De Jong Beleidsadvies

Pro Facto
JURIDISCH EN BESTUURSKUNDIG ONDERZOEK EN ADVIES

Wat niet weet, wat niet deert

Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk

H.B. Winter

P.O. de Jong

A. Sibma

F.W. Visser

M. Herweijer

A.M. Klingenberg

H. Prakken

rijksuniversiteit groningen

Dit rapport is uitgebracht in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) te Den Haag.

Inhoud

Voorwoord

Het recht op privacy is een fundamenteel recht binnen een rechtsstaat. Het belang van dat recht wordt onderstreept door vastlegging daarvan in artikel 10 lid 1 van de Grondwet en in de Europese Privacyrichtlijn. Ter uitwerking daarvan is de Wet bescherming persoonsgegevens (Wbp) op 1 september 2001 in werking getreden. In dit evaluatieonderzoek is voor het eerst een empirisch beeld geschetst van de werking van de Wbp in de praktijk. Het onderzoek laat zien dat het privacyrecht nog niet in de volle breedte tot gelding is gekomen. De ontwikkeling van codes en gedragsregels ter invulling van de open normen in de wet heeft in belangrijke mate gestalte gekregen, maar is nog niet voltooid. Het onderzoek laat zien dat burgers en organisaties die met de wet te maken hebben nog niet altijd gemakkelijk in staat zijn daarmee om te gaan. Een op de bescherming van persoonsgegevens gerichte cultuur, ondersteund door voldoende experts en belangenbehartigers, is nog niet uitgekristalliseerd.

Dit rapport is geschreven door een onderzoeksteam van Pro Facto RuG en de Vakgroep Bestuursrecht en Bestuurskunde van de RuG. Kern van het onderzoeksteam werd gevormd door Edwin de Jong (De Jong Beleidsadvies), Anna Sibma (Pro Facto) en Feikje Visser (Pro Facto). Heinrich Winter trad als projectleider op. Wij zijn tijdens onze werkzaamheden ondersteund door Michiel Herweijer (bestuurskunde, RuG), Aline Klingenberg (bestuursrecht, RuG) en Henry Prakken (recht en ICT, RuG). Veel dank zijn wij verschuldigd aan de informanten bij bedrijven en overheden, die hun medewerking hebben verleend aan de gegevensverzameling. Bijzondere dank gaat uit naar het Cbp dat op verschillende manieren een bijdrage leverde aan het slagen van het onderzoek. Tot slot willen wij voorzitter en leden van de begeleidingscommissie bedanken, die ons tijdens het onderzoek van advies hebben voorzien. De samenstelling van de begeleidingscommissie is opgenomen in bijlage 1 van dit rapport.

Groningen, september 2008

Dr. H.B. Winter
Dr. P.O. de Jong
Mr. A. Sibma
Mr. drs. F.W. Visser

Samenvatting

De wettelijke regeling
De Wet bescherming persoonsgegevens (hierna: Wbp) is op 1 september 2001 in werking getreden. De Wbp is de opvolger van de Wet persoonsregistraties (Wpr). Met de Wbp is de Richtlijn betreffende de bescherming van de natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna: Privacyrichtlijn) geïmplementeerd.[1]

In de Wbp zijn de belangrijkste regels voor het vastleggen en gebruiken van persoonsgegevens vastgelegd. Het doel van de Wbp is allereerst om waarborgen te bieden waarmee een evenwicht tussen privacybescherming en andere belangen wordt bewerkstelligd. Daarnaast wordt de positie van de persoon wiens gegevens worden verwerkt, versterkt door hem rechten toe te kennen en aan verantwoordelijken daarmee corresponderende plichten op te leggen. Versterking van de positie van deze betrokkene vindt eveneens plaats door het aanwijzen van het College bescherming persoonsgegevens (hierna: Cbp) als toezichthouder en het opleggen van een plicht voor verantwoordelijken om de verwerking van persoonsgegevens te melden bij het Cbp of bij een Functionaris Gegevensbescherming (hierna: FG) als die is aangesteld (meldingsplicht).

Onderzoekskader
Artikel 80 van de Wbp vormt de grondslag voor de wetsevaluatie. In dat artikel is bepaald dat de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties binnen vijf jaren na de inwerkingtreding van de Wbp aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van de Wbp in de praktijk zenden. Volgens de wetgever zal bezien moeten worden of bepalingen wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer onvoldoende garanderen. De evaluatie ging van start met een knelpuntenonderzoek waarvan in 2007 verslag is gedaan. Anders dan dat knelpuntenonderzoek is dit evaluatieonderzoek empirisch georiënteerd. In dit onderzoek wordt onderzocht of de knelpunten zich in de praktijk daadwerkelijk voordoen. Bovendien wordt beschreven hoe informatie-uitwisseling verloopt en wat partijen zich daarbij voorstellen.

Onderzoeksvraag
De probleemstelling van het onderzoek luidt:

> *In hoeverre voldoet de werking van de Wbp in de praktijk aan de doelstellingen van de wet, in het bijzonder gelet op de in de literatuur gesignaleerde knelpunten en welke aanpassingen zijn mogelijk en wenselijk binnen het kader van de EU-richtlijn?*

Ter uitwerking van deze probleemstelling hebben we 18 deelvragen gesteld en beantwoord, verdeeld over een drietal categorieën; normeren, informeren en toezicht en rechtsbescherming.

Onderzoeksopzet
Voor het onderzoek is gebruik gemaakt van verschillende onderzoeksmethoden. Naast het bestuderen van relevante literatuur, zijn drie vragenlijsten uitgezet. Het eerste

[1] Richtlijn 95/46/EG, PbEG L 281, p. 0031-0050

enquêteonderzoek is gehouden onder een steekproef van overheidsorganisaties en organisaties uit het Handelsregister. De tweede vragenlijst is gericht aan een aantal organisaties die zijn geselecteerd door middel van een steekproef uit het meldingenregister bij het Cbp. De derde enquête is gestuurd naar alle FG's. De vragenlijsten zijn gebaseerd op het beschrijvingskader van het onderzoek dat in hoofdstuk 3 is opgenomen. Daaraan lag, naast het knelpuntenonderzoek en literatuurstudie, een aantal oriënterende interviews ten grondslag. De enquêteresultaten zijn geïnterpreteerd met behulp van de bevindingen uit een aantal expertmeetings, onder meer met FG's. Ook hebben we met dat doel een aantal diepte-interviews afgenomen met privacy officers, juridische experts en de voorzitter van het Cbp. Om meer zicht te verkrijgen op de rol die de wet speelt bij gegevensuitwisseling in samenwerkingsverbanden is een tweetal casestudies uitgevoerd. Tot slot is gesproken met een aantal burgers en hun rechtshulpverleners die een geschil hadden over de verwerking van hun persoonsgegevens.

Bevindingen
Voor de interpretatie van de uitkomsten van het onderzoek is het van belang vast te stellen dat het responspercentage bij één van de uitgezette enquêtes voldoende was, bij één matig en bij één enquête onvoldoende. Dat noopt tot enige terughoudendheid bij de presentatie en het veralgemeniseren van de bevindingen. Dat neemt niet weg dat door de uitkomsten van de enquêtes onderling te combineren, en ook te vergelijken met de informatie die met behulp van de kwalitatieve onderzoeksmethoden is verzameld, een redelijk consistent beeld naar voren komt.

De algemene conclusie van dit evaluatieonderzoek is dat de doelstellingen van de Wbp, het waarborgen van evenwicht tussen het privacybelang en andere grondrechten en het versterken van de positie van personen van wie gegevens worden verwerkt, nog niet ten volle worden gerealiseerd. Uit het enquêteonderzoek, interviews met experts, FG's, vertegenwoordigers van burgerbelangen, casestudies en interviews met burgers die een geschil aanhangig hebben gemaakt, komt het beeld naar voren van een wet die in de rechtspraktijk nog niet erg leeft, betrekkelijk lastig hanteerbaar wordt geacht en waarbij een op de toepassing gerichte privacygemeenschap en -cultuur nog niet in de volle breedte tot ontwikkeling is gekomen.

Door de open normen die de wet kent, is normontwikkeling wenselijk in nadere regelingen per organisatie of per sector of branche. Het onderzoek laat zien dat er aan de ene kant bij ruim de helft van de organisaties een privacyregeling van kracht is. Dat betekent tegelijkertijd dat er anderzijds veel organisaties zijn die een nadere regeling (nog) ontberen. Daarnaast wijzen zowel de enquêteresultaten, als de bevindingen uit interviews en expertmeetings, uit dat de kennis over de wet bij de doelgroepen van de wet (verantwoordelijken en betrokkenen) nog zou kunnen toenemen. Ook de bewustwording van het belang van privacy is niet bij alle verantwoordelijken en betrokkenen even groot. Dat kan onder meer worden afgeleid uit het beperkte gebruik dat betrokkenen maken van hun rechten tot inzage, correctie, aanvulling en verwijdering. Het kan ook blijken uit het zeer geringe aantal geschillen dat bij rechterlijke colleges en het Cbp aanhangig wordt gemaakt. Privacy is voor burgers wel een onderwerp, maar de gevoelige plek zit 'diep'. Burgers maken onderscheid tussen privacy in het algemeen, die in dat denkkader aan andere belangen, zoals veiligheid, ondergeschikt kan zijn, en de eigen privacy. Wanneer het persoonlijk wordt is er sneller sprake van een issue van grote zorg.

Organisaties kunnen – meestal op vrijwillige basis – een FG benoemen. De activiteiten van een dergelijke functionaris lijken in de praktijk bij te dragen aan een bewuste omgang met persoonsgegevens binnen die organisaties. Toch is er bij slechts 0,3 promille van de

organisaties in ons land een FG aangesteld. Aanstelling van een dergelijke functionaris zou voor veel organisaties ook een te zwaar middel zijn om privacybescherming te waarborgen. Het branchegewijs, samen met andere organisaties aanstellen van een FG (overeenkomstig art. 62 van de wet), zou daarom gestimuleerd moeten worden. Het belang van de functie zou ook verder kunnen toenemen door daaraan meer dan op dit moment eisen te stellen op het vlak van kwaliteit, opleiding en vaardigheden. De bedoeling van de verplichting bepaalde verwerkingen van persoonsgegevens te melden is om de bewustwording van de omgang met die gegevens te versterken, de naleving van het doelbindingsprincipe te bevorderen en de betrokkene duidelijk te maken wie verantwoordelijk is voor het vaststellen van doel en middelen van de verwerking. De onderzochte praktijk laat een zekere terughoudendheid zien bij het gebruik van persoonsgegevens en de meldingsprocedure lijkt inderdaad een preventief effect te hebben. Opnemen van een melding in het meldingenregister bij het Cbp lijkt op zichzelf niet erg zinvol. Uit gesprekken met rechtshulpverleners en burgers die een geschil aanhangig hebben gemaakt komt naar voren dat dat register bij veel betrokkenen weinig bekendheid geniet. Onze respondenten geven bovendien aan dat de transparantie van het meldingenregister te wensen over laat.

Een centrale uitkomst van het onderzoek is daarmee dat normontwikkeling, voorlichting en advisering op maat nadrukkelijk aandacht behoeven. Het intensiveren van de toezichtsinspanningen door het Cbp, dat zijn activiteiten in 2007 in die richting meer nadruk heeft gegeven, kan daarbij een rol spelen, maar dient ondersteund te worden door uitleg over de normen. Ook zouden betrokkenen kunnen worden geactiveerd inspanningen te leveren ten behoeve van het privacybelang. De behoefte aan normontwikkeling en uitleg moet ook worden gezien tegen de achtergrond van het feit dat de Wbp nog niet erg lang bestaat, hoewel de wet in de Wpr een verwante rechtsvoorganger had. Kenmerkend voor de Wbp is dat het gaat om een wettelijke regeling met open normen die nadere invulling behoeven. Dat kost tijd. En – zo luidt een rode draad van de onderzoeksbevindingen – de rechtsontwikkeling in de zin van sectorale normen en jurisprudentie, die vraagt om contextspecifieke kennis (branche, sector, technologie), is nog niet over de hele linie uitgekristalliseerd.

Hoofdstuk 1 Inleiding, vraagstelling en onderzoeksaanpak

1.1 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (hierna: Wbp) is op 1 september 2001 in werking getreden.[2] De Wbp is de opvolger van de Wet persoonsregistraties (hierna: Wpr). Met de Wbp is de Richtlijn betreffende de bescherming van de natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna: Privacyrichtlijn) geïmplementeerd.[3]

In de Wbp zijn de belangrijkste regels voor het vastleggen en gebruiken van persoonsgegevens vastgelegd. Het doel van de Wbp is allereerst om waarborgen te bieden waarmee een evenwicht tussen privacybescherming en andere grondrechten wordt bewerkstelligd. Daarnaast wordt de positie van de personen wiens gegevens worden verwerkt versterkt door hen rechten toe te kennen en aan verantwoordelijken daarmee corresponderende plichten op te leggen. Versterking van de positie van deze betrokkenen vindt eveneens plaats door het opleggen van een meldingsplicht en het aanwijzen van het College bescherming persoonsgegevens (hierna: Cbp) als toezichthouder.[4]

1.2 Onderzoekskader

1.2.1 Evaluatie in twee fasen

Deze rapportage betreft een onderzoek waarin de werking van de Wbp in de praktijk centraal staat. Dit onderzoek is een vervolg op het knelpuntenonderzoek waarvan in 2007 een rapport is uitgebracht.[5] Dat onderzoek betrof een literatuurstudie waarin is geïnventariseerd in hoeverre en op welke wijze de Wbp een bijdrage heeft geleverd aan het realiseren van de doelstellingen van deze wet, alsmede welke knelpunten zich in de praktijk hebben voorgedaan bij de uitvoering en toepassing daarvan. In tegenstelling tot dat knelpuntenonderzoek is dit evaluatieonderzoek empirisch georiënteerd. In dit onderzoek wordt onderzocht of de knelpunten zich in de praktijk daadwerkelijk voordoen. Bovendien wordt beschreven hoe informatie-uitwisseling verloopt en wat partijen zich daarbij voorstellen.

Artikel 80 van de Wbp vormt de grondslag voor de wetsevaluatie. In dat artikel is bepaald dat de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties binnen vijf jaren na de inwerkingtreding van de Wbp aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van de Wbp in de praktijk zenden. In de memorie van toelichting bij de Wbp is aangegeven dat deze evaluatiebepaling is opgenomen gelet op de snelle informatietechnologische ontwikkelingen. Volgens de wetgever zal bezien moeten worden of bepalingen wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer onvoldoende garanderen.[6]

---

[2] Wet bescherming persoonsgegevens, Stb. 2000, 302
[3] Richtlijn 95/46/EG, PbEG L 281, p. 0031-0050
[4] Zwenne e.a. 2007, p. 10
[5] Zwenne e.a. 2007
[6] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 197

Het praktijkonderzoek is door de opdrachtgever afgebakend naar een beperkt aantal van de knelpunten die uit het voorgaande onderzoek naar voren zijn gekomen. Voor dit onderzoek is deze afbakening bepalend. In de afbakening die door de opdrachtgever is vastgesteld komen weinig knelpunten voor die betrekking hebben op technologische ontwikkelingen. Als gevolg hiervan is de aandacht die wordt besteed aan dit onderwerp, beperkt. (zie de volgende paragraaf - deelvraag 4).

Parallel aan het onderzoek naar de werking van de wet in de praktijk is door de Adviescommissie veiligheid en de persoonlijke levenssfeer onder voorzitterschap van Brouwer-Korf gekeken naar de relatie tussen veiligheid en privacy (zie hierna paragraaf 1.2.2). Tevens is onderzoek uitgevoerd naar de administratieve lastendruk die samenhangt met de wet (zie paragraaf 1.2.3).

1.2.2 Veiligheid en privacy

In januari 2008 is de Commissie veiligheid en persoonlijke levenssfeer geïnstalleerd. Deze commissie, naar haar voorzitter de commissie Brouwer-Korf genoemd, onderzoekt onder meer wat het kabinet kan doen om het mogelijk te maken dat hulpverleners, preventiemedewerkers en criminaliteitsbestrijders noodzakelijke gegevens vlot en verantwoord kunnen uitwisselen. Verder kijkt de commissie naar de verhouding tussen criminaliteitsbestrijding en de waarborgen voor de omgang met persoonsgegevens. Ook heeft de commissie tot taak het kabinet te adviseren in hoeverre de technische mogelijkheden worden benut om burgers te informeren over wat er met hun persoonsgegevens gebeurt.[7]

De commissie is ingesteld naar aanleiding van een tweetal onderzoeksrapporten die in 2007 zijn uitgebracht.[8] Beide onderzoeken gaan over de verhouding tussen maatregelen in het kader van terrorismebestrijding en criminaliteitsbeheersing en de privacy van burgers. Gedacht kan worden aan antiterrorisme wetgeving, de bewaarplicht voor telecommunicatiegegevens of de identificatieplicht. Uit beide onderzoeken blijkt dat privacy nauwelijks een rol van betekenis speelt in het debat over opsporings- en veiligheidsmaatregelen en dat privacy en veiligheid als tegengesteld aan elkaar worden gezien: privacy en veiligheid vallen niet met elkaar te combineren.[9] [10]

1.2.3 Administratieve lastendruk

Zowel door het Cbp als door VNO-NCW zijn de afgelopen jaren voorstellen gedaan om de administratieve lasten van de Wbp te beperken. Op dit moment loopt er een interdepartementaal project over de administratieve lastendruk van de wet, in welk verband er een (nieuwe) nulmeting wordt gedaan naar de lastendruk van de Wbp. De Minister van Justitie heeft op 22 november 2007 in een algemeen overleg met de vaste kamercommissies voor Justitie en Binnenlandse Zaken en Koninkrijksrelaties aangegeven nog voor het kerstreces een wetsvoorstel aan de ministerraad te zullen voorleggen dat tegemoetkomt aan de bezwaren over de verhoging van de administratieve lastendruk die met de Wbp samenhangen. Een aantal praktische suggesties van het Cbp en van VNO-NCW zullen hierin worden opgenomen.[11] Inmiddels heeft de Raad van State advies uitgebracht over het wetvoorstel dat

[7] MvJ 2008
[8] Vedder e.a. 2007 en Muller e.a. 2007
[9] Vedder e.a. 2007, p. 11
[10] Muller e.a. 2007, p. 54
[11] *Kamerstukken II 2007-2008*, 31 051, nr. 2, p. 4

naar aanleiding van de bevindingen van de commissie is opgesteld. Het wetsvoorstel zal naar verwachting op korte termijn bij de Tweede Kamer worden ingediend.

In het onderhavige evaluatieonderzoek wordt eveneens aandacht besteed aan de administratieve lasten van de Wbp.[12] Het is niet de bedoeling om onderzoek te doen naar de administratieve lasten van de Wbp volgens de zogenaamde Actal-methode.[13] De vragen over de administratieve lasten zijn bedoeld om inzicht te krijgen in de voor- en nadelen van open normen en in de overwegingen van de verantwoordelijke om de Wbp al dan niet na te leven. Bij het vergelijken van de voor- en nadelen van open normen versus gedetailleerde voorschriften is het criterium administratieve lasten in de bevraging van de respondenten meegenomen.

1.3 Probleemstelling en deelvragen

De probleemstelling van het onderzoek luidt:

> *In hoeverre voldoet de werking van de Wbp in de praktijk aan de doelstellingen van de wet, in het bijzonder gelet op de in de literatuur gesignaleerde knelpunten en welke aanpassingen zijn mogelijk en wenselijk binnen het kader van de EU-richtlijn?*

Ter uitwerking van deze probleemstelling hebben we verschillende deelvragen gesteld, verdeeld in een drietal categorieën; normeren, informeren en toezicht en rechtsbescherming.

1.3.1 Normeren

De wetgever heeft in de Wbp gebruik gemaakt van open normen. Onder een 'open norm' wordt verstaan een norm met een globaal geformuleerde doelstelling of een norm met globaal geformuleerde gedragsvoorschriften die de normadressaat, degene tot wie een wettelijk voorschrift zich richt, ruimte laten om zelf te bepalen op welke wijze het doel wordt gerealiseerd of aan de gedragsvoorschriften wordt voldaan.[14] De keus voor de open normen is gemaakt omdat de Wbp een ruim toepassingsgebied kent en vanwege de zich snel ontwikkelende ICT-technologie.

Eén van de belangrijkste conclusies van het knelpuntenonderzoek was dat de begrippen van de Wbp in de praktijk moeilijk hanteerbaar zijn. Dit komt zowel door het gebruik van open normen als door de samenloop van de Wbp met andere wetgeving.[15] De gehanteerde normen worden als te vaag ervaren.[16] In de praktijk blijkt het bijvoorbeeld lastig te bepalen te zijn wat moet worden verstaan onder het op 'behoorlijke en zorgvuldige wijze' verwerken van persoonsgegevens (artikel 6) en het verzamelen van persoonsgegevens voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden' (het zogenaamde doelbindingsbeginsel van artikel 7).

[12] Zie deelvraag 1 en deelvraag 12
[13] Adviescollege Toetsing Administratieve Lasten (ACTAL) is een onafhankelijk adviescollege dat regering en Staten-Generaal adviseert over (reductie van) administratieve lasten voor bedrijven (Stb. 2000, 162) en (later ook) burgers (Stb. 2005, 113). Zie ook www.actal.nl.
[14] Dorbeck-Jung e.a. 2005, p. 20
[15] Zwenne e.a. 2007, p. 167
[16] Idem, p. 74

Vraag 1: Wat zijn de voor- en nadelen van open normen, in het algemeen en specifiek voor de Wbp? Hoe werkbaar zijn de open normen uit de Wbp? Is altijd duidelijk wanneer gegevens mogen worden uitgewisseld?

Volgens de wetgever moeten de open normen geconcretiseerd worden door middel van zelfregulering.

Eén van de manieren om tot zelfregulering over te gaan, is door het opstellen van een gedragscode. In artikel 25 van de Wbp is bepaald dat een organisatie een gedragscode kan opstellen waarin de wettelijke regels voor een bepaalde sector worden gepreciseerd. Het CBP dient de opgestelde gedragscode goed te keuren. Tot nu toe zijn er slechts negen gedragscodes goedgekeurd door het Cbp, waarvan twee goedkeuringsverklaringen alweer zijn verlopen. Uit het knelpuntenonderzoek blijkt dat de invloed van het Cbp bij het goedkeuren van de gedragscode als een knelpunt wordt ervaren.[17] Daarnaast wordt het opstellen van een gedragscode als tijdrovend en kostbaar beschouwd en staan er weinig concrete voordelen tegenover.[18]

Naast het opstellen van een gedragscode kan zelfregulering ook plaatsvinden door op basis van artikel 62 van de Wbp een zogenaamde Functionaris voor de Gegevensbescherming (hierna: FG) aan te stellen. Een FG is een interne toezichthouder.

In het knelpuntenonderzoek is geconcludeerd dat de door de wetgever gewenste zelfregulering moeizaam van de grond komt.

2. Wat is de achtergrond van het ontbreken van sectorale regelgeving en/of gedragscodes? Vervulde het Cbp hierbij een 'ontwikkelende' en stimulerende rol?

3. Op welke wijze kan worden voorzien in de ontwikkeling van sectorale normen en door wie?

In de paragraaf hiervoor is al aangegeven dat de evaluatiebepaling in de Wbp is opgenomen gelet op de snelle ontwikkelingen in de informatietechnologie. Volgens de wetgever zal bezien moeten worden of bepalingen wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer onvoldoende garanderen.[19] De Wbp maakt gebruik van open normen om de regeling zo technologieonafhankelijk mogelijk te maken.[20] In de praktijk blijken er toch knelpunten te zijn die samenhangen met de technologische ontwikkelingen. Het gaat er dan met name om dat de begrippen van de Wbp niet zijn afgestemd op de ontwikkelingen in 'de wereld van het Internet.[21] Het is niet altijd duidelijk wie als 'verantwoordelijke' moet worden aangemerkt en welke verwerkingen van persoonsgegevens meldingsplichtig zijn.[22] Ook is de Wbp niet toegesneden op biometrie, het aanpakken van

[17] Zwenne e.a. 2007, p. 79 en Holvast 2005, p. 114-119
[18] Cuijpers 2006
[19] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 197
[20] TK 1997-1998, 25 892, nr. 3, p. 41
[21] Zwenne e.a. 2007, p. 96
[22] Idem, p. 101

spam en toepassing van RFID-technologie.[23] Spam is voor particulieren reeds verboden op basis van de Telecommunicatiewet en sinds kort geldt ook een spamverbod voor bedrijven.

Naast negatieve invloeden op de privacy kunnen technologische ontwikkelingen ook positief zijn voor de bescherming van persoonsgegevens. Gedacht kan worden aan Privacy Enhancing Technologies (PET). De term Privacy Enhancing Technologies (PET) wordt gehanteerd om alle ICT-middelen aan te duiden die gebruikt kunnen worden om persoonsgegevens te beschermen.

4. Wat kan worden gezegd over de mate waarin technologische ontwikkelingen een rol spelen bij de toepassing van de wet?

In de publieke en semi-publieke sector wordt telkens meer samengewerkt tussen verschillende organisaties. Uitwisseling van persoonsgegevens is hierbij vaak een vereiste. Uit het knelpuntenonderzoek blijkt dat er verschillende knelpunten worden ervaren bij de gegevensuitwisseling in samenwerkingsverbanden. Bij de samenwerkingspartners is het niet altijd duidelijk welke ruimte de Wbp biedt om tot gegevensuitwisseling over te gaan. In de praktijk bestaat het beeld dat de Wbp de uitwisseling van persoonsgegevens in samenwerkingsverbanden belemmert. Volgens het Cbp is dit niet (altijd) het geval en stelt de Wbp slechts randvoorwaarden aan de gegevensuitwisseling in samenwerkingsverbanden.[24]

Om te beoordelen of gegevensuitwisseling in de praktijk echt wordt bemoeilijkt door de Wbp, is de volgende deelvraag geformuleerd.

5. Op welke manier vormt de normering van de Wbp een knelpunt in de (keten)samenwerking?

1.3.2 Informeren

Voor een goede naleving van de wet is het een vereiste dat de normadressaten op de hoogte zijn van (de inhoud van) de wet. Van belang hierbij is het feit dat van open normen gebruik wordt gemaakt. Omgang met open normen vereist meer (juridische) kennis dan omgang met gedetailleerde normen. Als de open normen zijn geconcretiseerd door middel van zelfregulering, is andere kennis van de Wbp nodig dan wanneer dit niet is gebeurd. Bovendien is het niet onwaarschijnlijk dat verschillende doelgroepen (verantwoordelijken, professionele gebruikers en burgers) een andere informatiebehoefte hebben.

6. Hoe duidelijk is de wet en op welke wijze en in welke mate worden normen verduidelijkt door het Cbp en de jurisprudentie?

7. Welke informatie wordt, onder meer door het Cbp, aan de doelgroepen van de wet (verantwoordelijken, professionele gebruikers en burgers) gegeven? Is die informatie voldoende? Welke verbeteringen zijn mogelijk?

[23] Zwenne e.a. 2007, p. 116
[24] Idem, p. 125

8. Hoe is de naleving van de informatieplicht en leidt dat er toe dat de burger regie voert over zijn gegevens?

Transparantie is het uitgangspunt van de Wbp; iedereen moet kunnen nagaan waar gegevens over hem zijn vastgelegd en worden verwerkt.[25] De Wbp legt hiertoe aan verantwoordelijken een meldings- en informatieplicht op.[26] Anderzijds zijn aan betrokkenen verschillende rechten toebedeeld. Het gaat hierbij om het recht gegevens in te zien en het recht te vragen om verbetering, aanvulling, verwijdering en afscherming van de persoonsgegevens. Daarnaast kunnen zij in een aantal gevallen verzet aantekenen tegen de verwerking van hun persoonsgegevens.

Uit het knelpuntenonderzoek blijkt dat de meldplicht voor problemen zorgt. De ruime werking van de meldplicht (melden, tenzij) wordt als knelpunt gezien. Daarnaast worden vraagtekens geplaatst over de bijdrage die de meldplicht levert aan de beoogde transparantie.[27] Verder blijkt dat vaak wordt geklaagd over de hoogte van de administratieve lasten van de meldplicht.[28]

Ook zijn knelpunten geconstateerd bij het vormgeven en naleven van de informatieplicht.
Het vooraf informeren van betrokkenen is arbeidsintensief en botst in sommige gevallen met het vertrouwelijke karakter van de betreffende gegevensverwerking. Daarnaast wordt de informatieplicht als lastig toepasbaar ervaren door het gebruik van open normen.[29] Verder zijn er signalen dat de informatieplicht en het toestemmingsvereiste bij 'grote' uitvoeringsorganisaties zorgen voor relatief hoge uitvoeringskosten. [30] Als gevolg van onduidelijkheid rond de verantwoordelijkheid voor de informatieplicht en de onbekendheid met deze verplichting laat de naleving in sommige gevallen te wensen over.[31]

Ten aanzien van de rechten van betrokken, blijkt uit het knelpuntenonderzoek dat hiervan door betrokkenen weinig gebruik wordt gemaakt. Het is dan ook de vraag of betrokkenen wel op de hoogte zijn van het bestaan van hun rechten. Bovendien blijkt uit het knelpuntenonderzoek dat er onduidelijkheid over de reikwijdte en invulling van de rechten bestaat. Er zijn aanwijzingen dat procedures en maatregelen vaak ontbreken om de rechten van burgers binnen de wettelijke termijnen op een zorgvuldige wijze te kunnen effectueren.[32]

9. Hoe groot is de naleving van de meldingsplicht (bij Cbp en FG)?

10. Tot welke administratieve lasten leidt de naleving van de meldingsplicht?

11. Heeft de meldingsplicht de omgang met persoonsgegevens beïnvloed? Is de bescherming van de privacy daardoor verbeterd?

12. Wat is de rol van de FG's en het Cbp bij de meldingsplicht?

[25] Hooghiemstra en Nouwt 2007, p. 18
[26] Memorie van toelichting, p. 18
[27] Holvast 2005, p. 208 -211
[28] Zwenne e.a. 2007, p. 93
[29] Idem, p. 11
[30] Idem, p. 12
[31] Idem, p. 151
[32] Idem, p. 170 en 171

13. Welke rol spelen FG's en Cbp bij voorlichting over en controle op het doelbindingsprincipe? Is een afweging tussen het privacybelang en het doel van de registratie voldoende gewaarborgd?

14. Welke verbeteringen zijn mogelijk rond meldingsplicht en informatieplicht?

1.3.3 Toezicht en rechtsbescherming

De onderzoekers die het knelpuntenonderzoek hebben uitgevoerd, hebben aangegeven dat het intern functioneren van het Cbp buiten het bereik van het onderzoek valt. Niet het functioneren van de toezichthouder, maar van de wet is onderwerp van de evaluatie.[33] In dit tweede deel van de evaluatie wordt wel aandacht besteed aan het functioneren van de toezichthouder. Nagegaan wordt welke invulling het Cbp aan de hem toegekende wettelijke functies geeft.

Een verantwoordelijke kan ook een eigen, interne toezichthouder aanstellen. Uit het knelpuntenonderzoek blijkt dat FG's met name in de publieke sector zijn aangesteld. Hoewel in artikel 62 van de Wbp is bepaald dat de bevoegdheden van het Cbp onverlet blijven als een toezichthouder is aangesteld, geeft het Cbp zelf aan terug te treden als eerstelijns toezichthouder wanneer een FG is aangesteld. FG's willen deze terughoudende rol graag geformaliseerd zien, zo blijkt uit het knelpuntenonderzoek.[34] Verder blijkt dat het kunnen waarborgen van de onafhankelijkheid van de FG als knelpunt wordt gezien.[35]

15. Waarom gaan verantwoordelijken (niet) over tot benoeming van een FG?

16. Welke invulling geven het Cbp en de FG's aan de wettelijk aan hen toegekende functies bij het toezicht en hoe vaak doen ze dat?

Als een burger het niet eens is met de verwerking van zijn persoonsgegevens, kan hij beroep aantekenen bij de civiele rechter (artikel 46 Wbp). Als de gegevensverwerking plaatsvindt door een bestuursorgaan kan de burger, na het volgen van een bezwarenprocedure, bij de bestuursrechter terecht (artikel 45 Wbp). Uit het knelpuntenonderzoek blijkt dat betrokkenen weinig gebruik maken van hun rechtsbeschermingmogelijkheden, waardoor de open normen niet nader worden ingevuld. De rechtsingang is door het gedifferentieerde systeem niet erg eenduidig en voor het privaatrecht hoogdrempelig.[36] Het feit dat er weinig jurisprudentie is, kan bovendien worden veroorzaakt door de onbekendheid met de Wbp.[37] Daarnaast heeft de burger alternatieven voor (dure) rechtspraak, namelijk de gang naar een geschillencommissie of het doen van een bemiddelingsverzoek bij het Cbp (artikel 47 Wbp).

17. Wat zijn overwegingen voor betrokkene al dan niet te klagen en te procederen?

[33] Zwenne e.a. 2007, p. 18 en 172
[34] Idem, p. 80
[35] Idem, p. 80
[36] Idem, p. 171-172.
[37] Idem, p. 24

18. In hoeverre heeft de jurisprudentie preventieve werking en hoe zou deze kunnen worden vergroot?

1.4 Onderzoeksaanpak

Om tot beantwoording van de deelvragen te komen zijn de volgende onderzoeksactiviteiten uitgevoerd:

I Oriëntatie
- Desk- en literatuuronderzoek
- Oriënterende interviewronde

II Gegevensverzameling
- Enquêteonderzoek
- Casestudyonderzoek
- Interviewronde
- Expertmeetings

III Rapportage

Hierna wordt uiteengezet hoe deze onderzoeksactiviteiten zijn uitgevoerd en welke deelvragen met welke deelonderzoek zijn beantwoord.

1.4.1 Desk- en literatuuronderzoek

Het onderzoek is gestart met een verkenning van de literatuur, documenten en jurisprudentie over de Wbp. Deze verkenning heeft geleid tot het aanscherpen van de vraagstelling van het onderzoek, maar vooral tot het operationaliseren van de verschillende deelvragen in vragenlijsten voor nader onderzoek. Grondslag daarvoor is het beschrijvingskader van het onderzoek dat in hoofstuk 3 van deze rapportage is opgenomen. Daarmee heeft dit deelonderzoek antwoord verschaft op deelvraag 1 over de voor- en nadelen van open normering in het algemeen en specifiek voor de Wbp. Ook deelvraag 6, over de duidelijkheid van de wet en de wijze waarop en de mate waarin het Cbp en de jurisprudentie bekendheid verschaffen over de normen van de wet, is op basis van dit deelonderzoek beantwoord.

Verder zijn in dit deelonderzoek de beschikbare kwantitatieve gegevens van het Cbp geanalyseerd.

1.4.2 Oriënterende interviewronde

Op basis van het literatuuronderzoek zijn zes oriënterende interviews gehouden met de voorzitter en twee medewerkers van het Cbp, een Functionaris voor de Gegevensbescherming (hierna: FG), een jurist van het Ministerie van Justitie en een jurist van het ministerie van Binnenlandse Zaken en Koninkrijksrelatie, een adviseur op het gebied van privacy, twee vertegenwoordigers van het bedrijfsleven en een vertegenwoordiger van een bedrijf dat diensten aanbiedt op het Internet. Het doel van deze interviewronde was om te komen tot een nadere oriëntatie op de knelpunten in de wet, zoals die uit het knelpuntenonderzoek naar

voren komen. Daarnaast dienden de oriënterende interviews er toe vragenlijsten te kunnen opstellen voor het kwantitatieve deelonderzoek.

In bijlage 2 is aangegeven met welke personen gesprekken zijn gevoerd.

1.4.3 Enquêteonderzoek

De kern van het evaluatieonderzoek bestaat uit een drietal schriftelijke/elektronische enquêtes en diepteinterviews met burgers. Twee enquêtes zijn verricht bij bedrijven, maatschappelijke ondernemingen en bestuursorganen en één enquête is naar de FG's verstuurd. Met de enquêtes en interviews is een belangrijk deel van het onderzoek meer kwantitatief aangepakt. In dit vragenlijstenonderzoek konden vragen worden gesteld over feitelijke gegevens, ontwikkelingsgegevens en opinies. De gehanteerde vragenlijsten zijn beschikbaar via www.pro-facto.nl. In hoofdstuk 4 wordt meer gedetailleerde informatie gegeven over de wijze waarop het vragenlijstonderzoek is uitgevoerd.

De volgende schriftelijke/enquêtes zijn uitgezet:

1. Algemene enquête
Onder bedrijven, instellingen en bestuursorganen die zijn geselecteerd uit een lijst van bestuursorganen en het handelsregister van de Kamer van Koophandel is een korte schriftelijke enquête uitgeschreven. Om in totaal 100 enquêtes geretourneerd te krijgen zijn in totaal 638 organisaties aangeschreven. De steekproef die we hebben uitgevoerd is gestratificeerd, dat wil zeggen dat we hebben gezocht naar categorieën van organisaties die naar verwachting vaak persoonsgegevens verwerken. De respons van deze enquête was niet erg groot. In totaal heeft 13 procent van de aangeschreven organisaties gereageerd. Daarbinnen is sprake van een oververtegenwoordiging van de zakelijke en financiële dienstverlening, de gezondheidszorg en de overheid. Ook hebben de grotere organisaties (> 100 werknemers) die we hebben aangeschreven beduidend vaker gereageerd dan de overige groepen. In paragraaf 4.2.1 wordt aan deze enquête en de respons daarop nader aandacht geschonken.

2. Meldingenenquête
De doelgroep van deze enquête waren bedrijven, instellingen en overheden die in de periode 2002 – 2007 aan het Cbp ten minste één melding hebben gedaan van het verwerken van persoonsgegevens. Uit deze groep is via het meldingenbestand van het Cbp een steekproef getrokken van organisaties die te maken hebben met het verwerken van persoonsgegevens. In totaal zijn 647 vragenlijsten verzonden. Daarvan is 25 procent geretourneerd. Verhoudingsgewijs hebben maatschappelijke instellingen (vooral op het terrein van de gezondheidszorg) en semi-overheden beter gereageerd op de enquête. Het bedrijfsleven heeft relatief veel minder vaak gereageerd. In paragraaf 4.2.2 wordt een nadere toelichting op de gegevensverzameling onder meldende organisaties gegeven.

3. Enquête FG's
Er zijn in Nederland 215 FG's aangewezen. Deze groep is op te vatten als een groep experts op het gebied van gegevensverwerking. Daarom zijn aan hen zowel feitelijke, normatieve als ontwikkelvragen worden gesteld. Het enquêteren van deze groep was van groot belang om te achterhalen hoe de werkwijze van de FG's is en onder welke omstandigheden zij hun werkzaamheden uitvoeren. De gegevens van de FG's zijn verkregen via het openbare register

op de website van het Cbp. We hebben 215 FG's aangeschreven. Daarvan heeft 34 procent gereageerd. FG's bij (semi-)overheidsorganisaties hebben relatief goed gereageerd.

De resultaten van deze enquêtes zijn verwerkt in hoofdstuk 4 en 5 van dit rapport. We moeten vaststellen dat de respons op de FG-enquête voldoende is. De respons op de meldingenenquête is in vergelijking daarmee aan de magere kant. De respons op de algemene enquête is onvoldoende. Dat brengt beperkingen met zich mee voor de wijze waarop de bevindingen uit het enquêteonderzoek kunnen worden veralgemeniseerd. Daarover wordt dan ook met enige terughoudendheid gerapporteerd. Daar staat tegenover dat de resultaten van de drie enquêtes – bij onderlinge vergelijking – een redelijk consistent beeld te zien geven. De drie groepen verschillen van elkaar waar het gaat om hun mate van betrokkenheid bij de wet. Bij de FG's is die het grootst, bij de organisaties die in de algemene enquête zijn bevraagd is die – gemiddeld genomen – het kleinst. Wannneer de bevindingen tegen die achtergrond worden bezien komt daaruit een duidelijk en consistent beeld naar voren. En hoewel niet bij elke enquête de respons bevredigend was, stelt nadere interpretatie van de bevindingen van het vragenlijstenonderzoek op basis van de interviews en de expertmeetings ons niettemin in staat tot het trekken van enkele algemene concluderende lijnen in het laatste hoofdstuk.

1.4.4 Interviews burgers

Wij zijn er vanuit gegaan dat de gemiddelde burger niet of nauwelijks over de Wbp geïnformeerd is. Om die reden is besloten om niet willekeurige burgers, maar betrokkenen die een geschil aanhangig hebben gemaakt, te enquêteren. Doordat zelfregulering niet sterk op gang is gekomen is het aantal geschillencommissies beperkt. In het enquêteonderzoek zijn burgers betrokken die een geschil aanhangig hebben gemaakt bij rechtbanken en het Cbp. Door betrokkenen met een geschil te ondervragen is het burgerperspectief in het onderzoek gebracht.

Dit 'burgeronderzoek' is langs telefonische weg uitgevoerd. Omdat de groep betrokkenen een diverse en moeilijk benaderbare groep respondenten is en het uitvoeren van kwantitatieve technieken daarom lastig uitvoerbaar zou zijn, is gekozen voor het voeren van verdiepende gesprekken met een wat kleinere groep betrokkenen. Interviews zijn gehouden met negen burgers (of hun rechtshulpverlener) die een geschil aanhangig hebben gemaakt bij de civiele rechter, de bestuursrechter en het Cbp. Uit de contacten die met acht geschillencommissies zijn gelegd kwamen geen bruikbare zaken voort die aan nader onderzoek zouden kunnen worden onderworpen. In hoofdstuk 6 wordt verslag gedaan van het onderzoek naar ervaringen met geschilbeslechting.

1.4.5 Casestudyonderzoek

Naast het kwantitatieve deel van het onderzoek was het noodzakelijk om kwalitatieve gegevens te verzamelen. Sommige vragen lieten zich moeilijk kwantitatief beantwoorden. Uit het knelpuntenonderzoek is gebleken dat problemen worden ervaren bij de gegevensuitwisseling in samenwerkingsverbanden. Wij hebben een tweetal casestudies uitgewerkt op beleidsterreinen in de publieke en semi-publieke sector waarbij sprake is van intensieve samenwerking: een veiligheidshuis waarin onder andere politie, justitie en hulpverleningsinstanties samenwerking met het oog op onder meer het voorkomen van strafbare feiten en het terugbrengen van overlast en een instelling voor geestelijke gezondheidszorg waarin verslavingszorg en GGZ samenwerken met het oog op het behandelen van dakloze verslaafden met psychiatrische stoornissen. Het casestudyonderzoek

bestond uit een dossieronderzoek en een interviewronde. In hoofdstuk 7 wordt van dit casestudyonderzoek verslag gedaan.

1.5 Interviewronde

Na het enquêteonderzoek en het casestudyonderzoek zijn verdiepende interviews gehouden met de voorzitter van het Cbp, juridische experts en een aantal privacyofficers van bedrijven. Daarnaast is een expertmeeting met FG's georganiseerd en een expertmeeting met vertegenwoordigers van organisaties die de belangen van burgers behartigen. Deze gesprekken zijn vooral gevoerd met als doelstelling het interpreteren van de onderzoeksbevindingen uit het enquêteonderzoek.

In bijlage 2 is aangegeven met welke personen gesprekken zijn gevoerd.

1.6 Leeswijzer

In het rapport dat voor u ligt zal allereerst in hoofdstuk 2 een korte toelichting worden gegeven op de totstandkoming van de Wbp en de kernbegrippen en –bepalingen van de Wbp. Vervolgens wordt in hoofdstuk 3 het theoretisch kader geschetst. Hierin worden veronderstellingen geformuleerd op grond waarvan verklaringen kunnen worden gegenereerd voor de knelpunten uit het onderzoek van Zwenne e.a.. In de hoofdstukken 4 en 5 worden de resultaten van het enquêteonderzoek uiteengezet en in de daarop volgende hoofdstukken 6 en 7 worden de bevindingen uit de diepte-interviews met burgers en de casestudies gepresenteerd. Hoofdstuk 8 bevat een slotbeschouwing waarin de onderzoeksbevindingen worden samengevat en antwoorden worden gegeven op de probleemstelling en de deelvragen.

Hoofdstuk 2 De Wet bescherming persoonsgegevens

2.1 Inleiding

In dit hoofdstuk wordt, naast een schets van de totstandkoming van de Wbp, een toelichting gegeven op de kernbegrippen en -bepalingen van de Wbp. Hiermee wordt inzichtelijk gemaakt wat het wettelijke kader van dit evaluatieonderzoek is.

