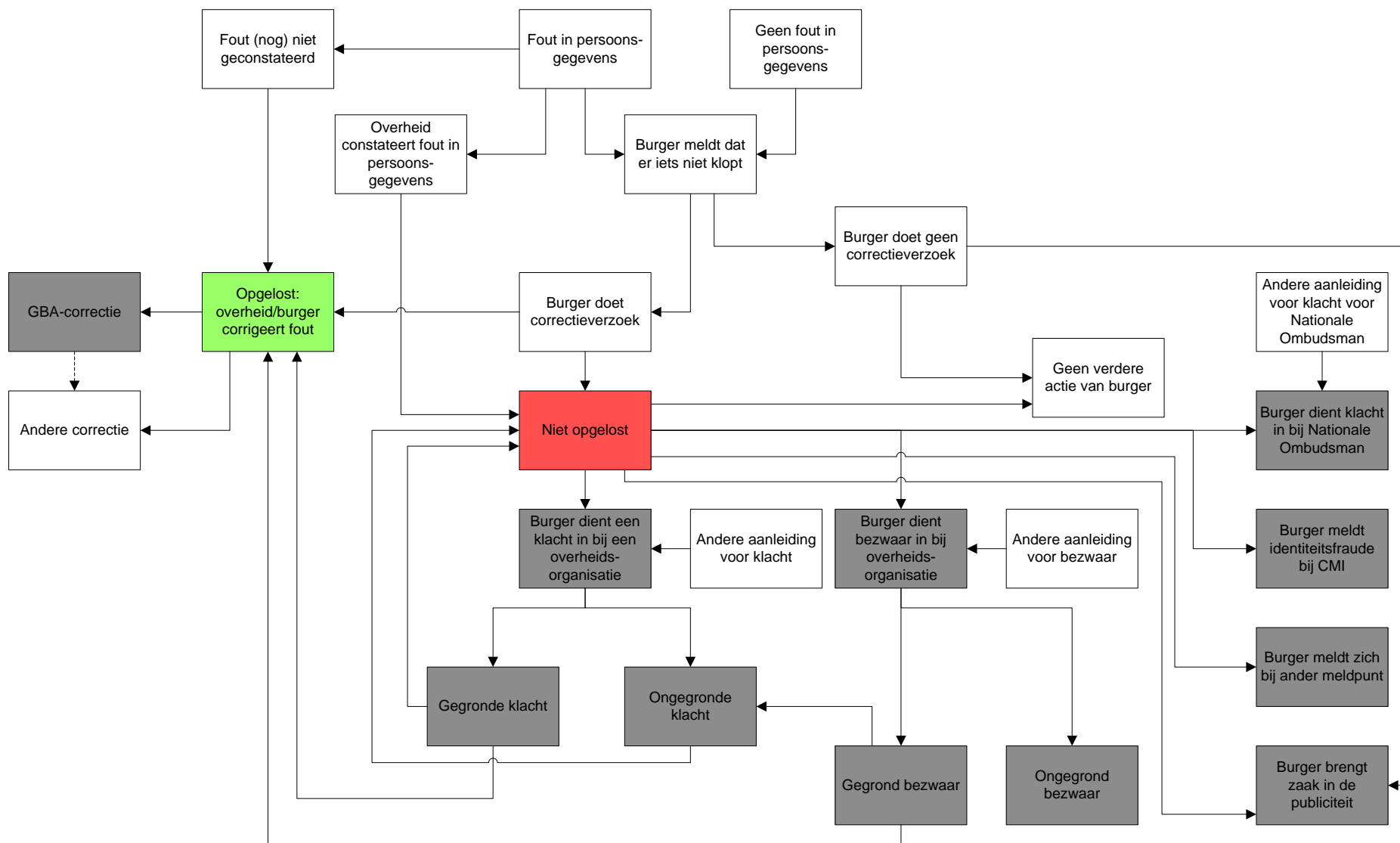
Het gaat daarbij om gevallen, waarbij de burger door fouten in zijn persoonsgegevens bijvoorbeeld vastloopt bij overheden en niet in staat is om de foutieve persoonsgegevens gewijzigd te krijgen.

Uit de bronnen die voor dit onderzoek gebruikt zijn, is niet gebleken dat overheidsorganisaties dit soort gevallen systematisch registreren of op een andere wijze tot schattingen kunnen komen van de omvang van de problematiek. Dat is ook niet verwonderlijk, omdat er vele foutbehandelroutes kunnen zijn die uiteindelijk tot een situatie kunnen leiden waarin de burger benadeeld wordt. Het schema in Figuur 3 geeft een (onvolledige) indruk van de mogelijk routes die de afhandeling van een fout kan volgen. In grote lijn kan een fout in de persoonsgegevens, wanneer deze niet wordt opgelost door een correctie, leiden tot een klacht, een bezwaar of een melding bij een meldpunt. In bijzondere gevallen kunnen de gevolgen van een fout in de publiciteit komen. Bezwaren en klachten worden door veel overheidsorganisaties wel geregistreerd, maar onbekend is welk deel daarvan betrekking heeft op fouten in de persoonsgegevens. In de figuur stellen de donkergrijze blokken situaties voor, waarvan bij organisaties volumes bekend zijn. De situaties die met de witte blokken in het diagram overeenkomen, zouden iets kunnen zeggen over de omvang van het probleem, maar de volumes van die situaties (de 'witte vlekken') zijn niet bekend.

In het onderzoek is gebruik gemaakt van openbare bronnen, zoals beheersverslagen en jaarverslagen van Belastingdienst, UWV en SVB. Een overzicht van deze bronnen is te vinden in de lijst met geraadpleegde literatuur. Geen van deze bronnen geeft direct inzicht in de volumes van fouten en correctieverzoeken. Vaak wordt in de verslagen wel melding gemaakt van het aantal klachten en het aantal bezwaren, maar de relatie tussen correctieverzoeken en klachten en bezwaren is dus, zoals uit het schema in Figuur 3 blijkt, niet bekend.

Eenzelfde constatering wordt ook gedaan door Choenni et al., die in hun analyses laten zien dat registraties bij al deze instanties niet direct dan wel slecht te relateren zijn aan de rol die de toepassing van informatietechnologie (en dus ook het gedistribueerd vastleggen van persoonsgegevens) heeft gespeeld bij klachten van burgers.





Figuur 3 Mogelijke behandelroutes foutcorrecties.



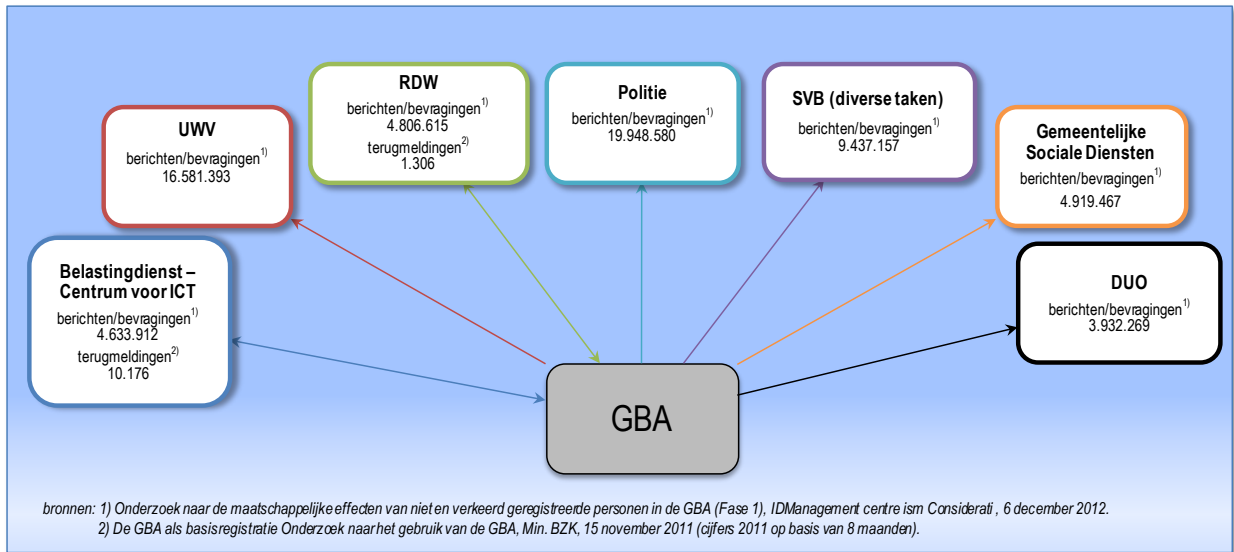
De cijfers in Figuur 4 geven een (gedeeltelijk) beeld van het beschikbaar cijfermateriaal. Zoals eerder opgemerkt, zeggen deze cijfers dus indirect iets zegt over de omvang van de problematiek. Ook het aantal correcties in de GBA die gemeld worden via de GBA-terugmeldvoorziening, wijst op een geringe (kwantitatieve) omvang van problematiek. Daarbij moet wel de kanttekening geplaatst worden dat de wettelijk verplichte GBA-terugmelding niet in volle omvang wordt nageleefd.

Verder zijn in de deskresearch diverse zaken naar voren gekomen die uiteindelijk door hun bijzondere karakter, in de media zijn terecht gekomen (de excessen in Figuur 7). Ook deze berichten wijzen niet op een grote kwantitatieve omvang van de problematiek.