De Wet bescherming persoonsgegevens (hierna: Wbp) is op 1 september 2001 in werking getreden.[38] Met de wet is de Richtlijn betreffende de bescherming van de natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens tot stand gekomen (hierna: Privacyrichtlijn) geïmplementeerd.[39]

Het doel van de Wbp is waarborgen te bieden waarmee een evenwicht tussen privacybescherming en andere grondrechten wordt bewerkstelligd. Daarnaast heeft de Wbp het doel de positie van de personen wiens gegevens worden verwerkt te versterken. Dit wordt gedaan door aan deze betrokkenen rechten toe te kennen (inzagerecht, correctierecht) en aan de andere kant plichten op te leggen aan verantwoordelijken (meldings- en informatieplicht). Als onafhankelijk toezichthouder op naleving van de Wbp is het Cbp aangewezen.[40]

2.2 Totstandkoming van de Wet bescherming persoonsgegevens

Door de komst van nieuwe technieken, waarmee grote hoeveelheden persoonsgegevens gemakkelijk konden worden opgeslagen en ontsloten, ontstond het besef dat hiervan misbruik zou kunnen worden gemaakt. Gegevens zijn een bron van informatie; informatie is de basis van kennis en kennis is macht.[41] Vóór de komst van deze nieuwe technieken vormden persoonsgegevens niet zelfstandig het voorwerp van regelgeving; verschillende onderdelen van het recht boden bescherming tegen aantasting van eer en goede naam en tegen inbreuken op de persoonlijke levenssfeer. Het ging hierbij om jurisprudentie inzake onrechtmatige daad bij ontoelaatbare publicaties over iemands persoon, strafbepalingen inzake belediging, smaad en laster, regelingen over archivering van overheidsdocumenten en de geheimhoudingsplicht van hulpverleners.[42] Met de komst van de informatiemaatschappij ontstond de behoefte een afzonderlijke regeling te treffen over de bescherming van persoonsgegevens.

De bescherming van de persoonlijke levenssfeer is sinds de herziening van de Grondwet van 1983 één van de klassieke grondrechten. In het eerste lid van artikel 10 van de Grondwet is bepaald dat iedereen recht heeft op eerbiediging van de persoonlijke levenssfeer. De grondwetgever geeft in het tweede lid opdracht aan de wetgever om regels te stellen in verband met het vastleggen en verstrekken van persoonsgegevens. Volgens het derde lid moet de wet regels stellen inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op de verbetering van zodanige gegevens.

---

[38] Wet bescherming persoonsgegevens, Stb. 2000, 302
[39] Richtlijn 95/46/EG, PbEG L 281, p. 0031-0050
[40] Zwenne e.a. 2007, p. 10
[41] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 7
[42] Idem, p. 6

Artikel 10 van de Grondwet sloot aan bij zich gelijktijdig ontwikkelende jurisprudentie van het Europese Hof voor de rechten van de mens over de omvang van het recht op respect voor het privé-leven van het individu, neergelegd in artikel 8 van het Europees Verdrag inzake de rechten van de mens en de fundamentele vrijheden (hierna: EVRM), in relatie tot de opslag en het gebruik van persoonsgegevens.[43] Volgens dit artikel heeft een ieder recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

Met de Wpr is uitvoering gegeven aan het tweede en derde lid van artikel 10 van de Grondwet. Deze wet[44] is op 1 juli 1989 in werking getreden. In 1995 zijn een juridische en een sociaal wetenschappelijke evaluatie van de Wpr verschenen.[45] Beide evaluaties hebben duidelijk gemaakt dat de Wpr slechts in beperkte mate de rechtsvorming in de omgang met persoonsgegevens heeft beïnvloed. Dit bleek onder meer uit het feit dat er weinig jurisprudentie over de Wpr was. Uitvoering van de administratieve voorschriften, zoals het inzenden van meldingsformulieren en het opstellen van reglementen, heeft veel energie gekost. Het doel achter deze voorschriften is hierbij enigszins uit zicht geraakt. Wel bleek dat de bescherming van persoonsgegevens als buitengewoon wenselijk wordt ervaren.[46]

Zoals gezegd is met de Wbp de Privacyrichtlijn geïmplementeerd, die op 24 oktober 1995 is vastgesteld.[47] Deze richtlijn is vastgesteld omdat bleek dat het vrije verkeer van persoonsgegevens werd belemmerd door de verschillen in de privacyregelgeving van de afzonderlijke lidstaten. Deze belemmeringen konden niet worden overwonnen met het Verdrag inzake gegevensbescherming van de Raad van Europa dat in 1981 tot stand is gekomen en sindsdien door alle landen binnen de Europese Unie (hierna: EU) is bekrachtigd.

De Wbp is niet zonder slag of stoot tot stand gekomen.[48] Onder andere de Consumentenbond, de vereniging VNO/NCW en het Rathenau Instituut hadden kritiek op het wetsvoorstel.[49] Na de kabinetswisseling in 1998 werd de behandeling van het wetsvoorstel in de Tweede Kamer eerst enige tijd opgeschort en vervolgens diende de nieuwe minister van Justitie een Nota van Wijziging in bij de Tweede Kamer. Omdat het met name ging om wijzigingen met betrekking tot de positie van de Registratiekamer, reageerde deze hier weer kritisch op. De Tweede Kamer gaf tijdens de plenaire behandeling aan dat de Wbp erg ingewikkeld was geworden, maar toch werd het voorstel met een ruime meerderheid aanvaard. Na een grote hoeveelheid schriftelijke vragen te hebben gesteld, is ook de Eerste Kamer uiteindelijk met algemene stemmen akkoord gegaan. Uiteindelijk is de Wbp op 20 juli 2000 gepubliceerd in het Staatsblad.[50] Na vaststelling van de zogenaamde Veegwet, waarbij naast de Wbp ook andere wettelijke regelingen moesten worden gewijzigd[51], is de Wbp op 1 september 2001 in werking getreden.

---

[43] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 7
[44] Staatsblad 1988, 655
[45] Overkleeft-Verburg 1995 en Prins e.a. 1995
[46] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 37
[47] Richtlijn 95/46/EG
[48] Prins en Berkvens 2002, p. 76
[49] De Consumentenbond en VNO/NCW waren van mening dat de wet doorsloeg. Zij wilden een versobering van het voorstel tot de hoofdlijnen van de richtlijn, waarna de details van de omgang met persoonsgegevens in gedragscodes geregeld konden worden. Het Rathenau Instituut vond dat de wet haar doel voorbij schoot. Volgens het Rathenau Instituut was het voorstel gericht op de bescherming van persoonsgegevens, terwijl de wet de burgers zou moeten beschermen tegen de effecten van de gegevensverwerkende praktijk.
[50] Staatsblad 2000, 302
[51] Staatsblad 2001, 180

2.3 Privacyrichtlijn

Onderdeel van de doelstelling van dit evaluatieonderzoek is na te gaan welke aanpassingen van de Wbp mogelijk en wenselijk zijn in het kader van de EU-richtlijn. Hierbij is derhalve van belang na te gaan welke ruimte de Privacyrichtlijn biedt voor wijzigingen. In 2006 is onderzoek gedaan naar de verschillen tussen de Privacyrichtlijn en de implementatie daarvan in de Wbp.[52].

Voorts is het van belang te weten wat de doelstellingen van de gemeenschapswetgever waren. In het knelpuntenonderzoek is onderzoek gedaan naar de doelstellingen van de gemeenschapswetgever. Door enerzijds een bijdrage te leveren aan de totstandbrenging en werking van de interne markt en anderzijds waarborgen te bieden voor de bescherming van fundamentele rechten en vrijheden, wil de Privacyrichtlijn bijdragen aan de algemene doelstellingen van de Gemeenschap. Door te kiezen voor een ruime werkingssfeer van de richtlijn, die met name ziet op geautomatiseerde verwerkingen, tracht de gemeenschapswetgever de marktbelemmeringen weg te nemen die kunnen voortvloeien uit de verschillen tussen nationale regelingen voor de verwerking van persoonsgegevens. Om te komen tot een gelijkwaardig beschermingsniveau wil de richtlijn door middel van harmonisatie van de nationale privacywetten van lidstaten ervoor zorgen dat in de verschillende lidstaten soortgelijke aanspraken en verplichtingen gelden ten aanzien van de bescherming van persoonsgegevens. Ook door de transparantie van gegevensverwerkingen te verbeteren en te voorzien in waarborgen voor betrokkenen, moet het hoge beschermingsniveau worden bereikt. De richtlijn wil ten slotte zoveel mogelijk rekening houden met de specifieke omstandigheden en behoeften van een sector of branche. Zo kan tegemoet gekomen worden aan de bijzonderheden van bepaalde categorieën van gegevens of verwerkingen. In dit kader voorziet de richtlijn in de mogelijkheid dat op branche- en sectorniveau gedragscodes worden opgesteld.[53]

2.4 De wet in hoofdlijnen

2.4.1 Algemene karakterisering

De Wbp bestaat uit verschillende onderdelen met elk een eigen karakter.[54] De wet verleent subjectieve rechten aan degenen van wie persoonsgegevens worden verwerkt. Daarnaast is de Wbp een organieke wet gericht op de vormgeving van een grondrecht. Ten slotte is van belang dat de Wbp zowel een civielrechtelijke als een bestuursrechtelijke component bevat. De memorie van toelichting geeft aan dat persoonsgegevens kunnen worden verwerkt na een zorgvuldige afweging van de belangen van de verantwoordelijke en de belanghebbende. Deze belangenafweging blijkt uit artikel 8 onder f van de Wbp. In artikel 8 staan de doeleinden voor rechtmatige verwerking limitatief opgesomd. De onderdelen b tot en met e zijn specifiek en f is een restbepaling. Hierin is een belangenafweging neergelegd; is de verwerking noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke en is de verwerking evenredig in verhouding tot het belang van de betrokkene?

[52] Cuijpers 2006
[53] Zwenne e.a. 2007, p. 9
[54] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 14

De wet bevat derhalve geen sluitend stelsel van concrete materiële normen over wat wel en niet is toegestaan.[55] Een uitzondering geldt voor bijzondere persoonsgegevens; deze gegevens mogen alleen worden verwerkt als de wet dat toestaat. De wetgever geeft in de toelichting aan dat de bepaling inzake de afweging van belangen in zoverre een kameleontisch karakter heeft dat de toets in rechte achteraf of een aanvaardbare afweging heeft plaatsgevonden zich kleurt naar gelang het gaat om een gegevensverwerking in de publieke, dan wel in de private sector. Als het gaat om gegevensverwerking in de publieke sector wordt getoetst of bij de afweging is voldaan aan de bestuursrechtelijke beginselen van behoorlijk bestuur. Bij de private sector wordt getoetst of is voldaan aan de zorgvuldigheid die volgens het ongeschreven recht in het maatschappelijk verkeer betaamt.[56]

2.4.2 Belangrijkste begrippen

De wet definieert in artikel 1 een aantal belangrijke begrippen. Een 'persoonsgegeven' is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1 onder a). Onder de 'verwerking van persoonsgegevens' wordt verstaan elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen etc. (art. 1, sub b, Wbp). 'Verantwoordelijke' is degene die zeggenschap heeft over doel en wijze van verwerking van de persoonsgegevens (art. 1, sub d, Wbp). Dat kan een natuurlijke persoon, een rechtspersoon of een bestuursorgaan zijn. Naast de 'verantwoordelijke' wordt in artikel 1, sub e, Wbp nog de 'bewerker' onderscheiden. Dat is degene die gegevens bewerkt ten behoeve van de verantwoordelijke zonder aan zijn rechtstreeks gezag te zijn onderworpen. 'Betrokkene' in de zin van de wet is degene op wie de gegevens betrekking hebben (art. 1, sub f, Wbp).

De Wbp onderscheidt een categorie van gevoelige gegevens, de zogenaamde bijzondere persoonsgegevens. Volgens artikel 16 van de wet gaat het hier om persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Voor verwerking van deze bijzondere persoonsgegevens geldt een stringenter regime. Het uitgangspunt is dat verwerking is verboden, tenzij een wettelijke verwerkingsgrond van toepassing is.

2.4.3 Wijzigingen ten opzichte van de Wpr

De Wbp is op een aantal punten gewijzigd ten opzichte van de Wpr. Deels vloeit dit voort uit de richtlijn, deels uit de beide evaluaties.[57]

Zo is, in verband met de vereiste transparantie, de informatieverplichting van de verantwoordelijke ten opzichte van de betrokkene aangescherpt. Onder de Wpr mocht de verantwoordelijke de informatieplicht achterwege laten als de betrokkene redelijkerwijs kon weten van de opname in een persoonsregistratie. Op grond van de Wbp moet de verantwoordelijke de betrokkene altijd op de hoogte stellen, tenzij deze al daadwerkelijk over de betreffende informatie beschikt. Verder is bepaald dat de verantwoordelijke de herkomst van de gegevens moet vastleggen als het voldoen aan de informatieplicht onmogelijk is of een onevenredige inspanning vereist.

[55] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 37
[56] Idem, p. 38
[57] Idem, p. 16

Om de transparantie ten opzichte van betrokkenen te vergroten, geldt naast de informatieplicht ook een meldingsplicht. Deze meldingsplicht is in de Wbp vereenvoudigd. De Wpr maakte onderscheid tussen de private en de publieke sector. Voor de private sector gold een meldingsplicht en voor de publieke en semi-publieke sector gold een reglementsplicht. Omdat uit de evaluaties bleek dat dit systeem niet goed functioneerde, is het onderscheid komen te vervallen. Over de gehele linie geldt nu de meldingsplicht. Daarnaast hoeven handmatige verwerkingen niet te worden gemeld en is een vrijstellingsbesluit vastgesteld.

Net als de Wpr kent de Wbp een abstract normenkader dat door middel van sectorale wetgeving of zelfregulering verdere invulling moet krijgen. Bij de zelfregulering kan allereerst worden gedacht aan het opstellen van een gedragscode. In artikel 25 van de Wbp wordt organisaties hiertoe de mogelijkheid geboden. Het achterliggende idee is dat door de vaststelling van een gedragscode de algemene normen voor een betrokken sector kunnen worden geconcretiseerd. Ook onder de werking van de Wpr bestond de mogelijkheid gedragscodes op te stellen. In de juridische evaluatie is uitvoerig aandacht geschonken aan dit instrument. Hoewel er een aantal problemen is aangewezen, is het algemene oordeel over gedragscodes echter positief.[58] De regeling van de gedragscode is dan ook hoofdzakelijk ongewijzigd overgenomen in de Wbp.

De wetgever is van mening dat de meldingsplicht een bijdrage levert aan zelfregulering. Volgens de wetgever heeft de meldingsplicht naast het bieden van transparantie tot doel de verantwoordelijke te prikkelen om zich rekenschap te geven van de doeleinden waarvoor hij persoonsgegevens wil verwerken en verslag te doen van de overwegingen welke persoonsgegevens noodzakelijk zijn voor het bereiken van het doel en van het gebruik van de gegevens in verband met dat doel.[59]

Verder is het ook onder de Wbp nog mogelijk in reglementen vast te leggen hoe binnen de organisatie met de verwerking van persoonsgegevens wordt omgegaan. Tot slot zal een deel van de concretisering volgens de wetgever plaats moeten hebben in de jurisprudentie.[60]

Net als in de Wpr zijn in de Wbp rechten voor betrokkenen vastgelegd. Nieuw in de Wbp is dat de betrokkene op grond van artikel 40 van de Wbp het recht van verzet toekomt bij een gegevensverwerking op grond van artikel 8 onder e en f van de Wbp. Een verantwoordelijke kan na een afweging van belangen tot de conclusie komen dat de gegevensverwerking gerechtvaardigd is. Het is echter mogelijk dat de bijzondere persoonlijke omstandigheden van een bij de verwerking betrokkene de balans doen doorslaan naar de andere kant.[61] Een rechtmatige gegevensverwerking kan na verzet derhalve onrechtmatig worden geacht.

Ook ten aanzien van het toezicht heeft zich een aantal wijzigingen voorgedaan. In de volgende subparagrafen wordt ingegaan op de toezichthouders, het Cbp en de FG.

[58] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 37
[59] Idem, p. 140
[60] Idem, p. 6
[61] Idem, p. 163

2.4.4 Het Cbp

Door de wetgever is het Cbp aangewezen als toezichthoudend orgaan voor de Wbp (artikel 51 Wbp). Onder de Wpr was de Registratiekamer met het toezicht belast.

De positie van het Cbp is in een aantal opzichten gewijzigd ten opzichte van die van de Registratiekamer. Allereerst heeft het Cbp als rechtshandhavende instantie de beschikking gekregen over een aantal bevoegdheden waarmee ze daadwerkelijk in een proces van gegevensverwerking kan ingrijpen. Gewezen kan worden op met name de bevoegdheden geregeld in hoofdstuk 10 van de Wbp (bestuursdwang en dwangsom). Daarmee werd de toezichthoudende functie van het Cbp uitgebreid in die zin dat waar het Cbp onrechtmatig gedrag constateert, deze constatering kan leiden tot een rechtens afdwingbare beslissing van het Cbp. Aan de andere kant wordt ook de rechtspositie van de verantwoordelijke versterkt omdat deze, anders dan onder de Wpr, de beslissing van het Cbp in rechte kan aanvechten.[62]

In het kader van haar uitvoerende taken kan het Cbp onder bepaalde omstandigheden goedkeuren dat gevoelige gegevens in aanvulling op het wettelijk regime worden verwerkt (artikel 23, eerste lid, onder e). Verder bevat artikel 77, tweede lid, de bevoegdheid middels de afgifte van een vergunning de doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt, mogelijk te maken. Voorts heeft hij bij bepaalde gegevensverwerkingen met bijzondere risico's de bevoegdheid voorafgaand onderzoek te doen, beoordeelt hij gedragscodes en houdt hij een openbaar register van binnengekomen meldingen. Ook voor de uitoefening van deze uitvoerende taken geldt dat de rechtsbescherming tegen handelingen van het Cbp is versterkt.[63]

De toezichthoudende taak van het Cbp betreft niet alleen de Wbp, maar strekt zich ook uit tot andere wetten, algemene maatregelen van bestuur en andere wettelijke regelingen op grond waarvan persoonsgegevens worden verwerkt.[64] Naast een toezichthoudende taak, heeft het Cbp ook een adviserende taak. De regering is verplicht het Cbp om advies te vragen over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens.[65]

Uitgaande van de verticale werking van het grondrecht op bescherming van de persoonlijke levenssfeer richten de bevoegdheden van het Cbp zich mede tot de gegevensverwerkingen binnen de overheidssector. Om deze reden is een onafhankelijke positie van het Cbp ten opzichte van de overheid vereist. Het Cbp moet bijvoorbeeld in zijn toezichthoudende en handhavende taak volledig vrij zijn in de prioriteitstelling, in het bepalen welke gegevensverwerkingen zijns inziens nader onderzocht moeten worden en in welke gevallen daadwerkelijk moet worden ingegrepen wegens vermeende onrechtmatigheid. Net als de Registratiekamer is op basis van het voorgaande aan het Cbp de vorm gegeven van een zelfstandig bestuursorgaan, zijnde een bestuursorgaan op het niveau van de centrale overheid dat hiërarchisch niet ondergeschikt is aan een minister.[66]

[62] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 27
[63] Idem, p. 27
[64] Idem, p. 177
[65] Idem, p. 178
[66] Idem, p. 27

Wel beschikt de Minister van Justitie over een minimumpakket aan noodzakelijke ministeriële bevoegdheden. In de Wbp zijn de volgende bevoegdheden voor de minister opgenomen:

- een algemeen inlichtingenrecht van de Minister (artikel 59, eerste lid);
- goedkeuring van het bestuursreglement (artikel 56, vierde lid);
- een bevoegdheid om beleidsregels te stellen met betrekking tot de door het Cbp op te leggen bestuurlijke boete (artikel 74);
- regeling van de rechtspositie van de leden van het Cbp bij algemene maatregel van bestuur (artikel 55);
- benoeming van de leden van het CBbp (artikelen 53 en 54).[67]

De Wet openbaarheid van bestuur (hierna: Wob) en de Wet Nationale ombudsman (hierna: WNo) zijn op het Cbp van toepassing.[68]

Zoals op elk bestuursorgaan, zijn ook op het handelen van het Cbp de algemene beginselen van behoorlijk bestuur, waaronder het zorgvuldigheidsbeginsel, van toepassing. Dit houdt onder meer in dat in voorkomend geval het college het beginsel van hoor en wederhoor toepast.[69]

Op grond van artikel 58 van de Wbp moet het Cbp jaarlijks een verslag opstellen van de werkzaamheden, het gevoerde beleid in het algemeen en de doelmatigheid en doeltreffendheid van zijn werkwijze in het bijzonder.

2.4.5 De Functionaris voor de Gegevensbescherming

Ook geheel nieuw ten opzichte van de Wpr is de mogelijkheid van de verantwoordelijke om een interne toezichthouder, een FG, aan te stellen.

De constructie van het aanstellen van een interne toezichthouder is afkomstig uit het Duitse recht.[70] In Duitsland is het in de particuliere sector gebruikelijk dat bij bedrijven boven een bepaalde omvang het toezicht op de verwerking van persoonsgegevens plaatsvindt door een toezichthouder binnen het bedrijf. Deze bedrijven zijn in principe uitgezonderd van een meldingsplicht.[71]

Een FG is een onafhankelijke interne toezichthouder. Van het aanstellen van een FG moet melding worden gedaan aan het Cbp, die een openbaar register bijhoudt van FG's (artikel 63 lid 3 van de Wbp). De verantwoordelijke moet er zorg voor dragen dat de FG over gelijkwaardige bevoegdheden bezit als de toezichthouder in de zin van afdeling 5.2 van de Algemene wet bestuursrecht. Het gaat hier onder andere om de bevoegdheid ruimtes te betreden en inlichtingen en inzage te vragen. Tot de taken van de FG behoren het bijhouden van een register van de gegevensverwerkingen (artikel 30 Wbp) en het opstellen van een jaarverslag (artikel 62 Wbp). De FG kan aanbevelingen doen aan verantwoordelijke die strekken tot een betere bescherming van de gegevens die worden verwerkt (art. 64 Wbp).

In de Wbp wordt een aantal inhoudelijke eisen gesteld waaraan de FG moet voldoen (artikel 63 Wbp). Allereerst moet de FG over toereikende kennis beschikken. Hieronder wordt

[67] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 27 en 28
[68] Artikel 1 Besluit bestuursorganen WNo en Wob (Stb. 1998, 580)
[69] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 28
[70] Idem, p. 28
[71] Hooghiemstra en Nouwt 2007, p. 203

verstaan kennis van de organisatie, de gegevensverwerkingen die zich binnen de organisatie afspelen, de belangen die daarbij betrokken zijn en uiteraard kennis van de privacywetgeving die op de verwerkingen binnen zijn organisatie van toepassing is. Ook moet hij voldoende betrouwbaar worden geacht. Deze betrouwbaarheid uit zich bijvoorbeeld in het vermogen alle bij de verwerkingen betrokken belangen op een onafhankelijke wijze tegen elkaar te kunnen afwegen. De functionaris moet in staat zijn op een juiste en zorgvuldige wijze gebruik te maken van zijn bevoegdheden zoals geregeld in afdeling 5.2 van de Algemene wet bestuursrecht.[72]

In artikel 62 van de Wbp is bepaald dat de benoeming van een FG de toezichthoudende bevoegdheden van het Cbp onverlet laat. In de memorie van toelichting wordt hierover opgemerkt dat de FG het Cbp slechts vervangt voor wat betreft de meldingen van de meldingsplichtige gegevensverwerkingen. [73] Desalniettemin geeft het Cbp in een informatieblad aan terug te treden als eerstelijns toezichthouder als de verantwoordelijke een FG aanstelt.[74]

2.4.6 Voorwaarden rechtmatige verwerking

In het tweede hoofdstuk van de Wbp zijn de voorwaarden aangegeven waaronder de verwerking van persoonsgegevens rechtmatig is. Vanuit het gezichtspunt van de verantwoordelijke kunnen een aantal stappen worden onderscheiden om te bepalen of gegevensverwerking is toegestaan. [75] De basisvoorwaarde is dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt (artikel 6). Vervolgens moet worden gekeken naar het doelbindingsprincipe van artikel 7. In dit artikel is bepaald dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Op basis van dit principe moet voorafgaand aan de gegevensverzameling een duidelijke omschrijving worden gegeven van het doel. Het doel mag niet zo vaag of ruim zijn dat het geen toetsingskader biedt en hoofd- en nevendoelen moeten met elkaar verenigbaar zijn. Het derde element van artikel 7, persoonsgegevens worden verzameld voor 'gerechtvaardigde doeleinden', is uitgewerkt in artikel 8. In dit artikel is een limitatieve opsomming gegeven van de gronden die een gegevensverwerking rechtvaardigen. Elke gegevensverwerking moet herleidbaar zijn tot ten minste één van de in artikel 8 opgesomde gronden. Als sprake is van bijzondere persoonsgegevens, is bovendien het strengere regime van de tweede paragraaf van hoofdstuk 2 van toepassing (de artikelen 16 tot en met 23). Als na het doorlopen van de hiervoor genoemde stappen vaststaat dat de gegevensverwerking toelaatbaar is, dan moet vervolgens worden bepaald of voldaan wordt aan de eisen met betrekking tot de wijze waarop de gegevens mogen worden gebruikt. In artikel 9 is bepaald dat gegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Getoetst moet worden of het gebruik voor andere doeleinden verenigbaar is met het doel waarvoor de gegevens zijn verkregen. Het begrip 'verenigbaar gebruik' is niet afgebakend in de richtlijn. In de Wbp wordt de verantwoordelijke een aantal handvatten geboden; er is een niet-limitatieve opsomming gegeven van factoren die de verantwoordelijke bij zijn afweging in elk geval dient te betrekken. Artikel 11 heeft vervolgens betrekking op de inhoudelijke kwaliteit van de gegevens: gegevens moeten toereikend, relevant, niet bovenmatig en juist en nauwkeurig zijn. In de artikelen 12, 13 en 14 zijn vervolgens

[72] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 184
[73] TK 1997-1998, 25 892, nr. 3, p. 184 en 185
[74] Cbp 2004
[75] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 22

bepalingen opgenomen over de beveiliging van de gegevens. Ten slotte geldt op grond van artikel 10 dat de persoonsgegevens niet langer dan noodzakelijk voor de verwerkingsdoeleinden mogen worden bewaard.

In dit hoofdstuk is het wettelijke kader van het onderzoek geduid. In het volgende hoofdstuk wordt het beschrijvingskader geschetst.

Hoofdstuk 3 Beschrijvingskader

3.1 Inleiding

De evaluatie van de werking van de Wbp in de praktijk is in belangrijke mate gestuurd door de bevindingen van het knelpuntenonderzoek dat in 2007 werd afgerond. Dat onderzoek betrof een literatuurstudie en een inventarisatie van de knelpunten bij de uitvoering en toepassing van de Wbp op basis van interviews. De uitkomsten van het knelpuntenonderzoek zijn gebruikt als bouwstenen voor het empirische evaluatieonderzoek. Daarbij is gekozen voor het groeperen van de knelpunten in een drietal categorieën, normeren, informeren en toezicht en rechtsbescherming. In dit hoofdstuk gaan we nader op deze categorieën in, waarbij we literatuur bespreken die in het knelpuntenonderzoek niet of in mindere mate aan bod is gekomen. Dit hoofdstuk bevat naast informatie uit diverse wetenschappelijke onderzoeken ook uitkomsten van opinieonderzoeken en feitelijke constateringen en reflecteert op de motieven voor het opstellen van de Wbp. Daarmee wordt in dit hoofdstuk de context beschreven waarbinnen de wet gelding moet krijgen.

3.2 Normeren

3.2.1 Open normen

Omnibuswet
Met de Wbp is gekozen voor een omnibuswet, een algemene wet die op alle maatschappelijke sectoren gelijkelijk van toepassing is, in plaats van meer specifieke wetgeving voor verschillende sectoren en verwerkingen.

Open normen, zoals die zijn opgenomen in de Wbp, hebben voor- en nadelen. In dit onderzoek wordt daarom onderzocht welke voor- en nadelen open normen in het algemeen hebben en welke er specifiek met betrekking tot de Wbp bestaan. Ook de werkbaarheid van open normen komt aan de orde.

In het knelpuntenonderzoek is geconstateerd dat het begrippenapparaat van de Wbp moeilijk hanteerbaar blijkt in de praktijk, zowel door het gebruik van algemeen en technologie-onafhankelijk bedoelde begrippen als door de aansluiting tussen de Wbp en andere sectorale en bijzondere wetgeving.[76] Bij de analyse van knelpunten komt het beeld naar voren dat het opgestelde begrippenapparaat onvoldoende houvast biedt in concrete situaties, uiteenlopende mogelijkheden tot interpretatie biedt die ten dele onbenut worden gelaten en in sommige gevallen tendeert naar overregulering door overlap met sectorale regelgeving.[77] Volgens verschillende auteurs is de Wbp onpraktisch omdat deze ervan uitgaat dat élke verwerking aan de normen van de Wbp getoetst wordt, en omdat die normen te vaag zijn.[78]

Deze vaagheid heeft betrekking op vrijwel alle belangrijke normen uit de wet. Het gaat dan bijvoorbeeld om de bepaling dat persoonsgegevens op ‘behoorlijke en zorgvuldige wijze’

[76] Zwenne e.a. 2007, p. 167
[77] Idem, p. 169
[78] Idem, p. 74

moeten worden verwerkt (artikel 6) en de bepaling dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld (het zogenaamde doelbindingsbeginsel van artikel 7). Ook de betekenis van begrippen als 'toestemming' (art. 8, sub a, van de Wbp) en 'gerechtvaardigd belang' (art. 8, sub f, van de Wbp) zijn lastig bepaalbaar.

De door auteurs aangedragen oplossingen ten aanzien van de onduidelijkheid en onbepaaldheid van de wettelijke begrippen lopen uiteen van een terughoudende interpretatie en een verstandige flexibele toepassing tot een vergaande heroverweging van de wijze van regulering.[79] De personen die in kader van dit onderzoek zijn geïnterviewd, zijn overwegend van mening dat het onderwerp privacy niet anders kan worden geregeld dan met open normen.[80] Open normen hebben immers niet alleen nadelen maar ook voordelen. Open normen staan een meer individuele beoordeling toe. Casusspecifieke omstandigheden kunnen bijvoorbeeld worden betrokken. Ook kunnen onvoorziene situaties eenvoudiger onder een bepaalde norm worden geschaard. Theoretisch zouden open normen ook tot een grotere rechtsontwikkeling moeten leiden.

Regeldruk
De openheid van een norm kan invloed hebben op de administratieve lasten die gepaard gaan met naleving van die norm. Over de vraag of open normen zorgen voor minder regeldruk zijn verschillende publicaties verschenen, waarvan hier twee worden besproken.

In 2005 is in het kader van het programma Bruikbare rechtsorde door de Universiteit Twente onderzoek gedaan naar open normen en regeldruk.[81] Hoewel in dit onderzoek open normen op het gebied van de kwaliteitszorg in de gezondheidszorg, het hoger onderwijs en de bedrijfsinterne milieuzorg centraal staan, worden er enkele interessante conclusies getrokken die ook relevant kunnen zijn voor het onderhavige onderzoek.[82] In het onderzoek wordt onderscheid gemaakt tussen materiële en immateriële regeldruk. Bij materiële regeldruk gaat het om de kosten die moeten worden gemaakt als gevolg van de verplichting tot naleving van een open norm. De naleving van een open norm kan ook immateriële regeldruk veroorzaken. Hieronder wordt verstaan de last of irritatie die normadressaten bij de naleving ervaren.[83]

Verder blijkt er een sterk verband te bestaan tussen de bruikbaarheid van het normenstelsel en de immateriële regeldruk. Als de normen als bruikbaar worden ervaren en als zij aansluiten bij de doelen en belangen van de organisatie, ontstaat weinig regeldruk. Andersom neemt de regeldruk toe als men in de praktijk de normen weinig nuttig vindt. Uit dit evaluatieonderzoek moet blijken of de open normen in de Wbp als nuttig worden ervaren. Als dit in mindere mate het geval is, kan dit een verklaring zijn voor de kritiek op de open normen in de Wbp.

Van belang voor de regeldruk zijn ook de stijlen van toezicht, handhaving en beoordeling. Naast stringente en repressieve handelwijzen wekken ook gebrek aan feedback en deskundigheid, belerend gedrag en als te soepel ervaren handelwijzen veel ergernis. Bij deze irritaties speelt een grote rol dat de normadressaten teleurgesteld zijn dat de toezichthouder of certificeerder geen oog heeft voor de grote inspanningen die men in de uitvoering heeft verricht. Open en informele communicatie vermindert de irritaties. Dit zou een rol kunnen

[79] Zwenne e.a. 2007, p. 65
[80] In bijlage 2 is aangegeven welke personen zijn geïnterviewd
[81] Dorbeck-Jung e.a. 2005
[82] Idem, p. 64-67
[83] Idem, p. 11

spelen bij de meldingsplicht. Het Cbp voert naar aanleiding van de ingekomen meldingen een globale toets uit op de juistheid van de melding. Het hebben voldaan aan de meldingsplicht is dan ook geen garantie dat de gegevensverwerking rechtmatig plaatsvindt. Wellicht dat verantwoordelijken zich afvragen waarom gemeld moet worden als het Cbp vervolgens nauwelijks naar de melding kijkt.

Ten slotte wordt in het Twentse onderzoek geconcludeerd dat open normen in het veld worden gewaardeerd en in de regel niet tot een toename van formele geschillen en meningsverschillen leiden. Een wettelijk kader dat de zelfregulering structureert, wordt gewaardeerd omdat het rechtszekerheid biedt ten aanzien van de verantwoordelijkheden en de bevoegdheden van de betrokken partijen. Een toename van geschillen kan worden verwacht, als de beslissing van een beoordelaar of toezichthouder van essentieel belang is voor de bekostiging van de activiteiten van de normadressaat. De open normen in de Wbp zouden dus als voordeel kunnen hebben dat er minder formele geschillen ontstaan.

Volgens Westerman wordt regeldruk niet veroorzaakt doordat er teveel regels zijn, maar doordat regels van de verkeerde soort worden gebruikt.[84] Westerman geeft aan dat er veelal gebruik wordt gemaakt van resultaatsnormen en doelvoorschriften. Onder resultaatsnormen worden verstaan regels die niet een handeling voorschrijven maar tot een bepaald resultaat verplichten. Een voorbeeld hiervan is de bepaling die voorschrijft dat de ondergrond van speeltoestellen op gemeentelijke speelplaatsen moet bestaan uit rubberen tegels van 60x60 cm.[85] Omdat het gebruik van resultaatsnormen heeft geleid tot een enorme hoeveelheid regels die bovendien een zeer hoog niveau van precisie en detaillering kennen, is de trend nu om deze regels te vervangen door doelvoorschriften. Deze voorschriften schrijven direct het doel voor dat door de wetgever als nastrevenswaardig wordt beschouwd. De resultaatsnorm met betrekking tot rubberen tegels wordt vervangen door de bepaling dat speelplaatsen veilig moeten zijn.

Er kunnen verschillende doelvoorschriften worden onderscheiden. Allereerst zijn er de optimaliseringsplichten; voorschriften die oproepen een bepaald doel zo dicht mogelijk te benaderen. Vervolgens zijn er doelvoorschriften die oproepen om een bepaald nastrevenswaardig doel te bevorderen of om iets zorgvuldig, veilig of verantwoord te verrichten. Het gaat hierbij bijvoorbeeld om zorgplichten. Ten slotte zijn er doelvoorschriften die niet deregulering ten doel hebben, maar worden toegevoegd aan bestaande resultaatsnormen om te voorkomen dat de normadressaat zich te gemakkelijk kan beroepen op gaten in de wet.

Volgens Westerman leiden al deze doelvoorschriften niet tot deregulering, aangezien ze uiteindelijk specificatie behoeven. Deze specificatie vloeit voort uit het feit dat de gebruikte termen onduidelijk en de gehanteerde positieve normen vaag zijn. Doordat de concretisering van de doelvoorschriften niet door de wetgever zelf ter hand wordt genomen, maar aan de doelgroepen wordt overgelaten, zal de samenhang tussen de regels ontbreken en zullen de regels soms zelf tegenstrijdig zijn. Uit het knelpuntenonderzoek is gebleken dat er problemen worden ervaren bij de gegevensuitwisseling in samenwerkingsverbanden onder andere door de samenloop van de Wbp met andere privacywetten.

Westerman vindt dat er een keuze moet worden gemaakt. Als deregulering van het hoogste belang wordt geacht, moet de wetgever zich weer gaan beperken tot het stellen van grenzen

[84] Westerman 2006
[85] Idem

en marges, tot het bepalen van wat niet mag in plaats van wat wel moet. Aangezien de hele maatschappij inmiddels doel- en resultaatsgericht denkt en werkt, zal het niet eenvoudig zijn deze omslag te bewerkstelligen. Als de wetgever van mening is dat het van het grootste belang is om te streven naar een bepaald doel, dan moet de grote hoeveelheid specificerende regels volgens Westerman op de koop toe worden genomen. In dat geval moet ook aandacht worden besteed aan de prioritering van de diverse doelstellingen die worden nagestreefd om tegenstrijdigheden te voorkomen.

Uit het voorgaande kan worden afgeleid dat een nadeel van doelvoorschriften die in open normen zijn opgenomen, is dat deze in praktijk niet tot deregulering leiden. Een ander nadeel is dat open normen tot gevolg hebben dat doelgroepen zelf regels zullen stellen, waardoor de samenhang tussen regels kan ontbreken. Uit de redenering van Westerman kan echter ook worden afgeleid dat een regelarme samenleving een illusie is. Administratieve lasten kunnen laag zijn als de sector zelf regels opstelt. Uit een onderzoek onder stralingsdeskundigen blijkt tevens dat wanneer regels nauwelijks omstreden zijn en de weerstand van de gebruikers tegen de regels laag is, de regeltoepassing en –handhaving wordt vergemakkelijkt.[86]

3.2.2 Zelfregulering

De wetgever acht zelfregulering gewenst om de open normen van de Wbp te concretiseren. Bij zelfregulering kan worden gedacht aan het opstellen van gedragscodes en het aanstellen van een FG. De vraag is of op het gebied van gegevensbescherming wordt overgegaan tot zelfregulering en wanneer dat niet het geval is, waarom die zelfregulering niet van de grond komt. In dit onderzoek wordt tevens aandacht geschonken aan de rol die het Cbp daarbij speelt.

Een organisatie kan een gedragscode opstellen waarin de wettelijke regels voor een bepaalde sector worden gepreciseerd (artikel 25 Wbp). Alvorens de gedragscode vast te stellen, kan de organisatie aan het Cbp vragen te beoordelen of de code voldoet aan de wettelijke vereisten. Uit het knelpuntenonderzoek blijkt dat bij het opstellen van gedragscodes moeilijkheden worden ondervonden. De invloed die het Cbp heeft op grond van zijn goedkeuringsbevoegdheid blijkt een knelpunt te zijn.[87] Het opstellen van gedragscodes wordt daarnaast als een langdurig, tijdrovend en kostbaar proces ervaren waar weinig concrete voordelen tegenover staan.[88] Een gevolg is dat er momenteel minder dan tien gedragscodes zijn goedgekeurd door het Cbp.[89] Wel hebben sommige overheidsinstellingen beleidsregels vastgesteld. De SVB heeft bijvoorbeeld beleidsregels vastgesteld over de omgang met persoonsgegevens. Tegelijkertijd heeft het SVB er echter van afgezien deze te laten goedkeuren door het Cbp als gedragscode.[90]

Een tweede manier om tot zelfregulering te komen is door het aanstellen van een FG, een interne toezichthouder. In het vorige hoofdstuk is aangegeven dat het Cbp terugtreedt als eerstelijns toezichthouder als de verantwoordelijke een FG aanstelt.[91] Als het Cbp zich

[86] Arentsen, p.372
[87] Zwenne e.a. 2007, p. 79 en Holvast 2005, p. 114-119
[88] Cuijpers 2006
[89] Ze zijn te vinden op www.cbpweb.nl.
[90] Mondelinge mededeling prof. dr. G. Vonk, voormalig hoofd juridische zaken SVB
[91] Cbp 2004

inderdaad beperkt tot toezicht op toezicht zou er sprake kunnen zijn van lagere administratieve lasten.[92] In paragraaf 3.4.2 wordt nader ingegaan op de FG.

De conclusie uit het knelpuntenonderzoek is dat zelfregulering in de zin van de Wbp moeizaam van de grond komt. Op het terrein van de milieuzorg heeft zich een vergelijkbare ontwikkeling voorgedaan. Ook daar gelden open normen zoals het voorzorgprincipe en ook daar bleek zelfregulering niet vanzelf tot stand te komen. Dat leidde er toe dat uiteindelijk de nationale overheid een sterk stimulerende rol ging spelen, onder meer door middel van subsidieprogramma's zoals het Bijdragenbesluit uitvoering gemeentelijk milieubeleid.[93]

Uit het onderzoek van de Universiteit Twente blijkt dat zelfreguleringsruimte een essentiële voorwaarde is voor vermindering van de immateriële regeldruk. De materiële regeldruk kan als gevolg van veel ruimte voor zelfregulering echter toenemen. Als er sprake is van een prikkel om op basis van de open norm tot zelfregulering over te gaan, dan zullen deze zelfreguleringsactiviteiten onvermijdelijk gepaard gaan met nalevingskosten. Het vaststellen van de precieze omvang van de nalevingskosten blijkt gecompliceerd te zijn door de vervlechting van de primaire processen en de processen van kwaliteitszorg. In de volgende paragraaf wordt nader ingegaan op zelfregulering. Uit het knelpuntenonderzoek blijkt dat nauwelijks zelfreguleringsactiviteiten worden ondernomen, ook omdat er weinig concrete voordelen tegenover staan. Uit dit onderzoek moet blijken of de materiële regeldruk van de Wbp tot nu toe beperkt is omdat niet tot zelfregulering is overgegaan.

Ook toont het Twentse onderzoek aan dat zelfreguleringsactiviteiten meerwaarde hebben voor de normadressaten. Normadressaten ervaren als baten van zelfregulering een betere aansluiting bij de doelen en belangen van de eigen organisatie of van de sector, een grotere transparantie van processen en activiteiten in de organisatie, een verbetering van het imago en een toename van de legitimiteit van het handelen van de organisatie. In dit onderzoek moet onder meer worden nagegaan of normadressaten dergelijke baten ook verwachten en ervaren als zij over gaan tot zelfregulering op basis van de Wbp. Uit het Twentse onderzoek blijkt voorts dat zelfreguleringsactiviteiten van brancheorganisaties in de regel de acceptatie van het normenstelsel bevorderen. Onder bepaalde omstandigheden roepen de activiteiten van een brancheorganisatie echter irritaties op. Er ontstaat ergernis over zelfreguleringsnormen van de brancheorganisaties, als deze zeer gedetailleerd zijn of als de brancheorganisatie geen ondersteuning biedt bij het implementeren van de normen. Het is denkbaar dat daarin de mogelijkheid voor een stimulerende rol van het Wbp ligt.

3.2.3 Technologische ontwikkelingen

Gelet op de snelle informatietechnologische ontwikkelingen is in de Wbp een evaluatiebepaling opgenomen. Volgens de wetgever zal bezien moeten worden of bepalingen wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer ontoereikend garanderen.[94] In de onderzoeksopzet van dit onderzoek naar de werking van de wet is daarom een vraag opgenomen over de verhouding tussen open normen en technologische ontwikkelingen.

[92] Dorbeck-Jung e.a. 2005, p. 105
[93] C. Lambers, *De ontbrekende schakel in het milieurecht: het tekort aan normen in de Wet milieubeheer*, Deventer, Kluwer: 1994
[94] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 197

In de memorie van toelichting bij de Wbp is aangegeven dat wordt gestreefd naar zo technologieonafhankelijk mogelijke regelgeving.[95] Om deze reden is ook gekozen voor open normering. Uit het knelpuntenonderzoek blijkt dat de technologische ontwikkelingen toch knelpunten opleveren. Zo blijkt het begrippenapparaat in de wet met name niet te zijn opgewassen tegen de ontwikkelingen op het Internet.[96] Het is vaak lastig te bepalen wie aangemerkt moet worden als 'verantwoordelijke' en welke verwerkingen van persoonsgegevens, gegevens betreffende geïdentificeerde of te identificeren natuurlijke personen, meldingsplichtig zijn.[97] Zo blijkt men bij de toepassing van biometrie tegen de grenzen van de toepassing van de Wbp aan te lopen. Verder brengt de toepassing van RFID-technologie nieuwe privacyvraagstukken met zich mee.[98] Door het gebruik van chips met Radio Frequency Identifier kunnen overheden, winkels en anderen aan grote hoeveelheden – soms gevoelige – gegevens komen, zonder dat de burger hiervan op de hoogte is.

In december 2007 heeft het Cbp een publicatie uitgebracht over de Wbp en Internet. Het doel van deze publicatie is duidelijkheid te verschaffen over het toepassen van de open normen in de Wbp in een Internetomgeving.