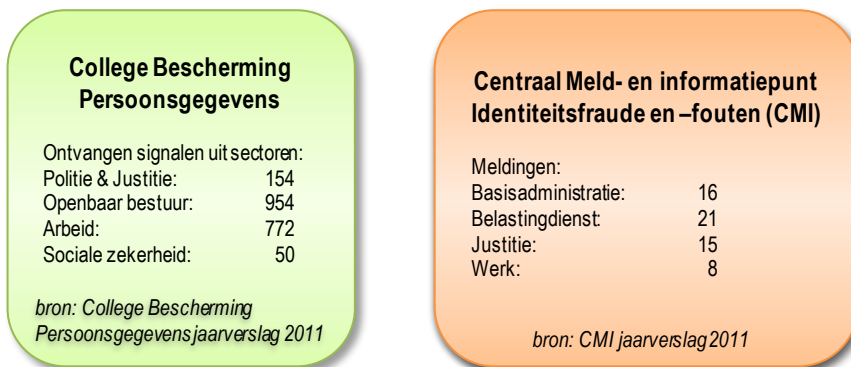
Naast de deskresearch zijn interviews met deskundigen bij diverse overheidsorganisaties uitgevoerd. Uit deze interviews komt naar voren dat de omvang van deze problematiek in relatie tot bijvoorbeeld het aantal cliënten of in relatie tot het aantal transacties zeer laag is. Bij de RDW, bijvoorbeeld, gaat het om een tiental klachten of problemen per jaar; dat is weinig t.o.v. van de ca. 50.000 mutaties per dag. In de interviews wordt wel steeds opgemerkt, dat de problematiek van administratieve ficties vanuit overheidsperspectief klein is, maar vanuit het perspectief van de individuele burger groot kan zijn en opgelost dient te worden.



**Figuur 4 Administratieve omvang (2011).**



Figuur 5 Bevestigingen en terugmeldingen GBA (2011).



Figuur 6 Aantallen meldingen bij CBP en CMI (2011).



Figuur 7 Excessen in de media.

# 3 Oplossingsrichting

## 3.1 VOORGESTELDE OPLOSSINGSRICHTING

Uit zowel de interviews met experts als de analyse van de casuïstiek komt een aantal mogelijkheden naar voren om de correctieproblematiek aan te pakken. Een deel van de oplossingsrichting is van preventieve aard, een ander deel heeft te maken met de effectievere behandeling van (schrijnende) probleemgevallen. Omdat uit het onderzoek naar voren komt dat het aantal probleemgevallen niet groot is, ligt een proportionele oplossingsrichting voor de hand. Proportioneel betekent dat er geen maatregelen worden voorgesteld die een onevenredig zware belasting voor (ketens van) overheidorganisaties betekenen in termen van procedures, werkwijzen en kosten. De voorgestelde oplossingsrichting ziet er als volgt uit:

### A. Preventie van schrijnende zaken

Hier is het credo “voorkomen is beter dan genezen”. Op dit vlak lopen inmiddels diverse verbeterprogramma’s en de voorgestelde preventieve oplossingsrichtingen bevestigen deze ingeslagen weg:

#### 1. Verbeteringen aan de voorkant

Fouten ontstaan door onvolkomenheden in het verwerkingsproces of door (identiteits)fraude. Onvolkomenheden in het verwerkingsproces zijn bijvoorbeeld vergissingen, onzorgvuldigheden en verkeerde interpretaties van zowel ambtenaren als burgers, systeemfouten (denk aan correcties die overschreven worden bij de batchverwerking) en onjuiste koppelingen van gegevens. Fraude heeft vaak te maken met gestolen, verloren of vervalste identiteitsbewijzen. Betere controles van gegeven kunnen dit soort fouten voorkomen.

#### 2. Kwaliteitsverbetering van persoonsgegevens

In deze richting zijn diverse initiatieven te noemen die moeten leiden tot een kwaliteitsverbetering. We geven in dit verband enkele voorbeelden.

- **Digimelding** als instrument voor het terugmelden van onjuistheden in de basisregistraties, bijvoorbeeld GBA (persoonsgegevens), BAG (adressen en gebouwen) en NHR (handelsregister).
- Het programma **i-Spiegel** dat gericht is op het beter intergemeentelijk gebruik van basisregistraties en het verbeteren van de kwaliteit van de basisregistraties.
- **Bestandsvergelijkingen** en *business intelligence* waarmee inconsistenties en fraude aan het licht gebracht worden.
- De **inkijk- en correctiemogelijkheden** van MijnOverheid, zoals voorgesteld in het WRR-rapport iOverheid en dat nu nader onderzocht wordt door het Ministerie van Binnenlandse Zaken; zie PBLQ HEC (2012).

### B. Effectieve behandeling van schrijnende zaken

#### 3. Samenwerking in de keten

Dat schrijnende gevallen niet opgelost (kunnen) worden heeft er vooral mee te maken dat individuele organisaties niet de verantwoordelijkheid (kunnen) nemen voor het herstellen van een fout die doorwerkt in een hele keten. Bovendien is het oplossen van individuele zaken tijdrovend en kostbaar voor organisaties. Een organisatie zal

daarom (gelet op haar prioriteiten), niet snel geneigd zijn om een gemeld probleem uit te zoeken. Zeker als de problematiek een (deel van de) keten betreft. Zelfstandig handelen door organisaties is bovendien vaak niet voldoende, gezamenlijk handelen in de keten is daarom nodig. Daarvoor is in de eerste plaats **bestuurlijke wil** nodig om schrijnende gevallen te willen oplossen. Belangrijk is dat voor de afhandeling van een zaak de **betrokken partijen in de keten geïdentificeerd** worden en dat men zorgt voor **continuïteit** in de zaakafhandeling.

#### 4. Opschonen van dossiers

Behalve het maken van afspraken in ketens is het ook belangrijk dat fouten (administratief) met **terugwerkende kracht** kunnen worden hersteld en dossiers opgeschoond worden. Functionarissen moeten daarvoor handelingsbevoegd worden gemaakt. Op termijn valt te denken aan 'opschoningsbrigades' die binnen een keten (over organisatiegrenzen heen) deze handeling uit kunnen (laten) voeren.

In deze oplossingsrichting is het van groot belang om de burger betrokken te houden. De burger voelt zich dan serieus genomen en dan gaan zaken lopen, komt de schrijnendheid ook aan het licht: mensen lossen problemen op, niet organisaties.

In deze oplossingsrichting is een **verbindende rol voor het CMI** weggelegd, als centraal aanspreekpunt dat weet wat er speelt. Het CMI vervult de rol van katalysator, die over ketens heen kijkt, de hiaten in de samenwerking in ketens signaleert, een aanjaagfunctie vervult en die alert is op signalen (zoals de bij de campagne rondom de kopie van het identiteitsbewijs).

### 3.2 WAAROM DEZE OPLOSSINGSRICHTING?

De oplossingsrichtingen 3. (*Samenwerking in de keten*) en 4. (*Opschonen dossiers*) zijn ter toetsing voorgelegd aan een panel van deskundigen, de expertsessies. Bovendien is bij de deskundigen getoetst of er draagvlak is voor de voorgestelde oplossingsrichting, zonder overigens van de betrokkenen commitment namens hun organisatie te vragen.

Samenwerking in ketens is niet nieuw. Voorbeelden van deze ketens zijn de voertuigketen, strafrecht en vreemdelingen, sociale zekerheid en allerlei sectorale overleggen. In die zin is er reeds draagvlak en gaat de oplossingsrichting meer om een structurele aanpak van een bestaande praktijk en over uitbreiding naar andere ketens. Het opschonen van dossiers gaat verder en kan behoorlijke ingrijpend zijn, bijvoorbeeld omdat dossiers dikwijls (fysiek en digitaal) gedistribueerd zijn over meerdere organisaties.

Een mooi voorbeeld van samenwerking in de keten is te vinden in de voertuigketen. Het overleg in de voertuigketen is naar aanleiding van een werkcongres in 2009 tot stand is gekomen. In deze overleggen worden de casussen van probleemgevallen besproken. De deelnemers aan deze overleggen zijn business managers die ook betrokken zijn bij het ontwerpen van werkprocessen. De overleggen leiden altijd tot een oplossing, uiteraard niet altijd in het voordeel van de indiener. Wat belangrijk is, is dat er bestuurlijke dekking is: de bestuurlijke wil om probleemgevallen op te lossen. Casussen worden ingebracht in het overleg op basis van vakmanschap van de deelnemers. Er worden ook zaken ingebracht waar men een sterk vermoeden heeft van fraude, maar waar er geen andere middelen zijn om de

zaak te kunnen behandelen. In het voertuigketenoverleg zijn de afgelopen 3 jaar zo'n 160/170 gevallen besproken. In het overleg zit namens RDW altijd dezelfde coördinerend ambtenaar, die het contact met de burger ook onderhoudt en hem verder helpt. Dit is erg belangrijk: mensen voelen zich dan serieus genomen.

Een ander voorbeeld betreft de eerste inschrijving van vreemdelingen in Enschede. De gemeente beschikt niet over voldoende kennis om de inschrijving te kunnen doen en zoekt in een werkgroep samenwerking met bijvoorbeeld IND, Marechaussee, Justitie, en de NVVB (Nederlandse Vereniging voor Burgerzaken). Men werkt aan een kenniscentrum en de samenwerking gaat leiden tot een samenwerkingsconvenant. Hierdoor kunnen ook fraudezaken beter aangepakt worden en hoeft minder vaak geseponeerd te worden. Er wordt nu vaak geseponeerd omdat de processen verbaal van politie en gemeente niet aan de eisen voldoen en er niet van geleerd wordt, omdat het OM niet terugkoppelt. Ook in de regio Den Haag is er samenwerking in de stafrechtketen. Van een (dergelijk) structureel overleg in alle regio's met de diverse belanghebbende/betrokken ketenpartners is nog geen sprake. De experts wijzen er verder op dat uitvoeringsorganisaties in Manifestgroepverband al op diverse vlakken samenwerken en dat er lijnen naar de gemeenten lopen.

De experts zien weinig belemmeringen om de problemen in ketenoverleggen aan te pakken. De belangrijkste belemmering is misschien wel van budgettaire aard. Organisaties moeten het met steeds minder middelen doen en zullen geneigd zijn de rekening bij de vrager neer te leggen. Op het vlak van samenwerking in ketens ziet men weinig belemmeringen. Iedere organisatie weet wat er wel en niet uitgewisseld mag worden, bijvoorbeeld binnen de kaders van de privacywetgeving. Je hoeft ook niet alles te delen om een (andere) organisatie verder te helpen, is de mening: "ik mag jou niets geven, maar het je wel vertellen". Men accepteert elkaars grenzen. Bovendien stelt men dat het goed is dat men, in het belang van de burger, de grenzen van de wet opzoekt.

Voor wat het opschonen van dossiers betreft zullen wat meer juridische horden genomen moeten worden. Met name het correctierecht zal juridisch zover moeten gaan, dat fouten bij andere organisaties ook gecorrigeerd kunnen worden. De artikelen 36 tot en met 38 van de Wet bescherming persoonsgegevens (waarin het correctierecht staat beschreven) , zouden daarbij wellicht tegen het licht gehouden moeten worden. Door de vernetwerking van de informatievoorziening kan het voor organisaties moeilijk te achterhalen zijn waar de fouten hersteld moeten worden.

### **3.3 VOORGESTELDE WERKWIJZE EN ONDERSTEUNING**

Het is belangrijk om door te gaan met de reeds ingezette **preventieve initiatieven** voor het voorkomen van schrijnende zaken: verbeteringen aan de voorkant en kwaliteitsverbeteringen. Alle signalen in dit onderzoek wijzen er op dat het aantal schrijnende zaken vooralsnog meevalt in relatie tot de omvang van de overheid als massale gegevensverwerkende instantie. Om zo goed mogelijk te borgen dat die aantallen relatief laag blijven of nog verder verminderen, is het vanwege de voortschrijdende informatisering van de overheid zaak om de kwaliteit van persoonsgegevens scherp in het oog te houden. Gewoonweg door fouten te voorkomen of zo nodig tijdig te herstellen, voordat ze verderop in het proces tot grotere problemen leiden. Daarom is het raadzaam om te blijven werken aan kwaliteitsprogramma's, correctiemechanismen via MijnOverheid, etc.

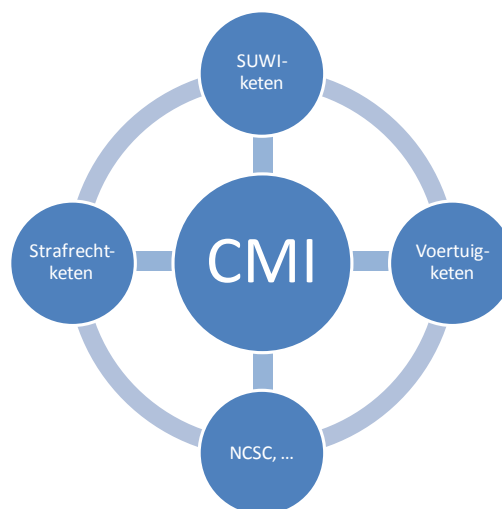
Preventie is echter niet voldoende. Fouten zullen altijd gemaakt worden of ontstaan. Het is dan belangrijk dat deze

fouten op een snelle en effectieve manier gecorrigeerd worden om langsturende en schrijnende gevallen te voorkomen. Voor het herstellen van schrijnende gevallen doen we, zoals hierboven al aangegeven, een beroep op de 'mens achter de machine', de behandelend ambtenaren. De samenwerking waar her en der al sprake van is, kan en moet naar een hoger niveau getild worden. Er moet een verzameling of een stelsel van afspraken komen. Dat stelsel moet er enerzijds voor zorgen dat behandelend ambtenaren elkaar sneller vinden en sneller oplossingen in beeld krijgen voor individuele gevallen. Anderzijds moet er van het stelsel een lerende werking uitgaan, waardoor sneller structurele problemen herkenbaar en zichtbaar worden en oplossingen hiervoor beschikbaar komen. Denk bijvoorbeeld aan het aanpakken van juridische randvoorwaarden die onbedoeld de oplossing in de weg blijven staan.

Om te komen tot een stelsel van afspraken, zijn de onderstaande mogelijke stappen tijdens de interviews met de experts naar voren gekomen. Deze stappen zijn door ons uitgewerkt en vervolgens getoetst in de expertsessies, zonder overigens van de betrokkenen commitment namens hun organisatie te vragen.

De stappen zijn niet noodzakelijkerwijs volgordelijk:

- 1) Breng goede **voorbeelden van ketenoverleg** in kaart en zorg dat hiervan een lerend effect uitgaat: schrijnende zaken kunnen door hun vaak organisatiegrensoverstijgende karakter (natuurlijk) alleen in samenhang en door samenwerking met verschillende organisaties worden opgelost. Er zijn al goed functionerende ketenoverleggen die het corrigeren van persoonsgegevens structureel behandelen, bijvoorbeeld in de voertuigketen en de strafrechtketen. Ook kan kennis van andere organisaties benut worden om deze ketenoverleggen beter te laten functioneren. Denk bijvoorbeeld aan het Nationaal Cyber Security Centrum (NCSC), dat bij (de gevolgen van) identiteitsfraude bij de oplossing van zaken met zijn kennis behulpzaam kan zijn. Deze ketens en organisaties moeten in beeld worden gebracht en voor het CMI benaderbaar zijn: wie zitten er in, wat zijn de vergaderfrequenties. Het zijn uitstekende platforms om vanuit het CMI zaken aan te kaarten die burgers bij het CMI hebben aangemeld. Of vice versa, waarbij vanuit het ketenoverleg het CMI benaderd wordt om te helpen of advies te geven. Figuur 8 geeft een beeld van een mogelijke positie van het CMI, waarin het CMI zowel informatie ontvangt, als informatie deelt met een aantal 'satellieten'.



**Figuur 8 Ketenoverleggen en de positie die het CMI hierin kan innemen.**



- 2) Ontwikkel een **sociaal netwerk** van behandelend ambtenaren. Gebruik daarbij uit efficiencyoverwegingen ook beveiligde elektronische omgevingen: verschillende organisaties hebben beveiligde intranetten die wellicht als extranet gebruikt kunnen worden. Doel van dit sociaal netwerk is tweeledig.
  - Ten eerste: elkaar snel vinden voor het zoeken naar een oplossing, zeker als er sprake is van een ketenoverstijgende zaak.
  - Ten tweede: kennisdelen en meedenken bij bijvoorbeeld het herkennen van mogelijke probleem- of fraudegevallen, het zoeken van een oplossing, het waarschuwen voor en omzeilen van juridische valkuilen, etc.
- 3) Een stap verder dan het sociaal netwerk gaat een **netwerk** van zogenaamde **meldpunten**: veel organisaties hebben meldpunten voor fouten in persoonsgegevens. Als deze meldpunten een netwerk gaan vormen (door op zijn minst van elkaar weet te hebben, maar liever nog organisatiegrens- of ketenoverstijgende meldingsgevallen kenbaar te maken in een gezamenlijk systeem), kan het op een aantal manieren een waardevolle rol gaan spelen.
  - Het is veel sneller duidelijk waar zich bij de overheid op een bepaald moment welke gevallen voordoen i.v.m. incorrecte persoonsgegevens. Hier kan dan beter op geacteerd worden. Bijvoorbeeld door daar waar nodig een ketenoverleg of domeinoverleg te initiëren.
  - Zodra duidelijk wordt dat de organisatie van een meldpunt niet de veroorzaker van een fout is, kan een casus zorgvuldig worden overgedragen aan het meldpunt van de organisatie waar de fout zit.
  - Efficiënte overdracht geïdentificeerde en opgeloste problemen tussen ketens onderling, om te voorkomen dat het wiel steeds opnieuw moet worden uitgevonden.
- 4) Na verloop van tijd ontwikkelt zich naar verwachting uit de ketenoverleggen, het sociaal netwerk en het netwerk van meldpunten zeer waardevolle kennis, herbruikbaar voor toekomstige, gelijksoortige schrijnende gevallen. Die kennis moet geborgd en voor de daartoe geautoriseerde ambtenaar ontsloten worden. Ontwikkel daarom een **kennisbank** waarmee behandelend ambtenaren worden ondersteund, bijvoorbeeld bij het herkennen van (mogelijke) probleem- of fraudegevallen (indicatoren), het delen van (geanonimiseerde) casuïstiek en 'good practices'.
- 5) Ontwikkel **domein- of ketenoverstijgende correctieprocedures**; binnen ketenoverleggen zijn veel zaken formeel of informeel geregeld: wie brengt wanneer wat in, wie is en blijft de case manager, etc. Dit zal ook moeten gebeuren voor zogenaamde domein- of ketengrensoverstijgende procedures. De bestaande procedures en vigerende werkafspraken binnen ketenoverleggen kunnen als uitgangspunt dienen.
- 6) Met het corrigeren van foute persoonsgegevens is de oplossing in een aantal gevallen nog niet in zicht. Door jarenlang hergebruik van verkeerde gegevens heeft de fout zich in een aantal gevallen als een olievlek over de systemen van de overheid verspreid, met verstrekking of langdurige gevolgen voor de gedupeerde. Het kost echter veel tijd en het vergt speciale competenties en bevoegdheden om dit op te lossen. Het antwoord op de vraag hoe dat precies moet, overstijgt dit onderzoek. We adviseren echter wel om de ontwikkeling van mogelijkheden voor het **opschonen van dossiers** en de praktische uitwerking daarvan, bijvoorbeeld door handelingsbevoegde 'opschoningsbrigades', te agenderen.



## 4 Aanbevelingen voor vervolg

In aansluiting op de voorgestelde en met experts getoetste oplossingsrichtingen worden in dit hoofdstuk aanbevelingen gedaan voor vervolg.

De ervaring leert dat overheidsorganisatieoverstijgende afspraken er niet vanzelf komen. Daarom moet er volgens ons een instantie voor worden aangewezen die als een spin in het web kan acteren, een instantie met enige doorzetmacht. Bij voorkeur staat er daarom ook een politiek verantwoordelijk bewindspersoon op, die dit dossier onder zijn hoede neemt.