Technologische ontwikkelingen hebben niet alleen negatieve effecten op de privacy. Zo kan gebruik worden gemaakt van Privacy Enhancing Technologies (PET). De term Privacy Enhancing Technologies (PET) wordt gehanteerd om alle ICT-middelen aan te duiden die gebruikt kunnen worden om persoonsgegevens te beschermen. Dit begrip omvat mede de inrichting van de architectuur van informatiesystemen. Met PET wordt het vertrouwen van de burger vergroot en kan nieuwe technologie door de overheid worden aangewend om de service aan de burger te verbreden, te verdiepen en te verbeteren.[99] Een voorbeeld van PET zijn slimme beveiligingscamera's die pas beelden opnemen zodra ergens door de camera een opstootje wordt gesignaleerd. PET is een manier om invulling te geven aan de norm dat 'de gegevens die worden verzameld of vervolgens worden verwerkt toereikend, ter zake dienend en niet bovenmatig zijn' (art. 11, lid 1, Wbp). Daarnaast kan software worden gebruikt voor de beveiliging van bestanden. Volgens art. 13 Wbp legt de verantwoordelijke 'passende technologische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen (…).' De beveiliging dient in overeenstemming te zijn met de 'stand der techniek'. Beveiligingssoftware kan daarbij behulpzaam zijn, maar is cumulatief ten opzichte van organisatorische beveiliging (zoals fysieke afscherming).[100] Welke technologische en organisatorische maatregelen 'passend' zijn, zal overigens van geval tot geval moeten worden afgewogen. Ook hier blijft de normering vaag omwille van de technologische ongevoeligheid van de wet.

Nog een ander aspect van technologische ontwikkelingen is dat het Internet de burger de middelen verschaft om zelf drukker, uitgever en distributeur van informatie te zijn. Alberdingk Thijm stelt vast dat informatie in de fysieke wereld overwegend op een bepaald centraal niveau ontsloten wordt door commerciële centrale schakels zoals uitgeverijen en producenten. Dit zijn veelal vindbare en controleerbare schakels. Het Internet werkt anders. Daar worden handelingen decentraal verricht, in de beslotenheid van de woning. De mate waarin deze nieuwe actoren hun rol kunnen spelen is omgekeerd evenredig aan de mate

[95] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 41
[96] Zwenne e.a. 2007, p. 96
[97] Idem, p. 101
[98] Idem, p. 116
[99] Koorn e.a. 2004, p. 5
[100] Hooghiemstra en Nouwt 2004, p. 91 en 92

waarin zij gedwongen kunnen worden hun activiteiten te beëindigen.[101] Dit leidt ertoe dat burgers niet alleen slachtoffer van privacyschending zijn, maar ook dader worden. De Wbp hanteert het begrip 'verantwoordelijke' als het om het verwerken van persoonsgegevens gaat. De vraag is in hoeverre dit begrip de burger die gegevens op internet plaatst, kan omvatten.

Dat technologische ontwikkelingen de bescherming van persoonsgegevens enerzijds bemoeilijken, maar er anderzijds ook veelbelovende garanties voor kunnen bieden, mag genoegzaam blijken uit het bovenstaande. Vanwege hun relevantie voor het functioneren van de wet schenkt het onderhavige onderzoek nadrukkelijk aandacht aan – onder meer de genoemde – technologische ontwikkelingen.

3.2.4 Samenwerkingsverbanden

In het knelpuntenonderzoek is geconstateerd dat de Wbp als belemmering wordt ervaren bij gegevensuitwisseling in samenwerkingsverbanden. De vraag is op welke manier dit gebeurt. Bij samenwerkingsverbanden zijn naast de Wbp vaak andere wetten van toepassing waarin regels zijn gesteld over gegevensverwerking. In combinatie met het hoge abstractieniveau van de Wbp, leidt dit tot een voor de praktijk ondoorgrondelijk regelstelsel. Verder blijkt dat er, door onbekendheid met de interpretatieruimte van de Wbp, soms ten onrechte van wordt uitgegaan dat gegevensuitwisseling niet mogelijk is.

Om de problemen rondom gegevensuitwisseling in samenwerkingsverbanden nader te onderzoeken is in dit onderzoek naar de werking van de Wbp een casestudyonderzoek uitgevoerd. In hoofdstuk 7 worden de resultaten van dit hoofdstuk besproken. Ook wordt daar nader ingegaan op de problemen rondom gegevensuitwisseling in samenwerkingsverbanden. Op deze plaats worden daarvoor alvast een aantal aandachtpunten geformuleerd.

Verschillende personen waarmee een interview is gehouden, hebben aangegeven dat gelet op de open normstelling van de Wbp er altijd een mogelijkheid is om gegevens uit te wisselen in een samenwerkingsverband. Alleen bij samenloop met andere wetgeving, als een beroepsgeheim geldt en het gaat om bijzondere gegevens, doen zich problemen voor.

Uit het knelpuntenonderzoek blijkt dat mogelijkheden voor gegevensuitwisseling onbenut worden gelaten vanwege de onbekendheid met de wet. Deze onbekendheid met de wet zou er echter ook toe kunnen leiden dat persoonsgegevens worden verwerkt terwijl daarvoor geen wettelijke grondslag bestaat. Volgens het Cbp wordt bij samenwerkingsverbanden regelmatig in strijd gehandeld met de artikelen 8, 9 en 11 van de Wbp doordat deelnemers informatie krijgen over betrokkenen waarmee zij niets te maken hebben of, als het gaat om een betrokkene waarmee ze wel een relatie hebben, die voor de uitvoering van hun taak niet noodzakelijk is.[102] Wellicht dat privacy voor verantwoordelijken, door een gebrek aan bekendheid met de wet, geen item is en zij overgaan tot gegevensuitwisseling zonder zich af te vragen of dat is toegestaan.

In de praktijk wordt de Wbp als belemmering ervaren, zo blijkt uit het knelpuntenonderzoek. Of de Wbp inderdaad belemmerend werkt, is onduidelijk. Het Cbp is van mening dat dit niet het geval is; er moet slechts aan bepaalde randvoorwaarden worden voldaan.[103] Het feit dat verantwoordelijken de Wbp als belemmering zien, hangt wellicht samen met het beeld dat zij

[101] Alberdingk Thijm 2004, p.31 en 32
[102] Zwenne e.a. 2007, p. 145
[103] Idem, p. 125

van privacywetgeving en privacybescherming hebben. Wellicht vinden zij privacy ondergeschikt aan de primaire taak van het samenwerkingsverband en het maatschappelijke belang dat gediend is met de gegevensuitwisseling in het samenwerkingsverband. Het zou dan ook best kunnen dat in samenwerkingsverbanden willens en wetens in strijd wordt gehandeld met de Wbp. Volgens het Cbp is onbekendheid met de wet inderdaad niet de enige oorzaak van een nalevingstekort. Het Cbp geeft aan dat de Wbp onvoldoende wordt nageleefd, omdat de zogenaamde 'stok achter de deur' ontbreekt.[104]

3.3 Informeren

3.3.1 Bekendheid

Bekendheid met (de inhoud van) de wet is een noodzakelijke voorwaarde voor een goede uitvoeringspraktijk. Zowel betrokkenen als verantwoordelijken moeten op de hoogte zijn van de rechten en plichten van de Wbp. Bekendheid moet in samenhang met de complexe aard van het systeem van open normen bestudeerd worden. Het is de vraag over welke informatie verantwoordelijken moeten beschikken om uitvoering te kunnen geven aan de open normen. Omgang met open normen vereist meer juridische kennis dan omgang met gedetailleerde normen. In sectoren waarin de normen door middel van gedragscodes zijn uitgewerkt, is andere kennis van de Wbp nodig dan in sectoren waarin dit nog niet is gebeurd en de normen meer een open karakter hebben. Het is daarbij niet onwaarschijnlijk dat de informatiebehoefte van de onderscheiden doelgroepen (publiek, privaat) verschillend is.

Bekendheid burgers

De afgelopen jaren is verschillende malen onderzocht of burgers bekend zijn met de privacyregelgeving en welk belang zij hechten aan privacy.[105] Deze onderzoeken kunnen inzicht geven in de vraag hoe duidelijk de wet is voor burgers en over welke informatie burgers zouden moeten beschikken om de regie te kunnen voeren over hun persoonsgegevens. Ook kunnen de gegevens uit deze onderzoeken, als deze worden afgezet tegen de resultaten van het onderhavige onderzoek, een antwoord geven op de vraag welke verbeteringen in de communicatie mogelijk zijn.

Uit het onderzoek van TNS NIPO blijkt dat het belang van de bescherming van persoonsgegevens voor burgers duidelijk is. Bij de definitie van persoonsgegevens leggen burgers de nadruk op de privésfeer, dat wat van jezelf is. Er worden heel verschillende dingen genoemd: NAW-gegevens, telefoonnummer, creditcard nummer, informatie over koopgedrag, medische gegevens etc. Burgers hechten veel waarde aan het juist omgaan met hun persoonsgegevens door organisaties. Ze hebben er echter niet veel vertrouwen in dat dat altijd zorgvuldig gebeurt. Burgers hebben meer vertrouwen in officiële instanties (belastingdienst, gemeenten, politie, uitkeringsinstanties) dan in commerciële organisaties (banken, financiële instellingen, verzekeringsmaatschappijen en credit card maatschappijen). Ze vertrouwen de overheid meer dan het bedrijfsleven.[106] Negen op de tien burgers hecht (zeer) veel belang aan wetgeving voor de bescherming van persoonsgegevens.[107] De kennis over de Wbp is echter niet groot.[108] Het Cbp is bij weinig burgers bekend. Gelet op het belang dat burgers hechten

[104] Gesprekken met de voorzitter van het Cbp, J. Kohnstamm, op 25 februari 2008 en 22 april 2008
[105] TNS NIPO 2005, Consumentenbond 2005, Van den Heuvel e.a. 2007
[106] TNS NIPO 2005, p. 22
[107] Idem, p. 23
[108] Idem, p. 24

aan de bescherming van persoonsgegevens en het feit dat zij niet altijd het vertrouwen hebben dat juist met hun persoonsgegevens wordt omgegaan, is er behoefte aan de functie die het Cbp vervult in de samenleving.[109] Volgens de onderzoekers van TNS NIPO is naast het geven van informatie en voorlichting ook van belang dat de maatschappelijke waarde van de bescherming van persoonsgegevens wordt geagendeerd in de maatschappelijke discussie.[110]

De Consumentenbond heeft in 2005 onderzoek gedaan naar de mening van burgers over privacy.[111] De resultaten van het onderzoek zijn vergeleken met die van een vergelijkbaar onderzoek in 1995. Uit het onderzoek blijkt dat de helft van de ondervraagden in 2005 evenveel waarde aan hun privacy hecht als in 1995, maar dat 44% privacy belangrijker is gaan vinden. Belangrijke redenen die hiervoor worden genoemd zijn de grote kans op misbruik van gegevens, het feit dat persoonsgegevens nu eerder worden gebruikt voor oneigenlijke doelen en het feit dat er nu meer gegevens worden vastgelegd die vroeger tot de privé-sfeer behoorden. Van de ondervraagden is 80% zich ervan bewust dat bedrijven en instanties gegevens over hen vastleggen. De helft weet echter niet welke gegevens en wanneer of waar gegevens worden vastgelegd. 66% van de ondervraagden realiseert zich dat gegevens over hun in handen van onbevoegden kan komen. Gebruikersnamen, wachtwoorden en pincodes staat nu bovenaan op de lijst van privacygevoelige gegevens. Verder zijn nu belangrijk het surfgedrag op Internet evenals gegevens over waar men zich ophoudt, koopgedrag en bezit. In vergelijking met tien jaar geleden vindt men over het inkomen, vermogen, schulden, de gezondheidstoestand (psychisch en lichamelijk), de seksuele geaardheid en het strafrechtelijk verleden nog steeds privacygevoelig. Ook uit dit onderzoek blijkt dat burgers overheidsorganisaties meer vertrouwen dan commerciële organisaties in het correct omgaan met persoonsgegevens.

In 2007 is onderzoek gedaan naar de mening van burgers over RFID. RFID staat voor Radio Frequency Identification (RFID). Het gaat hierbij om kleine op afstand afleesbare chips die worden gebruikt om goederen en/of mensen te identificeren. RFID wordt toegepast bij bijvoorbeeld de OV-chipkaart, het biometrisch paspoort en een werknemerspas. Hierbij kan RFID dienen als toegangssleutel of elektronische portemonnee. RFID wordt in het bedrijfsleven vaak gebruikt om de logistiek te verbeteren.[112] Uit het onderzoek blijkt dat niemand echt tegen RFID is. De RFID-toepassingen hebben voordelen voor het gebruiksgemak en het algemene gevoel van de respondenten is dat de technologie toch niet te stoppen is. Wel vindt men het belangrijk dat de toepassing goed gereguleerd wordt en dat er niet één grote database komt waar iedereen alles van af kan lezen.[113] Wederom blijkt dat burgers de overheid meer gegevens toevertrouwen dan het bedrijfsleven. Burgers zijn bang dat bedrijven, gelet op hun winstoogmerk, de gegevens zullen misbruiken.[114]

De voorgaande onderzoeken, waaruit blijkt dat burgers waarde hechten aan de bescherming van hun privacy, staan haaks op de hierboven in paragraaf 1.2.2 genoemde onderzoeken waaruit blijkt dat privacy nauwelijks een rol van betekenis speelt in het debat over opsporings- en veiligheidsmaatregelen en dat privacy en veiligheid als tegengesteld aan elkaar worden gezien: privacy en veiligheid vallen niet met elkaar te combineren.[115] [116] Naast het

[109] TNS NIPO 2005, p. 25
[110] Idem, p. 26
[111] Consumentenbond 2005
[112] Idem, p. 9
[113] Idem, p. 7
[114] Idem, p. 8
[115] Vedder e.a. 2007, p. 11
[116] Muller e.a. 2007, p. 54

Cbp zijn er eigenlijk geen organisaties die specifiek opkomen voor de bescherming van de privacy van de burger.[117] Zo heeft de stichting Bits of Freedom, die zich sinds 2000 heeft ingezet voor digitale burgerrechten zoals privacy op Internet en vrijheid van meningsuiting, in september 2006 haar activiteiten gestaakt vanwege het vertrek van haar twee vaste medewerkers.[118] Wellicht is het feit dat er weinig belangenbehartigers zijn op het gebied van de privacybescherming, er de oorzaak van dat de mening van burgers over privacy in het publieke en politieke debat niet goed naar voren komt.

Het onderzoek naar de bekendheid met de wet heeft zich tot nu toe in hoofdzaak gericht op burgers en nog weinig op verantwoordelijken. Uit een onderzoek van TNS NIPO van 2006 onder huisartsen, onderwijsinstellingen en woningcorporaties bleek dat een ruime meerderheid van de onderwijsinstellingen en woningcorporaties op de hoogte was van de Wbp. Van de huisartsen echter kende slechts 35% de Wbp.[119] Gelet hierop is het goed mogelijk dat vooral kleine bedrijven (bedrijven met minder dan twintig werknemers) de Wbp niet kennen of zich onvoldoende realiseren dat hun bestanden onder de Wbp vallen.

Een opvallende conclusie uit het knelpuntenonderzoek is dat ook bij (civiele) rechters de nodige kennis ontbreekt, waardoor soms wordt verzuimd de Wbp bij een rechterlijke afweging te betrekken.[120] Over welke rol het Cbp kan spelen bij de verduidelijking van de normen en de bekendheid daarvan, wordt in paragraaf 3.4.1 nader ingegaan.

3.3.2 Meldings- en informatieplicht

Het uitgangspunt van de Wbp is dat iedereen in de gelegenheid moet zijn om na te kunnen gaan waar gegevens over hem zijn vastgelegd en worden verwerkt.[121] Aan betrokkenen zijn verschillende rechten toebedeeld. Zo kunnen zij gegevens inzien, vragen om verbetering, aanvulling, verwijdering en afscherming en kunnen zij verzet aantekenen. Om van deze rechten gebruik te kunnen maken, moet de betrokkene wel van het bestaan van de gegevensverwerking op de hoogte zijn. In de Wbp wordt deze transparantie afgedwongen door aan verantwoordelijken een meldings- en informatieplicht op te leggen.[122]

Uit het knelpuntenonderzoek blijkt dat betrokkenen weinig gebruik maken van hun kennisnemingsrechten. Gelet op de in de paragraaf hiervoor genoemde onderzoeken waaruit blijkt dat burgers privacy wel degelijk belangrijk vinden, is in dit onderzoek de vraag gesteld of zij wel van het bestaan van de rechten op de hoogte zijn. Uit de in de voorgaande paragraaf genoemde onderzoeken blijkt dat veel burgers niet op de hoogte zijn van het bestaan van het Cbp. Dit betekent dat zij ook niet op de hoogte zijn van het bestaan van het openbare meldingsregister. Ook als ze wel op de hoogte zijn, is het de vraag of dit register voor de gewenste transparantie zorgt, gelet op het feit dat het register niet eenvoudig doorzoekbaar is.

De kennisnemingsrechten gaan bovendien gepaard met de nodige knelpunten. De vraag is of verantwoordelijken de procedure voor het wijzigen en inzien van gegevens kennen en hoe vaak zij daar gebruik van maken als de procedure wel bekend is. Er bestaat onduidelijkheid over de reikwijdte en invulling van de kennisnemingsrechten. Daarnaast blijkt zorg te bestaan

[117] Muller e.a. 2007, p. 50
[118] Bits of Freedom 2006
[119] TNS NIPO 2006, p. 33
[120] Zwenne e.a. 2007, p. 172
[121] Hooghiemstra en Nouwt 2007, p. 18
[122] *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 18

over de naleving van het kennisnemings- en correctierecht.[123] Uit het hiervoor genoemde onderzoek van TNS NIPO naar de naleving van de informatieplicht door huisartsen, onderwijsinstellingen en woningbouwcorporaties blijkt dat men niet altijd op de hoogte is van de (inhoud van de) plicht. De informatieplicht wordt dan ook niet altijd (juist) nageleefd.[124] De onderzoekers van het knelpuntenonderzoek geven aan dat er aanwijzingen zijn dat procedures en maatregelen vaak ontbreken om de rechten van burgers binnen de wettelijke termijnen op een zorgvuldige wijze te kunnen effectueren.[125]

Ook de meldingsplicht zorgt voor problemen. De ruime werking van de meldingsplicht (melden, tenzij) wordt als knelpunt gezien. Daarnaast worden vraagtekens geplaatst bij de bijdrage die de meldingsplicht levert aan de beoogde transparantie.[126] Uit dit onderzoek naar de werking van de wet moet blijken of de bescherming van privacy verbeterd is door de meldplicht en de informatieplicht. Uit onderzoeken van het Cbp naar het meldgedrag in verschillende sectoren blijkt steevast dat veel verwerkingen van persoonsgegevens waarop een meldingsplicht rust niet worden gemeld. Er zijn daarom al enkele boetes uitgedeeld. In 2004 heeft het Cbp veertien boetes opgelegd aan gemeenten. Daarnaast zijn drie direct marketing bedrijven beboet, hebben drie zorgverzekeraars een boete ontvangen en is aan negen arbodiensten een boete opgelegd.[127] Dat deze boetes tot een betere naleving van de meldingsplicht zullen leiden, is zeker niet gegeven. Uit onderzoek over de naleving van milieuvoorschriften blijkt dat voor de naleving van groot belang is dat de bereidheid van de overheid om normering af te dwingen zichtbaar is. De kans op handhaving is bij algemene regels echter relatief gering.[128] Burgers die in een bestand zijn opgenomen dat niet is gemeld bij het Cbp zullen daartegen, gezien de onbekendheid van de Wbp en het Cbp, bijvoorbeeld zelden opkomen. Daarnaast kan het Cbp eenvoudiger optreden tegen een onjuiste melding dan tegen het uitblijven van een melding. Daarbij moet worden aangetekend dat het Cbp niet de vrijheid heeft om iedere melding te onderzoeken.

Naast het zorgen voor transparantie voor zowel betrokkenen als de toezichthouder, is de meldingsplicht volgens het Cbp ook van belang omdat het de verantwoordelijke bewust maakt van de wettelijke eisen en de verantwoordelijke dwingt de gegevenshuishouding door te lichten.[129] Door de meldingsprocedure te doorlopen wordt de verantwoordelijke gedwongen na te denken over de rechtmatigheid van de verwerking. Het is de vraag of de formele activiteit van melden een materiële verbetering oplevert in de omgang met persoonsgegevens. In dit onderzoek wordt die vraag aan de orde gesteld. In de praktijk blijken meldingen niet altijd correct te zijn. De doelstelling is vaak heel algemeen geformuleerd en ten aanzien van de opgenomen gegevens, de bijzondere gegevens en de categorieën van ontvangers worden ook de nodige fouten gemaakt.[130] Wellicht hangt dit samen met een gebrek aan toetsing van de melding. Gelet op het hoge aantal meldingen (ongeveer 4000 per jaar) geeft het Cbp aan geen uitgebreide inhoudelijke toets naar aanleiding van de melding te kunnen verrichten.[131]

---

[123] Zwenne e.a. 2007, p. 170 en 171
[124] TNS NIPO 2006, p. 33
[125] Zwenne e.a. 2007, p. 129
[126] Holvast 2005a, p. 211
[127] Cbp 2004a 'Boetes voor gemeenten en bedrijven na controle meldingsplicht 2003', 26 juli 2004, te vinden op: http://www.cbpweb.nl/documenten/med_20040726_mo2003.stm, geraadpleegd op 24 augustus 2008
[128] Van Geest e.a. 1998, p.93
[129] Holvast 2005, p. 117
[130] Holvast 2005a, p. 211
[131] Cbp 2008 en Oriënterend interview met het Cbp

Verder blijkt dat vaak wordt geklaagd over de hoogte van de administratieve lasten van de meldingsplicht.[132]

3.4 Toezicht en rechtsbescherming

3.4.1 College bescherming persoonsgegevens

In het vorige hoofdstuk is aangegeven dat het Cbp is aangewezen als toezichthouder voor de Wbp. Onder de Wpr was de Registratiekamer toezichthouder. Een van de vragen in dit onderzoek is hoe het Cbp invulling geeft aan toegekende functies bij toezicht, naleving en handhaving.

Sinds 1998 hebben de Registratiekamer en het Cbp, om te komen tot een uitoefening van de toezichthoudende taak met maximaal resultaat, gehandeld op basis van het zogenaamde 'viersporenbeleid'. De volgende vier sporen zijn bewandeld:

1. het bevorderen van bewustwording;
2. het bevorderen van normontwikkeling;
3. het op de voet volgen van technologische ontwikkelingen;
4. het in voorkomende gevallen handhavend optreden.[133]

In 2007 heeft het Cbp besloten om de prioriteit te verleggen naar het vierde spoor.[134] Volgens het Cbp hebben voorlichting en advisering er niet tot geleid dat de Wbp voldoende wordt nageleefd. De reden hiervoor is dat de zogenaamde 'stok achter de deur' ontbreekt.[135]

Jaarlijks ontvangt het Cbp veel verzoeken om voorlichting, bemiddeling en het instellen van een onderzoek.[136] Het Cbp legt bij verzoeken om hulp en bijstand de prioriteit bij ernstige overtredingen met een structureel karakter en grote gevolgen voor een flink aantal burgers of voor groepen van burgers.[137]

Burgers en organisaties die bij een verzoek om hulp en bijstand een negatieve reactie van het Cbp krijgen, zullen zoveel mogelijk geholpen worden om zelf zicht te krijgen op de rechten en plichten van de Wbp zodat zij zelf de nodige actie kunnen ondernemen. Het Cbp geeft aan in dit kader te zullen investeren in de inhoud van de website www.cbpweb.nl en www.mijnprivacy.nl.[138] Gelet op het feit dat er weinig andere belangenbehartigers zijn, kan de vraag worden gesteld of de positie van de burger hierdoor zal verbeteren. Aan de andere kant zou echter gesteld kunnen worden dat de burger gediend is met de koerswijziging omdat verantwoordelijken nu worden gedwongen om de Wbp na te leven. Ook heeft de burger, naast het zich wenden tot het Cbp, nog meer mogelijkheden voor rechtsbescherming.

Voordat handhavend wordt opgetreden, moet duidelijkheid worden verschaft over de normstelling op basis waarvan het Cbp in actie komt.[139] De activiteiten op het gebied van

[132] Zwenne e.a. 2007, p. 93
[133] Cbp 2008, p. 3
[134] Idem, p. 3
[135] Gesprekken met de voorzitter van het Cbp, J. Kohnstamm, op 25 februari 2008 en 22 april 2008
[136] In 2007 zijn via het telefonisch spreekuur en de e-mail 5.928 verzoeken om algemene voorlichting ontvangen. Er waren 396 zaken van bemiddeling en klachten.
[137] Cbp 2008, p. 4
[138] Idem, p. 4
[139] Idem, p. 3

toezicht en handhaving gaan derhalve gepaard met een bepaalde vorm van voorlichting. Deze paragraaf vormt daarom niet alleen het kader voor de beantwoording van de vragen over toezicht en handhaving, maar ook voor de vraag welke rol het Cbp kan spelen bij de bij de verduidelijking van de open normen en het stimuleren van zelfregulering.

Handhaving en communicatie

In opdracht van het WODC is in 2007 onderzoek gedaan naar de rol van informatie en communicatie bij het handhavingsbeleid.[140] Handhaving is gedragsbeïnvloeding: men wil een bepaalde doelgroep bewegen tot gedrag dat in overeenstemming is met de wettelijke regels. Zonder communicatie is gedragsbeïnvloeding niet mogelijk.[141] Er kunnen drie hoofdvormen van handhavingscommunicatie worden onderscheiden, die zich elk richten op een andere gedragsdimensie:

1. *Dreigende communicatie.* Deze vorm van communicatie heeft tot doel potentiële overtreders af te schrikken van het plegen van een overtreding. Dit kan door te dreigen met een wettelijke sanctie of door iemand angst aan te jagen ten aanzien van de gevolgen van het ongewenste gedrag voor diens gezondheid of veiligheid.[142]
2. *Educatieve communicatie*. Als de doelgroep niet op de hoogte is van de regels, deze niet goed begrijpt of onjuist interpreteert, kan regelgeving niet correct worden nageleefd. Educatieve communicatie is erop gericht de doelgroep te informeren over het bestaan van de regels en de juiste toepassing ervan. Ook kan communicatie zijn gericht op het trainen van vaardigheden die nodig zijn voor de correcte naleving. Als er minder onbedoelde fouten worden gemaakt bij de naleving, blijft er meer capaciteit beschikbaar voor de opsporing van bewuste overtredingen.[143]
3. *Normatieve communicatie*. Traditionele opvattingen van handhaving zijn gericht op controleren en bestraffen, vanuit de gedachte dat de doelgroep een rationele afweging maakt tussen de kosten en baten van overtredingen. In werkelijkheid is de pakkans in veel gevallen niet de enige, en ook niet de belangrijkste reden voor de naleving van regels. Die naleving komt ook voort uit normbesef of plichtsgevoel. Regels die legitiem zijn en onderdeel uitmaken van de eigen normen of waarden van een persoon of organisatie, worden ook gevolgd zonder dat daar afschrikwekkende handhaving bij nodig is. Relevant voor communicatie bij handhaving zijn de sociale of persoonlijke normen voor 'goed' of gepast gedrag en de rechtvaardigheid van de regelgeving of de handhaving.[144]

Geconcludeerd wordt dat de drie vormen van communicatie alle in enige mate noodzakelijk zijn en in combinatie moeten worden ingezet omdat alle gedragsdimensies van invloed zijn op het nalevingsgedrag. Nalevings- of overtredingsgedrag komt voort uit een mix van normen, doelrationele motieven en kennis.[145] Educatieve voorlichting is vereist om het kennisniveau op peil te brengen en te houden en om de doelgroep ondersteuning te bieden bij de juiste toepassing van regels om fouten te voorkomen. Een duurzame gedragsverandering wordt met educatieve voorlichting alleen echter niet bereikt. Daarvoor moet de doelgroep ook worden gewezen op de risico's van overtreding (dreigende communicatie) en moet worden bevorderd

[140] Van Erp 2007
[141] Idem, p. 79
[142] Idem, p. 31
[143] Idem, p. 65
[144] Idem, p. 71
[145] Idem, p. 87 en 88

dat de doelgroep de regels in zeker mate vrijwillig naleeft omdat ze het betreffende gedrag goed of gepast vinden (normatieve communicatie).[146]

De conclusie van het onderzoek is dat communicatie te allen tijde respectvol moet zijn, vertrouwen moet uitstralen in de bereidheid tot naleving van de doelgroep en de gedeelde belangen van de handhaver en de doelgroep moet onderstrepen. Er moet gebruik worden gemaakt van dreigende communicatie die bestaande normen niet ondergraaft en normatieve communicatie die de handhaving niet ongeloofwaardig maakt. Van belang is allereerst dat in de communicatie niet teveel aandacht moet worden gevestigd op het feit dat er overtreden wordt. Vervolgens moet benadrukt worden dat 'de ander' overtreedt. Ten slotte kan het normatieve kader het best bestaan uit objectieve informatie over het (hoge) nalevingsniveau en kan hierbij verwezen worden naar de krachtige en effectieve handhaving die hieraan heeft bijgedragen.[147]

Uit het hiervoor aangehaalde onderzoek van de Universiteit Twente blijkt dat de stijlen van toezicht en handhaving van groot belang zijn voor de immateriële regeldruk. De 'feedback' en de deskundigheid van de externe organisaties blijken van groot belang te zijn. Indien de toezichthouder of de certificatie- of accreditatieorganisaties geen feedback geven op de in jaarverslagen en via andere kanalen aangeleverde informatie of als zij de aangeleverde informatie niet gebruiken ('iets mee doen') blijkt dit te leiden tot irritaties. Soortgelijke irritaties ontstaan bij een te soepele uitvoeringsstijl. De normadressaten krijgen het gevoel dat zij de (administratieve) inspanningen voor niets hebben geleverd.[148]

In het onderzoeksrapport 'Veiligheid en privacy' is aangegeven dat het Cbp in het huidige veiligheidsklimaat onmiskenbaar in het defensief is gedrongen.[149] De rol van het Cbp in het privacy- en veiligheidsdebat is erg belangrijk. Volgens de onderzoekers is het verstandig als het Cbp zich richt op de verbindende factoren in het debat en hierover realistische verwachtingen heeft.[150] Het Cbp moet voorkomen dat door een defensieve houding het imago wordt versterkt van een college waarvan niets mag. De onderzoekers geven aan dat het Cbp zich kan opstellen als partij die door de uitvoering van haar wettelijke taken een belang nastreeft waar in onze samenleving weinig tegenstanders voor te vinden zijn, namelijk vrijheid. In dat kader kan vervolgens uiteengezet worden wat de precieze betekenis en waarde van privacy is.[151]

Werkwijze andere toezichthouders

De voorzitter van het Cbp heeft aangegeven te willen werken zoals de NMa en de OPTA dat doen.[152] Relevant in dit kader is dat het kabinetsstreven is om te komen tot een 'high trust benadering' in het toezicht: toezicht moet zoveel mogelijk gebeuren vanuit vertrouwen.[153] Het gaat hierbij om risicogeoriënteerd toezicht en vermindering van de toezichtlasten.[154] Bij een high trust benadering zetten toezichthouders minder middelen in om overtredingen op te sporen, maar treden zij hard op als de de regels toch worden overtreden. Om de beschikbare

[146] Van Erp 2007, p. 88
[147] Idem, p. 89
[148] Dorbeck-Jung e.a. 2005, p. 54
[149] Muller e.a. 2007, p. 42
[150] Idem, p. 67
[151] Idem, p. 67
[152] Interview op 25 februari 2008.
[153] Coalitieakkoord 2007, p. 11
[154] *Kamerstukken II 2007-2008,* 31 200 XIII, nr. 51, p. 3

middelen binnen de high trust benadering efficiënt en effectief te kunnen inzetten, is een goede risicoanalyse nodig.[155]

De Minister van Economische Zaken is van mening dat de NMa voor een goede inbedding van de high trust benadering heeft gezorgd.[156] Het doel van het communicatiebeleid van de NMa is het geven van voorlichting, het inzicht geven in en het verantwoording afleggen over haar activiteiten. De NMa heeft in haar 'Werkwijze communicatie' belangrijke onderdelen van haar communicatiepraktijk vastgelegd. De Werkwijze gaat met name over pers- en nieuwsberichten en is niet van toepassing op de doelgroepgerichte voorlichting. Volgens de NMa zijn helderheid en duidelijkheid voor de naleving van de Mededingingswet van belang. De NMa maakt dan ook kenbaar wat zij doet via haar website, www.nmanet.nl, en via de website www.consuwijzer.nl. Deze website is het gezamenlijk informatieloket van de NMa, OPTA en de Consumentenautoriteit. Consumenten kunnen er terecht voor praktisch advies over hun rechten. Op de eigen website heeft de NMa verschillende brochures en andere vormen van doelgroepgerichte voorlichting (zowel voor consumenten als bedrijven) geplaatst.

Ook de OPTA heeft op haar website voorlichtingsmateriaal gepubliceerd.[157] De OPTA heeft onlangs in een richtsnoer haar aangepaste visie op toezicht en handhaving bekendgemaakt.[158] De OPTA gaat in haar handhavingsbeleid een sterker accent leggen op preventie, het voorkomen van overtredingen van wet- en regelgeving.[159] Hierbij wordt de vraag gesteld hoe OPTA in haar toezicht ervoor kan zorgen dat marktpartijen zich zodanig gedragen dat zij zelf de verantwoordelijkheid nemen voor het naleven van de Telecommunicatiewet en Postwet en in het verlengde hiervan schade wordt voorkomen.[160] Gelet op de high trust benadering – partijen zijn primair verantwoordelijk voor het naleven van wet- en regelgeving en de verplichtingen die OPTA aan hen oplegt - kan en wil OPTA op afstand toezicht houden. OPTA kan nog steeds gebruik maken van haar formele toezicht- en handhavingsbevoegdheden, maar zal dit pas doen als daarvoor aanleiding is. Naarmate een marktpartij meer 'compliant' wordt, zal er minder vaak aanleiding zijn om dergelijke bevoegdheden toe te passen.[161] OPTA wil de ontwikkeling, implementatie en uitvoering van compliance-programma's door marktpartijen stimuleren. Een compliance-programma binnen een onderneming bestaat uit een doeltreffend systeem van 'checks and balances' dat door de gehele organisatie is opgezet, waarbij deze organisatie door middel van gedragsregels, procedures en (controle)systemen (hard en soft controls) de naleving van wet- en regelgeving structureel wil waarborgen. OPTA kan daarbij actieve ondersteuning bieden.[162] OPTA gaat er in beginsel vanuit dat alle ondernemingen waarop zij toezicht houdt zich aan de op hen van toepassing zijnde wet- en regelgeving houden (compliant zijn). Partijen kunnen met OPTA afspraken maken over een Compliance Handvest. Hiermee beoogt OPTA in algemene zin duidelijk te maken wat ten minste wordt verwacht van een partij die onder toezicht staat op het vlak van een goed werkend compliance-programma. Het boetebeleid is aangepast naar aanleiding van de accentverschuiving. Van boetematiging kan sprake zijn bij overtredingen die begaan zijn ondanks een goed werkend compliance-programma. Een boeteverhoging kan plaatsvinden bij organisaties die aangeven over een goed werkend compliance-programma te

[155] *Kamerstukken II 2007-2008,* 31 200 XIII, nr. 51, p. 3
[156] Idem, p. 4
[157] Website OPTA onder 'publicaties'
[158] OPTA 2008
[159] Idem, p. 1
[160] Idem, p. 1
[161] Idem, p. 3
[162] Idem, p. 3

beschikken, maar waar bij later onderzoek blijkt dat het programma wel is opgesteld, maar niet is geïmplementeerd.[163]

Geconcludeerd kan worden dat ook bij andere toezichthouders een combinatie plaatsvindt van taken op het gebied van voorlichting en taken op het gebied van toezicht en handhaving. Een groot verschil tussen het Cbp en de NMa en OPTA lijkt echter te zijn dat sprake is van een heel andere doelgroep waarop toezicht moet worden gehouden. De NMa en OPTA houden toezicht op professionals. Hun toezicht ziet op een bepaalde economische sector of activiteit. Bij spam is er geen sprake van toezicht op professionals, maar ook daar is duidelijk wat de regels zijn. Bij het Cbp is het voorgaande niet het geval. De Wbp moet door verantwoordelijken van heel verschillende beleidsterreinen worden nageleefd, het overgrote deel van verantwoordelijken kan niet worden aangemerkt als professional en de gestelde regels zijn niet duidelijk zo, is gebleken uit het knelpuntenonderzoek.

De Nationale ombudsman beschermt de burger tegen onbehoorlijk overheidsoptreden. Hij is geen toezichthouder als de NMa of het Cbp maar draagt er wel aan bij dat overheden aan de door hem gehanteerde behoorlijkheidscriteria voldoen.[164] Uit het jaarverslag van de Nationale Ombudsman blijkt dat hij jaarlijks vele bijeenkomsten organiseert voor contactambtenaren, klachtenfunctionarissen en klachten-ambassadeurs.[165] Ook is er een actieve vereniging voor klachtrecht die regelmatig studiemiddagen organiseert en publiceert over het onderwerp. Deze activiteiten van de Nationale Ombudsman en de vereniging stimuleren de bewustwording en leiden tot een nadere uitwerking van normen. Dit heeft tot gevolg dat de naleving vooral een communicatief proces is waarin de manier waarop klachten kunnen worden behandeld een van de belangrijkste gespreksthema's is. De behoorlijksheidsnormen worden niet ter discussie gesteld.

3.4.2 Functionaris voor de gegevensbescherming

In paragraaf 3.2.2 is al aangegeven dat een FG kan worden aangesteld om de open normen van de Wbp in te vullen en zo te komen tot zelfregulering. Inmiddels hebben meer dan 200 organisaties een FG aangesteld.[166] Vrijwel alle ministeries en zo'n 10 % van de gemeenten hebben een FG in dienst. Ook zijn er FG's bij bijvoorbeeld ziekenhuizen, hogescholen en politiekorpsen.[167]

De kwaliteitseisen die de Wbp aan de FG stelt, zijn zeer algemeen van aard. Uit de afgenomen interviews blijkt dat vraagtekens worden gezet bij de deskundigheid van FG's. Bij de geïnterviewden bestaat het beeld dat aan opleiding van de FG niet altijd evenveel wordt gedaan, dat een FG wordt aangesteld voor een heel beperkt aantal uren en dat een FG soms enkel wordt aangesteld om het Cbp op afstand te houden. De vraag die zich dan ook opdringt is op welke manier FG's invloed hebben. Uit het knelpuntenonderzoek blijkt verder dat het kunnen waarborgen van de onafhankelijkheid van de FG als knelpunt wordt gezien.[168] Gelet op het voorgaande is het de vraag of verantwoordelijken die een FG hebben aangesteld de Wbp beter naleven dan verantwoordelijken die daartoe niet zijn overgegaan.

[163] OPTA 2008, p. 4
[164] www.ombudsman.nl
[165] Jaarverslag Nationale ombudsman 2007
[166] Cbp 2007, p. 23
[167] Dubbeld 2007, p. 70
[168] Zwenne e.a. 2007, p. 80

Zoals in paragraaf 3.2.2. al is aangegeven, geeft het Cbp aan terug te treden als eerstelijns toezichthouder wanneer een FG is aangesteld. In artikel 62 Wbp is echter bepaald dat de bevoegdheden van het Cbp onverlet blijven als een FG is aangesteld. Uit het knelpuntenonderzoek blijkt dat FG's het terugtreden van het Cbp graag geformaliseerd zien.[169] Als het Cbp dezelfde rol behoudt wanneer een FG is aangesteld, is er voor een verantwoordelijke weinig meerwaarde om tot aanstelling van een FG over te gaan. Als de toezichthoudende rol van het Cbp inderdaad beperkt wordt als een FG is aangesteld, zou sprake kunnen zijn van lagere administratieve lasten (toezicht op toezicht).[170]

In de onderzoeksopzet is ook de vraag gesteld welke verschillen bestaan tussen bedrijven, maatschappelijke ondernemingen en bestuursorganen met en zonder FG. Uit de interviews komt naar voren dat bij bedrijven het commerciële belang een rol speelt in de overwegingen om de Wbp na te leven. De naleving geschiedt dan niet alleen of niet zozeer vanuit de gedachte dat bescherming van persoonsgegevens van belang is, maar omdat door de naleving van de Wbp het imago van het bedrijf wordt versterkt en het vertrouwen van de klant in het bedrijf wordt vergroot. Bedrijven ondervinden, anders dan de overheid, ook sneller schade als er fouten worden gemaakt. Onjuist omgaan met persoonsgegevens kan tot omvangrijke schadeclaims leiden. Overigens is dat tot op heden nog niet gebeurd. Bovendien kunnen klanten besluiten niet meer gebruik te maken van de diensten van een bedrijf of hun producten niet meer aan te schaffen. Ten aanzien van de overheid kan een burger deze keuze nauwelijks maken.

3.4.3 Klachten en beroep

Een burger die klachten heeft over de verwerking van zijn persoonsgegevens kan, afhankelijk van de organisatie die zijn gegevens verwerkt, beroep aantekenen bij de civiele rechter of, na bezwaar, bij de bestuursrechter. De situaties waarin dit mogelijk is, zijn beschreven in de artikelen 45 en 46 van de Wbp. Daarnaast kunnen burgers met klachten over de verwerking van persoonsgegevens terecht bij geschillencommissie van verschillende branches, het Cbp en bij de Nationale ombudsman.

Eén van de kritieken op de Wbp is dat de open normen in geringe mate worden ingevuld door jurisprudentie, terwijl open normen in theorie juist tot een sterke rechtsontwikkeling kunnen leiden. Er wordt door geregistreerden weinig gebruik gemaakt van de rechtsbescherming-mogelijkheden. De rechtsingang is door het gedifferentieerde systeem niet erg eenduidig en voor het privaatrecht hoogdrempelig.[171] Het feit dat er weinig jurisprudentie is, kan bovendien worden veroorzaakt door de onbekendheid met de Wbp en het bestaan van verschillende procedures doet afbreuk aan de rechtseenheid.[172] De vraag is welke overwegingen ertoe leiden dat verantwoordelijken en geregistreerden al dan niet klagen dan wel procederen en in hoeverre de jurisprudentie hierbij een preventieve rol vervult.

De oorzaak van het gebrek aan jurisprudentie zou gelegen kunnen zijn in het feit dat de burger veel alternatieven heeft voor (dure) rechtspraak. Enerzijds zijn in de gedragscodes veelal geschillencommissies ingesteld, die mogelijk een meer laagdrempelige vorm van rechtsbescherming vormen dan de rechter. Anderzijds kan de burger met klachten bij het Cbp terecht (art. 47 Wbp), die kan bemiddelen met de verantwoordelijke. Indien het Cbp

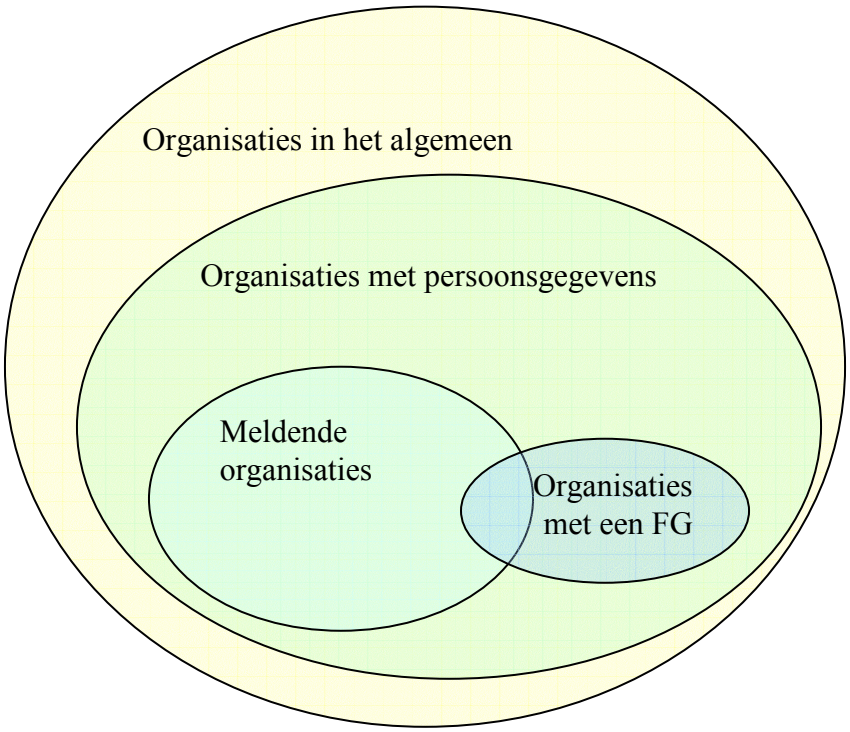
[169] Zwenne e.a. 2007, p. 80
[170] Dorbeck-Jung e.a. 2005, p. 105
[171] Zwenne e.a. 2007, p. 171-172
[172] Idem, p. 24

onrechtmatig handelen constateert, kan (of moet: beginselplicht tot handhaving) zij overgaan tot handhaving. Gezien de in paragraaf 3.4.1. genoemde prioritering van het Cbp kan de burger daar echter vaak niet terecht.

Hoofdstuk 4 Ervaringen van organisaties

4.1 Inleiding

In dit hoofdstuk worden de resultaten weergegeven van drie enquêtes die in het kader van het onderhavige onderzoek zijn uitgevoerd. Met behulp van deze enquêtes is getracht een goed beeld te krijgen van de feitelijke uitvoering van de Wbp.



Figuur 1 De in dit onderzoek onderscheiden (deel)populaties

Figuur 1 geeft een overzicht van de (deel)populaties die in dit onderzoek worden onderscheiden. Iedere (deel)populatie heeft zijn eigen relatie met de Wbp. Uit een drietal (deel)populaties is een steekproef getrokken ten behoeve van het enquêteonderzoek. De resultaten uit de enquêtes van de volgende (deel)populaties komen in dit hoofdstuk aan de orde:

1. De organisaties in het algemeen. Uit deze populatie is een gestratificeerde steekproef getrokken uit alle bedrijven, instellingen en overheden. Organisaties zijn allereerst geselecteerd op organisatietype. Er is een selectie gemaakt binnen de categorieën detailhandel, transport en communicatie, zakelijke en financiële dienstverlening, onderwijs, gezondheidszorg en de overheid. Binnen deze organisaties is specifiek gezocht naar organisaties die bovengemiddeld met persoonsgegevens te maken zouden hebben. Zo is bijvoorbeeld binnen de categorie detailhandel naast de reguliere supermarkten en warenhuizen (i.v.m. klantenkaarten) specifiek gezocht naar postorderbedrijven (i.v.m. adresgegevens en financiering) en winkels in optische artikelen (i.v.m. medische gegevens). Er zijn verder vier categorieën voor organisatiegrootte onderscheiden (1–19, 20–49, 50–100 en groter dan 100). Binnen iedere categorie zijn 20 organisaties

geselecteerd. Doel van deze gestratificeerde steekproef was ervoor te zorgen dat er een groot aandeel organisaties met persoonsgegevens deel zou uitmaken van de selectie. Hoewel deze steekproef zich grotendeels binnen de organisaties met persoonsgegevens bevindt, was niet te garanderen dat alle aangeschreven organisaties ook werkelijk persoonsgegevens verwerken. Daarom wordt deze groep verder met de *organisaties in het algemeen* aangeduid.

2. Meldende organisaties. Met deze groep worden die organisaties bedoeld die ten minste één melding bij het Cbp hebben gedaan. Om deze groep te bereiken is een gestratificeerde steekproef uit het Cbp-meldingenregister getrokken. Deze groep wordt verder de *meldende organisaties* genoemd.
3. Organisaties met een FG. Er is getracht de totale (deel)populatie te benaderen. Deze groep wordt verder de *organisaties met een FG* genoemd, of wanneer de FG als functionaris zelf wordt bedoeld kortweg *FG*. Voor een deel is er overlap met de groep van de *meldende organisaties*, omdat sommige *organisaties met een FG* ook meldingen doen bij het Cbp, hoewel dit strikt genomen niet nodig is.

Naarmate men meer naar de binnenste cirkels van het diagram beweegt, is er sprake van een specifiekere groep organisaties die steeds intensiever te maken heeft met de Wbp. Omdat de Wbp op zeer veel gebieden van toepassing is, is met name de buitenste groep erg diffuus. De *organisaties in het algemeen* is de groep waarbinnen alle overige geënquêteerde groepen vallen. Er zijn zeer weinig *organisaties met een FG* binnen deze groep aanwezig en de meeste organisaties binnen deze groep hebben nooit een verwerking bij het Cbp gemeld. Het is niet onwaarschijnlijk dat de Wbp niet erg leeft binnen deze groep. Het is dan ook lastig gebleken een goede respons op de aan deze groep gerichte enquête te krijgen. Het is echter wel een belangrijke en interessante groep in dit onderzoek omdat juist over deze groep zeer weinig bekend is. Als we het hebben over de uitvoering van de Wbp, dan geeft deze groep het beste beeld hoe deze wet 'gemiddeld' wordt uitgevoerd. Dit kan een sterke tegenstelling vormen met de (juridische) literatuur en het eerste faseonderzoek, die meer focussen op grote, belangrijke en wellicht ook atypische zaken. Juist over de typische uitvoering van de Wbp is bijzonder weinig bekend. Ondanks de lage respons (zie paragraaf 4.2.1) geeft deze enquête daarom bijzonder veel nieuwe informatie.

De *meldende organisaties* is een deelpopulatie van de *organisaties in het algemeen*. Het melden van een verwerking van persoonsgegevens is een uiting van privacybesef. De verwachting is dan ook dat privacy binnen deze deelpopulatie meer leeft, en dat er vaker persoonsgegevens worden verwerkt dan bij de *organisaties in het algemeen*. Doel van de enquête is overigens een getrouw beeld te krijgen van de uitvoering van de meldingsplicht. In deze enquête is daarom niet alleen aandacht voor grote of belangrijke zaken, maar wordt een zo getrouw mogelijk beeld geschetst hoe de uitvoering van de meldingsplicht in het merendeel van de gevallen in zijn werk gaat. Voor een deel zijn de vragen overlappend met die van de *organisaties in het algemeen*, zodat het mogelijk is om sommige kenmerken van beide populaties met elkaar te vergelijken.

De *organisaties met een FG* is een deelpopulatie van de *organisaties met persoonsgegevens*. Meldingen hoeven niet bij het Cbp te worden ingediend, maar er kan worden volstaan met een melding bij de FG. De deelpopulatie *organisaties met een FG* valt daarom niet (geheel) binnen de deelpopulatie van de *meldende organisaties*. Omdat sommige *organisaties met een FG* hun meldingen (ook) bij het Cbp doen, is er toch een geringe overlap met de deelpopulatie van de *meldende organisaties*. De *organisaties met een FG* vormen een atypische groep omdat FG's vooral zijn benoemd in een bijzondere categorie organisaties (groot, informatie-

intensief en veel (semi)overheid). Het benoemen van een FG kan duiden op een hoog privacybesef, maar ook op een neiging het toezicht in eigen hand te houden of een boventallige werknemer een functie te geven. De FG's zijn ondervraagd omdat zij kunnen worden beschouwd als een groep praktijkdeskundigen op het gebied van privacybeleid. Het doel van deze enquête was tweeledig. Enerzijds is getracht inzicht te krijgen in de wijze waarop FG's hun functie invullen, anderzijds zijn zij gebruikt als deskundigenpool om dieper op openstaande vragen te kunnen ingaan. Gedeeltelijk is er een overlap met de vraagstelling uit de vorige twee enquêtes, zodat soms een vergelijking tussen twee, en soms tussen drie (deel)populaties kan worden gemaakt.

De resultaten uit de enquêtes uit de drie (deel)populaties worden in dit hoofdstuk niet na elkaar, maar door elkaar heen behandeld. Hiervoor is gekozen omdat op deze wijze de verschillende belangrijke thema's uit de Wbp aan bod kunnen komen en er per thema – waar mogelijk – vergelijkingen kunnen worden gemaakt tussen de drie onderzochte groepen. Op deze wijze kan een genuanceerd beeld worden gekregen van de uitvoering in de praktijk. Ieder thema is terug te vinden in een eigen paragraaf. In het bijschrift van figuren en tabellen zal steeds tussen haakjes worden aangegeven uit welke (deel)populatie de informatie afkomstig is.

In paragraaf 4.2 wordt een overzicht gegeven van de kenmerken van de steekproef en de grootte en verdeling van de respons. Paragraaf 4.3 geeft achtergrondinformatie over de geënquêteerde organisaties. In paragraaf 4.4 wordt ingegaan op de vraag hoe de FG zijn taak in de praktijk invult. Zo komt onder meer aan de orde hoe hij zijn tijd verdeelt over adviserende en handhavende activiteiten. In paragraaf 4.5 wordt nader ingegaan op kenmerken van databases die in de organisaties aanwezig zijn. Er wordt een beschrijving gegeven hoe veel databases er zijn, waar die te vinden zijn en of persoonsgegevens worden uitgewisseld. Daarnaast wordt achterhaald hoe de organisatie aan de persoonsgegevens komt en wat de inhoud van de database is. Ten slotte wordt een beschrijving gegeven van de mate van beveiliging van de persoonsgegevens in de database. In paragraaf 4.6 wordt nader ingegaan op de meldingsprocedure. Het spreekt voor zich dat de meeste gegevens uit deze paragraaf afkomstig zijn uit de enquête onder de meldende organisaties. Er wordt onder meer gekeken hoeveel kennis de meldende organisaties over de meldingsplicht hebben, hoe vaak wordt gemeld en waarom dat gebeurt. Verder wordt een inschatting gemaakt van de positieve effecten van melden (in de zin van versterking van het privacybewustzijn) en de administratieve lasten. De manier waarop betrokkenen gebruik maken van hun recht op informatie, inzage, wijziging, bezwaar, verzet en beroep komt aan de orde in paragraaf 4.7. Tevens wordt de vraag beantwoord hoe vaak betrokkenen gebruik maken van deze rechten. Paragraaf 4.8 gaat kort in op administratieve lasten die bij de uitvoering van de Wbp worden ervaren. In paragraaf 4.9 wordt nog ingegaan op nieuwe ontwikkelingen en de gevaren die dit voor de privacy met zich meebrengt. In paragraaf 4.10 tenslotte wordt dit hoofdstuk kort samengevat.

4.2 Respons

4.2.1 Organisaties in het algemeen

In Nederland waren in 2006 in totaal 826.305 bedrijfsvestigingen.[173] Uit deze populatie is een steekproef van 640 bedrijven, instellingen en overheden geselecteerd, waaraan via de post een

[173] Bron: www.cbs.nl. Dit aantal is inclusief overheden en semi-overheden, zoals onderwijs en gezondheidszorg.

mailing is gestuurd met daarin een vragenlijst. De bedrijven zijn geselecteerd uit het handelsregister van de Kamer van Koophandel. Omdat in een aselecte steekproef waarschijnlijk veel organisaties zouden zitten die naar hun aard weinig met de Wbp te maken zouden hebben, is gekozen voor een gestratificeerde steekproef. In deze steekproef is gezocht naar categorieën van organisaties die naar verwachting vaak persoonsgegevens verwerken. Er is een onderverdeling gemaakt naar bedrijfstakken en bedrijfsgrootte. Bij de selectie is verder een geografische spreiding over Nederland gerealiseerd. Bij de categorie overheid is de grootte van de organisatie niet als selectiecriterium gebruikt. Bij de overheid is uitgegaan van een functionele spreiding over overheidsinstellingen, zoals gemeenten en ZBO's. Er is bij de selectie rekening mee gehouden dat binnen bepaalde overheden mogelijk gevoelige persoonsgegevens worden verwerkt. Te denken valt aan: RDW, UWV, CWI, IND, gemeentelijke sociale diensten, GGD en de reclassering.

Tabel 1 Verdeling van de aangeschreven organisaties

	Aantal werknemers				Totaal
	0-19	20-49	50-99	100+	
Detailhandel	20	20	20	20	80
Direct marketing	20	20	20	20	80
Zakelijke + fin. dienstverlening	20	20	20	20	80
Transport	20	20	20	20	80
Communicatie	20	20	20	20	80
Onderwijs	20	20	20	20	80
Gezondheidszorg	20	20	20	20	80
Overheid	n.v.t.	n.v.t.	n.v.t.	n.v.t.	80
Totaal	160	160	160	160	640

Van de 640 organisaties die zijn aangeschreven bleek van twee organisaties het adres niet te kloppen. Dat betekent dat 638 organisaties de mailing hebben ontvangen. Ongeveer twee weken nadat de mailings verstuurd waren, heeft een beperkt aantal organisaties een rappel via de e-mail ontvangen. Ruim 400 organisaties zijn telefonisch benaderd om hen aan de vragenlijst te herinneren. Deze inspanning heeft ertoe geleid dat 83 organisaties een enquêteformulier hebben ingevuld. 28 organisaties hebben dat via een internetformulier gedaan en 55 hebben hun enquêteformulier schriftelijk ingediend. Het responspercentage ligt daarmee op 13 procent.

Aan een deel van de 400 organisaties die telefonisch zijn benaderd is, wanneer zij aangaven niet aan het onderzoek te willen deelnemen, gevraagd naar de reden daarvoor. Een grote meerderheid van deze organisaties gaf aan daarvoor geen tijd te hebben. Een beperkt deel van de organisatie was van mening dat zij geen persoonsgegevens verwerkten.

De respons is volgens het onderstaande schema verdeeld over de categorieën organisaties en hun grootte. Wat opvalt is dat een aantal categorieën beter vertegenwoordigd is dan andere. De zakelijke en financiële dienstverlening heeft het best gereageerd, gevolgd door de gezondheidszorg en de (centrale en decentrale) overheid. Ook het onderwijs heeft relatief goed gerespondeerd. Het slechtst scoren de sectoren transport en direct marketing. Wat verder opvalt is dat de bedrijven en instellingen met meer dan 100 werknemers beduidend beter hebben gereageerd dan de overige groepen.

Tabel 2 Verdeling respondenten over typen organisaties en aantal werknemers[174]

	Aantal werknemers				Totaal
	0-19	20-49	50-99	100+	
Detailhandel	3	0	1	2	6
Direct marketing	0	1	0	2	3
Zakelijke + fin. dienstverlening	6	2	1	11	20
Transport	1	0	1	1	3
Communicatie en ICT	1	5	1	1	8
Onderwijs	0	6	1	5	12
Gezondheidszorg	2	2	2	10	16
Centrale overheid	0	0	1	4	5
Decentrale overheid	1	0	1	7	9
Totaal	14	16	9	43	82

De bovenstaande verdeling heeft tot gevolg dat de uitspraken die op basis van de enquête onder *organisaties in het algemeen* weinig zicht geeft op een groot deel van de organisaties in Nederland. Gedeeltelijk gaat dit om organisaties waarvan het nagenoeg zeker is dat zij veel persoonsgegevens verwerken, zoals de categorie direct marketing. Voor een ander deel gaat het om organisaties als de detailhandel, die waarschijnlijk weinig persoonsgegevens verwerken. Het is te verwachten dat vooral organisaties die affiniteit hebben met bescherming van persoonsgegevens hebben gereageerd. De enquête geeft dan ook geen representatief beeld, maar laat een topje van de ijsberg zien. Dat betekent dat de resultaten informatief kunnen zijn als indicatie voor bijvoorbeeld beweegredenen van bepaalde acties, maar dat er geen absolute waarde aan kan worden toegekend.

4.2.2 Meldende organisaties

Bij de enquête onder de meldende organisaties is eveneens gekozen voor een gestratificeerde steekproef. In het Cbp meldingenbestand waren in 2007 in totaal 32.349 meldingen aanwezig. Een beperkt deel van de organisaties heeft meer dan één melding gedaan, waardoor de populatie van organisaties in het meldingenregister iets lager zal uitvallen. Er is door het Cbp een groot aantal organisaties aangeschreven die vallen in de categorieën bedrijven, overheid en maatschappelijke instellingen en semi-overheden (zoals gezondheidszorg- en onderwijsinstellingen). Per categorie is door het Cbp aan ruim 300 organisaties een mail gestuurd met de vraag of zij willen meewerken aan het onderzoek. Er is gekozen voor een opt-outsysteem, organisaties moesten reageren als zij niet mee wilden werken. Dit heeft ertoe geleid dat er 216 bedrijven, 291 overheidsinstellingen en 280 maatschappelijke instellingen en semi-overheden zijn overgebleven in de uiteindelijke selectie. Deze 787 organisaties hebben een mail gehad waarin zij werden verwezen naar een internetsite met daarop een vragenlijst. In 140 gevallen bleek het mailadres niet te kloppen en deze organisaties hebben daardoor geen mailing gehad. 159 organisaties hebben een bruikbare respons geleverd. Dit komt neer op een respons van 25 procent. De volgende typen organisaties zijn teruggevonden in de respons.

[174] Aantal ontbrekende gegevens = 1.

Tabel 3 Respons per type organisatie (meldende organisaties)

Organisatietype	Aantal	Percentage
Bedrijven	35	22
Overheden	50	31
Maatschappelijke instellingen en semi-overheid	74	47
Totaal	159	100

Niet alle organisatietypen hebben even goed op het verzoek om aan de enquête deel te nemen gereageerd. De maatschappelijke instellingen en semi-overheden hebben verhoudingsgewijs goed gereageerd op onze enquête, het bedrijfsleven heeft beduidend minder gereageerd. De respons van de overheid is met een relatief aandeel van een derde ongeveer zoals dat kon worden verwacht, omdat ook éénderde van de aangeschreven organisaties tot de overheid behoort. Zoals uit Tabel 4 blijkt, is de sterke respons van de maatschappelijke instellingen en semi-overheid vooral te danken aan de instellingen in de gezondheidszorg. Ook de decentrale overheden zijn relatief goed vertegenwoordigd. De grootste categorie van het bedrijfsleven zijn de zakelijke en financiële dienstverlening en communicatie en ICT. Dit was ook in de enquête onder de *bedrijven in het algemeen* een groep die relatief goed gereageerd heeft.

Tabel 4 Verdeling van de respondenten over typen organisaties (meldende organisaties)

Organisatie	Percentage
Gezondheidszorg	38
Decentrale overheid	27
Zakelijke of financiële dienstverlening, uitzendbureau's en beveiliging	7
Centrale overheid	4
Onderwijs	4
Communicatie en ICT	3
Overig (divers)	17
Totaal	100

De gestratificeerde steekproeftrekking in combinatie met de enigszins scheve respons heeft gevolgen voor de conclusies die kunnen worden getrokken. Er kan worden verwacht dat vooral de organisaties met affiniteit voor bescherming van persoonsgegevens hebben gereageerd. Net zo min als we op basis van Tabel 4 kunnen stellen dat 27 procent van de meldende Nederlandse organisaties behoren tot de decentrale overheid, kunnen we geen absolute waarde toekennen aan de uitkomsten van de enquête. De enquêtes geven wel goed inzicht in de beweegredenen en acties van organisaties die (waarschijnlijk) relatief veel waarde hechten aan bescherming van persoonsgegevens.

4.2.3 Organisaties met een FG

In de enquête onder de *organisaties met een FG* is getracht de totale populatie te benaderen. De FG's zijn benaderd op basis van het openbare register zoals dat op de website van het Cbp staat. Alle 215 FG's zijn aangeschreven om een enquête in te vullen. Van vijf FG's bleek het adres niet meer actueel te zijn. In totaal hebben 210 FG's de mogelijkheid gehad om een enquête in te vullen. Van deze FG's hebben 71 een enquêteformulier ingevuld. 45 FG's hebben het formulier schriftelijk ingevuld en 26 via Internet. Twee formulieren bleken voor

het computerprogramma onleesbaar te zijn. Omdat niet meer te achterhalen viel wat de FG's op deze formulieren hebben ingevuld, blijft een bruikbare respons over van 69. Dit komt neer op een percentage van 34 procent. FG's werken voor een breed scala aan organisaties. De volgende verdeling over typen organisaties is gevonden:

Tabel 5 Verdeling respondenten over typen organisaties

Organisatie	Aantal	Percentage
Decentrale overheidsorganisatie	18	26
Gezondheidszorg	11	16
Centrale overheidsorganisatie	10	14
Onderwijsinstelling	7	10
Overig[175]	23	37
Totaal	69	100

Zoals uit Tabel 5 blijkt zijn (semi) overheden goed vertegenwoordigd in deze selectie. Van zes organisaties is met zekerheid komen vast te staan dat het om het bedrijfsleven gaat en er heeft één belangenvereniging / stichting gereageerd. Mogelijk is het aantal bedrijven nog wat hoger omdat er in de vragenlijst een categorie 'overig' is opgenomen die door 14 FG's is ingevuld. Overigens zijn in de populatie van 240 FG's verreweg de meeste in dienst van een (semi) overheid. De verdeling in de respons wijkt hierin dus niet veel af van die van de totale populatie.

4.3 Kenmerken van organisaties

4.3.1 Grootte van de organisatie

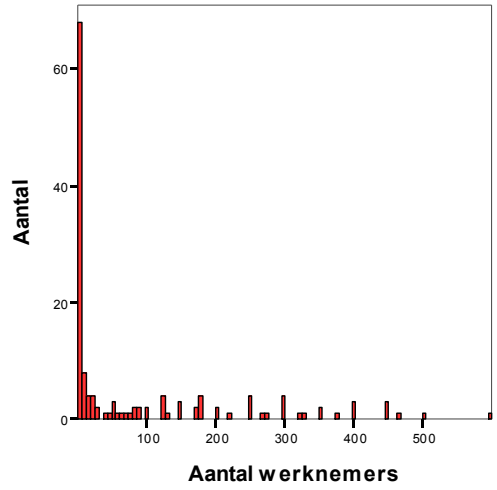
De *organisaties in het algemeen* hebben een mediaan van 100 medewerkers. Het is echter weinig zinvol waarde toe te kennen aan deze mediaan. We hebben gezien dat er in de enquête onder *organisaties in het algemeen* een gestratificeerde steekproef is getrokken, waarin een onderverdeling naar bedrijfsgrootte is gemaakt en waardoor de grote organisaties zijn oververtegenwoordigd. Dit was een bewuste keuze omdat door de opdrachtgever werd verondersteld dat de kans dat kleine organisaties te maken zouden hebben met de Wbp gering was. Bovendien hebben we gezien dat zelfselectie heeft plaatsgevonden waardoor de 100+ organisaties zijn oververtegenwoordigd.

[175] De categorie overig bestaat uit een groot aantal categorieën organisaties, die allemaal slechts één of twee maal voorkomen. Voorbeelden zijn automatiseringsbedrijven (2 maal), ICT-bedrijven (2 maal), verzekeraars (1 maal), een belangenvereniging/stichting (1 maal), een beveiligingsbedrijf (1 maal), een brancheorganisatie (1 maal).

Tabel 6 Organisatiegrootte en spreiding in de grootte (organisaties in het algemeen, meldende organisaties en organisaties met een FG)

	Organisaties in het algemeen[176]	Meldende organisaties	Organisaties met een FG
Gemiddelde	(414)	271	2698
Mediaan	(100)	15	775
Standaarddeviatie	(1245)	814	6537
Minimum	(1)	0	3
Maximum	(10000)	8000	42000

De organisaties die een melding doen zijn in ieder geval over het algemeen betrekkelijk klein. Het mediane aantal werknemers bedraagt 15.[177] Dat betekent dat 50 procent van de responderende organisaties 15 werknemers of minder heeft (zie Figuur 2). De veronderstelling vooraf dat vooral grote organisaties te maken hebben met de Wbp blijkt daarmee onjuist te zijn. De onderstaande figuur laat de verdeling van het aantal medewerkers per organisatie zien. We zien hier de sterke vertegenwoordiging van betrekkelijk kleine organisaties.



Figuur 2 Aantal werknemers (meldende organisaties)[178]

Uit het onderzoek komt naar voren dat de organisaties die over een FG beschikken qua grootte fundamenteel afwijken van de overige organisaties. FG's zijn voornamelijk te vinden bij grote organisaties, maar de spreiding is erg groot en varieert van 3 tot 42000 werknemers. De mediaan van bedrijven met een FG komt uit op 775 werknemers.[179] Daarmee zijn de

[176] De centrum- en spreidingsmaten voor de organisaties in het algemeen hebben weinig betekenis, omdat in deze steekproeftrekking binnen vier categorieën van een bepaalde organisatiegrootte is geselecteerd. Daardoor is er een enorme overschatting van het aantal grote organisaties.
[177] De respondenten vertegenwoordigen een organisatie waarin gemiddeld 271 werknemers werkzaam zijn. Dit gemiddelde wordt nogal sterk omhoog getrokken door een klein aantal zeer grote organisaties.
[178] Organisaties met meer dan 600 werknemers worden in deze verdeling statistisch aangemerkt als 'extreme waarden'. Deze organisaties zijn omwille van de leesbaarheid van de grafiek weggelaten.
[179] Gemiddeld vertegenwoordigen de ondervraagde FG's een organisatie met 2698 werknemers. Dit gemiddelde wordt echter 'scheefgetrokken' door twee zeer grote organisaties.

organisaties die een FG hebben meer dan 50 maal zo groot als de organisaties die alleen maar een melding doen.

4.3.2 Privacydeskundigheid

Kennis van de Wbp is essentieel voor een goede uitvoering van het privacybeleid in deze wet. Alle respondenten uit de *organisaties in het algemeen* hebben van de Wbp gehoord. Bijna driekwart van de ondervraagden geeft aan goed op de hoogte te zijn van de Wbp en de overigen geven aan wel eens van de Wbp gehoord te hebben, maar niet precies te weten wat er in staat.

Anders dan bij de organisaties die over een FG beschikken, is er bij de overige organisaties meestal geen deskundige op het gebied van privacy in dienst (zie Tabel 7). De *organisaties in het algemeen* en de *meldende organisaties* laten hierin een vergelijkbaar beeld zien. Het is opvallend dat 7 procent van de *meldende organisaties* een FG in dienst heeft, terwijl zij toch hebben gekozen voor melding bij het Cbp. Strikt genomen was dit niet nodig en volstond een melding bij de FG. De belangrijkste reden om geen privacydeskundige te benoemen is dat de organisatie zichzelf daarvoor te klein acht. Dit argument wordt door 60 procent van de *organisaties in het algemeen* zonder privacydeskundige aangevoerd. Zo'n 17 procent van deze organisaties geeft aan dat ze nauwelijks persoonsgegevens verwerken en 15 procent laat zich ondersteunen door een externe adviseur. Daarnaast worden nog tal van andere redenen voor het niet hebben van een privacydeskundige aangevoerd. De meest voorkomende redenen voor het ontbreken van een privacydeskundige zijn dat er een privacyprotocol bestaat en een deskundige daarom niet nodig wordt geacht (8 procent) of dat meerdere of alle werknemers zelf op de hoogte zijn van de Wbp en daarnaar handelen (5 procent). Een privacydeskundige is verder afwezig omdat het bedrijf uit slechts één persoon bestaat, de adressen niet in het bezit zijn van de ondervraagde organisatie of omdat privacy onderdeel is van het veiligheidsbeleid en is ondergebracht bij de security officer (allemaal in 1 procent van de gevallen).

Een privacyofficer is een werknemer die bescherming van privacy in zijn takenpakket heeft, maar die niet is aangemeld bij het Cbp en geen toezichthoudende bevoegdheden heeft. Een privacyofficer kan de enige privacyfunctie binnen een organisatie zijn, maar privacyofficers kunnen ook naast een FG functioneren. Wanneer er een FG in dienst van de organisatie is, komt het in 13 procent van de gevallen voor dat er privacyofficers zijn aangesteld. De hoofdreden die hiervoor wordt gegeven is dat de organisatie te groot of te gespreid is om door één FG te kunnen worden bediend. Op deze manier wordt getracht tot een spreiding van de werklast te komen.

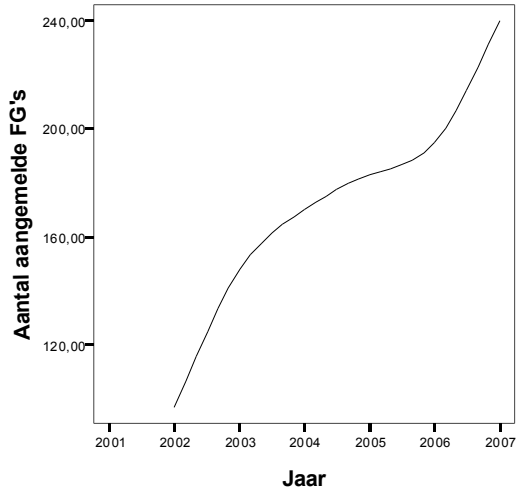
Tabel 7 Privacydeskundigheid (organisaties in het algemeen, meldende organisaties en organisaties met een FG)

	Organisaties in het algemeen Percentage	Meldende organisaties Percentage	Organisaties met een FG Percentage
Geen privacydeskundige	69	59	0
Privacydeskundige	21	30	-
FG	6	7	100
Privacyofficer	4	4	13
Totaal	100	100	

Lidmaatschap van een branche kan belangrijk zijn omdat de branchevereniging organisaties een helpende hand kan bieden, bijvoorbeeld door het verschaffen van specifiek op de branche toegesneden informatie of door het opstellen van een eigen privacycode. Binnen de groep van de *organisaties in het algemeen* is 53 procent van de organisaties lid van een branche. In 45 procent van die gevallen heeft de branche een eigen privacycode en in 2 procent van de gevallen wordt nog aan een privacycode gewerkt. In 19 procent van de gevallen is komen vast te staan dat zo'n code er niet is. Opvallend is dat 32 procent van de ondervraagden het antwoord op deze vraag niet weet. Blijkbaar leven privacycodes bij deze bedrijven niet erg. Van de organisaties die de privacycode van de branche kennen, hanteert ruim vier op de vijf deze code ook. Van alle organisaties hanteert 36 procent een eigen privacycode die los staat van een branche. Samenvattend betekent dit dat ruim de helft van de ondervraagde organisaties al dan niet via de branchevereniging een privacycode hanteert.

4.4 De Functionaris voor de Gegevensbescherming

Een specifieke deskundige op het gebied van privacy is de FG. De Wbp ziet de FG vooral in een toezichthoudende rol waarvoor hij wettelijke bevoegdheden heeft gekregen. Naast een toezichthoudende rol zal de FG veel deskundigheid over de privacyaspecten op kunnen bouwen, waardoor het voor de hand ligt dat hij in de praktijk tevens een informele voorlichtings- en adviesrol op zich neemt. In art. 64 Wbp wordt aangegeven dat de FG aanbevelingen aan de verantwoordelijke kan doen ter bescherming van de verwerkte persoonsgegevens. Organisaties kunnen op vrijwillige basis een FG benoemen en dienen deze aan te melden bij het Cbp.[180] Wanneer een FG wordt aangesteld neemt deze een deel van de taken van het Cbp over, die zich op haar beurt meer zal gaan opstellen als een tweede lijnstoezichtshouder. De FG wordt dus aangesteld en betaald door de organisatie zelf en houdt toezicht op en geeft advies aan de organisatie waarvoor hij werkzaam is.

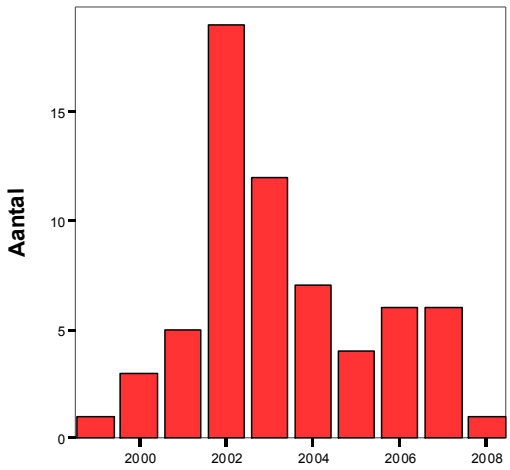


Figuur 3 Aantal aangemelde FG's[181]

[180] In een enkel geval – bij de IB-Groep – bestaat daartoe een bijzondere wettelijke plicht (zie art. 8a Wet verzelfstandiging informatiseringsbank).
[181] Bron: jaarverslagen Cbp

Figuur 3 toont het totale aantal aangemelde FG's sinds de inwerkingtreding van de Wbp in 2001 zoals dat in de jaarverslagen van het Cbp te vinden is (dus de ontwikkeling van de totale populatie FG's). Sinds de inwerkingtreding van de Wbp is het aantal FG's van jaar tot jaar gegroeid. Meteen in het 2001 hebben zich enkele tientallen FG's bij het Cbp geregistreerd en in 2007 waren het er volgens het jaarverslag 2007 240. Begin 2008 waren er 215 FG's in het online register op www.cbpweb.nl opgenomen. Klaarblijkelijk geeft het online register geen volledig of actueel overzicht.

Ondanks de groeiende trend van het aantal FG's is – gezien het grote aantal bedrijven, instellingen en andere organisaties in Nederland dat persoonsgegevens verwerkt – het aantal FG's nog bijzonder laag te noemen. Uit de enquête onder de FG's blijkt dat deze functie niet erg populair is bij de ondervraagde organisaties. De hoofdreden waarom deze vorm van zelfregulering zo moeizaam van de grond komt, is dat de organisaties privacy weliswaar belangrijk vinden, maar dat er geen behoefte bestaat aan een interne toezichthouder (41 procent van de *organisaties in het algemeen* geeft dit aan). Een andere belangrijke reden is onbekendheid. Van de ondervraagde organisaties geeft 14 procent aan niets van het bestaan van FG's af te weten. Daarnaast worden talloze andere redenen gegeven, waarvan de meeste er op neer komen dat het onderwerp privacy al ergens in de organisatie is ondergebracht. De meerwaarde van het benoemen van een FG wordt niet direct ingezien.



Figuur 4 Het jaar waarin een FG is aangesteld (organisaties met een FG)

Bij de organisaties die wel een FG hebben benoemd is doorgevraagd naar de manier waarop deze functie wordt ingevuld. Figuur 4 laat zien in welk jaar de functie van FG is geïntroduceerd bij de geënquêteerde organisaties.[182] We zien duidelijk dat het grootste aantal van de ondervraagde FG's direct na de inwerkingtreding van de Wbp in september 2001 is aangesteld. In de jaren daarna loopt het aantal nieuwe organisaties met een FG snel terug. Opvallend is dat enkele respondenten aangeven dat er al een FG was benoemd voordat de

[182] De gegevens die de basis van deze figuur vormen zijn afkomstig uit de enquête onder de FG's. Omdat hier slechts een deel van de populatie wordt bekeken, zijn de gegevens uit figuur 4 niet te vergelijken met die uit figuur 3.

Wbp in werking was getreden, en dus feitelijk voordat de functie bestond. Mogelijk is hier sprake van anticipatie. Een andere mogelijkheid is dat er sprake is van verwarring (in jaar of type functie). Ongeveer de helft van de FG's geeft aan dat zij direct vanaf de inwerkingtreding van de Wbp als zodanig werkzaam zijn.

De redenen voor benoeming van een FG zijn uiteenlopend. De belangrijkste reden voor benoeming van een FG is – volgens de FG's zelf – omdat binnen de organisatie een groot belang wordt gehecht aan bescherming van privacy. In ongeveer 50 procent van de gevallen is dit als hoofdreden genoemd. In 10 procent van de gevallen was vermindering van de toezichtlast van het Cbp de belangrijkste reden om een FG te benoemen. Door een FG te benoemen hopen deze organisaties niet meer aan toezichtacties van het Cbp te worden onderworpen. Zeven procent geeft aan dat een goed en beveiligd informatiebeheer van groot belang is en een FG past daar blijkbaar bij.

Bijna alle FG's zijn intern geworven en al dan niet na een interne sollicitatieprocedure aangesteld. Slechts één van de ondervraagde FG's kwam van buiten de organisatie. De FG kan op vele manieren binnen de organisatie gepositioneerd zijn. Het vaakst is de FG onderdeel van de juridische staf (26 procent), iets minder vaak is hij onderdeel van de centrale directie (23 procent). In 13 procent van de gevallen is de FG ingedeeld bij de afdeling die zich bezighoudt met kwaliteitszorg. De overige posities van de FG's zijn erg divers. Waar de FG ook gepositioneerd is, zijn onafhankelijkheid is een groot goed. Art. 63 lid 2 Wbp stelt dat de FG voor wat betreft de uitvoering van zijn functie geen aanwijzingen kan ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. Zeer opvallend is dat ondanks het wettelijke verbod bijna een kwart van de FG's aangeeft verplicht te zijn aanwijzingen van de leiding op te volgen. Dit lijkt in tegenspraak te zijn met de onafhankelijke positie die de FG volgens de Wbp hoort te hebben. Het kan echter ook zijn dat de FG voor een beperkt deel van zijn tijd FG-taken uitvoert en voor een ander deel van zijn tijd een andere functie heeft waarin hij wel ondergeschikt is aan zijn leidinggevende. Anderzijds hebben FG's op een expertmeeting wel aangegeven dat het soms lastig is om onafhankelijk tegen de eigen werkgever op te treden.

De Wbp stelt geen specifieke eisen aan de opleiding van FG's. De enige eis die wordt gesteld is dat hij over 'toereikende kennis beschikt' (art. 63 lid 1 Wbp). Een klacht die zeer expliciet door één van de FG's is geuit, is dat er nauwelijks toegesneden cursussen worden aangeboden. Dat deze cursussen wel bestaan blijkt uit het feit dat 10 procent van de FG's jaarlijks ten minste één maal wordt bijgespijkerd. 38 procent van de FG's geeft aan dat zij ten minste één maal een gerichte cursus of opleiding hebben gevolgd. 35 procent krijgt deze opleidingen wel aangeboden, maar maakt hiervan geen gebruik en 13 procent van de FG's krijgt deze cursussen zelfs niet aangeboden.

FG's zijn verplicht een jaarverslag op te stellen. In 2007 is door 41 procent van de FG's géén jaarverslag opgesteld. Wanneer wel een jaarverslag is opgesteld, werd dit door 64 procent van de FG's naar het Cbp gestuurd. Het blijkt dat het Cbp nogal verschillend op deze jaarverslagen reageert. In 35 procent van de gevallen is er geen reactie van het Cbp. In 26 procent van de gevallen ontvangt de FG een ontvangstbevestiging van het Cbp. In 9 procent van de gevallen geeft het Cbp een formele reactie en in 30 procent van de gevallen is de reactie inhoudelijk.

De toegankelijkheid van het jaarverslag voor het grote publiek verschilt sterk. In 23 procent van de gevallen waarin een FG een jaarverslag maakt, wordt dit jaarverslag niet gepubliceerd

en is dit voor het publiek niet opvraagbaar. In 31 procent van de gevallen is het rapport in principe niet openbaar, maar er wordt aangegeven dat het desgevraagd kan worden opgestuurd. Een kwart van de jaarverslagen wordt op papier uitgegeven en is voor het publiek openbaar en 23 procent van de jaarverslagen is voor iedereen toegankelijk op Internet.

Inhoudelijk komt een divers aantal onderwerpen aan bod in de jaarverslagen van de FG's (zie Tabel 8). Onderwerpen die in meer dan de helft van de jaarverslagen te vinden zijn, zijn voorlichting en advisering door de FG's, de invulling van de toezichtfunctie door de FG, privacy van medewerkers en beveiliging van gegevens. Er wordt relatief weinig kwantitatief inzicht gegeven. Dat geldt zowel voor het aantal geconstateerde overtredingen en interventies, alsmede de aantallen vragen, klachten en formele procedures door betrokkenen. Ook het onderwerp gegevensuitwisseling met derden komt niet vaak aan de orde. Het lijkt erop dat de FG's in hun jaarverslagen graag kwalitatieve informatie geven, waarbij vooral wordt ingegaan op de (niet wettelijke) voorlichtende en adviserende rol van de FG.

Tabel 8 Onderwerpen in het jaarverslag van FG's (organisaties met een FG)

Onderwerp in jaarverslag	Percentage van de jaarverslagen
Advisering door de FG	78
Voorlichting door de FG	73
Invulling van toezicht	63
Beveiliging van gegevens	59
Privacy van medewerkers	54
Privacy van klanten/burgers	46
Aantal klachten, verzet en beroep	42
Aantal inzage/correctie	34
Aantal geconstateerde overtredingen	34
Gegevensuitwisseling met derden	32
Aantal interventies door de FG	20

Het geven van informatie over overtredingen die door de FG worden geconstateerd lijkt bij veel FG's gevoelig te liggen. In veel gevallen zijn over dit onderwerp vragen overgeslagen. Toch zijn er enkele bruikbare resultaten (zie Tabel 9). Gemiddeld worden jaarlijks 1,4 overtredingen geconstateerd door de FG. Volgens de *organisaties met een FG* zijn deze overtredingen vooral te wijten aan de onwetendheid van de werknemers die met de gegevens werken. Zoals te verwachten besteedt een FG daarom relatief veel tijd aan het uitoefenen van zachte handhavingsdruk, zoals het geven van uitleg en voorlichting. Naarmate de handhavende activiteit zwaarder wordt, komt zij minder vaak voor. Dit is te zien in Tabel 9.

Het bovenstaande duidt erop dat FG's nadruk leggen op de (informele) rol van interne deskundige en adviseur. Hieruit volgt niet direct dat ten onrechte geen toezicht wordt uitgeoefend. Wellicht gaat er niets mis en zijn zwaardere handhavingsinstrumenten niet nodig, maar het is ook goed mogelijk dat werkelijk toezichthoudend optreden weinig uit de verf komt. Bij meer toezichthouders (bijvoorbeeld de bedrijfsinterne milieucoördinator) komt voor dat zij door voorzichtig te opereren, voorlichting en informatie te geven en zachte druk uit te oefenen een organisatie stukje bij beetje de goede richting proberen uit te duwen.

Tabel 9 Handhavingsactiviteiten door FG's (organisaties met een FG)

Inzet handhavingsinstrumenten	Gemiddeld aantal keer per jaar
Voorlichting geven aan persoon	5,28
Overleggen met persoon	2,91
Persoon rechtstreeks aanspreken	2,24
Informele druk uitoefenen op persoon	1,00
Inlichtingen vorderen	0,71
Binnentreden van ruimtes (verplaatsen naar boven, na inlichtingen vorderen)	1,00
Inzage in stukken vorderen	0,59
Een onderzoek naar een overtreding instellen	0,65
Overtreding aan leidinggevende melden	0,56
Overtreding aan externe toezichthouder (Cbp) melden	0,02

4.5 Databases en verwerkingen

4.5.1 Aantal databases

Het aantal databases van de verschillende organisaties is weergegeven in Tabel 10. De doorsnee *organisaties in het algemeen* hebben 3 databases met persoonsgegevens (mediaan). Per organisatie kan één van deze databases worden geraadpleegd door functionarissen van andere organisaties. 91 procent van de databases is binnen de eigen organisatie aanwezig.

Tabel 10 Aantal databases met persoonsgegevens en hun spreiding (organisaties in het algemeen, meldende organisaties en organisaties met een FG)

	Organisaties in het algemeen	Meldende organisaties	Organisaties met een FG
Gemiddeld	15	47	62
Mediaan	3	3	12
Standaarddeviatie	60	278	130
Minimum	0	1	1
Maximum	500	2850	750

Ook bij de *meldende organisaties* ligt de mediaan op 3 databases.

Duidelijk hoger liggen de aantallen databases bij de *organisaties met een FG*. Het mediane aantal databases waarop – volgens de FG's – de Wbp van toepassing is, is 12. De FG's geven aan dat op 5 databases de meldingsplicht van toepassing is (mediaan) en dat 5 databases zijn vrijgesteld van melding (mediaan). Het feit dat FG's meer databases met persoonsgegevens waarnemen kan enerzijds een aandachtsaspect zijn. Omdat zij zich intensief met privacyaspecten bezig houden, zijn zij mogelijk meer gespitst op het waarnemen van databases. Anderzijds is het gezien de aard van de functie van de FG logisch dat de organisaties die een FG hebben benoemd een bijzondere groep vormen die relatief veel persoonsgegevens verwerken.

4.5.2 Uitwisseling persoonsgegevens

Door ongeveer tweederde van de *organisaties in het algemeen* worden persoonsgegevens gedeeld met derden. Het overige eenderde deel van de organisaties doet dat niet. De overheid is de grootste ontvanger van persoonsgegevens. Ook worden veel persoonsgegevens binnen de eigen organisatie verstrekt. Naar leveranciers, klanten en andere bedrijven worden relatief weinig persoonsgegevens doorgegeven (zie Tabel 11). De vraag of persoonsgegevens aan derden mogen worden verstrekt is voor de *organisaties in het algemeen* niet vaak problematisch. In ruim 70 procent van de gevallen geven de respondenten aan dat ze precies weten wanneer informatie verstrekt mag worden. Waarschijnlijk komt dat omdat er in ruim 80 procent van de gevallen interne regels zijn vastgesteld over het verstrekken van gegevens. Op dit gebied wordt dus geen kennisgebrek ervaren.

Tabel 11 Verstrekking van persoonsgegevens (organisaties in het algemeen)[183]

Met wie worden persoonsgegevens gedeeld?	Organisaties in het algemeen Percentage
De overheid	35
Andere afdelingen / organisatieonderdelen van de eigen organisatie	26
Personeelsleden	17
Klanten	16
Bedrijven	5
Leveranciers	4
Andere organisaties	

De *meldende organisaties* wisselen in veel gevallen geen informatie uit met derden. Gemiddeld kan één database door anderen worden ingezien (mediaan is 0). 37 procent van de *meldende organisaties* raadpleegt databases met persoonsgegevens bij andere organisaties. In een kwart van de gevallen kunnen functionarissen van andere organisaties databases raadplegen die binnen de organisatie van de respondent aanwezig zijn.