Wat die instantie betreft: het is gegeven de numerieke omvang van de problematiek naar onze mening niet proportioneel om een nieuw overheidsorgaan op te richten. Het huidige CMI kan door een uitbreiding van de taakopvatting en verruiming van het takenpakket een dergelijke rol naar onze mening uitstekend vervullen. Wij baseren dat op het beeld dat we hebben van de bekendheid van het CMI bij burgers en bij een groeiend aantal overheidsorganisaties. Er kan dus een vliegende start worden gemaakt.

Wij adviseren in het verlengde hiervan om naast de huidige taken acht additionele taken bij het CMI te beleggen:

- 1) Het verder specificeren van goed werkende ketenoverleggen (wie neemt deel, hoe vaak, etc.).
- 2) Het ontwikkelen van een sociaal netwerk van behandelend ambtenaren.
- 3) Het koppelen van de verschillende meldpunten in een netwerk.
- 4) Het expliciteren, borgen en ontsluiten van ontwikkelde kennis in bovenstaande overleggen en netwerken door ondermeer kennisbanken en een overheidsbreed meldsysteem voor de meldpunten.
- 5) Het inregelen van procedures om domein- of organisatieoverstijgende schrijnende gevallen aan te mogen dragen in ketenoverleggen.
- 6) (In eerste instantie werken aan) de bevoegdheid en het inregelen van procedures voor het initiëren van nieuwe ketenoverleggen: bijvoorbeeld wanneer het boven vermelde netwerk van meldpunten daar aanleiding voor geeft.
- 7) Het agenderen van het instellen van 'Opschoningsbrigades'.
- 8) (In eerste instantie werken aan) de bevoegdheid om juridische belemmering te benoemen en te agenderen voor bijvoorbeeld het repareren van wetgeving zodanig dat deze niet langer hindert bij de oplossing.

Deze acht taken moeten zo snel mogelijk worden opgepakt. Tegelijkertijd moet het stelsel van afspraken op een of andere wijze bekrachtigd worden, zodat de afspraken ook echt gaan leven. Dat kan doordat het CMI conventanten gaat afsluiten met allerlei overheidsorganisaties waarin de partijen aangeven zich te willen conformeren aan de taakuitvoering en de bevoegdheden van het CMI. Een dergelijke stap is naar onze mening te fors om in een keer te nemen. Het CMI moet hier langzaam naar toe werken. Het zou bijvoorbeeld kunnen beginnen met het organiseren van een werkconferentie om bovenstaande onderwerpen met het veld te bespreken en verdere mogelijkheden en de

bereidheid tot meewerken te toetsen. Naar aanleiding van dit onderzoek hebben wij de indruk dat de betreffende organisaties bereid zijn hier aan mee te werken. Op een dergelijke werkconferentie kan ook het idee rond de eerder vermelde opschoningsbrigades worden behandeld.

De taakverruiming van het CMI betekent uiteraard dat het CMI in termen van capaciteit (fte's) moet worden uitgebreid, zij het dat dit naar ons oordeel slechts een beperkte uitbreiding hoeft te zijn. Denk aan 4 tot 6 fte. Verder kan het betekenen dat de huidige ophanging van het CMI binnen het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties ter discussie moet komen te staan. Het CMI is nu belegd bij een Beleidsdirectie en past inhoudelijk meer bij een uitvoerend onderdeel.

Gegeven de beperkte uitbreiding speelt natuurlijk wel de vraag in hoeverre er in de buitenwereld meer ruchtbaarheid aan het CMI gegeven moet worden. We kunnen niet inschatten wat het betekent voor het aantal meldingen en of het (uitgebreide) CMI dat aantal aankan. Met de komst van het CMI is bij de Nationale Ombudsman het aantal meldingen over correctieproblemen verminderd. Je kunt hier voorzichtig uit afleiden dat het CMI op dit moment het in potentie aanwezige aantal meldingen in de samenleving afdekt. We zien het daarom op dit moment niet als een noodzakelijke maatregel, eerder een maatregel die een onbedoelde stroom klachten op gang kan brengen. De bedoeling is dat het CMI niet zelf de klachten gaat oppakken maar dat dit voornamelijk binnen de ketenoverleggen plaatsvindt. Daar moeten de klachten opgelost worden eventueel met het CMI als kennisbron of facilitator. Het is daarom van belang dat binnen de ketenoverleggen ruchtbaarheid aan het CMI gegeven wordt.

Het aantal toekomstige meldingen kunnen we niet inschatten. Het vermoeden bij verschillende experts binnen en buiten de overheid is dat het zeker gaat groeien. Belangrijke aanjagers hiervoor zijn het steeds meer elektronisch vastleggen van allerlei zaken, het almaar verder koppelen van bestanden en de toename van online identiteitsfraude. Maar hoe groot en hoe snel dat zal gaan, is ons niet duidelijk geworden. De casegerichte aanpak van bestaande gevallen in dit onderzoek leende zich helaas onvoldoende voor het doen van kwantitatieve uitspraken op dit gebied. Dat is natuurlijk een gemis in het kunnen benadrukken van het belang dat we zien bij de bovenvermelde stappen en taakuitbreiding.

Tot besluit nemen we in onze aanbeveling enkele beelden mee die we in het veld hebben gesignaleerd. Volgens enkele respondenten in het onderzoek is er weinig tot geen zicht op de voorkant van de persoonsgegevensregistratie. Vooral gemeenten lijken, rondom afwijkende gevallen, geen coherente procedures te volgen. Bij twijfel over de juistheid van gegevens, vermoedelijke fraude, of het ontbreken van gegevens lijken de gevolgde procedures per gemeente dan ook van elkaar te verschillen. Dit is eerder onderkend door de NVVB, die hier momenteel een professionaliseringsprogramma voor aan het ontwikkelen is. Daarnaast ontbreekt het gemeenten vaak aan middelen en kennis om fraude te kunnen detecteren (bijvoorbeeld om te kunnen controleren of een identiteitsbewijs geldig is). Juist gemeenten, als poortwachters van de basisregistraties, hebben vaak de sleutel in handen bij het vermijden van fouten, zo geven respondenten aan. Tegelijkertijd is er echter weinig zicht op de procedures die zij volgen, hoeveel fouten zij weten te vermijden en hoe zij gemaakte fouten weten te herstellen voordat deze de weg weten te vinden naar andere overheidsbestanden. Wanneer er meer helderheid wordt gegeven omtrent de risico's voor de overheid en de burger, worden noodzaak en urgentie van bovenstaande de maatregelen

waarschijnlijk nog sterker onderstreept. Dit kan bijdragen in een betere ondersteuning van gemeenten als het gaat om het correct kunnen identificeren van personen en hun persoonsgegevens.



# Geraadpleegde bronnen

## Rapporten

**Belastingdienst (2012)**, *Beheerverslag 2011*.

**CMI (2012)**, *Jaarverslag 2011, vooruitblik 2012*, Ministerie van Binnenlandse Zaken, Centraal Meld- en informatiepunt Identiteitsfraude en –fouten.

**Deloitte - Zenc (2011)**, *De GBA als basisregistratie - Onderzoek naar het gebruik van de GBA*.

**IDManagement Centre – Considerati (2012)**, *Onderzoek naar de maatschappelijke effecten van niet en verkeerd geregistreerde personen in de GBA (Fase 1)*.

**Inspectie SZW (2012)**, *Informatie-uitwisseling van de SUWI-keten met andere partijen - Programmarapportage Informatieprocessen*.

**CIFAS (2013)**, *Fraudescape - Depicting the UK's fraud landscape (2013)*,

<https://www.cifas.org.uk/secure/contentPORT/uploads/images/Cover%20Images/Internal-Fraudescape%20COVER.jpg>

**Kafkabrigade (2008)**, *Kafka in de polder*, Sdu Uitgevers.

**Nationale Ombudsman (2011)**, *Verslag van de Nationale Ombudsman over 2011*.

**Nationale Ombudsman (2011)**, *Alleen het UWV kan kiezen voor een beter UWV*.

**PBLQ HEC (2012)**, *Het versterken van de informatiepositie van de burger - Verkenning naar nieuwe (verplichte) functionaliteiten van MijnOverheid*.

**PwC (2011)**, *Omvang van identiteitsfraude & maatschappelijke schade in Nederland*.

**SVB (2012)**, *Sociale Verzekeringsbank SUWI-jaarverslag 2011*.

**UWV (2011)**, *Jaarverslag UWV 2011*.

**Wet bescherming persoonsgegevens**, <http://wetten.overheid.nl/BWBR0011468>.

**WRR (2011)**, *iOverheid*, WRR rapport no. 86, Wetenschappelijke Raad voor het Regeringsbeleid.

## Artikelen

**Choenni, S., E. Leertouwer & T. Busker (2011)**, *Klachten over toepassingen van informatietechnologie*.

*Analyse van een aantal overheidsbestanden*, in D. Broeders C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, wrr-verkenning nr. 25, Amsterdam: Amsterdam University Press.

**Meulen, Nicole van der en Bert-Jaap Koops**, *Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude - Een beschouwing naar aanleiding van de zaak-Romet*, Nederlands Juristenblad, 2012.





# Geconsulteerde organisaties

Organisatie
Belastingdienst
BKWI
BPR
CJIB
DUO
Gemeente Enschede
ICTU
Inspectie SZW
JustID, Ministerie van Justitie en Veiligheid
Nationale Ombudsman
Nationale Politie
NVVB
Politie IJsselland
Voorziening tot Samenwerking Politie Nederland
RDW
SVB
UWV
Vrije Universiteit

# Deelnemers interviews en expertsessies

Organisatie	Naam	Functie	Interview / Expertsessie <sup>2</sup>
BKWI	Yvette Memelink	Adviseur ketenontwikkeling (SUWI-keten)	I, E
BPR	Paul Hoogzaad	Adviseur stelselkwaliteit / Kwaliteitsmanager GBA en Reisdocumenten	I
CJIB	Walle Pietersen	Juridisch beleidsmedewerker (o.a. privacycoördinator)	I
Gemeente Enschede	Harrie Balke	Teamleider	I, E
ICTU	Marthe Fuld	Projectleider Stelsel van Basisregistraties	I
Inspectie SZW	Jos Urselmann	Projectmanager	I
JustID, Ministerie van Justitie en Veiligheid	Peter van den Bosch	Senior adviseur MatchingsAutoriteit	I, E
Nationale Ombudsman	Frank van Dooren	Substituut Ombudsman	I, E
Nationale Politie	Pieter Vermeulen	Expert Progis	I, E
Politie IJsselland	Arend Krale	Functioneel beheer opsporingsapplicaties	I
RDW	Gert Stel	Relatiemanager	I, E
UWV	Remco Siegerist	Adviseur	I, E
Vrije Universiteit	Nicole van der Meulen	Universitair Docent	I, E

De onderzoekers bedanken hierbij de geraadpleegde experts voor hun medewerking aan dit onderzoek.

<sup>2</sup> I = deelname interview, E = deelname expertsessie

# Bijlage: casuïstiek

Deze bijlage geeft aan de hand van een elftal casussen een beschrijving van de aard van de problemen waar burgers tegen aan kunnen lopen wanneer zij een verzoek doen om hun persoonsgegevens te corrigeren. De casussen worden steeds volgens het volgende patroon beschreven:

## Omschrijving

### Fase 1: constateren van de fout

- Door wie?
- Soort fout
- Soort gegevens

### Fase 2: procedure

- Bij welke partij?
- Aanwezig?
- Beschrijving

### Fase 3: uitvoering correctieproces

- Acties door burger
- Acties door overheid of andere organisaties
- Mogelijkheden en beperkingen in uitvoering, zoals techniek, organisatie (bevoegdheden, interne werkprocessen), wetgeving, etc.
- Resultaat

### Besturing

- Conclusies t.a.v. besturingsmogelijkheden in correctieproces.

## CASUS 1: EEN OF MEER ONBEKENDE BANEN OP JE CONTO

<b>Omschrijving</b>	Mevrouw V. ontdekt vijf Chinese restaurants als werkgever, terwijl ze daar niet heeft gewerkt. Er blijkt een, verder onbekende, man op een vervalst paspoort met haar BSN te hebben gewerkt. Een lijdensweg langs Belastingdienst en UWV volgt, en beide partijen wijzen naar elkaar. Niemand wil of kan deze gegevens wissen, want er zijn pensioenrechten opgebouwd, premies betaald etc. Voor CMI-gevallen wordt in ieder geval een halve oplossing bedacht: de Belastingdienst zal de signalen van het UWV over de betreffende banen handmatig negeren, zodat er geen belastingboetes ontstaan. De structurele oplossing voor compleet fouterstel is er nog niet. De man met het vervalste paspoort heeft onlangs nog in Zeeland gewerkt, maar is weer spoorloos.
<b>Fase 1: constateren</b>	
• Door wie?	De burger
• Soort fout	Misbruik van BSN via vervalst paspoort.
• Soort gegevens	Arbeidsverleden
<b>Fase 2: procedure</b>	
• Bij welke partij?	Belastingdienst en UWV.
• Aanwezig?	Nee, ingrijpen van CMI was noodzakelijk.
• Beschrijving	N.v.t..
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Vragen om correctie bij Belastingdienst en UWV.
• Acties overheid / anderen	Handmatig negeren van de incorrecte werkhistorie door Belastingdienst. Een structurele oplossing is er (nog) niet.
• Mogelijkheden / beperkingen	Raadplegen van register van valse paspoorten zou ervoor kunnen zorgen dat man met vals paspoort geen verdere schade meer kan aanrichten. BSN en gegevens in paspoort verifiëren om te controleren of ze kloppen. Gevolgen van de fraude zijn nauwelijks te verwerken omdat ze doorwerken in complexe systemen voor pensioenrechten, premies, etc.
• Resultaat	Minder fraude met vals paspoort mogelijk.
<b>Besturing</b>	
• Conclusies	Voorkomen is beter dan genezen. Echtheid van identiteitsbewijzen wordt slecht gecontroleerd. Een betere controle hierop kan fouten in persoonlijke gegevens voorkomen.

## CASUS 2: VAN TOESLAG NAAR LOVERBOY

<b>Omschrijving</b>	Meneer S. doet een melding van twee zaken: hij krijgt een boete van de Belastingdienst over een niet ontvangen toeslag. Uiteindelijk wordt de belastingzaak opgelost. Er is inderdaad een toeslag uitgekeerd maar die was onrechtmatig. De ontvanger van de toeslag bleek een slachtoffer te zijn van een loverboy die haar misbruikte om o.a. toeslagen te incasseren. Bij de politie was geen aangifte opgenomen om het meisje zelf de toegang tot de rekening had gegeven. Maar door deze toeslagfraude ging de zaak rollen. Door de melding van S. is dus belastingfraude opgelost én een loverboy opgepakt en zijn meerdere slachtoffers opgevangen. Een goed samenspel tussen Belastingdienst en de politie.
<b>Fase 1: constateren</b>	
<ul style="list-style-type: none"> <li>• Door wie?</li> </ul>	De burger
<ul style="list-style-type: none"> <li>• Soort fout</li> </ul>	De burger kreeg een boete over een niet ontvangen toeslag. Een uitgekeerde toeslag was onrechtmatig. Toeslagfraude.
<ul style="list-style-type: none"> <li>• Soort gegevens</li> </ul>	De burger geeft aan dat de boete onterecht is.
<b>Fase 2: procedure</b>	
<ul style="list-style-type: none"> <li>• Bij welke partij?</li> </ul>	De Belastingdienst
<ul style="list-style-type: none"> <li>• Aanwezig?</li> </ul>	De zaak is opgelost door de Belastingdienst i.s.m. de politie.
<ul style="list-style-type: none"> <li>• Beschrijving</li> </ul>	Het bankrekeningnummer van de toeslag leidde naar het slachtoffer van een loverboy.
<b>Fase 3: uitvoering correctieproces</b>	
<ul style="list-style-type: none"> <li>• Acties burger</li> </ul>	De burger maakt als slachtoffer melding van toeslag/belastingfraude bij de Belastingdienst.
<ul style="list-style-type: none"> <li>• Acties overheid / anderen</li> </ul>	De Belastingdienst lost de zaak op i.s.m. de politie.
<ul style="list-style-type: none"> <li>• Mogelijkheden / beperkingen</li> </ul>	De koppeling identiteit en bankgegevens wordt niet gecontroleerd. De vraag is hoe de loverboy het voor elkaar gekregen heeft om de toeslag van meneer S op de bankrekening van het meisje te krijgen. Het samenwerken tussen overheidsinstanties m.b.t. het delen van identiteitsgegevens werpt zijn vruchten af.
<ul style="list-style-type: none"> <li>• Resultaat</li> </ul>	Hiermee had de toeslagfraude voorkomen kunnen worden.
<b>Besturing</b>	
<ul style="list-style-type: none"> <li>• Conclusies</li> </ul>	De Belastingdienst is verantwoordelijk te controleren of een bankrekeningnummer inderdaad bij de betreffende persoon behoort. In het geval van fraude, moeten andere organisaties (bijvoorbeeld politie, maar misschien ook banken) hiervan op de hoogte gesteld worden.

### CASUS 3: NIET ALLE DIPLOMA'S IN MIJNOVERHEID.NL

<b>Omschrijving</b>	<p>Het betreft een werkloze man die via mijnoverheid o.a. zijn diploma's checkt. In zijn Digitaal Klantdossier Werk en Inkomen ontbreekt zijn MTS-opleiding, wat niet handig is als mogelijke banen gematcht worden aan alleen zijn LTS-profiel. Hij ontdekt dit in mei, en heeft sindsdien vergeefs aangeklopt bij:</p> <ol style="list-style-type: none"> <li>1. E-mail UWV werkbedrijf, werk.nl</li> <li>2. E-mail E-coach UWV werkbedrijf</li> <li>3. E-mail UWV werkbedrijf</li> <li>4. Telefonisch contact UWV Doetinchem</li> <li>5. Nogmaals telefonisch contact UWV Doetinchem</li> <li>6. Telefonisch contact met Postbus 51</li> <li>7. Telefonisch contact met DUO</li> <li>8. Telefonisch contact met de betreffende onderwijsinstelling</li> <li>9. Bezoek aan de gemeente Oost Gelre, afdeling burgerzaken.</li> <li>10. Bezoek aan UWV Werkbedrijf Doetinchem</li> <li>11. Telefonisch contact met Logius, de dienst digitale overheid"</li> <li>12. Klachtenbureau UWV</li> </ol> <p>Het is ook niet duidelijk of er iets fout gaat binnen DUO, binnen het UWV of wellicht tussen deze of andere organisaties. Maar niemand pakt de zaak op. Een gemeentemedewerker die zich dit verhaal aantrok, komt ook niet verder. Gek genoeg is niet alleen slechts één diploma bekend in de systemen, maar in de papieren bestanden van DUO is deze man niet bekend. Een medewerker van DUO voelt zich verantwoordelijk voor deze keten en gaat uitzoeken wat er aan de hand is. Wordt vervolgd.</p>
<b>Fase 1: constateren</b>	
• Door wie?	De burger
• Soort fout	Ontbreken van gegevens
• Soort gegevens	Afgeronde opleidingen – opleidingshistorie
<b>Fase 2: procedure</b>	
• Bij welke partij?	De burger wendde zich tot het UWV, DUO, Logius en de gemeente. Het is onduidelijk bij welke partij de fout zit.
• Aanwezig?	Nee. Niemand lijkt de zaak op te willen pakken. Uiteindelijk voelt DUO zich verantwoordelijk.
• Beschrijving	Het is onduidelijk wie verantwoordelijk is voor de correctie. De digitale bestanden in de systemen zijn vergeleken met de fysieke bestanden bij DUO. Beide bestanden zijn niet consistent.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	De burger neemt contact op met verschillende instanties.
• Acties overheid / anderen	DUO voelt zich uiteindelijk verantwoordelijk en pakt het op.
• Mogelijkheden / beperkingen	DUO, als bronhouder van opleidingsgegevens, zou een proces kunnen inrichten wat het voor burgers mogelijk maakt om hun opleidingen te kunnen opvoeren. De burger zal zich in dit proces moeten identificeren en kunnen aantonen dat hij/zij een bepaalde opleiding succesvol heeft afgerond.
• Resultaat	Alle opleidingsgegevens belanden op de juiste manier in de verschillende systemen.
<b>Besturing</b>	
• Conclusies	Bronhouders dienen processen in te richten voor het laten corrigeren of aanvullen van gegevens.