De *organisaties met een FG* geven aan dat er met gemiddeld 15 organisaties persoonsgegevens worden uitgewisseld. Ook rondom dit gemiddelde is een grote spreiding; enkele organisaties waarin een FG aanwezig is wisselen geen persoonsgegevens uit, terwijl er ook een organisatie in de steekproef zit die met 100 organisaties gegevens uitwisselt. Een op de drie organisaties waarin een FG in dienst is gebruikt gegevens om op patronen te analyseren (datamining) en een op de vijf organisaties levert gegevens aan andere organisaties ten behoeve van datamining. Er worden uiteenlopende redenen aangegeven waarom de datamining wordt uitgevoerd. Redenen zijn onder meer dat deze analyses worden uitgevoerd ten behoeve van de eigen bedrijfsvoering. Maar ook voor fraude- en criminaliteitsbestrijding, veiligheidsanalyses, wetenschappelijk onderzoek, gezondheidsonderzoek en marketingdoeleinden. Eenmaal is er een wettelijke plicht om dergelijke analyses uit te voeren.

[183] Deze vraag is niet beantwoord door de organisaties met een FG en de meldende organisaties.

4.5.3 Het vullen van databases

Bijna alle databases zijn binnen de *organisaties in het algemeen* zelf aanwezig. De databases worden vooral gevuld met informatie die van de betrokkene zelf is verkregen. In 90 procent van de gevallen worden (een deel van) de persoonsgegevens door de betrokkene zelf verstrekt. In een derde van de gevallen komt (een deel van) de gegevens van een andere organisatie en ook in één op de drie gevallen worden de gegevens verkregen uit eigen onderzoek.

Ook bij de *meldende organisaties* is het gebruikelijk dat de gegevens (gedeeltelijk) van de betrokkene zelf worden gekregen. Dat gebeurde in 61 procent van de gevallen. In 8 procent van de gevallen worden de gegevens gekregen van een andere organisatie en in 6 procent uit eigen onderzoek. In 3 procent van de gevallen slaan de *meldende organisaties* de gegevens van transacties met personen op.

Aan de *organisaties met een FG* zijn geen vragen gesteld over het vullen van de databases.

4.5.4 De inhoud van databases

De eerste vraag die hier gesteld wordt is: 'wie is de betrokkene'? Hoewel er verschillen zijn tussen de *organisaties in het algemeen* en de *meldende organisaties*, is er een aantal categorieën dat vaak voorkomt. In veel databases zijn klanten en werknemers de betrokkenen. Ook gegevens over burgers worden vaak verwerkt (zie Tabel 12). Bij de *meldende organisaties* zien we dat patiënten vaak betrokkene zijn. Deze categorie zien we in de enquête onder *organisaties in het algemeen* niet terug, waarschijnlijk omdat de categorie 'gezondheidszorg' niet expliciet is opgenomen in de selectie. Bij de *meldende organisaties* heeft deze groep juist bijzonder goed gerespondeerd.

Tabel 12 Typen betrokkenen in de databases (organisaties in het algemeen en meldende organisaties)[184]

Personen waarop de verwerking (mede) betrekking heeft	Organisaties in het algemeen Percentage	Meldingen Percentage
Klanten	63	32
Patiënten	-	34
Werknemers	34	13
Burgers	19	31
Leveranciers	8	0
Leerlingen	8	-
Leden	4	5
Anderen	7	14

De volgende vraag die kan worden gesteld is welke gegevens van deze betrokkenen worden verwerkt. Er is aan *organisaties in het algemeen* gevraagd van één belangrijke database aan te geven welke persoonsgegevens worden geregistreerd. Aan de *meldende organisaties* is gevraagd voor één melding aan te geven welke persoonsgegevens worden verwerkt. In Tabel 13 is opgesomd in welk percentage van deze databases welk type gegevens voorkomt. Het is geen verrassing dat naam- en adresgegevens in vrijwel iedere database voorkomen. Er is ook gevraagd naar enkele bijzondere persoonsgegevens. Voor bijzondere persoonsgegevens geldt

[184] Aan organisaties met een FG zijn geen vragen gesteld over specifieke verwerkingen of databases.

binnen de Wbp een streng regime. Art. 16 Wbp geeft een algemeen verbod op het verwerken van bijzondere gegevens. In art. 17 tot en met 22 Wbp worden de uitzondering op het verbod behandeld. Artikel 23 Wbp is de algemene restbepaling. Die bepaling geeft de mogelijkheid om indien het algemeen belang dit vereist en er voldoende waarborgen voor betrokkenen zijn getroffen toch tot verwerking van bijzondere gegevens over te gaan. Het is opvallend dat, ondanks het terughoudende regime, sommige bijzondere persoonsgegevens, zoals een wettelijk identificatienummer, gegevens over gezondheid, godsdienst, ras of etniciteit en strafrechtelijke gegevens in een betrekkelijk groot aantal databases voorkomt.

Tabel 13 Soorten gegevens in de databases (organisaties in het algemeen en meldende organisaties)[185]

Soort gegevens	Organisaties in het algemeen percentage	Meldende organisaties percentage
NAW	100	89
Financiële gegevens	51	27
Wettelijk identificatienummer	48	0
Gezondheid	31	50
Gegevens over gedragingen	31	18
Gegevens over functioneren werknemers of leerlingen	29	13
Betalingsachterstanden	24	17
IP-adres	24	11
Godsdienst of levensbeschouwing	16	9
Ras of etniciteit	11	9
Gegevens over opvattingen	11	8
Strafrechtelijke gegevens	10	10
Overtredingen	9	4
Vakbondslidmaatschap	6	1
Seksuele gedragingen	4	6
Politieke gezindheid	1	3
Andere gegevens	7	22
Weet niet	-	6
Totaal opgeteld (exclusief 'weet niet')	413	297

Als we een vergelijking maken tussen de *meldende organisaties* en de *organisaties in het algemeen*, dan blijkt dat de *meldende organisaties* 28 procent minder persoonsgegevens verwerken dan de respondenten uit de *organisaties in het algemeen*.[186] Ook verwerken de *meldende organisaties* bepaalde gevoelige gegevens duidelijk minder vaak, te weten het wettelijk identificatienummer en gegevens over godsdienst of levensbeschouwing. Het eerste is te verklaren uit het feit dat er veel personeels- en salarisadministraties bij de selectie van de *organisaties in het algemeen* zitten. Deze administraties bevatten weliswaar persoonsgegevens, maar hoeven volgens het Vrijstellingenbesluit in veel gevallen niet gemeld te worden. Daarom komen personeelsadministraties vaak voor in de steekproef van de *organisaties in het algemeen*, terwijl zij niet vaak tussen de meldingen worden gevonden. Bij

[185] Aan organisaties met een FG zijn geen vragen gesteld over specifieke verwerkingen of databases.
[186] In de vragenlijst voor de organisaties met een FG is deze vraag niet gesteld.

de meldingen worden juist relatief veel gegevens over gezondheid verzameld. Waarschijnlijk komt dat omdat in deze enquête instellingen uit de gezondheidszorg sterk oververtegenwoordigd zijn. De overige gevoelige gegevens lopen minder ver uiteen. Dat de *organisaties in het algemeen* meer persoonsgegevens verwerken dan *meldende organisaties* is opvallend. Men zou bij goede naleving van de Wbp verwachten dat de *organisaties in het algemeen* (die in meerderheid geen melding hebben gedaan) een beperkt aantal soorten persoonsgegevens kunnen verwerken dat onder het Vrijstellingenbesluit valt. Mogelijk is het feit dat *meldende organisaties* minder (gevoelige) persoonsgegevens registreren ten dele een gevolg van het melden. Deze redenering past goed bij het feit dat de helft van de *meldende organisaties* aangeeft dat de melding hen bewuster maakt van het privacyaspect en dat een derde van de *meldende organisaties* zegt zorgvuldiger te gaan handelen. In die zin lijkt de meldingsplicht organisaties aan te zetten tot meer privacybewust gedrag.

4.5.5 Het beveiligingsniveau van de databases

Beveiliging van persoonsgegevens is een belangrijk aspect van privacybescherming en daarmee een belangrijk thema in de Wbp. In art. 13 Wbp is vastgelegd dat de verantwoordelijke passende technische en organisatorische maatregelen treft om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Uitgangspunt is dat de beveiliging proportioneel is.

Een eerste vorm van beveiliging is het beperkt houden van de toegang tot de betreffende database. Om dit te realiseren zijn twee stappen nodig. In de eerste plaats moeten personen worden aangewezen die toegang hebben tot de persoonsgegevens. Deze personen worden geautoriseerd om de gegevens te verwerken. In de tweede plaats werkt het toekennen van de toegangsbevoegdheid tot de database alleen als de bevoegde persoon geïdentificeerd kan worden. Het blijkt dat gemiddeld 57 mensen geautoriseerd zijn voor de geselecteerde database. In 38 procent van de gevallen kan de toegang aan een ander worden overgedragen. In 19 procent van de organisaties hebben mensen van buiten de organisatie toegang tot de centrale database. Uit de verkregen gegevens komt verder naar voren dat het vrijwel niet meer voorkomt dat de toegang tot databases onbeveiligd is (in 3 procent van de gevallen). Een toegangscode of wachtwoord is het meest gebruikte identificatiemiddel, gevolgd door een pasje, chip of sleutel. Beveiliging door middel van een biometrisch kenmerk is slechts één maal aangetroffen (zie Tabel 14). Respondenten konden meer redenen aankruisen, zodat de percentages opgeteld niet op 100 procent uitkomen.

Tabel 14 Toepassing van identificatietechnieken (organisaties in het algemeen)[187]

Identificatie door	Organisaties in het algemeen Percentage
Toegangscode of wachtwoord	63
Pasje, chip of sleutel	13
Biometrisch kenmerk	1
Anders	10

Een tweede vorm van beveiliging is de beveiliging van de gegevens zelf. Dit kan bijvoorbeeld door identificerende informatie gescheiden op te slaan, na verzameling te vernietigen of te

[187] Deze vraag is niet gesteld aan de meldende organisaties.

versleutelen. In de enquête is over een viertal privacybeschermende technologieën gevraagd in hoeverre zij worden toegepast. Uit de gegevens blijkt dat autorisatie en identificatietechnieken weliswaar op ruime schaal worden toegepast, maar dat dat nog niet het geval is voor de beschikbare privacybevorderende technieken waarmee de data op een veilige manier kan worden opgeslagen (zie Tabel 15). Respondenten konden meer technieken aankruisen, zodat de percentages tot boven de 100 procent kunnen optellen. De lijst met privacybeschermende technieken is overigens niet uitputtend. Mogelijk past een deel van de organisaties dus andere privacybeschermende technieken toe.

Tabel 15 Toepassing van privacybeschermende technieken (organisaties in het algemeen)[188]

Privacybeschermende techniek	Organisaties in het algemeen Percentage
Privacymanagementsysteem	10
Gescheiden opslaan van identificerende en niet-identificerende gegevens	10
Versleuteling van gegevens	5
Anonimiseren; identificerende gegevens worden niet verzameld of na verzameling vernietigd	4

Bij de organisaties waarbinnen een FG werkzaam is, blijken de beveiligingsmaatregelen beter op orde te zijn. De *organisaties met een FG* hebben van een aantal beveiligingsmaatregelen kunnen aangeven of deze in hun organisatie worden gebruikt. In Tabel 16 zijn deze percentages weergegeven. Respondenten konden meer beveiligingsmaatregelen aankruisen, zodat de percentages tot boven de 100 procent optellen.

Tabel 16 Toepassing van beveiligingsmaatregelen (organisaties met een FG)

Beveiligingsmaatregel	Organisaties met een FG Percentage
Autorisatie en identificatie	
Wachtwoord of pincode	94
Organisatorische controle	90
Fysieke maatregelen voor toegangsbeveiliging	84
Controle op toegekende bevoegdheden	84
Pasje	67
Automatische logging van toegang tot gegevens	67
Biometrisch kenmerk	5
Beveiliging van gegevens	
Vastgesteld en geïmplementeerd beveiligingsbeleid	77
Versleuteling van gegevens	51
Overige beveiligingsmaatregelen (onbekend)	67

Bij de *organisaties met een FG* is een bovengemiddelde aandacht voor beveiliging van data. Dit is niet verwonderlijk omdat het vooral relatief grote organisaties zijn die grote

[188] Deze vraag is niet gesteld aan de meldende organisaties.

hoeveelheden persoonsgegevens verwerken. Duidelijk is dat zowel bij de organisaties zonder FG als bij de *organisaties met een FG* veel aandacht is voor de identificatie van geautoriseerde personen. Beveiliging van de gegevens zelf komt iets minder vaak voor, al scoren de *organisaties met een FG* hier beduidend beter dan de overige organisaties. Een beveiligingsbeleid en encryptie worden relatief vaak door de organisaties met een FG ingezet. Omdat beveiliging van persoonsgegevens proportioneel moet zijn, is er geen vaststaande norm waaraan getoetst kan worden welke mate van beveiliging voldoende is. Dat moet van geval tot geval worden afgewogen. Zowel voor de organisaties met als zonder FG is het op basis van deze gegevens daarom niet mogelijk om te bepalen of de beveiliging van de persoonsgegevens toereikend is.

4.6 De meldingsprocedure

4.6.1 Kennis over de meldingsplicht

Geautomatiseerde verwerkingen en verwerkingen die zijn onderworpen aan een voorafgaand onderzoek die niet in het Vrijstellingsbesluit zijn genoemd, moeten worden gemeld. Melding moet ofwel bij het Cbp gebeuren, ofwel – indien aanwezig – bij de FG. Ongeveer een kwart van de *organisaties in het algemeen* heeft wel eens een melding bij het Cbp gedaan. Zestig procent weet zeker dat dit nooit gebeurd is en 15 procent weet het niet. Organisaties kunnen om allerlei redenen niet overgaan tot het melden van verwerkingen van persoonsgegevens. In de eerste plaats kunnen er geen meldingsplichtige verwerkingen van persoonsgegevens binnen de organisatie plaatsvinden. Dit gaat – volgens de respondenten – in 81 procent van de gevallen op. Maar het niet melden kan ook het gevolg zijn van kennisgebrek. Dit is bij zeven procent van de *organisaties in het algemeen* het geval. Zij geven aan dat zij niet wisten dat deze verplichting bestond. Een derde mogelijkheid is dat niet wordt gemeld omdat er weerstand bestaat tegen deze plicht. Dat is in ten minste vijf procent van de *organisaties in het algemeen* het geval. In deze gevallen geven de respondenten aan dat zij niet hebben gemeld omdat zij vinden dat melding geen enkele meerwaarde voor de privacy oplevert. Zeven procent van de *organisaties in het algemeen* noemt andere redenen. Het lijkt er dus op dat kennisgebrek geen grote rol speelt bij het niet melden van verwerkingen van persoonsgegevens. We moeten echter wel in de gaten houden dat de respons op deze enquête betrekkelijk laag was en dat veel (vooral kleinere) organisaties niet hebben gereageerd. Het ligt voor de hand te veronderstellen dat bij de kleinere organisaties het kennisniveau gemiddeld lager ligt. Het aantal *organisaties in het algemeen* dat onvoldoende kennis heeft, is in de steekproef echter te klein om over het verband tussen kennis en organisatiegrootte statistisch verantwoorde uitspraken te doen. Tevens is in de selectie van cases specifiek gezocht naar groepen die relatief vaak te maken hebben met verwerking van persoonsgegevens. Het werkelijke gemiddelde kennisniveau zou daardoor een stuk lager kunnen zijn.

De *meldende organisaties* hebben allemaal een verwerking gemeld en zijn dus in principe bekend met deze procedure. De doorsnee *meldende organisatie* voert volgens eigen zeggen één verwerking uit die onder het vrijstellingenbesluit valt (mediaan)[189] en hij heeft twee verwerkingen bij het Cbp gemeld (mediaan)[190]. Het blijkt dat de groep *meldende organisaties* betrekkelijk actief met privacyregelgeving bezig is. Op de vraag hoe de *meldende organisatie*

[189] Gemiddelde is 6.
[190] Gemiddelde is 5.

te weten is gekomen dat hij verwerkingen van persoonsgegevens moet melden, geeft ruim de helft aan dat hij zelf de wettelijke ontwikkelingen goed in de gaten houdt. Toch spelen externe partijen, zoals de branchevereniging, het Cbp en collega-bedrijven een belangrijke rol in de kennisoverdracht over het melden van verwerkingen (zie Tabel 17). Respondenten konden meer redenen invullen, zodat de percentages op meer dan 100 procent uitkomen.

Tabel 17 Informatiebron meldingsplicht (meldende organisaties)

Informatiebron meldingsplicht	Meldende organisaties Percentage
Houden wettelijke ontwikkelingen zelf in de gaten	48
Informatie van de branchevereniging	38
Informatie van het Cbp	27
Informatie van collegabedrijven	19
Van algemene media (krant, t.v. e.d.)	15
Specialist in dienst	8
Van externe specialist	7

Wanneer een organisatie een FG heeft aangesteld, hoeft zij geen melding meer te doen bij het Cbp, maar kan er worden gemeld bij de FG. Ongeveer driekwart van de *organisaties met een FG* geeft aan dat de personen die met de persoonsgegevens werken overwegend op de hoogte zijn van de meldingsplicht. In ongeveer een kwart van de gevallen zijn zij niet goed op de hoogte. Geschat wordt door de FG's dat in ongeveer 80 procent van de verwerkingen waarin moet worden gemeld ook een melding plaatsvindt.

4.6.2 Redenen voor melden

Een derde van de *meldende organisaties* zegt precies te weten wat de juridische reden is waarom de gekozen melding gedaan moest worden en de helft geeft aan dit ongeveer te weten. 17 procent van de *meldende organisaties* kende de juridische reden niet. Wanneer wordt gevraagd de juridische reden aan te kruisen, komt er echter geen duidelijk beeld uit wat die juridische reden is geweest. Ongeveer een derde van de respondenten geeft aan dat er bewust geen gebruik is gemaakt van de mogelijkheid tot vrijstelling. De overige juridische redenen zijn nooit ingevuld. Mogelijk waren de *meldende organisaties* bij het zien van deze vervolgvraag met de ingewikkelde juridische formuleringen toch niet meer zeker van hun veronderstelling dat zij de juridische reden van de betreffende melding kenden.

Inhoudelijke redenen om te melden worden wel genoeg door de *meldende organisaties* gegeven. Daarbij scoren vooral de sociaal wenselijke antwoorden goed. In de helft van de gevallen wordt (mede) gemeld omdat de organisatie waarde hecht aan een transparante omgang met persoonsgegevens. In bijna een kwart van de gevallen is gemeld omdat de meldingsprocedure de verantwoordelijke ertoe aanzet nog eens goed over de gegevensverwerking na te denken. 68 procent van de *meldende organisaties* geeft aan te hebben gemeld omdat privacybescherming belangrijk is om het vertrouwen van de klant te behouden. Voor 62 procent is het feit dat het verplicht is een belangrijk argument om te melden. De helft van de *meldende organisaties* meldt omdat zij belang hechten aan een transparante omgang met gegevens. Er worden ook een paar antwoorden gegeven die niet sociaal wenselijk zijn. Zo geeft ongeveer 19 procent aan bang te zijn voor negatieve publiciteit en 11 procent geeft aan bang te zijn voor handhaving door het Cbp als er niet wordt

gemeld. Een zeer kleine minderheid van 6 procent weet niet waarom er is gemeld (zie Tabel 18). Respondenten konden meer redenen aankruisen, zodat de percentages tot boven de 100 procent optellen.

Tabel 18 Inhoudelijke redenen om te melden (meldende organisaties)

Reden	Meldende organisaties Percentage
Privacybescherming is belangrijk om het vertrouwen van de klant te behouden	68
Het moet, het is een wettelijke verplichting	62
Hechten belang aan een transparante omgang met persoonsgegevens	50
Meldingsprocedure dwingt ons nog eens goed na te denken over de gegevensverwerking	23
Risico op negatieve publiciteit wegnemen	19
Risico op handhaving door het Cbp wegnemen	11
Anders	11
Weet niet	6

N = 159, ontbrekende gegevens = 0

Wanneer een verantwoordelijke de beslissing neemt om een verwerking van persoonsgegevens bij het Cbp te melden, leidt dit nauwelijks tot intern verzet tegen het melden. Van de *meldende organisaties* geeft slechts drie procent aan dat er binnen de organisatie personen waren die argumenten *tegen* het melden van de verwerking hebben aangevoerd. In één geval werd dit gedaan door personen die rechtstreeks met de persoonsgegevens werkten. In de andere gevallen is niet bekend welke personen deze argumenten aanvoerden. Een reden die tegen melding is genoemd is dat melden te arbeidsintensief is. Het gaat echter om heel kleine aantallen waaruit geen statistisch verantwoorde conclusies te trekken zijn.

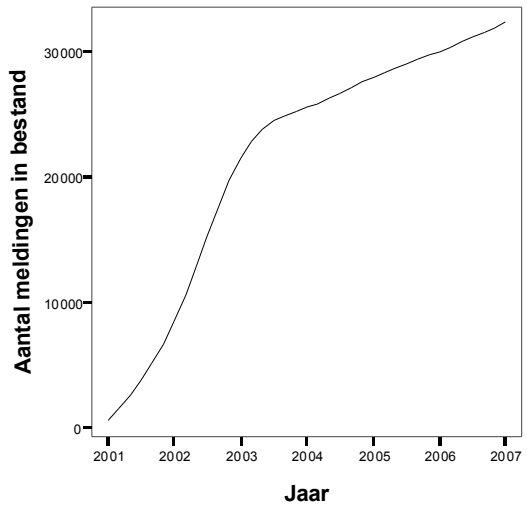
4.6.3 Hoe melden?

Er zijn drie manieren om de melding bij het Cbp in te dienen. Dat kan ‘ouderwets’ via een formulier, of modern via een meldingsprogramma. Dat meldingsprogramma kan van het Cbp worden verkregen op een diskette of via www.cbpweb.nl worden gedownload. In bijna de helft van de gevallen wordt de melding gedaan via het gedownloade meldingsprogramma van het Cbp. In ongeveer een kwart van de gevallen gebeurde dit middels het meldingsformulier en een op de tien instellingen meldde via een diskette. Zo’n 17 procent van de ondervraagden wist het niet meer. De *meldende organisaties* ervaren tussen de drie mogelijkheden om te melden geen verschil in de ingewikkeldheid van de meldingsprocedure.

4.6.4 Aantal meldingen

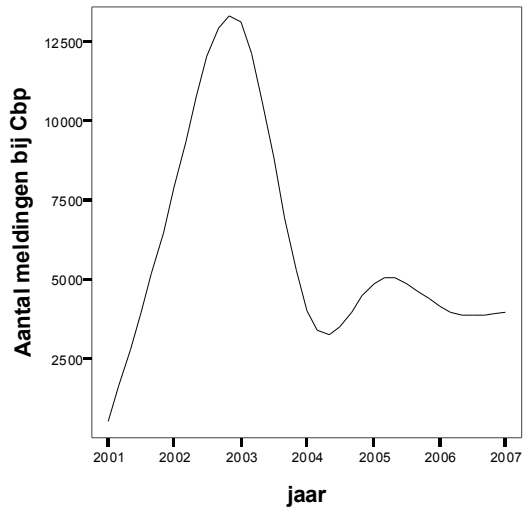
Alle meldingen van verwerkingen van persoonsgegevens die bij het Cbp binnenkomen worden opgenomen in een meldingenregister dat via de website www.cbpweb.nl te raadplegen is. In de loop der jaren is het aantal geregistreerde meldingen enorm gegroeid en hieraan lijkt voorlopig geen einde te komen. In 2007 waren er volgens het jaarverslag 2007

van het Cbp 32.349 meldingen in het register aanwezig. Figuur 5 geeft de kwantitatieve ontwikkeling van het aantal meldingen in dit register weer.



Figuur 5 Kwantitatieve ontwikkeling van het Cbp-meldingenregister[191]

De meldingsplicht is een jaar na inwerkingtreding van de Wbp, dus in 2002, van kracht geworden. In de beginjaren heeft het meldingenregister een enorme groeispurt doorgemaakt. In 2001 zijn 519 meldingen binnengekomen. Het jaar daarop was het aantal meldingen gegroeid tot 7.863 en in 2003 werden er maarliefst 13.083 verwerkingen bij het Cbp gemeld. In de jaren daarna heeft het jaarlijks aantal meldingen zich gestabiliseerd tot een waarde van rond de 4.000 (zie Figuur 6)



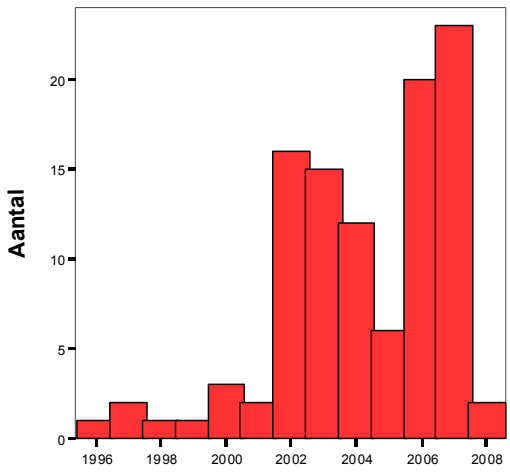
Figuur 6 Aantal meldingen bij het Cbp[192]

[191] Bron: jaarverslagen Cbp.

Het aantal verwerkingen van persoonsgegevens dat bij het Cbp wordt gemeld geeft slechts inzicht in een deel van de meldingsplichtige verwerkingen. Wanneer een organisatie een FG heeft benoemd, kunnen de verwerkingen bij de FG worden gemeld. De FG neemt de meldingen vervolgens op in een eigen register dat door een ieder kostenloos moet kunnen worden geraadpleegd (art. 30 lid 2 Wbp). Een deel van de meldingen wordt derhalve niet centraal geregistreerd door het Cbp, maar decentraal door de FG's. We kunnen door de groeicijfers van het Cbp-meldingenregister te combineren met gegevens uit de enquête onder de *organisaties met een FG* een indicatieve schatting maken van het totale aantal jaarlijkse meldingen en het aandeel van de FG's hierin. FG's geven aan dat er in 2007 gemiddeld 11 verwerkingen bij hen zijn gemeld. Volgens het jaarverslag 2007 van het Cbp waren er in dat jaar 240 FG's benoemd. Als wordt aangenomen dat de groep responderende FG's een representatieve steekproef vormt, dan zouden er bij alle FG's in Nederland 2.640 verwerkingen zijn gemeld. Bij het Cbp zijn in 2007 3.975 meldingen gedaan. In totaal zouden er dan in heel Nederland ongeveer 6.615 verwerkingen zijn gemeld. De FG's namen daarvan bijna 40 procent voor hun rekening.

4.6.5 Leeftijd en actualisering van meldingen

De meldingen in het meldingenbestand hebben een betrekkelijk jonge leeftijd. In Figuur 7 zien we de verdeling van het aantal de meldingen in de tijd. De meeste meldingen zijn voor het eerst gedaan na de inwerkingtreding van de Wbp in 2002. Ook onder de Wpr moesten veel verwerkingen van persoonsgegevens worden gemeld bij de Registatiekamer, en in een minderheid van de gevallen is de eerste melding nog onder het regime van de Wpr gedaan.



Figuur 7 Jaar waarin meldingen zijn gedaan (meldende organisaties)[193]

Het kan nodig zijn om een gedane melding van tijd tot tijd te actualiseren, bijvoorbeeld wanneer gegevens voor een ander doel worden verzameld dan ten tijde van de oorspronkelijke melding. Bij slechts 6 procent van de *meldende organisaties* zijn procedures aanwezig die erop toezien dat meldingen periodiek worden geactualiseerd. Bij 43 procent zijn deze

[192] Bron: jaarverslagen Cbp
[193] Ontbrekende gegevens = 55

procedures niet aanwezig, maar worden meldingen geactualiseerd als dat nodig is. Bij de overige 43 procent van de *meldende organisaties* zijn deze procedures in het geheel niet aanwezig. 8 procent van de *meldende organisaties* wist niet of procedures aanwezig zijn. Meer dan de helft van de meldingen zijn in de afgelopen 5 jaar niet geactualiseerd en ongeveer een derde is één maal geactualiseerd (zie Tabel 19). Dit kan te maken hebben met het afwezig zijn van de noodzaak tot actualisatie door de relatief jonge leeftijd van de meeste meldingen (zie Figuur 7), maar ook met het geconstateerde ontbreken van actualisatie-procedures.

Tabel 19 Aantal actualisaties van meldingen in de afgelopen 5 jaar (meldende organisaties)

Aantal actualisaties in de afgelopen 5 jaar	Meldende organisties Percentage
0	56
1	29
2	9
3	3
4	1
20	1
Totaal	100

4.6.6 Controle op de meldingen

Als een melding is ingediend geeft 69 procent van de ondervraagden aan een ontvangstbevestiging van het Cbp te hebben gehad. In deze ontvangstbevestiging wordt tevens het meldingsnummer aangegeven. 8 procent geeft aan niets van het Cbp te hebben vernomen. Bij geen enkele ondervraagde heeft de melding geleid tot een voorafgaand onderzoek in de zin van artikel 31 van de wet. 10 procent heeft een andere reactie van het Cbp gehad en 13 procent van de ondervraagden wist het niet meer. Het blijkt dat na de ontvangst-bevestiging de rol van het Cbp gewoonlijk is afgelopen. Een inhoudelijke reactie van het Cbp of een voorafgaand onderzoek naar aanleiding van de melding is in ons bestand nooit aangetroffen. Uit de enquêteresultaten kan niet worden afgeleid dat het Cbp een actieve rol vervult in de controle op de kwaliteit van de meldingen en de handhaving.

In tegenstelling tot het Cbp voeren FG's wel een intensieve controle uit op de meldingen, zo blijkt uit de enquête onder de *organisaties met een FG*. In de helft van de gevallen wordt gekeken of de feitelijke verwerking daadwerkelijk overeenkomt met het in de melding gestelde doel. Slechts in een beperkt aantal gevallen wordt de melding in het geheel niet gecontroleerd (Zie Tabel 20).

Tabel 20 Controle van meldingen door de FG (organisaties met een FG)[194]

	Organisaties met een FG Percentage
Controle of de feitelijke verwerking overeenstemt met het doel bij iedere melding	48
Controle op papier of een plausibel en concreet doel is opgenomen	27
Steekproefsgewijs wordt nagegaan of de feitelijke verwerking in overeenstemming is met het doel	15
Meldingen worden niet gecontroleerd	10
Totaal	100

4.6.7 Positieve effecten van de meldingsplicht

De meldingsplicht zou moeten leiden tot een grotere transparantie en betere mogelijkheden voor burgers om de regie over hun gegevens te kunnen voeren. Het is dan ook opvallend dat 46 procent van de *meldende organisaties* van mening is dat de melding bij het Cbp er niet toe bijdraagt dat betrokkenen beter zicht hebben op de gegevens die over hen worden verzameld. In 24 procent van de gevallen denkt de respondent dat melding wel een verbetering teweegbrengt. De overige 30 procent weet het niet. Van de 38 respondenten die vinden dat de meldplicht meer inzicht geeft voor betrokkenen denkt een kwart dat dat komt omdat de melding is opgenomen in een goed en transparant register dat voor iedereen opvraagbaar is. Een op de drie geeft aan dat het komt omdat de doelstelling en de omschrijving van de gegevensverwerking erg helder omschreven is in de melding en een kleine 40 procent omdat zij zelf bekendheid geven aan het bestaan van het meldingenbestand. Van de personen die denken dat betrokkenen niet meer inzicht krijgen in de gegevensverwerking denkt 39 procent dat de betrokkenen de Cbp-website met het meldingenregister niet kennen. 41 procent denkt dat de betrokkene niet geïnteresseerd is in de gegevensverwerking en om die reden niet zal zoeken naar de melding. Een zeer kleine minderheid van 6 procent vindt het meldingenregister niet goed doorzoekbaar en een zelfde percentage vindt de inhoud van de meldingen te summier om een goed beeld te geven. Daarnaast worden nog enkele zeer uiteenlopende redenen gegeven. 8 procent van de respondenten weet niet waarom betrokkenen door het meldingsregister niet meer inzicht krijgen in de gegevensverwerking. Het merendeel van de *meldende organisaties* is derhalve kritisch over de positieve effecten van het melden.

Naast het vergroten van de transparantie voor de betrokkene, zou de meldingsplicht een positief effect kunnen hebben op het denken en handelen van de verantwoordelijke. De meldingsprocedure kan het privacybewustzijn van de verantwoordelijke in sommige gevallen vergroten. In één op de drie gevallen heeft de *meldende organisatie* niet meer zicht gekregen op de doelen en risico's van de verwerking van persoonsgegevens. De helft van de *meldende organisaties* geeft aan door de melding zich meer bewust te zijn van privacyaspecten van de verwerking en bij 8 procent van de *meldende organisaties* heeft het melden ertoe geleid dat de legitimiteit van de doelen om de persoonsgegevens te verzamelen nog eens is heroverwogen. In een derde van de gevallen is men door de meldingsplicht zorgvuldiger gaan handelen. De helft van de *meldende organisaties* geeft aan dat er geen feitelijke effecten op de

[194] Ontbrekende gegevens = 2

zorgvuldigheid van handelen zijn geweest en 15 procent weet het niet. In paragraaf 4.5.4 hadden we al gezien dat *meldende organisaties* minder persoonsgegevens verwerken dan *organisaties in het algemeen*. Het is duidelijk dat de meldingsprocedure bij een deel van de *meldende organisaties* leidt tot een heroverweging van het doel en de middelen van de gegevensverwerking.

4.6.8 Administratieve lasten meldingsprocedure

Uit Tabel 21 blijkt dat de complexiteit van de meldingsprocedure door de meeste *meldende organisaties* niet als buitengewoon hoog wordt gezien.

Tabel 21 De ervaren complexiteit van de meldingsprocedure (meldende organisaties)

Complexiteit meldingsprocedure	Percentage
Zeer eenvoudig	3
Eenvoudig	19
Gemiddeld	47
Ingewikkeld	14
Zeer ingewikkeld	4
Weet niet	13

Actal heeft een nulmeting verricht van de administratieve lasten van de Wbp. Actal heeft vervolgens onderzoek laten uitvoeren door het bureau EIM naar de administratieve lasten van de Wbp. Door andere aannames berekent dit EIM-onderzoek op onderdelen hogere administratieve lasten dan de oorspronkelijke nulmeting. In deze onderzoeken wordt onder meer een schatting gemaakt van de tijdsduur die in meldingen wordt gestoken. Bij een melding zonder voorafgaand onderzoek berekent het EIM voor het invullen en opsturen van het formulier 90 minuten. Daarnaast worden nog 10 minuten berekend voor kennisneming van de wet- en regelgeving en 120 minuten voor extern advies om te bepalen of een verwerking onder het Vrijstellingsbesluit valt. In totaal komt EIM zo uit op 3,7 uur per melding. Overigens komt kennisneming van wet- en regelgeving ook voor wanneer de organisatie niet tot een melding komt. Wanneer naar aanleiding van een voorafgaand onderzoek wordt gemeld, berekent EIM 1440 minuten (24 uur) voor het melden.[195]

Uit de enquête onder de *meldende organisaties* in het onderhavige onderzoek blijkt dat de mediane tijd die in de totale meldingsprocedure wordt gestoken, inclusief informatie zoeken, formulering van doelen, heroverwegen van de te verzamelen gegevens en het invullen van het meldingenformulier 6 uur is. De onderstaande tabel geeft aan hoeveel tijd de *meldende organisaties* in de verschillende fasen van de melding steken. Opgemerkt moet worden dat een groot aantal *meldende organisaties* de tijdsinzet voor de deelfasen niet meer kon herinneren.[196] De gegevens in Tabel 22 zijn derhalve zeer indicatief. Opvallend is dat sommige organisaties veel meer tijd in de melding steken dan anderen. Maximaal is er 520 uur in een enkele melding gestoken. Het is opmerkelijk dat voor het invullen van het meldingenformulier en het zoeken van informatie nagenoeg dezelfde waarden worden gevonden als in het EIM-onderzoek. De wat lagere waarde voor de tijdsinzet in het EIM-onderzoek komt omdat in het onderhavige onderzoek een tweetal inhoudelijke stappen, te

[195] Boog e.a 2006, bijlage I.
[196] Het aantal 'missing cases' is 86, ofwel 56 procent.

weten de formulering van doelen en het heroverwegen van te verzamelen gegevens worden meegenomen.

Tabel 22 Tijdsinzet voor de meldingsprocedure (meldende organisaties)

Fase	Tijdsduur in uren (mediaan)
Informatie zoeken	2
Formulering van doelen	1
Heroverwegen van te verzamelen gegevens	1
Invullen van meldingsformulier	1
Overige tijdsinzet	1
Totale tijdsinzet	6

86 procent van de *meldende organisaties* is van mening dat de meldingsprocedure geen enkel tijdseffect heeft gehad op de geplande gegevensverwerking. 13 procent neemt een geringe vertraging waar. Een zeer kleine minderheid van minder dan een procent geeft aan dat er grote vertraging is opgetreden door de meldingsprocedure en een even klein percentage neemt een versnelling waar. Er is (net) geen statistisch significantie relatie tussen de totale tijd die een organisatie inzet om de melding in te dienen en de grootte van de (gepercipieerde) vertraging.[197]

4.7 Rechten van betrokkenen

4.7.1 Informatieverstrekking

Ongeveer 60 procent van de ondervraagden geeft aan dat de privacyregelgeving ertoe heeft geleid dat de organisatie zorgvuldiger omgaat met persoonsgegevens en privacy. Het recht om te weten dat persoonsgegevens verwerkt worden is fundamenteel in de Wbp. Tabel 23 geeft inzicht in de manier waarop de informatieplicht volgens de *organisaties in het algemeen*, de *meldende organisaties* en de *organisaties met een FG* wordt ingevuld. Bij 72 procent van *organisaties in het algemeen* worden betrokkenen geïnformeerd over het feit dat hun gegevens verwerkt worden. Driekwart van de *meldende organisaties* informeert de betrokkenen over de gegevensverwerking.

Voor informatieverstrekking worden de verschillende media door zowel de *organisaties in het algemeen*, de *meldende organisaties* als de *organisaties met een FG* goed gebruikt. De *organisaties in het algemeen* lijken daarbij een wat sterkere voorkeur voor informatie op aanvraagformulieren te hebben dan de overige categorieën. Mogelijk komt dat omdat binnen deze steekproef (semi) overheidsinstellingen sterk vertegenwoordigd zijn. De *organisaties met een FG* maken bij informatieverstrekking aan betrokkenen wat vaker gebruik van Internet. De informatie-intensieve organisaties waarvoor zij werken laten het in vergelijking met de andere groepen minder toe om alle betrokkenen persoonlijk te schrijven (zie Tabel 23).

[197] Nonparametrische correlatie: rho = 0,19, p = 0,062.

Tabel 23 Waar staat informatie over verwerkingen? (organisaties in het algemeen, meldende organisaties en organisaties met een FG)

Informatie over verwerkingen	Organisaties in het algemeen Percentage	Meldende organisaties Percentage	Organisaties met een FG Percentage
Op de website	26	33	51
Op aanvraagformulieren	51	27	35
In folders	24	24	25
Algemene voorwaarden	38	28	23
Persoonlijk schrijven	29	26	16
Anders	13	39	20

De *organisaties in het algemeen* en de *meldende organisaties* die de betrokkenen niet informeren geven daar verschillende redenen voor aan. Vooral bij de *organisaties in het algemeen* is overigens sprake van een zeer klein absoluut aantal respondenten dat aangeeft dat zij de betrokkenen niet informeert. Daarom kan aan deze uitkomst slechts een indicatieve waarde worden toegekend. De belangrijkste reden voor niet informeren door zowel de *organisaties in het algemeen* als de *meldende organisaties* is dat de verantwoordelijke van mening is dat de betrokkenen al op de hoogte zijn. Gezien het feit dat de meeste databases worden gevuld met gegevens die van de betrokkene zelf zijn verkregen, is deze veronderstelling niet onlogisch. Echter, het feit dat gegevens bij de betrokkene worden verzameld, impliceert niet dat de verantwoordelijke aan de meldingsplicht heeft voldaan. De verantwoordelijke moet niet alleen melden dat de gegevens worden verwerkt, maar onder meer ook voor welke doeleinden.

Onbekendheid met de informatieplicht kan ook een reden zijn voor het niet informeren. Door zowel de *meldende organisatie* als de betrokkene wordt het belang van het informeren niet altijd ingezien (zie Tabel 24). De categorie ‘anders’ bij de meldende organisatie bestaat uit een aantal gevarieerde redenen voor het niet informeren. In 8 procent van de gevallen wordt aangegeven dat hier te weinig aandacht aan wordt gegeven en dat dit in de toekomst nog moet worden opgepakt. Een enkele keer is informeren te kostbaar. Eén respondent gaf aan dat de ‘betrokkenen’ niet geïnformeerd hoefden te worden omdat het daarbij gaat om overleden weefseldonoren.[198]

[198] De Wbp is niet van toepassing op overledenen.

Tabel 24 Reden voor niet informeren van betrokkenen (organisaties in het algemeen en meldende organisaties)[199]

Reden voor niet informeren	Organisaties in het algemeen Percentage	Meldende organisaties Percentage
Betrokkenen zijn al op de hoogte	60	39
Wij wisten niet dat dit moet	0	18
Wij vinden het niet van belang	0	15
De database wordt door een andere organisatie beheerd; zij informeren de betrokkenen	7	13
Het informeren van betrokkenen brengt onevenredige kosten met zich mee	0	8
De betrokkenen vinden het niet belangrijk	7	8
Anders	5	25
	N = 15	N = 39

Er kunnen verschillende strategieën worden gevolgd o de database up to date te houden. Als we naar Tabel 25 kijken dan valt op dat veel organisaties een betrekkelijk passieve houding hebben met betrekking tot het actualiseren van de database. In veel gevallen wordt de verantwoordelijkheid om wijzigingen door te geven bij de betrokkene gelegd. Een actieve periodieke screening door de organisatie of het regelmatig sturen van statusinformatie komt maar weinig voor.

Tabel 25 Correctiestrategie (organisaties in het algemeen)[200]

Correctiestrategie	Organisaties in het algemeen Percentage
Mensen moeten op eigen initiatief wijzigingen doorgeven als hun situatie verandert	65
Mensen krijgen periodiek bericht om zelf wijzigingen door te geven	31
Als mensen contact opnemen worden zij met hun gegevens geconfronteerd	21
Periodieke screening	18
Ontvangen regelmatig nieuw bestand van een derde	18
Periodiek overzicht met statusinformatie	12

4.7.2 Acties door betrokkenen

Een vervolgvraag is in hoeverre de invulling van de informatieplicht leidt tot acties van de betrokkenen. Het blijkt dat betrokkenen niet vaak gebruik maken van de formele bevoegdheden die de Wbp biedt om de regie over hun gegevens te voeren. 45 procent van de

[199] Vragen over specifieke verwerkingen en databases zijn niet gesteld aan de FG's. De organisaties met een FG's ontbreken daarom in deze tabel.
[200] Deze vraag is niet gesteld aan de meldende organisaties en de organisaties met een FG.

organisaties in het algemeen geeft aan nooit verzoeken om inzage in de persoonsgegevens te krijgen van betrokkenen. Bij ongeveer een derde van de organisaties gebeurt dat soms. Correctie en aanvulling van gegevens komt iets vaker voor. 22 procent van de organisaties geeft aan dat dit regelmatig voorkomt, bij de helft van de organisaties komt die vraag soms voor en eenvijfde van de organisaties krijgt hier nooit mee te maken. De zwaardere instrumenten zoals officiële klachten, bezwaar of verzet over privacyaspecten komen maar weinig voor, en ook geschilbeslechtingsprocedures bij de rechter, het Cbp en geschillencommissies zijn een zeldzaamheid.

Ook het doorlopen van een meldingsprocedure leidt in veel gevallen niet tot meer vragen van betrokkenen. 78 procent van de *meldende organisaties* geeft aan nooit vragen te krijgen naar aanleiding van de melding, 13 procent krijgt soms vragen en de rest weet het niet. Bij 60 procent van de *meldende organisaties* worden nooit verzoeken om inzage van gegevens ontvangen, bij 28 procent soms en bij 4 procent regelmatig. Bij de helft van de *meldende organisaties* komt ook nooit een verzoek om correctie, aanvulling of wijziging binnen. Bij een derde gebeurt dat soms en bij 7 procent van de *meldende organisaties* regelmatig tot vaak. Bij driekwart van de *meldende organisaties* wordt nooit een officiële klacht, bezwaar of verzet ingediend, bij 14 procent soms en de rest van de *meldende organisaties* weet het niet. Bij slechts 2 procent van de *meldende organisaties* is ooit een formele procedure aangespannen bij een rechter, het Cbp of een geschillencommissie (zie Tabel 26).