## CASUS 4: TWEE PERSONEN VERSMELTEN TOT ÉÉN ADMINISTRATIEVE PERSOON

<b>Omschrijving</b>	Meneer B. heeft ruim 20 jaar last van een zwerver ('illegaal') die zich regelmatig bedient van zijn naam/adres maar met een andere geboortedatum. De zwerver wordt veroordeeld voor een aantal vergrijpen, gaat de gevangenis in en krijgt veel boetes. Door deze (niet complete) identiteitsfraude én door (waarschijnlijk) een interpretatiefout bij de gemeente ten behoeve van de strafrechtketen, raken B en de echte dader versmolten tot één persoon in de registraties van de strafrecht- en de vreemdelingenketen. Hierdoor werd alles wat de pseudo-B deed, geregistreerd op het conto van de echte B. Meneer B. wordt hierdoor 20 jaar lang regelmatig meegenomen voor verhoor voor strafbare feiten die hij niet had gepleegd. Ook kon hij onterecht boetes betalen op Schiphol, ontving hij dagvaardingen en hebben hij en zijn gezin eenmaal 's nachts een gewapende politie-inval in zijn woning gehad. Het gezinsleven van B is verwoest omdat uiteindelijk zijn vrouw en kinderen hem niet meer geloofden. Na escalatie door het CMI kwam in deze zaak en zijn grote inspanningen gepleegd door JustID, het Parket Rotterdam en uiteindelijk door V&J zelf. Meneer B. heeft namens de (gehele) overheid excuses en een schadevergoeding gekregen. Maar het belangrijkste is het feit dat hij verlost is van 51 strafdossiers en in de betrokken dossiers zijn alle mogelijke waarschuwingen opgenomen om toekomstige persoonsverwisselingen te voorkomen.
<b>Fase 1: constateren</b>	
• Door wie?	De burger
• Soort fout	Gedeeltelijke identiteitsfraude en (waarschijnlijk) een interpretatiefout bij de gemeente.
• Soort gegevens	NAW-gegevens, persoonsgegevens en daaraan gerelateerde dossiers (bijvoorbeeld strafdossiers).
<b>Fase 2: procedure</b>	
• Bij welke partij?	Gemeente
• Aanwezig?	Nee. CMI moest escaleren.
• Beschrijving	N.v.t.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Is slachtoffer van verschillende uitvoerende organisaties
• Acties overheid / anderen	Na inspanning van JustID, het Parket Rotterdam en V&J is de zaak opgelost.
• Mogelijkheden / beperkingen	Aan identiteit gerelateerde dossiers zijn kwijtgescholden en waarschuwingen zijn opgenomen om toekomstige persoonsverwisselingen te voorkomen.
• Resultaat	Slachtoffer is verschoond van verdere last – ondertussen is wel zijn privéleven geruïneerd.
<b>Besturing</b>	
• Conclusies	Het koppelen van dossiers aan identiteiten dient goed gecontroleerd te worden. Nalatige verificatie van identiteitsgegevens (naast NAW gegevens ook leeftijd) tijdens het koppelen van dossiers kan leiden tot veel problemen bij de burger.

## CASUS 5: PERSOONSVERWISSELING: DE VERPLICHTE CURSUS ALCOHOL EN VERKEER

<b>Omschrijving</b>	Meneer G. moet zich melden bij het CBR voor een verplichte cursus over alcohol en verkeer. Bezwaar levert niets op: hij is immers tweemaal betrapt met te veel alcohol op achter het stuur. De heer G. bestrijdt dit, maar het CBR verwijst naar de computer met daarin het gegeven dat meneer tweemaal is aangehouden met teveel alcohol op. De informatie is afkomstig van de politie. De politie heeft inderdaad meneer G. aangehouden, en heeft de gegevens van G gedeeld met het CBR. Die gegevens zijn: achternaam, eerste voorletter en geboortedatum. Maar in de GBA staan twee personen G. met dezelfde voorletter, achternaam en geboortedatum. Onbekend is hoeveel mensen met dezelfde kenmerken niet in de GBA staan maar wel in Nederland hebben gereden. Het CBR blijkt op de verkeerde persoon te hebben “geklikt”. Op het nippertje hoeft meneer G. de cursus niet te doen en ook niet te betalen. Zijn dossier bij CBR wordt geschoond. De politie had gelukkig wél de juiste G. geregistreerd. Dat scheelde veel werk voor het CMI. Geen partij hierin maar belangrijke communicatieschakel was de RDW. Die heeft in deze keten de zaak voor het CMI uitgezocht bij het CBR.
<b>Fase 1: constateren</b>	
• Door wie?	De burger
• Soort fout	Persoonsverwisseling
• Soort gegevens	GBA gegevens (voorletter, achternaam en leeftijd)
<b>Fase 2: procedure</b>	
• Bij welke partij?	CBR in eerste instantie, later de politie, GBA en RDW.
• Aanwezig?	Nee. CMI moest escaleren door RDW aan het werk te zetten.
• Beschrijving	N.v.t.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Dient bezwaar in tegen verplichte cursus CBR
• Acties overheid / anderen	Na tussenkomst van CMI pakt RDW de zaak op en zoekt het uit.
• Mogelijkheden / beperkingen	CBR heeft uit GBA de verkeerde gegevens opgehaald. Het kan voorkomen dat in GBA personen staan met dezelfde voorletter, achternaam en geboortedatum. Partijen zouden hierop beter geattendeerd moeten worden om persoonsverwisseling te voorkomen. Een andere aanpak is de set van unieke identificerende gegevens uit te breiden met bijvoorbeeld NAW-gegevens. Mogelijk is dit in strijd met WBP.
• Resultaat	Voorkomen van persoonsverwisseling.
<b>Besturing</b>	
• Conclusies	Uitvoerende organisaties moeten beter geattendeerd worden op het feit dat meerdere personen in GBA geregistreerd staan met dezelfde persoonsgegevens. Uitbreiden van de set van persoonsgegevens bij het uitvragen van GBA kan voor unieke identificatie zorgen.



## CASUS 6: NIEUW BSN GEKREGEN

<b>Omschrijving</b>	BPR waarschuwt de gemeenten Rotterdam en Zwolle over het feit dat zij dezelfde persoon in de GBA hebben staan. Omdat mevrouw G. toch echt in Zwolle woont, verwijdt Rotterdam de andere registratie uit de GBA. Het vermoeden is dat een onbekende persoon in Rotterdam illegaal verbleef op haar identiteit. Ooit was o.a. het paspoort van mevrouw G. gestolen op de Antillen, dus is dit scenario niet ondenkbaar. Om mevrouw G. te beschermen tegen mogelijk onheil als gevolg van het mogelijke illegale verblijf door een ander, geeft Zwolle mevrouw G. een nieuw BSN. Nu maar hopen dat mevrouw G. niet al haar historie in de overheidsbestanden kwijt is! Omdat mevrouw G. kanker heeft en veel zorg nodig heeft, wordt gevreesd voor verwarring in o.a. haar patiëntendossiers. De gemeente Zwolle stuurt alle mogelijke betrokkenen een brief met daarin de boodschap dat deze persoon terecht twee BSN's heeft: één tot een bepaalde datum, en één vanaf een bepaalde datum. Na een jaar hebben wij mevrouw G. opgebeld, en er waren zowaar nauwelijks problemen. Alleen had ze wat gedoe met het UWV. Goed gehandeld door de gemeente en de ketenpartners. De extra attentie heeft mogelijk veel gedoe bespaard.
<b>Fase 1: constateren</b>	
• Door wie?	BPR
• Soort fout	Persoonsverwisseling
• Soort gegevens	GBA gegevens
<b>Fase 2: procedure</b>	
• Bij welke partij?	BPR en gemeenten
• Aanwezig?	Deels, BPR maakt melding van het gevaar van persoonsverwisseling bij betrokken gemeenten. De gemeenten gaan daarna redelijk ad hoc te werk om het probleem op te lossen.
• Beschrijving	De oplossing om een nieuw BSN te geven is niet de meest gelukkige.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Uitvoerende instanties erop wijzen dat ze twee BSN's heeft.
• Acties overheid / anderen	Na tussenkomst van CMI pakt gemeente Zwolle de zaak op en verstrekt een nieuw BSN.
• Mogelijkheden / beperkingen	De burger krijgt een nieuw BSN met alle mogelijke risico's van dien. Een oplossing die niet schaalbaar is omdat heel veel partijen aangeschreven moeten worden om ze te informeren over het nieuwe BSN. Het slachtoffer heeft nu twee BSNs, de vraag is of systemen hiermee overweg kunnen.
• Resultaat	Voorkomen van persoonsverwisseling.
<b>Besturing</b>	
• Conclusies	Uitvoerende partijen weten niet goed hoe ze om moeten gaan met situaties waarin sprake is van persoonsverwisseling. Hiervoor zou een leidraad moeten komen.