Tabel 26 Vragen en klachten van betrokkenen (organisaties in het algemeen en meldende organisaties)[201]

	Organisaties in het algemeen Percentage	Meldende organisaties Percentage
Nooit vragen n.a.v. melding	-	78
Nooit verzoeken om inzage van gegevens	45	60
Nooit verzoek om aanvulling, correctie of wijziging	20	50
Nooit officiële klacht, bezwaar of verzet	100	45
Nooit formele procedure aangespannen bij rechter, Cbp of geschillencommissie	100	98

Tabel 26 geeft nog eens kort weer welk percentage van de organisaties in het algemeen en welk percentage van de meldende organisaties nooit te maken krijgt met de verschillende acties van betrokkenen. Al met al komt hieruit een beeld naar voren dat de betrokkene niet bijster actief bezig is met zijn gegevens die verwerkt worden. Vooral de zwaardere procedures komen weinig voor. Tabel 26 wijst er niet op dat een melding tot duidelijk meer acties van de betrokkenen leidt. Meldende organisaties lijken iets minder vaak verzoeken om inzage, aanvulling, correctie of wijziging te krijgen, en iets vaker officiële klachten, bezwaren of verzet. In de meeste gevallen leidt dit zelfs tot minder vragen en klachten.

[201] Aan de FG's is deze vraag niet in deze vorm gesteld.

Ondanks het feit dat betrokkenen weinig vragen stellen, heeft ongeveer een derde van de organisaties procedures ingericht om vragen, klachten, verzet en dergelijke af te handelen (zie Tabel 27). De respondenten uit de *organisaties in het algemeen* en de *meldende organisaties* wijken daarbij niet sterk van elkaar af. Wanneer er geen procedures zijn, worden daarvoor verschillende redenen aangegeven. In de eerste plaats worden procedures vaak niet nodig geacht omdat vragen en klachten sneller zonder formele procedures kunnen worden afgehandeld. Een belangrijk argument is dat vragen en klachten vrijwel niet voorkomen. Bij de *organisaties in het algemeen* wist ongeveer vijf procent niet van het bestaan van deze rechten van betrokkenen af.

Tabel 27 Aanwezigheid van procedures (organisaties in het algemeen en meldende organisaties)[202]

Procedure voor:	Organisaties in het algemeen Percentage	Meldende organisaties Percentage
Inzage	38	36
Correctie, aanvulling of verwijdering	36	32
Officiële klachten, verzet of bezwaar	33	28

Ook bij *organisaties met een FG*, en die veel persoonsgegevens verwerken, zijn betrokkenen weinig actief om hun rechten uit te oefenen. Aan de *organisaties met een FG* is gevraagd hoe vaak aan de balie, via formulieren of telefonisch om correctie van persoonsgegevens wordt gevraagd. Ook is gevraagd hoe vaak betrokkenen formeel vragen om persoonsgegevens in te zien. Dit zijn lastig te produceren getallen, wat tot een dermate lage respons heeft geleid dat over deze vragen geen betrouwbare uitspraken zijn te doen. De respons op de formele instrumenten was beduidend beter. Verzet en bezwaar komen nauwelijks voor (gemiddeld 0,2 maal). 21 procent van de FG's geeft aan dat de organisatie waarvoor zij werken aangesloten is bij een geschillencommissie. Er is geen enkele betrokkene die een geschil heeft voorgelegd aan een geschillencommissie. Er is ook nooit beroep gedaan op de rechter. Een enkele keer heeft het Cbp in een geschil bemiddeld.

Al met al kan worden geconcludeerd dat betrokkenen nauwelijks gebruik maken van de formele rechten die de Wbp biedt. Ondanks het geringe gebruik is bijna driekwart van de FG's er van overtuigd dat de rechten die in de Wbp aan burgers zijn gegeven de rechtspositie van betrokkenen heeft verbeterd. Ruim 60 procent van de ondervraagde FG's vindt dat het doel dat de wet nastreeft dermate belangrijk is dat de administratieve lasten van deze instrumenten gerechtvaardigd zijn.

4.8 Administratieve lasten

Actal heeft een nulmeting verricht van de administratieve lasten van de Wbp. Oorspronkelijk werd ervan uitgegaan dat de Wbp jaarlijks ruim 30 miljoen euro aan administratieve lasten voor het bedrijfsleven met zich meebrengt. In de door EIM gecorrigeerde nulmeting worden de jaarlijkse administratieve lasten voor het bedrijfsleven geraamd op bijna 42 miljoen

[202] Aan de FG's is deze vraag niet in deze vorm gesteld.

euro.[203] Daarbij moet de kantekening worden gemaakt dat deze bedragen hypothetisch zijn omdat zowel Actal als EIM bij hun berekeningen uitgaan van 100 procent naleving.

In het onderhavige onderzoek is niet getracht de totale (potentiële) administratieve lasten van de Wbp te kwantificeren. Wel is aan respondenten naar hun mening gevraagd over de lasten die zij ondervinden bij de uitvoering van de Wbp. Op de vraag of de organisatie wel eens in haar bedrijfsvoering wordt belemmerd door privacyregels antwoordt zeven procent uit de *organisaties in het algemeen* dat dat vaak gebeurt. Ruim de helft van deze organisaties wordt soms belemmerd in haar bedrijfsvoering en ongeveer een derde zegt geen last te hebben van privacyregels. Van de organisaties die last hebben van de privacyregels stelt ongeveer een derde dat de voorwaarden die de wet stelt lastig uitvoerbaar zijn. Gegevensverwerkingen blijken meer tijd te kosten en soms verbiedt de wet gegevensverwerkingen. Een op de zes organisaties vindt de regels soms zo onduidelijk dat ze om die reden afzien van gegevensverwerking (zie Tabel 28).

Tabel 28 Hoe wordt de bedrijfsvoering belemmerd door de Wbp? (organisaties in het algemeen)

Belemmering bedrijfsvoering	Organisaties in het algemeen Percentage
De voorwaarden die de wet stelt zijn lastig uitvoerbaar	31
Gegevensverwerkingen kosten meer tijd	24
De wet verbiedt gegevensverwerkingen die voor onze bedrijfsvoering nodig zijn	22
We hebben nieuwe procedures moeten vaststellen	20
De regels die de wet stelt zijn zo onduidelijk dat we bepaalde verwerkingen maar niet uitvoeren	16
Anders	17

Ruim de helft van de organisaties geeft aan dat de Wbp de bedrijfsvoering hindert. Aan deze organisaties is gevraagd welke activiteiten de Wbp belemmert. De Wbp knelt vooral bij het verstrekken van gegevens aan andere organisaties (in 45 procent van de gevallen). Ook worden de regels van de Wbp als belemmerend ervaren wanneer een organisatie bestanden wil combineren (in 30 procent van de gevallen). De Wbp hindert de bedrijfsvoering volgens onze respondenten ook vaak wanneer de organisatie wil samenwerken met een andere organisatie (in 30 procent van de gevallen). In ruim een kwart van de gevallen knellen de regels bij het verkrijgen van informatie van andere organisaties.

Wanneer de regels niet knellen komt dat vooral omdat de respondent aangeeft dat er binnen de organisatie nauwelijks privacygevoelige informatie wordt verwerkt (54 procent). In een derde van de gevallen wordt aangegeven dat de organisatie zelf een privacycode hanteert die ten minste even streng is als de wetgeving. Ongeveer een kwart geeft aan dat de privacyregels flexibel genoeg zijn. Onbekendheid met de regels wordt niet als een probleem gezien (5 procent). Niemand geeft aan bewust van de norm af te wijken.

[203] Boog e.a. 2006.

4.9 Technologische ontwikkelingen

Het beeld bestaat dat technologische ontwikkelingen snel gaan en dat een deel van deze ontwikkelingen gevaren kan opleveren voor de privacy van betrokkenen. Van een aantal ontwikkelingen is daarom gekeken hoe vaak zij voorkomen. Het blijkt dat het koppelen van bestanden het meest voorkomt. Verspreiding van persoonsgegevens via het Internet is eveneens een algemeen verschijnsel. Nieuwe technologieën als RFID en biometrische technologie komen nog nauwelijks voor. Opvallend is dat een hoog percentage van de organisaties geen van deze technologieën gebruikt. Verder valt op dat *organisaties met een FG* iets meer gebruik maken van deze technieken dan de organisaties zonder. Toch geeft nog bijna een derde van de *organisaties met een FG* aan dat zij geen van deze technologieën toepassen (zie Tabel 29).

Tabel 29 Toepassing van nieuwe technieken (organisaties in het algemeen en organisaties met een FG)[204]

Technologie	Algemeen Percentage	Organisaties met een FG Percentage
Koppelen van bestanden	40	62
Verspreiding via Internet	29	32
Biometrische technologie	4	4
RFID	1	3
Geen van deze technologie	43	28

Meer dan de helft van de *organisaties in het algemeen* ziet nieuwe gevaren voor de privacy in de nieuwe technologische trends. Voor de toekomst voorziet meer dan de helft van de organisaties ontwikkelingen die een bedreiging kunnen vormen voor de privacy van betrokkenen.

Bij de *organisaties met een FG* ziet een ongeveer even hoog percentage gevaren voor de privacy. In Tabel 30 wordt weergegeven hoeveel organisaties een specifieke technologie als risicovol voor de privacy hebben gekwalificeerd.

Tabel 30 Brengen deze recente technieken gevaren mee voor de privacy in uw branche?[205]

Technologie	Algemeen Percentage	Organisaties met een FG Percentage
Verspreiding van persoonsgegevens via Internet	23	38
Koppelen van bestanden	18	32
Biometrische technologie	1	4
RFID	0	6

Verspreiding van gegevens via het Internet wordt als het meest risicovol ervaren, op de voet gevolgd door het koppelen van bestanden. RFID en biometrie worden door weinig *organisaties met een FG* als privacyrisico beoordeeld. Door *organisaties met een FG* zijn nog

[204] Bij de meldende organisaties is vooral ingegaan op de meldingsprocedure. Om die reden is deze vraag niet in hun enquête opgenomen.
[205] Bij de meldende organisaties is vooral ingegaan op de meldingsprocedure. Om die reden is deze vraag niet in hun enquête opgenomen.

enkele andere risicovolle technieken genoemd. Het betreft EDP, GSM-camera's en onderscheppen van communicatie.

Bovenstaande technologieën kunnen ertoe leiden dat er nieuwe gevaren voor de privacy van betrokkenen ontstaat en dat de organisatie zijn privacybeleid op deze ontwikkelingen moet aanpassen. Ondanks het feit dat veel respondenten weinig gevaren zien, geeft ongeveer 60 procent van de *organisaties in het algemeen* van hen aan dat hun omgang met persoonsgegevens is veranderd door de technologische ontwikkelingen.

Dat percentage ligt even hoog bij de *organisaties met een FG* (58 procent). Dat komt vooral door de opkomst van het Internet en de mogelijkheden om bestanden te koppelen. De enige ontwikkeling die binnen de *organisaties met een FG* tot dusver aanleiding was voor aanpassing van het privacybeleid is de sterke opkomst van het Internet. In 42 procent van de gevallen zijn nieuwe onderdelen aan het privacybeleid van *organisaties met een FG* toegevoegd om in te kunnen spelen op deze technologische ontwikkelingen. In 9 procent van de gevallen moest het privacybeleid zelfs in zijn geheel worden herzien. Slechts 12 procent van de *organisaties met een FG* denkt dat zij hun privacybeleid in de komende 5 jaar niet aan technologische ontwikkelingen hoeft aan te passen. De overige *organisaties met een FG* geven uiteenlopende redenen voor aanpassing. Ook hier zijn weer de mogelijkheden van het Internet en koppeling van bestanden de belangrijkste redenen waarom verwacht wordt dat het privacybeleid van de organisaties op de helling moet.

4.10 Samenvatting

4.10.1 Organisaties

Veel organisaties in Nederland verwerken persoonsgegevens en hebben daardoor te maken met de Wbp. Het mediane aantal databases met persoonsgegevens dat de ondervraagde organisaties hebben bedraagt 3. Dat geldt zowel voor de *organisaties in het algemeen* als voor de *meldende organisaties*. Bij deze organisaties is over het algemeen geen privacydeskundige in dienst. De belangrijkste reden voor het niet aanstellen van een privacydeskundige is omdat de betreffende organisatie hiervoor te klein is. Dit betekent niet dat verantwoordelijken niet op de hoogte zijn van de Wbp. Organisaties geven over het algemeen aan dat zij voldoende kennis van de Wbp hebben om deze wet goed te kunnen uitvoeren. Veel organisaties hanteren eigen privacycodes of gebruiken een code van de branchevereniging.

Organisaties met een FG verschillen fundamenteel van de overige organisaties. De *organisaties met een FG* zijn gemiddeld 50 maal groter en verwerken veel meer persoonsgegevens. De reden waarom organisaties geen FG benoemen is omdat zij geen behoefte hebben aan een interne toezichthouder. Uit de enquête blijkt dat de FG zich in de praktijk zelden als een toezichthouder opstelt. De FG stelt zich binnen de organisatie in de eerste plaats op als deskundige op het gebied van privacy. Overtredingen worden zelden geconstateerd. Wanneer dat wel gebeurt, wordt eerst getracht via zachte druk de verantwoordelijke op het juiste spoor te zetten. Het inzetten van harde handhavingsinstrumenten gebeurt zeer sporadisch. Een andere reden is dat er geen concrete meerwaarde wordt gezien in het benoemen van een FG. Een punt van zorg is dat een kwart van de FG's aangeeft dat zij aanwijzingen van hun leidinggevende moeten opvolgen. Dit staat haaks op de wettelijk verankerde onafhankelijkheid van de FG.

4.10.2 Databases en privacyregels

De meeste databases worden gevuld met persoonsgegevens die de betrokkene zelf beschikbaar heeft gesteld. Andere belangrijke bronnen van persoonsgegevens zijn andere organisaties en eigen onderzoek. De overheid blijkt overigens de belangrijkste ontvanger van persoonsgegevens te zijn. Als we kijken welke typen betrokkenen er vooral in de databases zitten, dan zijn dat klanten, patiënten en werknemers. Van deze betrokkenen worden tal van persoonsgegevens bijgehouden. Het meest algemeen zijn (uiteraard) de NAW-gegevens. Maar ook financiële gegevens, wettelijke identificatienummers (in personeels- en salarisadministraties), gegevens over gezondheid en gedragingen en gegevens over het functioneren van werknemers of leerlingen komen vaak voor. Het is opvallend dat er relatief vaak gevoelige gegevens worden verwerkt, zoals gegevens over gezondheid, godsdienst, ras of strafrechtelijke gegevens. De vorengenoemde gevoelige gegevens komen stuk voor stuk in meer dan 10 procent van de databases voor. Het is overigens niet bekend geworden in hoeverre de verantwoordelijken gerechtigd waren om deze gegevens te verwerken.

De privacyregels uit de Wbp worden in een groot aantal gevallen als belemmerend ervaren. De voorwaarden uit de wet blijken lastig uitvoerbaar te zijn en gegevensverwerkingen kosten meer tijd. Soms verbiedt de wet een verwerking. Eén op de zes organisaties vindt de wettelijke regels zo onduidelijk dat ze soms afzien van gegevensverwerking. Uitwisselen van gegevens met andere organisaties levert de meeste problemen op. De Wbp knelt vooral bij het verstrekking van gegevens aan andere organisaties. Ook zijn de regels van de Wbp belemmerend wanneer een organisatie bestanden wil combineren. De Wbp hindert de bedrijfsvoering ook vaak wanneer de organisatie wil samenwerken met een andere organisatie. Iets minder vaak knellen de regels bij het verkrijgen van informatie van andere organisaties. Wanneer de wet niet knelt komt dat vooral omdat er nauwelijks privacygevoelige informatie wordt verwerkt. Ook heeft men weinig problemen met de wet als men een eigen privacycode heeft die tenminste even streng is als de wet.

Beveiliging van persoonsgegevens is een belangrijk item in de Wbp. Een eerste vorm van beveiliging is het beperken van de toegang tot de database. Daarvoor is het nodig bepaalde personen te autoriseren en deze te kunnen identificeren. Autorisatie vindt op grote schaal plaats en identificatietechnieken zijn de belangrijkste bron van beveiliging. Dit vindt bij vrijwel iedere organisatie plaats. Een tweede vorm is de beveiliging van de gegevens zelf. Deze technieken – bijvoorbeeld encryptie – worden nauwelijks toegepast. Het blijkt dat de *organisaties met een FG* dit soort technieken wel vaker gebruiken. Waarschijnlijk hangt dit samen met de schaalgrootte en het feit dat zij veel meer persoonsgegevens verwerken dan andere organisaties.

4.10.3 Meldingen

Momenteel zijn er meer dan 30.000 meldingen in het meldingenregister van het Cbp geregistreerd. Vooral in de beginjaren is de groei van het meldingenregister zeer snel gegaan. Momenteel heeft het aantal meldingen bij het Cbp zich gestabiliseerd op zo'n 4.000 meldingen per jaar. Een iets kleiner aantal van zo'n 2.600 meldingen wordt gedaan bij de FG's. Die houden elk een eigen register bij, waardoor deze meldingen decentraal – en mogelijk minder toegankelijk – aanwezig zijn. Het meldingenregister op www.cbpweb.nl laat dus een belangrijk deel van de meldingen zien, maar duidelijk niet alles.

Ongeveer een kwart van de *organisaties in het algemeen* geeft aan wel eens een verwerking van persoonsgegevens te hebben gemeld. In veel gevallen wordt er niet gemeld omdat de

verantwoordelijke van mening is dat er geen meldingsplichtige verwerkingen binnen de organisatie plaatsvinden. Bij een beperkt aantal (5 procent) van de organisaties is niet gemeld omdat er weerstand bestaat tegen de meldingplicht. Er wordt niet ingezien waarom de meldingsplicht tot een verbetering van de privacy van de betrokkene leidt. In zeven procent van de gevallen was de meldingsplicht niet bekend. Het feit dat veel organisaties dus niet melden is slechts in beperkte mate te wijten aan kennisgebrek, maar men is ervan overtuigd dat er niets te melden valt. In hoeverre die overtuiging terecht is, kon aan de hand van de enquête niet worden nagegaan. Wanneer wel wordt gemeld leidt dat intern vrijwel nooit tot verzet.

Voor melding wordt vooral gebruik gemaakt van het online meldingsprogramma van het Cbp. De procedure wordt over het algemeen niet erg ingewikkeld gevonden. De doorsnee organisatie is ongeveer 6 uur kwijt met het indienen van de melding, maar er zijn ook organisaties die daar veel langer over doen. Opvallend is dat wordt geconstateerd dat er vervolgens weinig met de melding gebeurt. Er wordt een ontvangstbevestiging en een meldingsnummer van het Cbp ontvangen en de melding wordt opgenomen in het meldingenregister. De organisaties merken nooit iets van een inhoudelijke controle door het Cbp. In dat opzicht lijkt de controle op de meldingen die bij de FG's binnenkomen intensiever te zijn. Zij voeren in bijna 50 procent van de gevallen bij iedere melding een toets uit of de feitelijke verwerking overeenstemt met het doel van de melding. Het lijkt er op dat door het relatief geringe aantal meldingen de FG de capaciteit heeft controle van de melding uit te voeren, terwijl bij het Cbp de meldingen mogelijk te veel als 'bulkgoed' worden gezien.

De meldingsplicht brengt niet veel administratieve lasten met zich mee. Gewoonlijk wordt ongeveer 6 uur in een melding gestoken, terwijl de meeste respondenten de meldingsprocedure gemiddeld ingewikkeld vonden. Bijna de helft van de respondenten is van mening dat de meldingsplicht weinig goeds voor de betrokkenen brengt. Betrokkenen kunnen volgens hen het meldingenregister niet vinden en zijn bovendien niet geïnteresseerd in de verwerking van hun persoonsgegevens. De grote meerwaarde van het melden lijkt te liggen in het gegeven dat het privacybewustzijn van de verantwoordelijke door het indienen van de melding versterkt. De helft van de *meldende organisaties* is zich meer bewust geworden van privacyaspecten en 8 procent heeft de legitimiteit van de doelen van de gegevensverwerking nog eens overwogen. In een derde van de gevallen is men door de meldingsplicht zorgvuldiger gaan handelen. Deze bevindingen kunnen worden gestaafd met de gegevens die volgens de respondenten worden verwerkt. Het blijkt dat de *meldende organisaties* zo'n 30 procent minder soorten persoonsgegevens verwerken dan *organisaties in het algemeen*.

4.10.4 Rechten van betrokkenen

Betrokkenen hebben in principe het recht te weten welke persoonsgegevens van hen worden verwerkt. In de Wbp is daarom een informatieplicht opgenomen. Bij 72 procent van de respondenten worden de betrokkenen op een of andere manier geïnformeerd over de verwerking van hun persoonsgegevens. In de gevallen waarin dat niet gebeurt, is de hoofdreden omdat de verantwoordelijke van mening is dat de betrokkene al op de hoogte is van verwerking, bijvoorbeeld omdat deze zijn gegevens zelf beschikbaar heeft gesteld. De organisaties gebruiken verschillende middelen voor het informeren van betrokkenen, zoals websites, aanvraagformulieren, folders, algemene voorwaarden en persoonlijke berichtgeving. Er lijkt geen grote voorkeur te zijn voor één van deze middelen. Volgens de meeste respondenten worden de betrokkenen goed geïnformeerd. Het is dan ook opvallend dat de betrokkenen nauwelijks op deze informatie reageren. Er worden zelden vragen gesteld naar

aanleiding van een melding. Er worden zelden verzoeken om inzage, aanvulling of correctie ingediend. Officiële klachten komen vrijwel nooit voor en datzelfde geldt voor het opstarten van een procedure bij de rechter, het Cbp of een geschillencommissie. Het beeld van een nauwelijks betrokken betrokkene dringt zich op.

Des te opvallender is het dat één op de drie organisaties procedures heeft voor inzage, correctie, aanvulling of verwijdering en officiële klachten, verzet of bezwaar. Gezien het bovenstaande wordt er van deze procedures nauwelijks gebruik gemaakt. Bij de organisaties die deze procedures niet hebben is dan ook het belangrijkste argument dat deze zaken toch vrijwel nooit voorkomen.

4.10.5 Technologische ontwikkelingen

Nieuwe technieken leveren nieuwe problemen op. Van de nieuwe technieken worden vooral het koppelen van bestanden en het verspreiden van gegevens via het internet toegepast. Volgens de respondenten brengen deze technieken ook meteen de grootste risico's voor de privacy met zich mee. Ongeveer 60 procent van de ondervraagden geeft aan dat hun omgang met persoonsgegevens veranderd is door deze technieken. In veel gevallen vormden deze technieken een aanleiding om het privacybeleid te herzien.

Hoofdstuk 5 Opinies van organisaties

5.1 Inleiding

In hoofdstuk 4 is getracht aan de hand van drie enquêtes een getrouw beeld te schetsen van de feitelijke handelingen die door Nederlandse organisaties worden verricht om invulling te geven aan de Wbp. In de betreffende enquêtes is niet alleen gevraagd naar het feitelijk handelen van deze organisaties. Ook is gevraagd naar de opinies van de respondenten over verschillende aspecten van de uitvoering van de Wbp. Deze opinies zijn gemeten aan de hand van stellingen waarop de respondenten konden reageren. In dit hoofdstuk komen deze opinies aan de orde. Ook hier wordt, net als in het vorige hoofdstuk, een onderscheid gemaakt tussen de *organisaties in het algemeen, meldende organisaties en organisaties met een FG*. Voor meer informatie over de respons op de enquêtes wordt verwezen naar paragraaf 4.2. Het is goed om nogmaals te noemen dat bij de *organisaties in het algemeen* 82 respondenten hebben gereageerd, bij de meldende organisaties waren dat er 159 en van de FG's hebben 69 een vragenlijst ingevuld. Vrijwel alle opinievragen zijn door alle respondenten ingevuld. Wij zien daarom af van het bij iedere tabel opnemen van een N.

Hoofdstuk 5 geeft een beschrijving van een aantal opinies van verschillende typen respondenten over de uitwerking van de Wbp op de bedrijfsvoering van de organisaties. Het belang van privacy komt in paragraaf 5.2 aan de orde. Vervolgens wordt in paragraaf 5.3 ingegaan op de manier waarop wordt omgegaan met de open normen in de wet. In paragraaf 5.4 wordt kort ingegaan op hoe de respondenten tegen de meldingsprocedure aankijken en vervolgens komen in paragraaf 5.5 de rechten van de betrokken aan bod. Paragraaf 5.6 zal ingaan op de positionering van de FG en zijn mening over de Wbp. In paragraaf 5.7 wordt getracht een beeld te schetsen van de hoogte van de ervaren administratieve lasten. De inschatting van de FG's over de impact van enkele maatschappelijke en technologische ontwikkelingen komt aan de orde in paragraaf 5.8. Tot zover is hoofdstuk 5 vooral beschrijvend van aard.

In paragraaf 5.9 wordt een model ontwikkeld voor *organisaties met een FG* waaruit moet blijken waarom de ene organisatie wel en de andere organisatie niet tevreden is over de Wbp als wet. Voor de overige organisaties waren te weinig gegevens bekend om deze analyse te kunnen uitvoeren. De technische aspecten van de analyse zijn uitgewerkt in bijlage 5. Ten slotte worden de belangrijkste bevindingen samengevat in paragraaf 5.10.

5.2 Belang van privacy

Het belang van privacybescherming wordt door vrijwel alle respondenten ingezien. Er zijn zowel onder de *organisaties in het algemeen* als onder de *meldende organisaties* nauwelijks respondenten te vinden die het niet eens zijn met de stelling "*het is belangrijk dat zorgvuldig met persoonsgegevens wordt omgegaan*" (zie Tabel 31). De tegenovergestelde stelling "*privacybescherming is grote onzin"* laat een vergelijkbaar beeld zien. Een zeer beperkt aantal respondenten is het (zeer) eens met deze stelling (respectievelijk 2,5 en 0,6 procent). Klaarblijkelijk wordt het principe van privacybescherming breed gedeeld door een groot aantal vertegenwoordigers van verschillende organisaties. Het hoge aantal respondenten dat het principe van zorgvuldige omgang met persoonsgegevens onderschrijft is niet erg

verwonderlijk omdat dit binnen de context van dit onderzoek een sociaal wenselijk antwoord is. Bovendien worden er aan het principe van privacybescherming geen consequenties verbonden, zoals hogere administratieve lasten. Feitelijk hoeft er door de respondent dus geen keuze tussen de baten van privacybescherming en haar kosten te worden gemaakt.

Tabel 31 Het belang van privacybescherming

	Het is belangrijk dat zorgvuldig met persoonsgegevens wordt omgegaan	
	Organisaties in het algemeen	Meldende organisaties
Zeer mee eens	75,0%	73,6%
Mee eens	21,3%	22,6%
Neutraal	2,5%	0,6%
Mee oneens	0,0%	0,0%
Zeer mee oneens	1,2%	3,2%
Totaal	100%	100%

Wanneer er wordt gevraagd te kiezen tussen de belangen voor de eigen organisatie en het privacybelang, zien we dat er iets vaker voor de belangen van de eigen organisatie wordt gekozen (zie Tabel 32). Toch valt op dat meer dan de helft van de respondenten aangeeft eerder voor bescherming van privacy te kiezen dan voor de belangen van de eigen organisatie. Wanneer wordt gevraagd of privacybescherming belangrijker is dan veiligheid, dan zien we dat het aantal respondenten dat voor privacybescherming kiest nog wat verder afneemt. Tussen de 7 (*organisaties in het algemeen*) en 10 procent (*meldende organisaties*) is het (zeer) met deze stelling eens. Wat hier opvalt is het grote aantal “neutraalstemmers” (meer dan de helft). De gegevens lijken er op te wijzen dat privacybescherming als waarde belangrijk wordt gevonden.

Tabel 32 Organisatiebelangen belangrijker dan privacy?

	Onze organisatiebelangen zijn belangrijker dan privacybescherming	
	Organisaties in het algemeen	Meldende organisaties
Zeer mee eens	2,6%	0,7%
Mee eens	11,5%	6,9%
Neutraal	26,9%	32,7%
Mee oneens	42,3%	27,0%
Zeer mee oneens	16,7%	32,7%
Totaal	100%	100%

Het is overigens niet zo dat de belangen van de organisatie per definitie haaks staan op het recht op een zorgvuldige omgang met persoonsgegevens van betrokkenen. Bij veel organisaties blijkt het uitdragen van het privacybeleid een belangrijk instrument gevonden te worden om vertrouwen van de cliënt te winnen of te behouden. Bij veel organisaties wordt privacybescherming zelfs als een belangrijk marketinginstrument gezien. In Tabel 33 zien we dat privacybescherming significant vaker als marketinginstrument wordt gezien binnen de semi-overheid en het bedrijfsleven dan binnen de overheid. Dat is logisch gezien de andere relatie van de overheid met haar clientèle. Verder geven organisaties die zeggen dat privacybescherming gebruikt wordt als marketinginstrument iets vaker aan dat het belangrijk

is dat er zorgvuldig met persoonsgegevens wordt omgegaan.[206] Ook vinden zij privacy iets vaker belangrijker dan hun eigen organisatiebelangen.[207] We zien hier dus dat het belang dat wordt gehecht aan bescherming van persoonsgegevens hand in hand gaat met het belang van de organisatie.

Tabel 33 Privacybescherming als marketinginstrument

	een goede en betrouwbare privacybescherming is een belangrijk marketinginstrument		
	Semi-overheid en maatschappelijke instellingen	Bedrijf	Overheid
(Zeer) mee eens	76,9%	63,2%	42,9%
Neutraal	19,2%	28,9%	21,4%
(zeer) mee oneens	3,9%	7,9%	35,7%
Totaal N	100 % N = 26	100 % N = 38	100% N = 14

Chi kwadraat = 11,2; P = 0,025

We hebben gezien dat veel organisaties groot belang hechten aan bescherming van persoonsgegevens. Verkoop van gegevens aan andere organisaties is voor vrijwel alle ondervraagde organisaties dan ook een brug te ver. Veel organisaties staan hier ronduit afwijzend tegenover. Dit beeld zien we terug bij zowel de *organisaties in het algemeen* als bij de meldenden organisaties. Slechts vijf *organisaties in het algemeen* (vier bedrijven en één overheid, samen bijna 7%) geven aan geld te kunnen verdienen met de verkoop van persoonsgegevens, maar op de vraag of dat ook wordt gedaan antwoordt geen enkele organisatie dat dat ook gebeurt.

5.3 De omgang met open normen

In de literatuur wordt met enige regelmaat geconstateerd dat de omgang met open normen problematisch is. Uit de gegevens blijkt dit probleem echter niet heel duidelijk. Op de vraag of het altijd duidelijk is welke persoonsgegevens mogen worden vastgelegd, wordt door zowel de *organisaties in het algemeen*, de *meldende organisaties* als de *organisaties met een FG* in meerderheid geantwoord dat dat zeker het geval is. Vooral de *organisaties in het algemeen* hebben geen problemen met de open normen uit de Wbp (zie Tabel 34). Ook de vraag welke gegevens aan derden mogen worden verstrekt levert bij slechts zes procent van de *organisaties in het algemeen* problemen op, terwijl dit voor de FG's in 23 procent van de gevallen vragen oplevert. FG's geven dan ook aan dat zij graag zouden zien dat het Cbp meer gerichte handleidingen opstelt in welke situaties gegevens mogen worden verwerkt.

[206] Nonparametrische correlatie; rho = 0,245, P = 0,031.
[207] Nonparametrische correlatie; rho = - 0,224, P = 0,050.

Tabel 34 Is duidelijk welke persoonsgegevens mogen worden verwerkt?

	Het is ons altijd volledig duidelijk welke persoonsgegevens we mogen verwerken		
	Organisaties in het algemeen	Meldende organisaties	Organisaties met een FG
Zeer mee eens	40,5%	5,7%	7,3%
Mee eens	35,4%	40,3%	37,7%
Neutraal	20,3%	31,4%	18,8%
Mee oneens	3,8%	18,2%	33,3%
Zeer mee oneens	0,0%	4,4%	2,9%
Totaal	100%	100%	100%

Organisaties in het algemeen en *meldende organisaties* geven aan weinig kennisproblemen te ondervinden bij de uitvoering van de Wbp. In ieder geval heeft binnen beide steekproeven slechts zo'n 15 procent onvoldoende informatie over de Wbp om deze wet goed uit te kunnen voeren. Opvallend is het verschil met de perceptie van de FG's. 55 procent van de FG's geeft aan over (veel) te weinig informatie over de Wbp te beschikken om deze wet goed te kunnen uitvoeren (zie Tabel 35).

Tabel 35 Volledigheid informatie om Wbp uit te voeren

	We hebben voldoende informatie om de Wbp goed uit te voeren		
	Organisaties in het algemeen	Meldende organisaties	Organisaties met een FG
Zeer mee eens	15,2%	9,4%	4,4%
Mee eens	43,0%	47,2%	15,9%
Neutraal	26,6%	27,0%	24,6%
Mee oneens	12,7%	14,5%	43,5%
Zeer mee oneens	2,5%	1,9%	11,6%
Totaal	100%	100%	100%

Het is de vraag of het geringe aantal problemen dat 'normale' organisaties hebben met de uitvoering van de Wbp voortkomt uit onwetendheid, of uit het feit dat zij relatief weinig met ingewikkelde problematiek te maken hebben. We zien over de gehele linie dat de FG's meer problemen ondervinden van de open normen. Het lijkt er op dat naarmate de kennis over het onderwerp groter is, er ook grotere problemen worden gezien. Enerzijds bestaat de mogelijkheid dat de grote informatie-intensieve organisaties waarin FG's werken meer complexe of problematische verwerkingen verrichten, anderzijds bestaat de mogelijkheid dat door de specialisatie van de FG's meer juridische problemen worden onderkend en dat zij een realistischer inschatting van deze problematiek maken. Zo lang je weinig over de Wbp weet, heb je er ook geen last van. Anders gezegd, wat niet weet, wat niet deert.

Wanneer er onduidelijkheid over het wel of niet mogen verwerken van persoonsgegevens bestaat, zijn FG's in groten getale van mening dat moet worden gekozen om deze persoonsgegevens niet te verwerken. Slechts 14 procent van de ondervraagde FG's is het (zeer) niet met deze stelling eens. Met de verstrekking van persoonsgegevens aan andere organisaties blijken de FG's nog voorzichtiger te zijn. Slechts in 5 procent van de gevallen is men het niet eens met de stelling dat persoonsgegevens niet verstrekt worden bij twijfel. Het

motto luidt hier duidelijk: “bij twijfel niet inhalen”. Een gevolg kan echter zijn, mede gezien de grote onzekerheid over de invulling van open normen bij de FG’s, dat regelmatig gegevens aan andere organisaties worden geweigerd of dat gegevens niet worden verwerkt, terwijl daar juridisch gezien eigenlijk geen aanleiding voor is. Onzekerheid kan zo al snel leiden tot onderbenutting van persoonsgegevens.

Omdat de FG’s als een groep praktijkdeskundigen kunnen worden beschouwd, is in de tot hen gerichte enquête wat verder doorgevraagd over de omgang en de gepercipieerde problemen met betrekking tot de open normen van de Wbp. Bijna de helft van de FG’s is van mening dat een onderwerp als privacy niet met concrete normen kan worden vervat, terwijl bijna een kwart van de FG’s vindt dat dit wel kan. Het resterende kwart staat hier neutraal tegenover. Bij de vraag aan FG’s of het ministerie van Justitie, het Cbp of de jurisprudentie de open normen op een goede manier invult vinden we veel ‘neutraalstemmers’. Als we de balans opmaken, zien we dat van het ministerie van Justitie weinig blijkt te worden vernomen over het concretiseren van open normen. Het Cbp doet dit in de ogen van de FG’s iets beter, maar de balans slaat nog steeds door naar een negatief oordeel. Ook de jurisprudentie laat geen duidelijk beeld zien (zie Tabel 36). Al met al lijken de FG’s niet een heel duidelijke mening te hebben over de invulling van de normen door het ministerie van Justitie, het Cbp en de jurisprudentie. Wat door de FG’s erg wordt gemist is dat het Cbp geen sluitend advies meer geeft op vragen over concrete verwerkingen van persoonsgegevens.

Tabel 36 Invulling open normen per informatiebron

	Organisaties met een FG			
	Het ministerie van Justitie vult de open normen goed in	Het Cbp vult de open normen goed in	De open normen worden goed verduidelijkt door de jurisprudentie	Er zijn voldoende handleidingen en best practices om de Wbp goed te kunnen toepassen
Zeer mee eens	2,9%	2,9%	2,9%	4,4%
Mee eens	7,3%	17,4%	17,4%	33,4%
Neutraal	60,9%	52,2%	58,0%	39,2%
Mee oneens	18,8%	23,2%	18,8%	21,7%
Zeer mee oneens	10,1%	4,3%	2,9%	1,3%
Totaal	100%	100%	100%	100%

5.4 De meldingsprocedure

Een belangrijk onderdeel van de Wbp is de meldingsplicht. Vragen over de meldingsplicht zijn uiteraard opgenomen in vragenlijst voor de *meldende organisaties*. Maar ook FG’s hebben te maken met een specifieke uitvoering van de meldingsplicht. Zij hoeven verwerkingen van persoonsgegevens weliswaar niet bij het Cbp te melden, maar verantwoordelijken kunnen hun melding bij de FG indienen. Voor organisaties die een FG hebben benoemd, gelden derhalve wat andere procedurele regels rondom het melden dan voor

organisaties die dat niet hebben gedaan. Om deze reden zijn ook vragen over het melden opgenomen in de vragenlijst die was bestemd voor de FG's.

De interpretatie van de meldingsplicht blijkt niet altijd eenvoudig te zijn (zie Tabel 37). Bij zowel *meldende organisaties* als bij de *organisaties met een FG* wordt in zo'n 40 procent van de gevallen aangegeven dat het niet altijd duidelijk is hoe de organisatie de meldingsplicht moet interpreteren. In ruim 30 procent van de gevallen hebben FG's onvoldoende informatie tot hun beschikking om de meldingsplicht goed te kunnen uitvoeren en in 30 procent van de gevallen is het niet volstrekt helder welke verwerkingen moeten worden gemeld. Ruim een kwart van de FG's vindt het meldingenformulier of –programma van het Cbp in meer of mindere mate onhelder. Ruim 20 procent vindt dat er onvoldoende handleidingen en best practices beschikbaar zijn om de meldingsplicht goed te kunnen uitvoeren. Bijna 50 procent van de FG's geeft daarom aan dat zij behoefte hebben aan een Cbp die op basis van de melding aangeeft of de gemelde gegevensverwerking rechtmatig is. Al met al is er nogal wat onzekerheid rondom de vraag of er moet worden gemeld en hoe de melding moet worden ingevuld.

Tabel 37 Duidelijkheid interpretatie meldingsplicht

	Hoe wij de meldingsplicht moeten interpreteren is altijd volstrekt duidelijk[208]	
	Meldende organisaties	Organisaties met een FG
Zeer mee eens	3,2%	4,3%
Mee eens	18,2%	27,5%
Neutraal	39,6%	29,1%
Mee oneens	31,5%	24,6%
Zeer mee oneens	7,5%	14,5%
Totaal	100%	100%

Als we bij de FG's doorvragen over de inhoud van de meldingen, dan blijkt dat driekwart van de FG's vindt dat zijn organisatie expliciete doelen voor de verwerking vaststelt en 18 procent is hierover neutraal. 7 procent van de FG's vindt dat dit doel niet goed wordt vaststeld. Over de inhoud van die doelstelling bestaat de nodige onzekerheid. Zo'n 45 procent van de FG's geeft aan dat ze graag van het Cbp horen hoe een goede doelstelling er uit hoort te zien. Blijkbaar bestaat er nog te veel interpretatieruimte en te weinig duidelijkheid aan welke criteria een goede doelstelling voor het verwerken van persoonsgegevens moet voldoen. Ruim 20 procent van de FG's vindt deze invulling van de plicht om een doelstelling te formuleren onnodig. In principe mogen alleen die verwerkingen worden uitgevoerd die binnen het in de melding geformuleerde doel passen. Opvallend is dat 28 procent van de FG's aangeeft dat doelen liever te ruim dan te krap worden geformuleerd, om te voorkomen dat persoonsgegevens niet voor andere activiteiten mogen worden gebruikt. In veel gevallen wordt de doelstelling dus geformuleerd met het oog op toekomstige gegevensverwerkingen.

De *meldende organisaties* zijn het er niet over eens of de meldplicht de privacybescherming van betrokkenen wel heeft verbeterd (zie Tabel 38 en Tabel 39). De FG's hebben een licht positieve houding. Verbetering in de omgang met persoonsgegevens wordt onder andere bewerkstelligd doordat de organisaties beter gaan nadenken over de doelen van de verwerking.

[208] Deze vraag is niet gesteld aan de *organisaties in het algemeen* omdat slechts een beperkt percentage (25 procent) ooit een melding heeft gedaan.

Tabel 38 Zorgvuldigheid door meldingsplicht

	Door de meldingsplicht gaan wij zorgvuldiger om met persoonsgegevens
	Meldende organisaties
Zeer mee eens	5,0%
Mee eens	28,9%
Neutraal	32,1%
Mee oneens	23,3%
Zeer mee oneens	10,7%
Totaal	100%

Verbetering wordt vooral gevoeld door de FG's (zie Tabel 39). De meldingsplicht lijkt er dus toe te leiden dat de verantwoordelijken nog eens nadenken over de doelen van de verwerking. Dit gaat zo ver dat ruim 60 procent van de FG's aangeeft dat door de meldplicht een serieuze afweging tussen het privacybelang en het doel van de registratie is gewaarborgd. Uit een vergelijking van Tabel 38 en Tabel 39 lijkt het patroon te komen dat organisaties met een FG een grotere positieve invloed van de wet signaleren dan meldende organisaties.

Tabel 39 Positieve invloed meldingsplicht op het handelen van organisaties met een FG

	Organisaties met een FG		
	De meldplicht heeft een positieve invloed op de privacy van burgers	Door de meldplicht zijn wij beter gaan nadenken over de bescherming van privacy van burgers	Door de meldplicht is een serieuze afweging tussen het privacybelang en het doel van de registratie gewaarborgd
Zeer mee eens	11,6%	17,4%	8,8%
Mee eens	47,8%	52,2%	53,6%
Neutraal	24,6%	20,3%	24,6%
Mee oneens	8,7%	8,7%	11,6%
Zeer mee oneens	7,3%	1,4%	1,4%
Totaal	100%	100%	100%

5.5 Rechten van betrokkenen

De Wbp heeft aan betrokkenen een aantal rechten gegeven waarmee zij in beperkte mate de (wijze van) verwerking van hun persoonsgegevens kunnen beïnvloeden.[209] Het recht om te weten welke gegevens van de betrokkene worden verwerkt staat aan de basis van deze rechten. Op de vraag of betrokkenen weten welke persoonsgegevens over hen worden bijgehouden, antwoordt het merendeel van de respondenten in alle drie de enquêtes positief. Toch wordt op deze vraag door de FG's in bijna een derde van de gevallen ontkennend geantwoord. Het lijkt

[209] Regievoering is maar tot op zekere hoogte mogelijk omdat verwijderen en / of corrigeren van gegevens aan beperkingen onderworpen is.

erop dat naarmate men intensiever met privacy bezig is, men kritischer naar deze vraag heeft gekeken (zie Tabel 40).

Tabel 40 Geïnformeerdheid van betrokkenen

	Betrokkenen weten precies welke gegevens we over hen bijhouden en wat we ermee doen		
	Organisaties in het algemeen	Meldende organisaties	Organisaties met een FG
Zeer mee eens	24,1%	25,8%	10,1%
Mee eens	41,7%	30,2%	31,9%
Neutraal	25,3%	27,0%	29,0%
Mee oneens	8,9%	13,9%	24,7%
Zeer mee oneens	0,0%	3,1%	4,3%
Totaal	100%	100%	100%

De FG's zijn het overwegend met elkaar eens dat de Wbp er aan heeft bijgedragen dat betrokkenen de regie over hun persoonsgegevens kunnen houden. De *organisaties in het algemeen* en de *meldende organisaties* zijn hier iets minder zeker van.

5.6 De Functionaris voor de Gegevensbescherming

Zoals uit paragraaf 4.4 is gebleken, kunnen FG's op diverse plaatsen in de organisatie gepositioneerd zijn. In de meeste gevallen maken zij deel uit van de juridische staf of de centrale directie. Dit is een centrale positie die dicht tegen de directie van de organisatie aanzit. Op de vraag of de FG vindt dat hij rechtstreeks toegang heeft tot het management, antwoordt vrijwel iedere FG dat hij het (zeer) met deze stelling eens is. Slechts 7 procent antwoordt in de categorie neutraal en er is geen enkele FG die deze rechtstreekse toegang niet heeft. Ook voelen FG's zich in hoge mate gesteund door het management en ook de steun van de medewerkers die met de persoonsgegevens werken is goed te noemen. In paragraaf 4.4 hebben we gezien dat een kwart van de FG's onvoldoende onafhankelijk lijkt te zijn ten opzichte van de directie. Dat blijkt ook uit de stellingen. Op de stelling of de FG kan doen wat hij wil zonder anderen om toestemming te vragen, stelt 16 procent het (zeer) oneens met deze stelling te zijn. De onafhankelijkheid van FG's blijft derhalve een aandachtspunt.