## CASUS 7: ECHT PASPOORT MET BSN VAN EEN ANDER

<b>Omschrijving</b>	Een Nederlander woont in Griekenland en krijgt een nieuw paspoort van het consulaat. Hoewel een consulaat geen BSN mag toekennen, krijgt meneer een BSN in zijn paspoort. Meneer verhuist naar Nederland en meldt zich bij de gemeentebalie. Daar ontdekt een oplettende burgerzakenambtenaar dat meneer onterecht een BSN in zijn paspoort heeft staan (die had hij pas aan de gemeentebalie mogen krijgen). Sterker nog: het BSN is gekoppeld aan iemand anders. De gemeente voorziet deze man van een nieuw document met daarin zijn echte, nieuwe, BSN. Onbekend is waarmee de man zich succesvol in systemen heeft laten inschrijven zonder dat iemand wist wat er aan de hand was.
<b>Fase 1: constateren</b>	
• Door wie?	Gemeenteambtenaar burgerzaken
• Soort fout	Onterecht en incorrect BSN in paspoort
• Soort gegevens	BSN
<b>Fase 2: procedure</b>	
• Bij welke partij?	Gemeente
• Aanwezig?	Ja.
• Beschrijving	Er wordt een nieuw paspoort gemaakt met daarin een nieuw en geldig BSN.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Geen.
• Acties overheid / anderen	Nieuw BSN en paspoort aanmaken.
• Mogelijkheden / beperkingen	Onduidelijk is wat hier precies is mis gegaan: wie mogen BSNs toekennen, waarom is voor de man een nieuw BSN aangemaakt? Na identificatie had het consulaat kunnen nagaan in GBA wat het BSN van de man was. Onduidelijk is in welke systemen de burger nog met het oude incorrecte BSN staat. Beter verificatie van de persoonsgegevens is nodig om te voorkomen dat nieuwe BSNs moeten worden aangemaakt. Dit kan door slechts enkele partijen gedaan worden. Ambtenaren dienen te weten hoe ze de echtheid en geldigheid van een paspoort kunnen controleren.
• Resultaat	Voorkomen onterecht aanmaken en toekennen van BSNs.
<b>Besturing</b>	
• Conclusies	Er moet beter toezicht komen op het aanmaken en toekennen van BSNs. Ambtenaren moeten kunnen herkennen of een paspoort authentiek en geldig is.

## CASUS 8: ADRESSERING VAN CORRESPONDENTIE

Een casus uit een rapport van de Nationale Ombudsman (zie

[http://www.nationaleombudsman.nl/sites/default/files/rapport\\_2011-325.pdf](http://www.nationaleombudsman.nl/sites/default/files/rapport_2011-325.pdf)).

<b>Omschrijving</b>	Mevrouw S. klaagt bij de Nationale Ombudsman over het feit dat haar medische gegevens ergens over straat zwerven. Haar dossier, dat is opgestuurd door het UWV, is nooit angekommen. Het antwoord van het UWV: "Er is gebleken dat bij de aanmaak van een brief uit ons geautomatiseerde brievenboek er een, naar nu blijkt, onjuist adres werd gepresenteerd. Dit brievenboek is gekoppeld aan de adresgegevens vanuit het uitkeringssysteem van de WAO en zou normaliter de juiste gegevens moeten presenteren. Uit nader onderzoek is echter gebleken dat in oktober 2009 een mutatie heeft plaatsgevonden in de basisregistratie personen (BRP). Er is een adres opgevoerd als zijnde verblijfadres. En dit verblijfadres is verschenen bij de aanmaak van de brief. Uit uw dossier blijkt niet dat u aan ons een verblijfadres heeft doorgegeven. Wij hebben helaas nog niet precies kunnen achterhalen op welke wijze dit (onjuiste) verblijfadres is toegevoegd. Er zijn echter meerdere klachten over dit onderwerp ontvangen en er loopt een onderzoek dat gecoördineerd wordt vanuit ons hoofdkantoor." Een uitslag op het onderzoek blijft uit en na vier maanden wachten grijpt de Ombudsman weer in. Het UWV reageert als volgt: "Wij hebben nu alsnog navraag gedaan bij onze divisie Gegevensdiensten. Daar werd ons verteld dat het systeem (de basisregistratie personen), van waaruit destijds het foutieve adres is ingevoerd, eind 2009 is opgeheven. Hiervoor is een nieuw systeem in de plaats gekomen. Dat betekent dat het een onevenredig grote inspanning zou kosten, die financieel niet te rechtvaardigen is, om na te gaan of nog terug te vinden is, door wie destijds een mutatie is ingevoerd. De enige verklaring die nu voorhanden is, is dat een niet te herleiden medewerker van het UWV per abuis op uw BSN een adreswijziging heeft gemuteerd. Gevolg daarvan is dat het onjuiste adres is gepresenteerd bij de aanmaak van de begeleidende brief bij verzending van de medische rapportage. Die medewerker heeft geen check uitgevoerd of het adres in de brief overeenkwam met het adres op uw dossier."
<b>Fase 1: constateren</b>	
• Door wie?	Burger
• Soort fout	Onjuiste mutatie van gegevens door verwerkende instantie
• Soort gegevens	Adresgegevens
<b>Fase 2: procedure</b>	
• Bij welke partij?	UWV
• Aanwezig?	Nee. UWV draagt slecht zorg voor de correcte adressering van de post.
• Beschrijving	De oorzaak wordt achterhaald doordat goed is bijgehouden (gelogd) wie, wat allemaal veranderd heeft in de gegevens en wanneer.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Klagen bij Nationale Ombudsman
• Acties overheid / anderen	Logging van mutaties.
• Mogelijkheden / beperkingen	Betere verificatie van adresgegevens had veel gedoe kunnen voorkomen. De gegevens in het GBA zijn niet altijd betrouwbaar. Bij twijfel is het wenselijk om andere bronnen te raadplegen en eventueel de burger zelf. Indien post geretourneerd wordt omdat het adres niet correct is, dient adresonderzoek plaats te vinden. Indien privacygevoelige informatie op een onjuist adres terecht is gekomen dient de verzendende partij ervoor te zorgen dat deze terug gehaald wordt. Gewaakt dient te worden voor de semantiek van gegevens: wat bedoelen we met een adres?
• Resultaat	Betere borging van privacygevoelige informatie.
<b>Besturing</b>	
• Conclusies	Uitvoerende organisaties dienen zich ervan te vergewissen dat adresgegevens kloppen. Mutaties in gegevens dienen te worden gelogd. De semantische betekenis van de gegevens dient duidelijk te zijn.

## CASUS 9: WERKSTRAF VOOR VALS ID

<b>Omschrijving</b>	<p>Toen hij zijn huis opruimde na een feestje, vond de 31-jarige Pool D. uit 't Loo het ID-bewijs van iemand die hij vaag kende. Omdat zijn eigen papieren niet rond waren, besloot hij het te houden en er een leven mee op te bouwen. In het jaar 2008 gebruikte hij het in 't Loo en Uddel om een bankrekeningnummer te openen en om te werken bij een uitzendbureau. Hij schreef zich onder de valse naam ook in bij de gemeente. Door aanslagen van de Belastingdienst, liep D. uiteindelijk tegen de lamp. De rechtmatige eigenaar van het identiteitsbewijs werd namelijk opeens aangeslagen voor werk waar hij niks vanaf wist. „Ik wilde het paspoort wel teruggeven, maar ik had ook werk nodig. Op een gegeven moment kon ik niet meer terug”, verweerde D. zich bij de politierechter. Nu hij een relatie heeft en een kindje, wil hij niets meer te maken hebben met criminaliteit. „Ik heb er echt spijt van, het had niet mogen gebeuren.” De openbare aanklager vond dat mooi, maar eiste alsnog een werkstraf van 100 uur tegen de man. „Dit is een heel ernstig misdrijf. Het gebruik van één vals ID-bewijs kost de maatschappij gemiddeld 40.000 euro. Dat zie je hier ook gebeuren. Het slachtoffer loopt tegen allerlei problemen aan, die hij maar weer moet zien op te lossen. Zoals met de belastingaanslagen bijvoorbeeld.” Wat hem betreft moest D. ook een schadevergoeding betalen van 2480 euro aan aanslagen en zo'n 820 euro aan kosten die het slachtoffer maakte door de situatie. Maar met dat bedrag was de advocaat van de man het niet eens. „De Belastingdienst kan die bedragen toch ook gewoon corrigeren? Waarom moet mijn cliënt die betalen aan het slachtoffer?” De politierechter kon zich daar wel in vinden. Zij veroordeelde D. tot een werkstraf van 100 uur, waarvan 40 uur voorwaardelijk. En vond een schadevergoeding van 600 euro voldoende. Voor het overige geld moet het slachtoffer aankloppen bij een civiele rechter. Maar daar stopt het niet bij voor het slachtoffer. De gegevens van de baan gaan van de Belastingdienst naar het UWV, namelijk in de polisadministratie. De polisadministratie deelt de gegevens met o.a. pensioenverzekeraars, uitkeringsinstanties, SVB, statistische instanties en ook weer met de Belastingdienst die de gegevens aanneemt als waar. Als je als slachtoffer aanklopt, word je door de Belastingdienst verwezen naar het UWV, net zoals bij de pensioenverzekeraar etc. Het UWV geeft aan de gegevens niet te mogen aanpassen van de wetgever. En zo gebeurt er niets, en kan het CMI zijn tanden hierop stuk bijten.</p>
<b>Fase 1: constateren</b>	
• Door wie?	Burger / slachtoffer n.a.v. onterechte aanslagen van de Belastingdienst
• Soort fout	Misbruik van identiteitsbewijs / vals ID bewijs
• Soort gegevens	Identiteitsgegevens
<b>Fase 2: procedure</b>	
• Bij welke partij?	Belastingdienst en UWV
• Aanwezig?	Nee, UWV zegt niets te kunnen doen. Belastingdienst verwijst door naar UWV.
• Beschrijving	N.v.t.
<b>Fase 3: uitvoering correctieproces</b>	
• Acties burger	Klagen politierechter, Belastingdienst en UWV om uiteindelijk bij het CMI uit te komen
• Acties overheid / anderen	Geen.
• Mogelijkheden / beperkingen	Wetgeving verhindert partijen om te corrigeren.
• Resultaat	Er gebeurt niets. Escalatie via CMI.
<b>Besturing</b>	
• Conclusies	Betere controle van de echtheid van het ID-bewijs had veel problemen kunnen voorkomen.

## CASUS 10: SAMENVOEGEN VAN ADRESSEN

<b>Omschrijving</b>	<p>Met de invoering van de BAG zijn in sommige gevallen meerdere GBA adressen samengevoegd tot een adres. Dit geldt bijvoorbeeld voor verzorgingshuizen, waar alle bewoners in het GBA een apart adres hebben. In de BAG krijgt het verzorgingstehuis een adres.</p> <p>Ook afzonderlijke appartementen complexen of studentenwoningen krijgen soms een adres. Het gevolg is dat beschikkingen, gebaseerd op een adres niet meer van toepassing zijn op de afzonderlijke adressen. Met als gevolg dat mensen geen recht meer hebben op toeslagen, zoals huurtoeslag of worden aangeslagen voor gemeentebelastingen voor alle bewoners.</p> <p>De casus is hier dat adressen van een appartement zijn samengevoegd, waardoor een persoon hoofdeigenaar is geworden en zowel de belastingen voor 4 appartementen betaalt, als ook de huurtoeslag voor 4 appartementen krijgt.</p>
<b>Fase 1: constateren</b>	
<ul style="list-style-type: none"> <li>• Door wie?</li> </ul>	De burger
<ul style="list-style-type: none"> <li>• Soort fout</li> </ul>	De burger kreeg aanslagen en toeslagen op naam die hij eerder niet kreeg.
<ul style="list-style-type: none"> <li>• Soort gegevens</li> </ul>	De burger constateerde dat de adresgegevens niet juist waren.
<b>Fase 2: procedure</b>	
<ul style="list-style-type: none"> <li>• Bij welke partij?</li> </ul>	De burger wendde zich tot de gemeente om de samenvoeging van de adressen ongedaan te maken. Voor zover bekend wendde hij zich niet tot de instanties die de verkeerde adresgegevens gebruikten als grond voor hun beslissing.
<ul style="list-style-type: none"> <li>• Aanwezig?</li> </ul>	Ja, het agentschap BPR heeft <a href="#">richtlijnen</a> ontwikkeld voor gemeenten hoe ze moeten omgaan met correcties van BAG gegevens.
<ul style="list-style-type: none"> <li>• Beschrijving</li> </ul>	In dit geval zal de gemeentelijke BAG-coördinator het geval moeten bekijken en een wijziging moeten aanbrengen in de gegevens.
<b>Fase 3: uitvoering correctieproces</b>	
<ul style="list-style-type: none"> <li>• Acties burger</li> </ul>	De burger neemt contact op met de gemeente om van het ene adres, weer meerdere te maken.
<ul style="list-style-type: none"> <li>• Acties overheid / anderen</li> </ul>	In dit specifieke geval hoort de burger niets van de gemeente.
<ul style="list-style-type: none"> <li>• Mogelijkheden / beperkingen</li> </ul>	Niet alle organisaties met een koppeling BAG-GBA maken alleen gebruik van dit BAG adres. Zij hebben de mogelijkheid om andere adressen te gebruiken. De vraag is of ze dat doen als ze die mogelijkheid hebben en waarom wel of niet.
<ul style="list-style-type: none"> <li>• Resultaat</li> </ul>	Niet iedere gemeente is in staat dit te veranderen.
<b>Besturing</b>	
<ul style="list-style-type: none"> <li>• Conclusies</li> </ul>	De gemeenten zijn verantwoordelijk voor de invoering van de BAG. En dus ook voor de aanpassing van adressen, om er voor te zorgen dat mensen recht houden op voorzieningen waar het adres de grond is van deze voorziening (zoals een huurtoeslag).

## CASUS 11: DE ZAAK ROMET – 1737 AUTO'S OP NAAM

Bron: Meulen, N.S. van der, & Koops, E.J. (2012). Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude. Een beschouwing naar aanleiding van de zaak-Romet. Nederlands Juristenblad, 87(25), 1709-1712.

<b>Omschrijving</b>	Het rijbewijs van de heer Romet wordt in 1995 gestolen. Romet doet aangifte en vraagt meer dan een jaar later een nieuw rijbewijs aan. Het oude, gestolen rijbewijs komt daarmee pas op dat moment te vervallen. Gedurende dat jaar zijn er 1737 auto's op Romet's naam geregistreerd, vermoedelijk op vertoon van het gestolen rijbewijs. Doordat de registraties op zijn naam staan, ontvangt Romet aanslagen voor motorrijtuigen- en houderschapsbelasting. Ook krijgt hij boetes voor overtredingen begaan met de op zijn naam geregistreerde auto's. Romet wordt min of meer gedwongen te betalen en verliest zijn uitkering. In 2004 verzoekt Romet de RDW om alle registraties ongedaan te maken. Dit doet de RDW maar niet met terugwerkende kracht omdat dat schadelijk zou zijn voor de betrouwbaarheid van het registratiesysteem. Romet maakt hiertegen bezwaar maar dat wordt afgewezen door de Raad van State. Romet doet in 2006 een beroep op het Europese Hof voor de Rechten van de Mens (EHRM). Het Hof komt in 2012 met een uitspraak waarin hij Romet gelijk geeft.
<b>Fase 1: constateren</b>	
<ul style="list-style-type: none"> <li>• Door wie?</li> </ul>	De burger
<ul style="list-style-type: none"> <li>• Soort fout</li> </ul>	Identiteitsfraude met gestolen paspoort. De aangifte van een gestolen rijbewijs leidt niet tot intrekken van het rijbewijs. Dit heeft geresulteerd in de mogelijkheid voor identiteitsfraude.
<ul style="list-style-type: none"> <li>• Soort gegevens</li> </ul>	Rijbewijsgegevens nodig voor het laten registreren van voertuigen.
<b>Fase 2: procedure</b>	
<ul style="list-style-type: none"> <li>• Bij welke partij?</li> </ul>	De burger wendde zich tot de RDW voor het ongedaan laten maken van de fouten. Daarna tot de rechter en uiteindelijk het EHRM.
<ul style="list-style-type: none"> <li>• Aanwezig?</li> </ul>	Deels, de registraties zijn ongedaan gemaakt, maar niet met terugwerkende kracht. Pas na escaleren bij het Hof is er een oplossing gekomen. Gezien de duur van dit traject (meer dan 15 jaar!) kan geconcludeerd worden dat er geen sprake is van een degelijke procedure.
<ul style="list-style-type: none"> <li>• Beschrijving</li> </ul>	Er is geen relatie tussen het aangeven van een gestolen rijbewijs en het intrekken ervan in het registratiesysteem van RDW. Klagen bij RDW heeft geresulteerd in een deeloplossing waarbij de problemen niet weggenomen zijn. Pas na escalatie bij het Hof is er een oplossing gekomen.
<b>Fase 3: uitvoering correctieproces</b>	
<ul style="list-style-type: none"> <li>• Acties burger</li> </ul>	De burger neemt contact op met de RDW en vraagt rechtshulp.
<ul style="list-style-type: none"> <li>• Acties overheid / anderen</li> </ul>	De Raad van State doet een verkeerde uitspraak; het Europese Hof moet er aan te pas komen.
<ul style="list-style-type: none"> <li>• Mogelijkheden / beperkingen</li> </ul>	Koppelen van systemen waarbij na aangifte bij de politie van een gestolen rijbewijs de RDW hiervan op de hoogte gesteld wordt.
<ul style="list-style-type: none"> <li>• Resultaat</li> </ul>	Voorkomen van identiteitsfraude met een gestolen rijbewijs.
<b>Besturing</b>	
<ul style="list-style-type: none"> <li>• Conclusies</li> </ul>	Identiteitsfraude kan voorkomen worden door systemen beter op elkaar aan te laten sluiten. Dit neemt niet weg dat gevallen van identiteitsfraude nooit helemaal zijn uit te sluiten en dat het voor dergelijke gevallen noodzaak blijft om te investeren in efficiënte en vriendelijke herstel mogelijkheden voor slachtoffers.

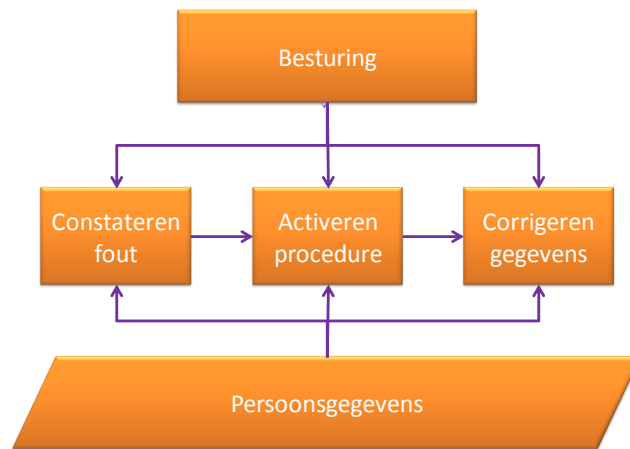
# Bijlage: interviewprotocol

- Rol van respondent in organisatie, hoe te maken met fouten in persoonsgegevens

Twee soorten vragen:

- Veel voorkomende gevallen
- Beleidsaspecten wat zou de politie en anderen moeten doen om proces van correctie te verbeteren.

Uitgangspunt van het onderzoek is het proces (constatering, correctieprocedure, correctie) en de besturing van dit proces. Besturing vanuit een netwerkperspectief:



## Onderwerpen proces:

Is er wel sprake van een proces, wat zijn de meest voorkomende processen (bijvoorbeeld kwijtraken paspoort of een procedure t.b.v. UWV)

- Wie constateert fout
- Is proces duidelijk
- Hoe is de uitvoering?
  - Zijn er overdrachtsmomenten, ketensamenwerking
  - Communicatie en toegankelijkheid naar burgers
  - Wettelijke kaders in procedures
  - Technische aspecten
  - Kwaliteit van gegevensbeheer
  - Andere aspecten?

## Besturing

- Taakverdeling en verantwoordelijkheden
- Duidelijkheid in taakverdeling

## Persoonsgegevens

Toegankelijkheid van informatie (beschikbaarheid, vindbaarheid, etc.)