FG's voeren toezichthoudende taken uit die bij alle overige organisaties door het Cbp zouden worden uitgevoerd. Eén van de afspraken die het Cbp maakt is dat wanneer een organisatie een FG aanstelt, en deze functioneert naar behoren, het Cbp terugtreedt als eerste lijnstoezichthouder. Het overgrote merendeel van de *organisaties met een FG* ervaart dat dit ook werkelijk gebeurt. Op de stelling 'Als een FG is aangesteld, treedt het Cbp terug als eerste lijnstoezichthouder' antwoordt 78 procent van de FG's dat zij het (zeer) met deze stelling eens zijn. Slechts bij vier procent van de ondervraagde FG's wordt geen verschil ervaren. Het contact tussen het Cbp en de FG's wordt door de FG's zeer wisselend ervaren. Slechts 13 procent van de FG's geeft op de stelling 'ik heb als FG regelmatig contact met mijn contactpersoon bij het Cbp' aan het (zeer) met deze stelling eens te zijn. 35 procent antwoordt neutraal, 17 procent is het oneens met de stelling en 35 procent is het zeer oneens met de stelling. Ruim de helft van de FG's geeft aan niet regelmatig contact met zijn contactpersoon van het Cbp te hebben. Enerzijds treedt het Cbp dus terug als eerste

lijnstoezichthouder, anderzijds lijkt het contact met de FG's niet erg intensief te zijn. Overigens zijn de FG's over het algemeen gematigd positief over de inhoudelijke ondersteuning door het Cbp. Tabel 41 vat het bovenstaande nog eens samen.

Tabel 41 Relatie tussen FG en Cbp

	Organisaties met een FG		
	Als een FG is aangesteld, treedt het Cbp terug als eerste lijnstoezichthouder	Ik heb als FG regelmatig contact met mijn contactpersoon bij het Cbp	Het Cbp geeft voldoende inhoudelijke ondersteuning
Dat is zeker het geval	26,1%	2,9%	2,9%
Dat is het geval	52,2%	10,1%	34,8%
Neutraal	17,4%	34,8%	36,3%
Dat is niet het geval	2,9%	17,4%	15,9%
Dat is zeker niet het geval	1,4%	34,8%	10,1%
Totaal	100%	100%	100%

Twee op de vijf FG's blijken ook (zeer) positief over de invloed die zij hebben op de privacy van betrokkenen. Slechts een klein percentage is sceptisch over de privacyeffecten van de eigen functie. Opvallend is dat een groot percentage neutraal invult, dus ofwel geen mening heeft, ofwel geen effect ziet.

5.7 Administratieve lasten

Het niet of pas na een doelformulering en/of een formele melding kunnen verwerken van persoonsgegevens kan tot administratieve lasten leiden. Deze administratieve lasten zijn gerechtvaardigd indien zij in een juiste verhouding staan tot het doel van de wet (bescherming van de persoonsgegevens van betrokkenen). Ongeacht het feit dat privacybescherming een belangrijk doel kan zijn, kunnen organisaties nadeel in hun bedrijfsvoering ondervinden van de bescherming die de Wbp tracht te bieden. Het blijkt echter dat relatief weinig organisaties sterk in hun bedrijfsvoering worden belemmerd door de Wbp. Dat geldt zowel voor de *organisaties in het algemeen*, alsmede voor de *meldende organisaties*. Hooguit 6 procent van deze organisaties geeft aan dat de privacyregelgeving een grote belemmering voor de bedrijfsvoering vormt. Een meer specifieke stelling is aan de FG's voorgelegd. Zij moesten reageren op de stelling of de Wbp een goede uitwisseling van gegevens in de weg staat. Dit laat een zelfde beeld zien als bij de *organisaties in het algemeen* en de *meldende organisaties*. Slechts bij vier procent van de *organisaties met een FG* wordt een belemmering van de gegevensuitwisseling ervaren. Opvallend is dat ook hier bijna een op de drie FG's 'neutraal' heeft aangevinkt. Al met al komt uit de drie enquêtes een beeld naar voren dat de Wbp nauwelijks een belemmering vormt voor de bedrijfsvoering en dat het tot weinig gepolariseerde standpunten leidt. Tabel 42 illustreert het bovenstaande.

Tabel 42 Belemmering van de bedrijfsvoering door de Wbp

	De privacyregelgeving vormt een grote belemmering voor onze bedrijfsvoering		De Wbp staat een goede uitwisseling van gegevens in de weg
	Organisaties in het algemeen	Meldende organisaties	Organisaties met een FG
Dat is zeker het geval	0,0%	0,6%	0,0%
Dat is het geval	6,3%	5,7%	4,4%
Neutraal	35,4%	25,8%	30,9%
Dat is niet het geval	43,1%	35,8%	52,9%
Dat is zeker niet het geval	15,2%	32,1%	11,8%
Totaal	100%	100%	100%

Ook uit de gegevens die betrekking hebben op de kosten of moeite die organisaties moeten doen om de Wbp op een verantwoorde wijze uit te voeren komt een beeld naar voren dat de administratieve lasten niet buitensporig hoog zijn. Mogelijk komt dat doordat de regels van de Wbp goed aansluiten bij de privacynormen die reeds vóór de inwerkingtreding van de Wbp in de organisatie of branche golden (52 procent van de *organisaties in het algemeen* en 39 procent van de organisaties met FG geeft dit aan, zie Tabel 43). Opvallend is ook hier weer het grote aantal 'neutraalstemmers'. In een minderheid van de gevallen wordt aangegeven dat de wettelijke regels niet goed aansluiten (respectievelijk 10 en 15 procent). Blijkbaar is de Wbp een wet die in veel gevallen een bestaande praktijk gecodificeerd, maar niet gemodificeerd heeft. Dit is lijn met de eerdere constatering dat de Wbp tot weinig modificaties heeft geleid omdat zij goed aansluit bij de heersende privacynormen. 29 procent van de *meldende organisaties* geeft aan dat er veel tijd in de implementatie van de Wbp is gestoken. Bij de overige organisaties is er weinig tijd aan de implementatie van de Wbp besteed. Ook hier valt het hoge percentage 'neutraalstemmers' weer op. Klaarblijkelijk levert de Wbp binnen deze organisaties weinig uitgesproken opvattingen op.

Tabel 43 De aansluiting van de Wbp op eigen privacynormen

	De regels van de Wbp sluiten goed aan op de in onze organisatie en branche geldende privacynormen	
	Organisaties in het algemeen	Organisaties met een FG
Dat is zeker het geval	6,3%	8,7%
Dat is het geval	46,2%	30,4%
Neutraal	37,5%	44,8%
Dat is niet het geval	6,2%	11,7%
Dat is zeker niet het geval	3,8%	4,4%
Totaal	100%	100%

Aan de *organisaties met een FG* zijn enkele stellingen voorgelegd die betrekking hebben op de hoogte van de administratieve lasten van enkele procedurele deelaspecten van de Wbp. Bijna een derde van de FG's vindt de administratieve lasten van de meldplicht te hoog. Een iets groter percentage vindt van niet. De administratieve lasten van het actueel houden van de

meldingen wordt door ongeveer een derde van de FG's als groot ervaren. Een gelijk percentage vindt dat niet. De administratieve lasten van het inzagerecht wordt door 17 procent van de FG's als te hoog ervaren. Een kleine 20 procent denkt dat de administratieve lasten hoog zijn door de open normen. Ruim 40 procent vindt dat de administratieve lasten in verhouding staan tot het doel van de wet. Ook hier is het aantal FG's dat neutraal heeft ingevuld hoog te noemen. Een en ander staat nog eens uitgewerkt in Tabel 44. Omwille van de leesbaarheid is deze tabel gekanteld ten opzichte van de overige tabellen.

Tabel 44 Stellingen over administratieve lasten (Organisaties met een FG)

	Zeer mee eens	Mee eens	Neutraal	Mee oneens	Zeer mee oneens
De administratieve lasten van de meldplicht zijn veel te hoog	7,4%	20,6%	38,2%	25,0%	8,8%
Het actueel houden van de meldingen is een grote administratieve last	7,2%	24,6%	39,2%	23,2%	5,8%
De administratieve lasten van het inzagerecht zijn veel te hoog	4,3%	13,0%	47,8%	29,1%	5,8%
De administratieve lasten van de Wbp zijn hoog door de open normen	5,8%	15,9%	49,3%	23,2%	5,8%
De administratieve lasten staan in verhouding tot het doel van de wet	7,2%	33,3%	36,3%	10,2%	13,0%

5.8 Maatschappelijke en technologische ontwikkelingen

De groep FG's vormt een groep die zich intensief met gegevensverwerking en privacy-bescherming bezighoudt. Omdat zij de ontwikkelingen op dit gebied nauwgezet volgen, is aan de FG's een aantal stellingen voorgelegd die betrekking hebben op toekomstige maatschappelijke en technologische ontwikkelingen. Het idee hierachter is dat de FG als praktijkdeskundige een geïnformeerde inschatting kan geven van de gevolgen van deze ontwikkelingen. Deze vragen zijn niet in de overige twee enquêtes gesteld, omdat binnen de groepen aangeschreven personen het aantal goed geïnformeerde praktijkdeskundigen een stuk lager werd ingeschat.

Uit Tabel 45 blijkt dat veel FG's geen duidelijke mening hebben over de technologie-onafhankelijkheid van de Wbp. Ongeveer 30 procent verwacht een snelle veroudering door technologische ontwikkelingen, maar 26 procent verwacht dat dit niet het geval zal zijn. De overige FG's hebben hier geen uitgesproken mening over. Iets duidelijker is dat FG's verwachten dat technologische ontwikkelingen een rol kunnen hebben in het waarborgen van de privacy van de burger. Te denken valt aan PET-technieken, zoals het gescheiden opslaan van identificerende en niet-identificerende informatie en versleuteling van data. In paragraaf 4.9 hebben we gezien dat dergelijke technieken nog weinig worden toegepast, dus hier is nog privacywinst te halen.

Tabel 45 Technologische ontwikkelingen

	Organisaties met een FG	
	Technologische ontwikkelingen leiden ertoe dat de Wbp binnen afzienbare tijd verouderd is	Technologische ontwikkelingen, zoals PET, leveren in de toekomst een belangrijke bijdrage aan het waarborgen van de privacy van de burger
Zeer mee eens	7,2%	10,1%
Mee eens	18,8%	31,9%
Neutraal	43,6%	46,5%
Mee oneens	24,6%	7,2%
Zeer mee oneens	5,8%	4,3%
Totaal	100%	100%

Aan de FG's is ook gevraagd een inschatting te geven over het belang dat de burger in de toekomst zal hechten aan privacybescherming. Zoals uit Tabel 46 blijkt, leiden deze stellingen tot sterker geformuleerde opinies dan veel andere stellingen. Burgers zullen hun privacy in de toekomst belangrijk blijven vinden. Ook zullen technologische veranderingen niet leiden tot minder aandacht voor privacybescherming. Verder wordt breed onderschreven dat privacybescherming voor de burger ook in de toekomst een actueel onderwerp zal blijven.

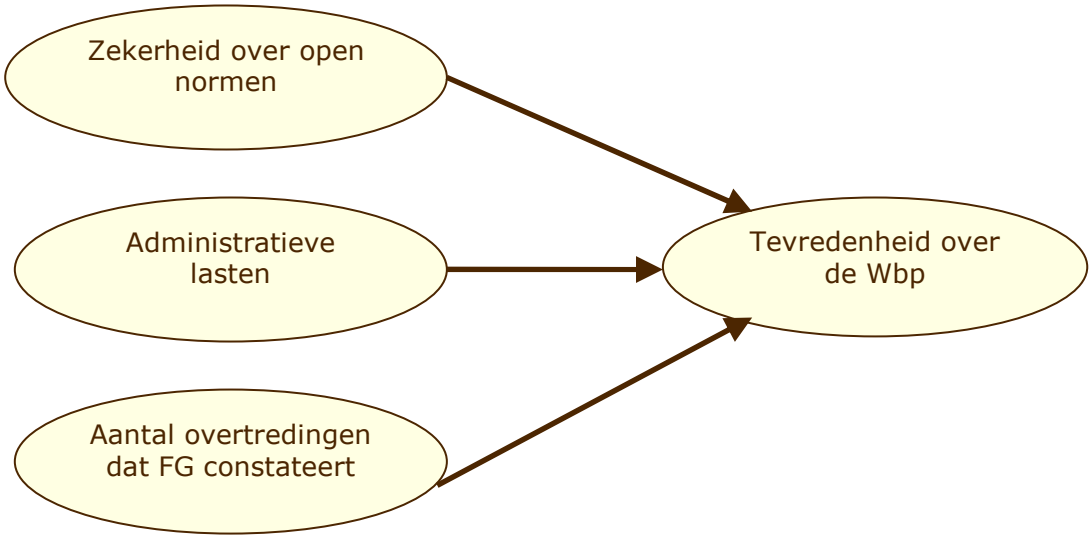
Tabel 46 Door FG's verwachte actualiteit van privacybescherming in de toekomst

	Organisaties met een FG		
	Burgers zullen hun privacy in de toekomst minder belangrijk vinden	Door verandering van technologie zal de privacybescherming in de toekomst actueel blijven	Door verandering van de houding van de consument zal het belang van privacybescherming actueel blijven
Zeer mee eens	2,9%	36,2%	18,8%
Mee eens	18,8%	52,3%	55,2%
Neutraal	17,5%	10,1%	24,6%
Mee oneens	47,8%	1,4%	1,4%
Zeer mee oneens	13,0%	0,0%	0,0%
Totaal	100%	100%	100%

5.9 Verklaring tevredenheid van FG's over de Wbp

Er is een analyse uitgevoerd op het bestand van de *organisaties met een FG*. Wanneer een statistische analyse wordt uitgevoerd met het 'rapportcijfer' voor de Wbp als afhankelijke variabele, blijken drie onafhankelijke variabelen de hoogte van dat rapportcijfer substantieel en statistisch significant te beïnvloeden. Figuur 8 geeft dat schematisch weer. Voor een

gedetailleerde beschrijving van de opbouw van de variabelen en de uitgevoerde analyse wordt verwezen naar bijlage 5.



Figuur 8 Verklaring van de tevredenheid van FG's over de Wbp

Met de drie variabelen die in Figuur 8 zijn weergegeven kan een groot deel (61 procent) van de hoogte van het rapportcijfer over de tevredenheid over de Wbp worden verklaard. De belangrijkste bron van tevredenheid over de Wbp blijkt duidelijkheid over de toepassing van de open normen in de wet te zijn. Daarnaast zijn de ervaren hoogte van de administratieve lasten en het aantal door de FG geconstateerde onjuiste verwerkingen van belang. Kort samengevat leiden de volgende zaken tot een *hoge waardering* voor de Wbp:

1. Er is duidelijkheid over de manier waarop de open normen in de Wbp moeten worden toegepast. Deze variabele is grofweg twee maal zo sterk als de andere twee variabelen. Duidelijkheid over de manier waarop de open normen moeten worden ingevuld leidt tot zekerheid over een juiste uitvoering van de Wbp. Wanneer deze duidelijkheid er onvoldoende is en men de gegevens toch gaat verwerken, heeft men te maken met niet goed in te schatten juridische risico's voor de organisatie, zoals het risico op constatering van normschending door het Cbp en juridische acties van betrokkenen. Maar ook het door de onduidelijkheid niet verwerken van de gegevens leidt voor de organisatie tot een ongewenste uitkomst, namelijk tot een onderbenutting van gegevens die men niet durft te verwerken of uit te wisselen. Duidelijkheid over hoe de wet moet worden uitgevoerd blijkt zowel bij organisaties die risico's accepteren als bij organisaties die risico's mijden een positieve uitwerking te hebben. Dit zou een verklaring kunnen zijn waarom de indicator voor risicovermijding geen verschil laat zien tussen deze twee groepen.
2. De administratieve lasten van de Wbp worden als laag ervaren. Lage administratieve lasten leiden tot een hoge waardering voor de wet omdat het de organisatie weinig tijd, geld of moeite kost om de wet uit te voeren.
3. De FG constateert jaarlijks veel onrechtmatige verwerkingen van persoonsgegevens. Wanneer de FG jaarlijks veel onrechtmatige verwerkingen constateert, betekent dit dat de FG er keer op keer aan wordt herinnerd dat de Wbp een nuttige functie vervult. Dat draagt bij aan de tevredenheid over de Wbp.

5.10 Samenvatting

In het onderhavige onderzoek zijn in de drie in hoofdstuk 4 onderscheiden steekproeven, te weten de *organisaties in het algemeen*, de *meldende organisaties* en de *organisaties met een FG*, vragen gesteld die betrekking hebben op de opinie van de vertegenwoordigers van deze organisaties. Dit is gebeurd aan de hand van stellingen waarop de respondent kon aangeven in hoeverre hij het ermee eens is of in hoeverre iets het geval is. Op deze wijze is behalve feitelijke informatie tevens informatie over houdingen, meningen en attitudes verkregen.

Veel respondenten geven aan dat zij privacy belangrijk vinden. Dit belang dat aan privacy wordt gehecht moet echter om drie redenen worden gerelativeerd. In de eerste plaats is belang hechten aan privacy binnen de context van het onderzoek een sociaal wenselijk antwoord. In de tweede plaats wordt de belangstelling voor privacy minder als deze moet worden afgewogen tegen het organisatiebelang en in de derde plaats blijkt dat zeer veel respondenten – waaronder de FG's – in veel gevallen, door de hele enquête heen de antwoordcategorie 'neutraal' hebben ingevuld. Daaruit valt af te leiden dat vragen over privacy vrijwel nooit tot stellige of gepolariseerde meningen leiden. Dit is mogelijk een gevolg van het onvoldoende leven van het onderwerp binnen de onderzochte organisaties.

De open normen in de Wbp leiden volgens de respondenten nauwelijks tot problemen. Veel respondenten geven aan geen kennisgebrek op dit gebied te hebben. De groep die de grootste problemen ondervindt van de open normen zijn de FG's. Enerzijds werken zij met veel meer (en mogelijk complexere) gegevensbestanden (zie hoofdstuk 4), anderzijds zijn zij beter in de wet ingevoerd, waardoor het waarschijnlijk is dat zij de problemen in de wet beter onderkennen. Het ontbreken van problemen met de open normen zou bij de *organisaties in het algemeen* en de *meldende organisaties* heel goed kunnen worden toegeschreven aan een gebrek aan aandacht. Wat niet weet, wat niet deert.

In ongeveer één op de drie gevallen stellen organisaties te weinig kennis te hebben om de meldingsplicht goed uit te voeren. Daarbij lijkt het kennisgebrek bij de FG's iets kleiner te zijn dan bij de *meldende organisaties*. Door een groot aantal *organisaties met een FG* wordt bij iedere verwerking een expliciet doel vastgesteld, maar toch weet bijna de helft van de FG's niet precies hoe zo'n doelstelling er uit hoort te zien. Waar de FG's het wel over eens zijn, is dat het melden een positieve invloed heeft op de privacy van betrokkenen. Die verbetering komt volgens de FG's voornamelijk omdat de meldingsprocedure het nadenken over de doelstelling en de op te verwerken persoonsgegevens stimuleert. In hoofdstuk 4 hebben we geconstateerd dat betrokkenen nauwelijks gebruik maken van hun rechten op inzage, correctie, verwijdering, verzet, bezwaar en beroep. Toch is een grote meerderheid van de FG's van mening dat deze rechten een positieve bijdrage hebben geleverd aan de privacy van betrokkenen. Er kan verondersteld worden dat ondanks dat betrokkenen hun rechten weinig gebruiken, de aandacht voor de Wbp en privacy ervoor heeft gezorgd dat organisaties meer privacybewustzijn hebben gekregen. Dit blijft echter speculatie, want er zijn ook aanwijzingen dat het onderwerp privacy niet erg leeft binnen deze organisaties.

Bij de meeste organisaties leiden de privacyregels uit de Wbp niet tot grote administratieve lasten. Het grote aantal 'neutraalstemmers' is hier met name opvallend. Blijkbaar hebben veel respondenten geen uitgesproken mening over dit punt. Slechts weinig organisaties geven aan belemmerd te worden in hun activiteiten. In hoofdstuk 4 hebben we gezien dat als de Wbp knelt, dit vooral gebeurt bij het verstrekken van gegevens aan andere organisaties, bij het combineren van bestanden, bij samenwerking en bij het verkrijgen van informatie van andere

organisaties. Ongeveer een derde van de FG's vindt de administratieve lasten te hoog. De Wbp sluit goed aan bij de heersende privacypraktijk bij de ondervraagde organisaties.

De FG's hebben over het algemeen goede toegang tot het management en zij voelen zich gesteund door de organisatie. De FG's ervaren over het algemeen dat zij een positieve invloed hebben op de privacy van betrokkenen. De veronderstelling dat het Cbp een rol van tweede lijnstoezichthouder op zich neemt als een FG wordt aangesteld komt overeen met de ervaring van de FG's. Wel is het zo dat er veel FG's geen regelmatig contact hebben met de contactpersoon van het Cbp. Wat een punt van zorg is, is de onafhankelijkheid van de FG's. Ook in dit deel van de enquête geven de FG's aan dat zij niet volledig onafhankelijk kunnen handelen van de directie. Volgens de ondervraagde FG's zal privacybescherming ook in de toekomst nodig blijven. Technologische ontwikkelingen zullen er volgens de FG's niet toe leiden dat de Wbp binnen afzienbare tijd zal zijn verouderd.

Sommige *organisaties met een FG* zijn meer tevreden over de Wbp dan andere. In dit hoofdstuk is getracht om factoren te vinden die verschillen in de algemene tevredenheid over de Wbp kunnen verklaren. Er springen drie variabelen uit, die een plausibele verklaring leveren voor verschillen in de algehele tevredenheid over de wet. De belangrijkste verklaring is de zekerheid over de open normen. Onzekerheid over de manier waarop de open normen moeten worden ingevuld leidt tot onzekerheid in de bedrijfsvoering en mogelijk juridische risico's. Wanneer deze onzekerheid groot is, krijgt de Wbp een laag cijfer. De tweede verklarende variabele is de hoogte van de administratieve lasten. Wanneer de wet moeilijk uitvoerbaar is, wanneer de organisatie veel tijd en geld in de uitvoering van de Wbp steekt, is de organisatie ontevreden over de wet. De derde verklaring is te vinden in het aantal onjuiste verwerkingen dat de FG constateert. Wanneer een FG veel onjuiste verwerkingen constateert binnen zijn organisatie, is hij meer geneigd een hoog cijfer voor de Wbp te geven. Hiervoor zijn twee verklaringen mogelijk. Enerzijds kan worden geredeneerd dat bij iedere geconstateerde overtreding voor de FG het belang van de Wbp nog eens wordt onderstreept. Anderzijds kan worden geredeneerd dat het de meer betrokken FG's zijn die veel overtredingen constateren. Dit zijn ook de FG's die de Wbp en de bescherming van de privacy serieus nemen.

Hoofdstuk 6 Burgers over geschilbeslechting

6.1 Inleiding

Tot het onderhavige hoofdstuk heeft het empirische deel van het onderzoek zich geconcentreerd op de gedragingen en meningen van verwerkers van persoonsgegevens. Er wordt echter ook getracht de belangen van betrokkenen een gezicht te geven. Betrokkenen vormen een zeer diffuse en daardoor lastig te benaderen groep, die bovendien vaak weinig heeft nagedacht over privacyaspecten. In dit hoofdstuk wordt daarom getracht met een specifiek deel van de betrokkenen in gesprek te komen. Het betreft de betrokkenen die een klachten- of beroepsprocedure tegen een verwerking van persoonsgegevens aanhangig hebben gemaakt. De groep klagende en procederende burgers is een kleine deelverzameling van de totale populatie van betrokkenen. Deze groep is welbepaald en heeft zich wellicht een mening gevormd over het functioneren van de Wbp. Deze doelgroep kan inzicht verschaffen in de vraag waarom een klachten- of beroepsprocedure wordt gestart, waarom voor de betreffende procedure is gekozen en hoe het proces verloopt. Daarnaast kunnen zij aangeven in hoeverre zij tevreden zijn over de gevolgde procedure. Voor de goede orde merken wij hier nog op dat het burgerperspectief meer in het algemeen ook in een expertmeeting met verscheidene burgerbelangenorganisaties aan bod is gekomen.

Wanneer een betrokkene het niet eens is met de verwerking van zijn persoonsgegevens, wanneer een verantwoordelijke weigert inzage te verlenen of gegevens uit een bestand te wijzigen, te verwijderen, aan te passen of af te schermen, staan binnen het regime van de Wbp verschillende wegen voor geschilbeslechting open.

1. Bij een publiekrechtelijke verantwoordelijke kan nadat een bezwaarschriftprocedure is doorlopen beroep worden ingesteld bij de bestuursrechter (art. 45 Wbp).
2. Wanneer de verantwoordelijke een privaatrechtelijke organisatie is, staat de verzoekschriftprocedure bij de civiele rechter open (art. 46 Wbp).
3. Verder kan bij het Cbp een verzoekschrift worden ingediend voor bemiddeling door het Cbp (art. 47 Wbp).
4. Daarnaast kunnen organisaties of branches op grond van art. 25 Wbp gedragscodes door het Cbp laten goedkeuren, waarin zij een eigen geschillencommissies instellen (art. 47 Wbp).
5. Ten slotte kan men als men een klacht heeft over het handelen van een overheid, waaronder het Cbp, in veel gevallen een verzoekschrift indienen bij de Nationale ombudsman.

Er is gepoogd betrokkenen te benaderen die ervaring hebben met procedures voor de civiele rechter, de bestuursrechter, een geschillencommissie en het Cbp. Daarnaast zijn 35 rapporten over privacybescherming van de Nationale ombudsman bestudeerd.

In paragraaf 6.2 wordt een overzicht van de respons gegeven. In paragraaf 6.3 wordt besproken waarom burgers de stap nemen om te procederen. In paragraaf 6.4 wordt de inhoud van het geschil besproken en in paragraaf 6.5 komt het procedurele verloop van de geschilbeslechtingsprocedure aan de orde. In paragraaf 6.6 wordt ingegaan op de uitspraak van de procedure en op welke wijze deze doorwerkt. In paragraaf 6.7 wordt ingegaan op de waardering van de geïnterviewde burgers over de gevoerde procedure. In paragraaf 6.8 wordt ingegaan op de zaken bij de Nationale ombudsman. Ten slotte wordt het hoofdstuk in paragraaf 6.9 samengevat.

6.2 Respons

Het Cbp bemiddelt jaarlijks in een groot aantal geschillen over privacyaspecten. Tabel 47 toont het aantal klachten waarin het Cbp sinds het jaar 2001 heeft bemiddeld. De laatste jaren ligt het aantal bemiddelingen tegen de 400. Uit de zaken waarin het bemiddelt, heeft het Cbp een aantal cases waarin de bemiddeling succesvol is verlopen geselecteerd en vervolgens de betrokkene om toestemming gevraagd om zijn gegevens aan het onderzoeksteam door te geven ten behoeve van het diepte-interview. Hieraan hebben 9 mensen meegewerkt.[210]

Tabel 47 Aantal bemiddelingen van klachten door het Cbp

Jaar	Aantal bemiddelingen
2007	396
2006	394
2005	355
2004	409
2003	316
2002	282
2001	290

Geschillencommissies zijn geselecteerd van www.sgc.nl. Daarbij is gezocht naar commissies die mogelijk privacyzaken behandelen. In totaal zijn acht commissies zowel schriftelijk als telefonisch benaderd om mee te werken aan het onderzoek. Bij de brief was een informatiepakket gevoegd met daarin een uitleg over het onderzoek, de vragenlijst, een aanbevelingsbrief van het WODC, een conceptverzoekbrief voor de burgers en voorbeelden van antwoordkaartjes. Op deze manier is deelname zo gemakkelijk mogelijk gemaakt voor de commissies omdat van hen enkel wordt gevraagd de burgers de aangeleverde brief te sturen. Dat leidde echter niet tot zaken die voor het onderzoek naar geschillenbeslechting bruikbaar waren. Tabel 48 geeft daarvan de redenen weer.

Tabel 48 Redenen voor niet meewerken van geschillencommissies

Reden van weigering	Aantal geschillencommissies
Geen zaken / uitsluitend oude zaken	3
Ondanks herhaalde rappelmails en telefoontjes niet gereageerd	2
Medewerking geweigerd	1
Bijzondere wetgeving van toepassing, medewerking niet zinvol	1
Onbekend	1

Ook bij de civiele en de bestuursrechter bleek het lastig om geschikte zaken te vinden. Er is gezocht in de uitspraken die op www.rechtspraak.nl zijn gepubliceerd en in andere

[210] Het lage aantal medewerkers aan de interviews is onder andere te wijten aan de noodzakelijkerwijs gevolgde aanschrijvingsprocedure. Het Cbp heeft cases geselecteerd en de betrokkenen verzocht om aan te geven of zij aan het onderzoek deel wilden nemen. Alleen wanneer de benaderde betrokkenen actief aangaven deel te willen nemen aan het onderzoek, kreeg het onderzoeksteam hun contactgegevens.

jurisprudentiedatabases. Ook de Nederlandse Orde van Advocaten en een tiental leden van de Nederlandse Vereniging voor Informatierecht Advocaten zijn benaderd. Er bleek bijzonder weinig jurisprudentie over privacy of de Wbp te vinden. Klaarblijkelijk worden niet veel beroepen over privacy bij de rechter aanhangig gemaakt. De gevonden zaken waren veelal te oud om in het onderzoek te betrekken, bijvoorbeeld van voor de inwerkingtreding van de Wbp. Ondanks de relatieve zeldzaamheid van rechtszaken over persoonsgegevens, is toch een beperkt aantal zaken gevonden. Omdat in de jurisprudentie de persoonsgegevens van de procederende betrokkene niet worden gepubliceerd, is telkens met de betrokken advocaat contact opgenomen met de vraag of zijn cliënt aan het onderzoek wilde meewerken. Bij civielrechtelijke zaken was soms echter alleen de procureur bekend en was de advocaat niet meer te achterhalen. In het bestuursrecht is soms geen advocaat bij de procedure betrokken, zodat ook dit spoor enkele keren doodliep. Om deze reden zijn er relatief weinig zaken gevonden die bij de civiele of de bestuursrechter dienden.

De bovenstaande inspanningen hebben geleid tot een beperkt aantal telefonische diepte-interviews. In totaal is met 9 betrokkenen met een geschil of hun rechtshulpverlener een gesprek gevoerd. Er zijn interviews gehouden met betrokkenen (of hun rechtshulpverlener) bij de volgende geschilbeslechters:
1. drie interviews bij de bestuursrechter
2. één interview bij de civiele rechter
3. vijf interviews bij het Cbp

Daarnaast zijn 35 rapporten over privacy vastgesteld door de Nationale ombudsman bestudeerd. Hiervan bleken 15 (mede) betrekking te hebben op de Wbp. Deze 15 rapporten zijn aan een analyse onderworpen, maar er zijn geen gesprekken gevoerd met de betrokkenen. De verslaglegging over de rapporten van de Nationale ombudsman vindt plaats in een afzonderlijke paragraaf.

In dit hoofdstuk wordt over deze gesprekken en rapporten gerapporteerd. De gegevens worden niet zoals in hoofdstuk 4 en 5 op een statistische manier gepresenteerd. De onderzochte procedures worden beschouwd als cases en als zodanig kwalitatief geïnterpreteerd.

6.3 De stap om te procederen

De geïnterviewden starten over het algemeen pas een procedure wanneer zij worden geconfronteerd met de materiële gevolgen van onjuiste gegevensverwerking. Confrontatie met onrechtmatige gegevensverwerking komt voor de geïnterviewde burgers veelal als een onaangename verrassing. De burger wordt geconfronteerd met een weigering of een afwijzing waaruit hij de conclusie trekt dat er persoonsgegevens onrechtmatig moeten zijn verwerkt. Ook kan het zijn dat hij te maken krijgt met een partij die onverwacht een claim op hem legt, zoals in een casus waarin plotseling conservatoir beslag op een auto van een klager werd gelegd. Uit het feit dat dit gebeurde, heeft de burger de conclusie getrokken dat er door de RDW aan de schuldeiser gegevens moesten zijn verstrekt uit het kentekenregister.

In geen enkele casus is de burger door de verantwoordelijke op de gegevensverwerking gewezen. De informatieplicht van de verantwoordelijke speelt derhalve nauwelijks een rol bij het door de burger signaleren van een (onrechtmatige) gegevensverwerking. Burgers nemen

vooral contact op over privacyaangelegenheden in het kader van een geschil over een andere kwestie.

De geïnterviewde klagers kennen de mogelijkheden tot rechtsbescherming die de Wbp kent nauwelijks. In vrijwel alle gevallen zijn zij door de algemene media op de mogelijkheid gewezen om tegen een onjuiste verwerking van persoonsgegevens een procedure te starten. Media die zijn genoemd zijn onder andere het televisieprogramma Tros Radar dat een aantal uitzendingen aan de Dexia-zaak heeft gewijd, een krantenartikel en Postbus 51. In een ander geval dat betrekking had op een arbeidsgeschil heeft de ondernemingsraad een werknemer doorverwezen naar de website van het Cbp. Via die website is vervolgens een bemiddeling door het Cbp opgestart. Zelfstandig kunnen de geïnterviewde burgers de website www.cbpweb en www.mijnprivacy.nl maar moeilijk vinden.

Het belang van het meldingenregister als kennisbron van gegevensverwerkingen kan gemakkelijk worden overschat. Daarvoor zijn grofweg drie redenen. In de eerste plaats kunnen de geïnterviewde klagers de website van het Cbp en daarmee het meldingsregister niet goed vinden. Informatie van derde partijen blijkt daarom van groot belang te zijn voor het starten van een procedure, zowel bij de rechter als bij het Cbp. Het meldingenregister van het Cbp is uitsluitend bekend bij advocaten en specialisten. De advocaten en deskundigen die het meldingenregister kennen, uiten veel kritiek op het register. In de tweede plaats blijkt het voor burgers lastig om het meldingenregister te doorzoeken. De zoektermen die moeten worden ingevuld om een melding te kunnen vinden, zijn volgens de geïnterviewde advocaten voor 'normale' burgers moeilijk te begrijpen. In geen enkele van de in het onderzoek geraadpleegde gevallen heeft de informatie uit het meldingenregister ertoe geleid dat een burger een (vermeend) onrechtmatige verwerking op het spoor is gekomen. In de derde plaats is de informatie die in de meldingen te vinden is volgens sommige geïnterviewden summier te noemen. Het register biedt nauwelijks relevante informatie om in een geschilbeslechtings-procedure mee uit de voeten te kunnen. Een gevolg is dat in de onderzochte procedures geen enkele betrokkene of zijn advocaat in het meldingenregister heeft gekeken om aan extra informatie over de bestreden gegevensverwerking te komen.

6.4 De inhoud van het geschil

Een geschil bevat altijd een claim van de betrokkene. In het onderstaand tekstblok zijn de claims van alle onderzochte cases in het kort inhoudelijk weergegeven. Opgemerkt dient te worden dat dit de weergave van het geschil is volgens de klagers of eisers zonder dat dit beeld is gecorrigeerd door de verantwoordelijke, de rechter of een geschillencommissie. Wanneer de claims worden doorgelezen, wordt duidelijk dat er over een zeer gevarieerd aantal onderwerpen geschillen ontstaan.

Claims van klagers en eisers

Bij de bestuursrechter:

1. Het tegen de Wbp en het eigen privacyreglement in verstrekken van kentekengegevens door de RDW aan derden (een schuldeiser)
2. Onterechte opname op een zwarte lijst van het Alijda-project (malafide huiseigenaren) door de Hoofdofficier van Justitie van Rotterdam. Eis tot verwijdering van deze lijst
3. Na een sollicitatie zonder toestemming van de eiser doorgeven van het personeelsdossier door de IND aan de Rechtbank Amsterdam, waardoor zij – nadat zij als laatste kandidaat

was overgebleven – toch niet werd aangenomen.

Bij de civiele rechter:
4. Het onterecht weigeren van het verstrekken van een overzicht van verwerkte persoonsgegevens aan de eiser door Dexia.

Bij het Cbp:
5. Het aangifteprogramma van de belastingdienst biedt sinds 2008 geen mogelijkheid om bestanden ergens anders op te slaan dan in 'mijn documenten'. Dit zou de mogelijkheden tot beveiliging van de gegevens te zeer beperken.
6. Een organisatie die opkomt voor de belangen van een specifieke groep chronisch zieken heeft zonder toestemming van haar leden haar ledenbestand aan een zorgverzekeraar ter beschikking gesteld. De zorgverzekeraar heeft alle leden een aanbod voor een collectieve korting op de zorgpremie gedaan.
7. In verband met een disciplinair onderzoek heeft de werkgever (politie Utrecht) de mailbox van klager ingezien, zonder dat om toestemming is gevraagd.
8. Aanvraag van een DigID door de Sociale Verzekeringsbank voor de klager zonder zijn toestemming.
9. Het opnemen van onterechte gegevens over de klager in het politieregister. Deze gegevens zijn tevens te lang bewaard.

In veel gevallen vragen de geïnterviewde klagers en eisers niet bij de verantwoordelijke om inzage in hun gegevens. In enkele gevallen wordt deze informatie geweigerd, wat een grond kan zijn om een procedure te starten. Wanneer wel informatie wordt verstrekt, wordt de kwaliteit van de gegevens door de geïnterviewde meestal als onvoldoende beschouwd. In één geval heeft de klager moeten betalen voor de informatie (4,80 euro).

De geïnterviewden procederen in enkele gevallen vanwege principiële belangen. Hieronder verstaan wij een belang waarbij er geen direct financieel of materieel gevolg voor de betrokkene bestaat. Een voorbeeld hiervan is een procedure bij het Cbp van een klager die principieel van mening was dat het aangifteprogramma van de belastingdienst de mogelijkheid moet bieden om de ingevulde belastingaangifte in een andere map op te slaan dan 'mijn documenten' omdat de gevoelige financiële gegevens bij inbraak in zijn computer anders voor anderen te gemakkelijk zouden kunnen worden gevonden. Deze claim is overigens door het Cbp niet-ontvankelijk verklaard omdat er geen sprake zou zijn van verwerking in het licht van de Wbp. Een ander voorbeeld is de aanvraag van een DigID door de Sociale Verzekeringsbank. Procedures om principiële belangen horen voor zover dat bij deze kleine aantallen kan worden gesteld tot een minderheid van de gevallen.

In een meerderheid van de gevallen komt een burger pas in actie wanneer zijn belang in een ander onderwerp wordt aangetast als gevolg van een verwerking van persoonsgegevens. Voorbeelden zijn ontslag, het plaatsen van een ondernemer op een zwarte lijst waardoor het lastig wordt om onroerend goed te kopen, het niet krijgen van een baan omdat de huidige werkgever persoonlijke gegevens over het functioneren van de werkgever heeft doorgegeven of het af willen van een aandelenleasecontract. Over het algemeen worden burgers geconfronteerd met een ander probleem, waarna zij de conclusie trekken dat er persoonsgegevens moeten zijn doorgegeven. Degene die daarvoor verantwoordelijk is wordt aangesproken, hoewel daardoor het oorspronkelijke probleem niet zal worden opgelost.

Inhoudelijk gezien kunnen procedures over privacy betrekking hebben op formele aspecten, zoals het verkrijgen van inzage in het dossier met persoonsgegevens. In dat geval maakt de procedure in het kader van de Wbp deel uit van een geschil dat in een andere procedure wordt uitgevochten. De gegevens uit het dossier worden vervolgens gebruikt als processtuk in het materiële geschil over de schadevergoeding of het ontslag. In de onderstaande casus over Dexia is een formele vraag om inzage aan de orde om informatie te vergaren voor een andere procedure met een materiële rechtsvraag.

Een formele rechtsvraag ligt voor in het geschil over de persoonsgegevens inzake de Dexiazaak. In deze zaak weigert Dexia inzage te geven in het dossier van de verwerkte persoonsgegevens. Zij voert daarin onder andere aan dat het opvragen van persoonsgegevens door de eisers misbruik van recht is. Er is volgens Dexia misbruik van recht omdat de eiser tevens een civiele procedure aanhangig heeft met daarin een schadeclaim en een verzoek tot ontbinding van het aandelenleasecontract. Daarnaast stelt Dexia dat de gegevens om verschillende redenen geen persoonsgegevens in de zin van de Wbp zijn en derhalve niet hoeven te worden verstrekt. De rechter maakt korte metten met deze redenering van Dexia.[211]

Naast een formele rechtsvraag kan een procedure over de Wbp een materiële rechtsvraag als grondslag hebben. Een rechtsvraag die dan voor kan liggen is of de verantwoordelijke gegevens mocht verstrekken aan een derde, hoe lang gegevens bewaard mogen worden en of een werkgever inzage mag hebben in de mailgegevens van een werknemer. Ook bij materiële rechtsvragen kan de procedure over de Wbp een middel zijn om aan argumenten of bewijs in een andere (materiële) beroepszaak te komen.

Dit is bijvoorbeeld gebeurd in het arbeidsconflict waar de rechtsvraag aan de orde was of de werkgever mocht inbreken in de persoonlijke mailbox van de klager. De voor de klager positieve uitspraak van het Cbp is toegevoegd aan het dossier van het hoger beroep van het arbeidsconflict bij de Centrale Raad van Beroep. De rechter heeft overigens nauwelijks naar het oordeel van het Cbp gekeken en er slechts één alinea in zijn uitspraak aan gewijd. Hieruit bleek dat de rechter zich niet gebonden achtte aan het oordeel van het Cbp omdat de inbraak in zijn persoonlijke mailbox “geen verband heeft met (het bewijs van) de aan het voorwaardelijk strafonderzoek ten grondslag gelegde feiten. De bevindingen van het Cbp kunnen niet afdoen aan de zorgvuldigheid van het onderzoek dat tot het voorwaardelijk strafontslag heeft geleid”.[212] Het oordeel van het Cbp heeft dan ook geen enkele materiële invloed gehad op de uitspraak in het arbeidsgeschil.

6.5 Het procedurele verloop

De inrichting van de procedures bij de drie onderzochte geschilbeslechtingsfora verschilt onderling nogal. Enerzijds zijn er de formele procedures bij de rechtbank, anderzijds de ‘lichtere’ procedure bij het Cbp. Wanneer de betrokkene een beroep doet op de rechter is de rechtsgang een gedwongen keuze. De keuze voor bemiddeling door het Cbp is daarentegen vrij en kan naast een rechtszaak plaatsvinden. De geïnterviewde klagers kiezen voor een procedure bij het Cbp omdat hen dit effectief lijkt. Overigens moeten we daarbij in ogenschouw nemen dat de procedure in veel gevallen deel uitmaakt van een groter geschil

[211] Rechtbank ’s Gravenhage, 19 mei 2005, LJN: AY5824.
[212] Centrale Raad van Beroep, 24 januari 2008, LJN: BC2900

over een andere aangelegenheid, waarbij van de procedure over de Wbp gebruik wordt gemaakt om extra informatie te verkrijgen.

De procedure bij het Cbp is eenvoudig en weinig formeel. Het kunnen starten van een procedure begint bij het herkennen van de juiste verantwoordelijke. Wanneer er persoonsgegevens van de ene naar de andere organisatie worden doorgegeven, kan het voor de klagende burger soms lastig zijn om de juiste verantwoordelijke te ontdekken. Zie de volgende casus.

Het betrof de zaak waarin een belangenorganisatie van een bepaalde groep chronisch zieken persoonsgegevens uit haar ledenadministratie had doorgegeven aan een zorgverzekeraar, die vervolgens aan de leden van de belangenorganisatie een goedkope zorgverzekering aanbood. De ondervraagde klager is vervolgens een procedure tegen de zorgverzekeraar gestart bij het Cbp. Volgens het Cbp moest deze procedure echter gericht worden tegen de belangenorganisatie. Vervolgens is de klager op advies van het Cbp tevens een procedure tegen de belangenorganisatie gestart. Toen de klager enige tijd later door het Cbp ongelijk kreeg in de zaak tegen de zorgverzekeraar, dacht ze dat daarmee de zaak was afgedaan. Toen enige tijd later de klager van het Cbp gelijk kreeg in de zaak tegen de belangenorganisatie, kwam dit als een volslagen verrassing. Doordat er twee procedures door elkaar liepen, is de klager het overzicht kwijtgeraakt.

De procedure bij het Cbp wordt als toegankelijk beoordeeld. Eén geïnterviewde gaf aan dat na het indienen van het verzoek de procedure vanzelf liep. Een andere gaf aan dat er nog veel brieven gestuurd moesten worden, maar dat was niet erg lastig. Ook geeft het Cbp duidelijk aan hoe het verloop van de procedure is. Wat sommige klagende burgers als problematisch ervaren, is dat men eerst moet afwachten of het Cbp de klacht in behandeling neemt. Wanneer de klacht wel in behandeling wordt genomen, bestaat de indruk dat het Cbp erg actief is in het boven water krijgen van informatie en dossiers van de verantwoordelijke, vooral wanneer het om een belangrijke zaak gaat. Wel vinden de geïnterviewden dat de procedure lang duurt. Het Cbp geeft in zijn folders aan dat het hoor en wederhoor toepast. Uit de reacties blijkt dat het Cbp de klagers niet structureel mondeling hoort. Als er wordt gehoord, dan gebeurt dat telefonisch. Het wordt erg gewaardeerd dat het Cbp voor een actieve opstelling kiest en zelf veel gegevens opvraagt bij de ‘gedaagde’ verantwoordelijke. De waardering voor de bemiddeling door het Cbp blijkt overigens afhankelijk te zijn van de medewerker die de bemiddeling uitvoert. In één geval heeft de geïnterviewde klager te maken gehad met drie verschillende personen die zijn zaak behandelden. Over de eerste bemiddelaar was hij zeer tevreden, over de tweede geheel niet en over de derde was hij weer behoorlijk tevreden.

In een civielrechtelijke procedure is het inschakelen van een advocaat verplicht. Bij de bestuursrechter kan een advocaat of een andere rechtshulpverlener worden ingeschakeld, maar dat is niet verplicht. In alle onderzochte gevallen heeft de eiser zich in de procedure bij de bestuursrechter laten bijstaan door een advocaat of een rechtshulpverlener. Het starten van een procedure bij de rechtbank kost de eisers nauwelijks moeite, mede omdat het opstellen van het verzoek- of beroepschrift wordt overgelaten aan de advocaat of rechtshulpverlener. Rechtbanken kiezen duidelijk een formelere en meer lijdelijke opstelling dan het Cbp. De geïnterviewde eisers gaven een aantal malen aan dat zij de procedure bij de rechter te formeel vonden. Ook is wel eens aangegeven dat de rechter minder inhoudelijk toetst dan het Cbp. Bij de rechterlijke procedures ligt de verantwoordelijkheid om stukken aan te dragen bij de (advocaat van) de eiser. Alle geïnterviewde eisers zijn gehoord op een zitting.

Ten aanzien van de rechtbank is een klacht dat de beroepsprocedures lang duren. De beroepsprocedures duren gemiddeld langer dan een jaar. Daar komt nog bij dat om bij de bestuursrechter te geraken eerst een bezwaarprocedure moet worden doorlopen. Enkele geïnterviewden hebben aangegeven dat het doorlopen van de bezwaarprocedure moeite kost. Dat had voornamelijk te maken met het gebrek aan medewerking van de verantwoordelijke.

In de zaak over de zwarte lijst van het Alijda-project moest eerst bezwaar worden aangetekend bij de Hoofdofficier van Justitie in Rotterdam. Geëist werd dat de gegevens van de eiser van de zwarte lijst zouden worden verwijderd. De procedure voor de Raad van State duurde relatief kort (32 weken). De bezwaarschriftprocedure was volgens de advocaat van de eiser een 'drama'. Deze duurde 30 weken. Volgens de advocaat lag deze zaak gevoelig omdat het OM niet bereid is de criteria voor de zwarte lijst aan te passen. Het beroep is – na een ongegrondverklaring door de Rechtbank Rotterdam – in hoger beroep voor de Raad van State volledig gegrond verklaard.[213] Dat betekent dat de Hoofdofficier van Justitie binnen 6 weken een nieuw besluit moet nemen dat recht doet aan de uitspaak van de Raad van State. Ten tijde van het interview – een jaar na de uitspaak in hoger beroep – moest de Hoofdofficier van Justitie dit nieuwe besluit nog nemen.

Bezwaarschriftprocedures nemen soms erg veel tijd in beslag doordat de verantwoordelijke geen belang heeft bij het voortvarend doorlopen van de bezwaarprocedure. Ook binnen de procedures die bij het Cbp worden doorlopen nemen de geïnterviewden soms waar dat de verantwoordelijke geen prioriteit geeft aan een goede en snelle medewerking. In een enkel geval vermoedt de geïnterviewde zelfs dat de verantwoordelijke de procesgang bewust traineert. Het Cbp moet soms bijvoorbeeld herhaalde verzoeken doen om inzage te krijgen in de stukken waarom het vraagt. De geïnterviewden geven aan dat er een stok achter de deur ontbreekt om tijdige en volledige medewerking van de verantwoordelijke af te dwingen. Bij geschillen met de overheid moet deze opmerking worden gerelativeerd omdat in de Algemene wet bestuursrecht termijnbepalingen staan. Daarnaast kan tegen de overheid beroep worden ingesteld wegens niet tijdig beslissen.

6.6 De uitspraak en daarna

In twee van de drie gevallen is in het beroep op de bestuursrechter de zaak gegrond verklaard. De zaak bij de civiele rechter is (grotendeels) door de burger gewonnen. Bij het Cbp is één zaak niet in behandeling genomen omdat er geen sprake was van verwerking van persoonsgegevens volgens de Wbp (de zaak over het aangifteprogramma van de belasting), maar in de overige gevallen geeft de klager aan dat de bemiddeling gelukt is. Burgers klagen meestal terecht over schending van hun privacyrechten.

Het oordeel van het Cbp is niet bindend. De uitspraak van de rechtbank is wel bindend voor alle partijen. In één procedure bij de bestuursrechter leidde dit niet direct tot het gewenste resultaat. De bestuursrechter heeft een besluit van de Hoofdofficier van Justitie vernietigd en deze zou een nieuw besluit moeten nemen. Dit herziene besluit laat inmiddels meer dan een jaar op zich wachten.

Uit een uitspraak van de rechter in de casus over de inbraak in de mailbox van een politiewerknemer blijkt dat de bestuursrechter vaststelt dat de werkgever volgens het Cbp de

[213] Raad van State, 4 juli 2007, LJN: BA8742

privacy van de werknemer weliswaar heeft geschonden, maar omdat er overigens op zorgvuldige wijze voldoende bewijs is verzameld kan de ontslagbeslissing toch stand houden.[214]

Ook wanneer bewijs is verkregen door schending van privacy kan het soms worden gebruikt in een (civiele) rechtszaak. De FNV geeft in een mail aan het onderzoeksteam aan dat "een specifiek probleem bij bescherming tegen aantasting van de privacy is dat de civiele rechter toelaat dat de werkgever in een rechtszaak bewijs tegen zijn werknemers inbrengt dat hij alleen heeft kunnen verkrijgen door de privacy van zijn werknemers te schenden." Onrechtmatig verkregen bewijs kan in het civiele recht gewoon worden gebruikt.

Voor verantwoordelijken is het oordeel van het Cbp niet bindend. Eén geïnterviewde heeft aangegeven dat het goed zou zijn dat het Cbp wél een bindend advies aan de verantwoordelijke kan geven. In deze casus moest het Cbp bij de politie in Geldrop verschillende malen herhalen dat de persoonsgegevens uit het politieregister moesten worden verwijderd. In een dergelijk geval zou het Cbp volgens deze geïnterviewde daadkrachtiger moeten kunnen optreden tegen de verantwoordelijke. In meer gevallen geven burgers aan dat de uitkomst van de procedure niet tot een verandering in het gedrag van de verantwoordelijke heeft geleid.

6.7 De waardering van de procedure

De waardering voor zowel de rechter als het Cbp is opvallend hoog. Wel lijken de waarderingcijfers afhankelijk te zijn van de uitkomst van het geschil. Vooral de inhoudelijke behandeling wordt goed gewaardeerd. Over het algemeen wordt zowel de rechter als het Cbp als objectief en deskundig beschouwd. Ook voelen de klagers zich serieus genomen, ongeacht of het gaat om een procedure bij het Cbp, de civiele rechter of de bestuursrechter.

Over de procedure zijn de klagers soms wat kritischer. De procedure bij de rechter wordt door sommige geïnterviewden als te formeel en lijdelijk aangemerkt. Ook het tijdsverloop wordt als een belangrijk punt van aandacht genoemd, vooral wanneer de verantwoordelijke weinig bereid is om mee te werken. Toch zijn deze kritiekpunten niet doorslaggevend. Wanneer de ondervraagden in een soortgelijke situatie terecht zouden komen, zouden ze allemaal opnieuw dezelfde procedure starten.

6.8 Procedures bij de Nationale ombudsman

Wanneer een burger een geschil heeft met de overheid kan hij in veel gevallen terecht bij de Nationale ombudsman. Deze instelling levert een laagdrempelige procedure om een geschil te beslechten. Het advies van de Nationale ombudsman is niet bindend. De ombudsman toetst aan verschillende behoorlijkheidsnormen. Eén van de behoorlijkheidsnormen is het recht op eerbiediging van de persoonlijke levenssfeer. De ombudsman omschrijft dit recht als volgt:

> *"eenieder heeft recht op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen. De overheid dient de persoonlijke levenssfeer van haar burgers te eerbiedigen. Bij dit 'recht op privacy' gaat het om bescherming van burgers tegen het vergaren en*

[214] Centrale Raad van Beroep, 24 januari 2008, LJN: BC2900.

doorgeven van persoonlijke gegevens. Dat betekent onder meer dat een bestuursorgaan de informatie die het over een burger bezit niet zonder meer aan derden (zoals andere burgers of bedrijven, of een ander bestuursorgaan of andere ambtenaren) kan overdragen."[215]

Verzoeken van burgers worden door de Nationale ombudsman op verschillende manieren behandeld. Klachten kunnen worden onderzocht, hetgeen leidt tot een rapport, maar er kan ook een interventie door de ombudsman plaatsvinden, een verzoek kan worden terugverwezen naar het bestuursorgaan en een geschil kan tussentijds worden beëindigd. Ongeveer driekwart van de verzoeken doet de Nationale ombudsman af door middel van een interventie, tien procent gaat terug naar het bestuursorgaan, over negen procent wordt een rapport opgesteld en in zes procent van de gevallen wordt het geschil tussentijds opgelost.[216]

In 2007 hadden 17 rapporten betrekking op het recht op eerbiediging van de persoonlijke levenssfeer. Zoals uit de vorige alinea blijkt, vormen deze rapporten een klein deel van het totale aantal geschillen. Deze 17 rapporten vormden 2,2 procent van het totale aantal rapporten van de Nationale ombudsman in 2007.[217] Tabel 49 toont aan dat dit aantal en percentage niet afwijkt van de aantallen en percentages in de voorgaande jaren. In de afgelopen 6 jaar is 41 procent van de verzoeken waarover een rapport is opgesteld gegrond verklaard.

Tabel 49 Aantal rapporten over het recht op eerbiediging van de persoonlijke levenssfeer bij de Nationale ombudsman[218]

	Aantal rapporten over het recht op eerbiediging van de persoonlijke levenssfeer			
	Aantal gegrond	Aantal ongegrond	Totaal aantal	% van alle rapporten
2007	10	7	17	2,2
2006	16	18	34	3,4
2005	9	9	18	1,7
2004	1	4	7[219]	0,5
2003	1	6	9[220]	0,6
2002	3	7	13[221]	1,1
Totaal	40	51	98	-

De Nationale ombudsman heeft ten behoeve van het onderzoek 35 rapporten die betrekking hebben op eerbiediging van de persoonlijke levenssfeer geselecteerd en deze aan het onderzoeksteam gegeven. Deze rapporten hebben betrekking op de jaren 2005 – 2008.

Wanneer een verzoek aan de Nationale ombudsman betrekking heeft op de eerbiediging van de persoonlijke levenssfeer, wil dat nog niet zeggen dat de Wbp in het geding is. In de rapporten is goed omschreven welk toetsingskader is gehanteerd bij de beoordeling van het

[215] http://www.nationaleombudsman.nl/pdf/Behoorlijkheidswijzer.pdf
[216] Jaarverslag Nationale ombudsman 2007
[217] Jaarverslag Nationale ombudsman 2007
[218] Bron: jaarverslagen Nationale ombudsman.
[219] Twee rapporten hebben niet tot een oordeel geleid.
[220] Twee rapporten hebben niet tot een oordeel geleid.
[221] Drie rapporten hebben niet tot een oordeel geleid.

geschil. Aan de hand van dit toetsingskader kon worden vastgesteld in welke geschillen de Wbp een rol heeft gespeeld. Van de 35 bestudeerde rapporten over privacy bleek de Wbp in 15 gevallen onderdeel van het toetsingskader uit te maken. In de overige 20 gevallen was een geschil dat binnen het kader van bijzondere privacyregelgeving speelde aan de orde. Opvallend is het grote aantal geschillen dat betrekking heeft op het optreden van politie en justitie. Het meest voorkomende toetsingskader na de Wbp is dan ook de Wet politieregisters (9 maal). Maar ook het wetboek van Strafrecht / Strafvordering (3 maal) is vaak toetsingskader bij de Nationale ombudsman wanneer het gaat om het gebruik van persoonsgegevens. Twee maal is verwezen naar de (oude) Wet Persoonsregistraties. De overige wetgeving is divers, variërend van de Kadasterwet, de Wet Justitiële en Strafvorderlijke gegevens, de WOB, de Algemene wet inzake rijksbelastingen en de Politiewet. Een verwijzing van de Nationale ombudsman naar art. 10 Grondwet en art. 8 EVRM komt ook regelmatig voor. Omdat in deze evaluatie de Wbp centraal staat, zal verder uitsluitend worden ingegaan op de 15 zaken waarin de Wbp het toetsingskader was.

In het onderstaande tekstblok is een korte omschrijving gegeven van de inhoud van de claim in de 15 onderzochte geschillen bij de Nationale ombudsman.

Claims van betrokkenen

1. De Officier van Justitie heeft verslagen van telefoongesprekken aan de raadsvrouw van één van de slachtoffers van een ontuchtzaak met minderjarigen verstrekt.
2. De gemeente Haarlem zond vrijwel het gehele dossier van verzoekster, met daarin informatie over verzoeksters persoonlijke problemen in het verleden naar het re-integratiebedrijf gestuurd.
3. Door een verschrijving bij het opgeven van zijn rekeningnummer aan de Belastingdienst werd een voor verzoeker bestemde teruggaaf gestort op rekening van een derde. De Belastingdienst kon pas na de vakantie van de behandelend ambtenaar de gegevens van deze derde verstrekken om het geld terug te krijgen.
4. Verzoeker klaagde erover dat een arbeidsdeskundige van het UWV met betrekking tot zijn verzoek om een deskundigenoordeel de voor verzoeker ter inzage aangeboden correspondentie tussen verzoeker en zijn werkgever niet wilde inzien.
5. Verzoeker klaagde dat zijn zorgverzekeraar hem vooraf niet afdoende had geïnformeerd over een overeenkomst met een ziekenhuis dat de nota van een behandeling rechtstreeks van het ziekenhuis naar de zorgverzekeraar werd gestuurd. Aan de verzoeker is niet de mogelijkheid geboden om van die overeenkomst te worden uitgesloten.
6. Ambtenaren van de AID waren bij verzoeker binnengetreden i.v.m. controle op een prepareervergunning. Na deze binnentreding is een verzoek gedaan om wijziging van persoonsgegevens in het register van de AID. In het besluit van de AID is geen rechtsmiddelenverwijzing opgenomen.
7. De zoon van de vriendin van verzoeker, de heer H., was cliënt bij de Reclassering. Een medewerker had verzoeker toegezegd om alle informatie over H. aan hem te verstrekken. Verzoeker klaagde dat deze toezegging niet werd nagekomen en dat hij is verwezen naar een klachtenregeling. Later bleek dat zijn klacht niet in behandeling kon worden genomen omdat hij niet tot de kring van klachtgerechtigden behoorde.
8. N.a.v. een aangifte van een vroegere echtgenote werd verzoeker gehoord als verdachte van seksueel misbruik van zijn kinderen. De zaak werd geseponeerd wegens gebrek aan bewijs. Verzoeker verzocht om afgifte van de aangifte/processen-verbaal vanwege een civiele procedure tegen zijn ex.
9. De Intergemeentelijke Sociale Dienst heeft een bezwaarschrift met alle bijlagen naar de bezwaarschriftcommissie gestuurd. De ISD heeft de verzoeker niet geïnformeerd over de

mogelijkheid de bankafschriften onleesbaar te maken.
10. Verzoekster heeft een verzoek bij het Cbp ingediend voor een onderzoek naar de onjuiste verwerking van haar gegevens door enkele medische instanties. Verzoekster klaagt dat het Cbp deze klacht niet in behandeling heeft genomen.
11. De gemeente Kampen heeft in verband met een verkort verzoek om kwijtschelding van gemeentelijke belastingen kopieën van bankafschriften aan verzoekster gevraagd.
12. In het kader van de Wet werk en bijstand heeft de gemeente Oirschot van verzoeker verlangd dat deze een blanco machtiging ondertekende voor het opvragen van informatie bij derden, de gemeente heeft alle gegevens betreffende persoonsgebonden budgetten bij haar opgevraagd en er is ten onrechte informatie opgevraagd bij een aantal instanties.
13. Verzoekster is werkzaam bij de Arbeidsinspectie. Haar werkgever liet haar schriftelijk weten dat tijdens een periode van ziekte haar teamleider haar mailbox heeft ingezien en dat hierbij berichten zijn aangetroffen waarin zij zich laatdunkend uitlaat over haar werk en haar teamleider.
14. De arbeidsinspectie is als toezichthouder op de naleving van de Wet arbeid vreemdelingen bevoegd om werknemers te controleren op hun identiteit en nationaliteit. Verzoeker klaagt dat de arbeidsinspectie tijdens een controle bij zijn werkgever zonder toestemming digitale foto's heeft gemaakt van de werkzame personen.
15. Consulenten van de gemeente hebben tijdens huisbezoeken in het kader van de Wet werk en bijstand zonder toestemming kasten geopend, voorwerpen aangeraakt en naar privacygevoelige informatie gevraagd.

De stap om een verzoek bij de Nationale ombudsman in te dienen wordt – net als bij de overige fora – vooral genomen omdat de burger wordt geconfronteerd met de materiële gevolgen van een onjuiste gegevensverwerking. De informatieplicht van de verantwoordelijke of het meldingenregister van het Cbp lijken ook nauwelijks een rol te spelen. Eén maal is een verzoek ingediend omdat een zorgverzekeraar de verzoeker niet afdoende had geïnformeerd over een overeenkomst met een ziekenhuis dat de nota van een behandeling rechtstreeks van het ziekenhuis naar de zorgverzekeraar werd gestuurd.

Net als bij de claims bij de andere geschilbeslechtingsfora is voor verzoeken bij de Nationale ombudsman een verdeling te maken naar principiële en materiële motieven om een procedure te starten. Het lijkt erop dat de geschillen bij de Nationale ombudsman wat principiëler van aard zijn dan de geschillen bij de overige fora, en dat in relatief veel gevallen de verzoeker geen duidelijk aanwijsbare materiële schade ondervindt van de gedraging van de verantwoordelijke. Een mogelijke verklaring hiervoor is dat de procedure bij de Nationale ombudsman dermate laagdrempelig is, dat er geen afweging hoeft te worden gemaakt om niet te procederen omwille van de hoge kosten.

Er zijn twee formele rechtsvragen gevonden in de bestudeerde rapporten. Eén formele vraag die voorlag was in het geval dat de AID geen rechtsmiddelenverwijzing heeft opgenomen in de weigering wijzigingen van persoonsgegevens aan te brengen in het register van de AID. Een andere formele vraag is of het Cbp de beleidsvrijheid heeft om verzoeken om een onderzoek in te stellen te weigeren. Volgens de Nationale ombudsman heeft het Cbp op basis van de Wbp deze beleidsvrijheid overigens. In één geval is komen vast te staan dat een verzoek bij de Nationale ombudsman is ingediend met het doel informatie te verkrijgen dat als bewijsvoering in een andere (civielrechtelijke) procedure kan worden gebruikt. In de overige gevallen komen vooral materiële rechtsvragen aan de orde.

In totaal zijn drie verzoeken ingediend vanwege verstrekking van gegevens aan derden. Ook is de Nationale ombudsman drie maal om een oordeel verzocht vanwege de weigering van het bestuursorgaan om gegevens van (onder andere) derden aan de verzoeker te verstrekken.

In precies tweederde van de onderzochte rapporten heeft de Nationale ombudsman geoordeeld dat de klacht gegrond was.

6.9 Samenvatting

Geschilbeslechtingsprocedures over privacyzaken komen weinig voor. Weliswaar bemiddelt het Cbp regelmatig in geschillen over privacyzaken, er worden slechts weinig rechtszaken over deze materie gevoerd. Ook bestaat de indruk dat er weinig zaken bij geschillencommissies aanhangig worden gemaakt. Deze waarneming past goed bij de constatering in hoofdstuk 4 dat betrokkenen nauwelijks betrokken zijn bij de bescherming van hun persoonsgegevens. Klaarblijkelijk weegt de te verwachten winst van de beroepsprocedure niet op tegen de kosten van een beroepsprocedure (met vaak hoge kosten voor rechtsbijstand). Procedures die uitsluitend betrekking hebben op principiële belangen worden nauwelijks gevoerd. Burgers komen pas in actie tegen een verwerking van persoonsgegevens wanneer de verwerking een objectieve aantasting van een ander belang teweeg brengt. Er wordt dan nog vaak gekozen voor de laagdrempelige bemiddelingsprocedure bij het Cbp. Privacyprocedures zijn instrumenteel voor het boven water krijgen van informatie in andere, materiële geschillen.

De bemiddelingsprocedure bij het Cbp is minder formeel dan de procedure bij de civiele of de bestuursrechter. Hierom wordt de procedure bij het Cbp hoog gewaardeerd door de klagers. Vooral de actieve opstelling van het Cbp, waarbij het Cbp veel werk verricht om informatie van verantwoordelijke te krijgen wordt door klagers gewaardeerd. De procedure is laagdrempelig, weinig formeel en gemakkelijk te volgen. Bij doorgifte van persoonsgegevens van de ene naar de andere verantwoordelijke bleek het voor een klagende burger onduidelijk welke verantwoordelijke moest worden aangeschreven en daalde de waardering iets. Het Cbp wordt door de ondervraagde klagers beschouwd als een onafhankelijke en deskundige geschilbeslechter.

De procedure bij rechtbanken is hoogdrempelig en vooral formeel. De rechter stelt zich lijdelijk op. Een sterk punt van rechtspraak ten opzichte van bemiddeling door het Cbp is het feit dat een rechterlijke uitspraak voor alle partijen bindend is. In de praktijk van het bestuursrecht blijkt echter dat een bestuursorgaan er soms lang over doet om na een onwelgevallige uitspraak een besluit te herzien. Toch wordt de binding van de uitspraak als een groot pluspunt gezien ten opzichte van een advies van het Cbp.

De doorlooptijd van de procedures wordt in veel gevallen als lang ervaren. Het is algemeen bekend dat beroepszaken lang kunnen duren. Bij de informelere procedures, zoals bezwaar en bemiddeling door het Cbp, bestaat bij ondervraagden vaak de indruk dat de verantwoordelijke weinig prioriteit geeft aan een vlotte afhandeling van het beroep. Dit leidt vaak tot termijnoverschrijding. Een stok achter de deur om de verantwoordelijke te dwingen de termijnen te halen wordt gemist.

Ook bij de Nationale ombudsman kunnen betrokkenen terecht met hun klachten over verwerkingen van persoonsgegevens door de overheid. De procedure bij de Nationale ombudsman is laagdrempelig. Na een voorprocedure bij het bestreden bestuursorgaan kunnen

burgers hun klacht bij de ombudsman indienen. Veel klachten worden via de ‘interventiemethode’ afgehandeld, een beperkt deel mondt uit in een rapport. Het merendeel van de klachten in de onderzochte rapporten die betrekking hebben op privacy valt echter niet binnen het regime van de Wbp. In die gevallen is vaak bijzondere wetgeving van toepassing. Opvallend is het grote aantal klachten dat betrekking heeft op informatie in politieregisters. Het aantal Wbp-gerelateerde rapporten is ten opzichte van het totale aantal rapporten relatief gering. De onderwerpen waarover binnen het regime van de Wbp bij de Nationale ombudsman wordt geklaagd zijn vergelijkbaar met de onderwerpen die bij het Cbp aan de orde komen.

Hoofdstuk 7 Het casestudyonderzoek

7.1 Inleiding

Om maatschappelijke problemen aan te pakken, wordt tegenwoordig vaak samengewerkt tussen verschillende instanties. In de publieke sector kan worden gedacht aan samenwerkingsverbanden gericht op het tegengaan van overlast en het bevorderen van de veiligheid. In de semi-publieke sector gaat het bijvoorbeeld om samenwerkingsverbanden bij de uitvoering van sociale zekerheidswetgeving en bemoeizorg. In beide gevallen wordt wel gesproken van ketenzorg. Voor de samenwerking tussen instanties op het niveau van cliënten met problemen is uitwisseling van persoonsgegevens een vereiste.

Uit het knelpuntenonderzoek blijkt dat bij gegevensuitwisseling in samenwerkingsverbanden knelpunten worden ervaren.[222] Allereerst is het met name bij samenwerkingsverbanden moeilijk vast te stellen wie als verantwoordelijke moet worden aangemerkt. Daarnaast is er in de publieke en semi-publieke sector vaak samenloop van de Wbp met andere wetten waarin regels zijn vastgelegd over het verwerken van persoonsgegevens. In combinatie met het hoge abstractieniveau van de Wbp, leidt dit tot een voor de praktijk tot wildgroei van niet samenhangende regels. Een ander punt dat uit het knelpuntenonderzoek naar voren komt, is de lange doorlooptijd van het aan de melding voorafgaande onderzoek. Dit kan vertragend werken bij het voortvarend kunnen oppakken van de maatschappelijk gewenste werkzaamheden door het samenwerkingsverband. Ook is er sprake van onbekendheid met de interpretatieruimte van de Wbp waardoor er, soms ten onrechte, van wordt uitgegaan dat gegevensuitwisseling op basis van bijvoorbeeld een geheimhoudingsplicht niet mogelijk is. In de praktijk, met name in de publieke sector, bestaat veelal het beeld dat gegevensuitwisseling in samenwerkingsverbanden wordt gehinderd door privacywetgeving.[223] Ook bij een 'klantgerichte dienstverlening' waarbij gegevens slechts eenmaal worden opgevraagd, wordt de Wbp als belemmerend ervaren. Ten slotte heeft het Cbp geconcludeerd dat bij samenwerkingsverbanden regelmatig in strijd wordt gehandeld met de artikelen 8, 9 en 11 van de Wbp doordat deelnemers informatie krijgen over betrokkenen waarmee zij niets te maken hebben of, als het gaat om een betrokkene waarmee ze wel een relatie hebben, informatie krijgen die voor de uitvoering van hun taak niet noodzakelijk is.[224]

In hoofdstuk 1 is aangegeven dat er met behulp van casestudies onderzoek is gedaan naar de geconstateerde knelpunten bij gegevensuitwisseling in samenwerkingsverbanden. Er is een tweetal samenwerkingsverbanden bestudeerd op beleidsterreinen in de publieke en semi-publieke sector. Het doel van het casestudyonderzoek was om een antwoord te vinden op deelvraag 5:

Op welke manier vormt de normering van de Wbp een knelpunt in de (keten)samenwerking?

Hierbij is gekeken of de in de literatuur geconstateerde knelpunten zich in de praktijk werkelijk voordoen en zo ja, wat de omvang daarvan is. Het casestudyonderzoek was niet in de eerste plaats gericht op het bepalen of de Wbp op de juiste wijze wordt nageleefd.

[222] Zwenne e.a. 2007, p. 10-12
[223] Idem, p. 124
[224] Idem, p. 145

De bevindingen van het casestudyonderzoek worden anoniem weergegeven.

Hierna wordt eerst kort in algemene zin ingegaan op het wettelijk kader voor gegevensuitwisseling in samenwerkingsverbanden (paragraaf 7.2). De eerste casestudy, bij een veiligheidshuis, wordt besproken in paragraaf 7.3 en in paragraaf 7.4 wordt de tweede casestudy, bij een organisatie voor geestelijke gezondheidszorg, behandeld. In beide paragrafen worden de organisatie en de doelstellingen van het samenwerkingsverband toegelicht en worden de bevindingen weergegeven. Elke paragraaf wordt afgesloten met een aantal conclusies. In de slotbeschouwing van paragraaf 7.5 wordt uitwisseling in de twee samenwerkingsverbanden vergeleken en geven we een antwoord op de deelvraag op welke manier de normering van de Wbp een knelpunt vormt in de (keten)samenwerking.

7.2 Wettelijk kader gegevensuitwisseling in samenwerkings-verbanden

In hoofdstuk 2 is ingegaan op de inhoud van de Wbp. In deze paragraaf gaan we dieper in op de Wbp in relatie tot de gegevensuitwisseling in samenwerkingsverbanden.

Bij gegevensuitwisseling in samenwerkingsverbanden in de publieke of semi-publieke sector is er vaak sprake van samenloop van de Wbp met andere wetten die regels bevatten over de verwerking van persoonsgegevens. Naast de Wbp moet ook met deze andere regelingen rekening worden gehouden. Regelingen die relevant zijn in het kader van het casestudyonderzoeken bij het veiligheidshuis zijn de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens, de Wet gemeentelijke basisadministratie, de Wet werk en bijstand, de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur en de Wet op de jeugdzorg.[225] De Wet op de Geneeskundige Behandelingsovereenkomst (hierna: Wgbo) en de Wet bijzondere opnemingen psychiatrische ziekenhuizen (hierna: Wet Bopz) geven bijzondere regels over de omgang met medische gegevens en zijn in het bijzonder relevant voor de casus bij de geestelijke gezondheidszorg.[226]

Daarnaast is van belang dat in artikel 9 lid 4 van de Wbp is bepaald dat de verwerking van persoonsgegevens achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep op wettelijk voorschrift daaraan in de weg staat. Een geheimhoudingsplicht kan voortvloeien uit het ambt of beroep van een persoon of uit de wet- en regelgeving. Ook hanteren sommige organisaties een beroepscode waarin een geheimhoudingsbepaling is opgenomen.

In deze paragraaf wordt de inhoud van de afzonderlijke wetten niet besproken. In paragraaf 7.3.3 worden de wetten besproken die van toepassing zijn op de casestudy bij het veiligheidshuis. In paragraaf 7.4.3 over de geestelijke gezondheidszorg wordt aangegeven hoe de in dat geval toepasselijke wetten zich tot elkaar verhouden.

In algemene zin kan hierover nog worden gezegd dat de Wbp een algemene wet is en dat de overige genoemde regelingen bijzondere wetten zijn, die wanneer zij van toepassing zijn,

[225] Het betreft hier een niet-limitatieve opsomming.
[226] Brochure Cbp, Informatie delen in samenwerkingsverbanden

voorgaan op de Wbp. Indien in een bijzondere wet niets is geregeld over een bepaald onderwerp, kan worden teruggevallen op de Wbp.

Stappenplan Wbp
Instanties die een samenwerkingsverband willen aangaan, kunnen informatie over het uitwisselen van gegevens in dat samenwerkingsverband vinden in het informatieblad 'Informatie delen in samenwerkingsverbanden' van het Cbp en de 'Handreiking criminaliteitspreventie' van het Ministerie van Justitie.[227] Volgens het Cbp vormen beide stukken een goede basis voor het inrichten van een samenwerkingsverband. Op basis van het informatieblad en de handreiking moeten, om te voldoen aan de normen van de privacywetgeving, een aantal stappen worden doorlopen.

Per organisatie moet allereerst vastgesteld worden welke taak de betrokken organisatie heeft en welke belangen bij het verwerken van gegevens daarmee samenhangen of daaruit voortvloeien. Vervolgens moet per individuele relatie of relaties bekeken worden of gegevensuitwisseling past binnen de taak van de organisatie en welk belang de organisaties hebben bij gegevensuitwisseling.

Daarna moet het doel of de doelen van gegevensuitwisseling worden bepaald. Gelet op het doelbindingsprincipe van de Wbp - persoonsgegevens mogen alleen verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden – is het doel waarvoor de gegevens zijn verzameld en vervolgens worden gebruikt bepalend voor de hoeveelheid en de soort informatie die mag worden uitgewisseld.

In het kader van de derde stap moet nagegaan worden welke wettelijke regelingen er naast de Wbp op de gegevensuitwisseling van toepassing zijn. De samenwerkingspartners moeten vervolgens bepalen welke persoonsgegevens ze willen en kunnen uitwisselen.

Als de vorige stappen zijn doorlopen, dan is in kaart gebracht welke organisaties met wie welke gegevens kunnen uitwisselen en voor welk doel. De netwerken en het daaraan ten grondslag liggende registratiesysteem moeten vervolgens worden ingericht conform dit totaaloverzicht.

Hierna moet worden vastgesteld wie als verantwoordelijke in de zin van de Wbp aangemerkt moet worden. Deze verantwoordelijke moet vervolgens de verplichtingen die gelden op basis van de Wbp uitwerken. Het gaat om:

- het op de hoogte stellen van betrokkenen van de identiteit van de verantwoordelijke en van het doel of doeleinden waarvoor de gegevens worden verzameld;
- betrokkenen de mogelijkheid geven hun rechten uit te oefenen. Hierbij gaat het om het inzage- en correctierecht en de mogelijkheid verzet en bezwaar aan te tekenen;
- het treffen van maatregelen om de persoonsgegevens te beveiligen;
- het maken van afspraken over de bewaartermijn;
- het doen van een melding bij het College bescherming persoonsgegevens;
- eventueel, het aanvragen van een voorafgaand onderzoek en het vragen van een ontheffing van het uitwisselingsverbod teneinde bijzondere persoonsgegevens wel te mogen verwerken.

[227] Cbp 2007a en Sauerwein 2003

Ten slotte raden zowel het Cbp als het Ministerie van Justitie aan de afspraken binnen een samenwerkingsverband vast te leggen in een convenant.

7.3 Casestudy I: Een veiligheidshuis

7.3.1 Inleiding

Het eerste casestudyonderzoek is verricht bij een zogenaamd veiligheidshuis. De afgelopen jaren zijn verschillende veiligheidshuizen opgericht met als doel te komen tot een persoonsgebonden aanpak waardoor overlast en criminaliteit kunnen worden voorkomen en bestreden. [228] Het Ministerie van Justitie streeft naar een landelijke dekking van veiligheidshuizen; in 2009 moeten alle grote steden een veiligheidshuis hebben.[229] In januari 2008 waren er ongeveer 25 veiligheidshuizen operationeel.[230]

Het casestudyonderzoek is verricht in april 2008 en bestond uit een dossieronderzoek en een interviewronde. In het kader van het dossieronderzoek zijn verschillende relevante documenten bestudeerd. Te denken valt aan het plan van aanpak, het conceptprivacyreglement, taakomschrijvingen van de casusoverleggen en enkele convenanten gegevensuitwisseling van casusoverleggen. Interviews zijn gehouden met vertegenwoordigers van verschillende samenwerkingspartners. De functies van de geïnterviewde personen zijn opgenomen in bijlage 2.

7.3.2 Doel en organisatie veiligheidshuis

Het onderzochte veiligheidshuis is sinds begin 2008 operationeel. De opdracht voor het bouwen van het veiligheidshuis is afkomstig van het Arrondissementaal Justitieel Beraad (hierna: AJB).[231] Het veiligheidshuis is ondergebracht bij het OM. De volgende organisaties hebben een werkplek in het veiligheidshuis: het OM, de politie, de RvdK, reclasseringsorganisaties, de gemeente, de DJI en de GGZ. Deze organisaties vormen samen met BJZ de zogenaamde 'binnenring' van het veiligheidshuis. Zij werken samen met organisaties in de 'buitenring' zoals het Advies- en Steunpunt Huiselijk Geweld, Halt, de sociale teams en het meldpunt overlast.[232]

Tot nu toe heeft het Ministerie van Justitie het veiligheidshuis grotendeels gefinancierd; in 2007 is een startsubsidie verleend en ook in 2008 wordt een subsidie verleend. De financiering van het veiligheidshuis wordt in de toekomst overgenomen door het OM. Ook de

[228] Snippe 2006, pagina 50
[229] MvJ 2007
[230] MvJ 2008a
[231] Aan het AJB, dat onder voorzitterschap staat van het OM, nemen de eindverantwoordelijken van het OM, de politie, reclasseringsorganisaties, penitentiaire inrichtingen, de RvdK, het BJZ en slachtofferzorg deel. Het doel van het AJB is de veiligheidsketen zo effectief mogelijk te laten opereren door de werkzaamheden onderling af te stemmen en gezamenlijk de prioritering te bepalen.
[232] Het *sociaal team* coördineert de hulpverlening bij mensen met meervoudige problemen. In het sociaal team werken de gemeente, de politie, woningbouwcorporaties, maatschappelijke ondersteuning en opvang, maatschappelijk werk, de GGZ, de GGD en verslavingszorg samen. Het *meldpunt overlast* is een samenwerkingsverband tussen onder andere politie, gemeente, woningbouwcorporaties en welzijnsinstellingen. Het doel van de samenwerking is te komen tot een centrale klachtenregistratie, het voorkomen van sociale overlast en het generen van beleidsmatige informatie.

gemeente subsidieert het veiligheidshuis de komende drie jaren. Alle deelnemende organisaties betalen zelf de personeelskosten en de kosten voor de werkplekken.

Met de samenwerking in het veiligheidshuis worden de volgende doelen nagestreefd:
- het voorkomen van strafbare feiten en het terugdringen van recidive;
- het terugbrengen en voorkomen van overlast;
- het verlenen van passende zorg aan het slachtoffer;
- het zijn van een betrouwbaar informatieknooppunt voor partners in veiligheid;
- het verlenen van nazorg;
- het versterken van de ketenregie.

De persoons- en gebiedsgerichte aanpak vormen samen met de oprichting van een kennis- en expertisecentrum de pijlers van het veiligheidshuis. Gegevensuitwisseling vindt plaats bij de persoonsgerichte aanpak. Deze aanpak richt zich op de volgende doelgroepen: meerderjarige veelplegers, jeugd, criminele en overlastgevende Antillianen, daders van huiselijk geweld, ex-gedetineerden en overlastgevende personen.

Bij de persoonsgerichte aanpak speelt het casusoverleg een centrale rol. In dit overleg worden betrokkenen besproken en wordt een persoonsgericht plan van aanpak opgesteld. Per casusoverleg zijn verschillende partners aanwezig. In bijlage 3 is een overzicht gegeven van de verschillende casusoverleggen, de doeleinden en de overlegpartners. De casusoverleggen huiselijk geweld en overlastgevende personen zijn nieuw, evenals het casusoverleg dat zich richt op kinderen van 0 tot 12 jaar, het Justitieel casusoverleg-extra en het casusoverleg nazorg. De overige casusoverleggen bestonden al. Wel zijn aan een aantal nieuwe casusoverleggen extra deelnemers toegevoegd.

Per casusoverleg worden persoonsgegevens vastgelegd in een bestand. Voor de verschillende casusoverleggen worden verschillende registratiesystemen gehanteerd. Het uiteindelijke streven is om binnen het veiligheidshuis een overkoepelend systeem te ontwikkelen dat een koppeling kan maken tussen verschillende bestanden. Tot het moment waarop een dergelijk systeem beschikbaar is, fungeren de zogenaamde informatiemakelaars als een soort van verwijsindex. Deze administratieve medewerkers houden in de gaten welke betrokkene bij welk casusoverleg bekend is.

7.3.3 Wettelijk kader en zelfregulering

7.3.3.1 Wettelijk kader

Binnen het veiligheidshuis werken verschillende partners met elkaar samen. Dit heeft tot gevolg dat ook veel verschillende regelingen van toepassing zijn op de uitwisseling van persoonsgegevens binnen het samenwerkingsverband. In het onderstaande wordt een overzicht gegeven van de wetgeving die van toepassing kan zijn binnen het veiligheidshuis. Daarbij is er niet naar gestreefd een volledig overzicht te geven maar alleen de belangrijkste wetgeving te bespreken.

Wet politiegegevens
Omdat de Privacyrichtlijn niet van toepassing is op de verwerking van gegevens met het oog op de opsporing en vervolging van strafbare feiten in de lidstaten is de Wbp is niet van

toepassing op de gegevensverwerking door de politie.[233] De verwerking van deze gegevens wordt beheerst door de Wet politiegegevens (hierna: Wpolg). De Wpolg is niet van toepassing op gegevens die de politie verwerkt in het kader van taken die niet zijn te scharen onder artikel 2 van de Politiewet 1993.[234] De gegevens die de politie in dat kader verwerkt, vallen onder het regime van de Wbp.

De omschrijving in artikel 2 Politiewet geeft de kern van de politietaak compact weer, maar blijft beperkt tot hoofdlijnen. Het is dan ook lastig om aan te geven wanneer de Wbp van toepassing is en wanneer de Wpolg.

Wet justitiële en strafvorderlijke gegevens
Op grond van artikel 16 van de Wbp is het verboden strafrechtelijke persoonsgegevens te verwerken. Volgens artikel 22 van de Wbp geldt een uitzondering als de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verantwoordelijken die deze hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens. De Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg) regelt de verwerking van justitiële gegevens, gegevens inzake de toepassing van het strafrecht of de strafvordering, en strafvorderlijke gegevens, gegevens die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt. Ook stelt de Wjsg regels aan de verwerking van persoonsgegevens in persoonsdossiers en aan de verklaring omtrent het gedrag. Het Cbp is aangewezen als toezichthouder op de naleving van de Wjsg. Een nadere uitwerking van de Wjsg is te vinden in het Besluit justitiële gegevens (Bjg).

In de Aanwijzing wet justitiële en strafvorderlijke gegevens is uiteengezet wanneer strafvorderlijke gegevens mogen worden verstrekt voor buiten de strafrechtspleging gelegen doeleinden.[235] In de bijlage van de Aanwijzing wordt ingegaan op gegevensuitwisseling bij samenwerking van het OM met andere organisaties. Onderscheid wordt gemaakt tussen twee soorten samenwerkingsverbanden; een samenwerkingsverband waarbij een apart bestand wordt gecreëerd en een samenwerkingsverband waarbij dat niet het geval is. In het tweede geval verstrekt het OM slechts gegevens; alleen de Wsjg en niet de Wbp is op deze verstrekkingen van toepassing. Volgens de Aanwijzing is in het volgende geval sprake van een apart bestand als in een samenwerkingsverband casusoverleggen worden gevoerd, daarvan notulen worden gemaakt en opgeslagen en/of gezamenlijke (integrale) actieplannen worden opgesteld ten aanzien van bepaalde personen en deze worden opgeslagen. Hierbij is van grote betekenis of het bestand voor de partijen van het samenwerkingsverband raadpleegbaar is.[236] Als sprake is van een samenwerkingsverband waarbij een apart bestand wordt gecreëerd zijn de Wjsg en de Aanwijzing van toepassing op de verstrekking van strafvorderlijke gegevens van het OM aan het samenwerkingsverband. De verwerkingen binnen het samenwerkingsverband worden beheerst door de Wbp. De verwerking van gegevens in het bestand zal in beginsel moeten worden aangemeld bij het CBP.

[233] *Richtlijn 95/46/EG*, PbEG L 281, p. 0031-0050, artikel 3, tweede lid
[234] Gedacht kan worden aan de toezichthoudende taken die de politie uitvoert op grond van bijzondere wetten die niet behoren tot de taken ten dienste van de justitie.
[235] Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden, Staatscourant 2008, 19, p. 29
[236] Aanwijzing wet justitiële en strafvorderlijke gegevens, p. 9

Wet gemeentelijke basisadministratie persoonsgegevens
In de gemeentelijke basisadministratie persoonsgegevens (hierna: gba) zijn persoonsgegevens opgenomen van iedereen die rechtmatig in Nederland verblijft en binnen de gemeente woonachtig is. Het gaat onder andere om gegevens als naam, geboortedatum, adres, huwelijk, kinderen, datum van overlijden. In de Wet gemeentelijke basisadministratie persoonsgegevens (hierna: Wgba) is precies bepaald welke gegevens in de gba mogen worden opgenomen (artikel 34). Het bijhouden van de gba is een taak van het college van burgemeester en wethouders van elke gemeente. De Wgba kent een eigen stelsel van regels voor de verwerking van persoonsgegevens die voorkomen in de gemeentelijke basisadministratie. De Wbp is niet van toepassing op de persoonsgegevens die in de gba voorkomen. Een uitzondering geldt voor de zogenaamde 'aangehaakte' gegevens. Dit zijn extra gegevens die een gemeente op grond van andere gemeentelijke taken in de gba opneemt. Op de aangehaakte gegevens in de GBA is voor wat betreft de bescherming van de persoonlijke levenssfeer niet de Wet GBA van toepassing, maar de Wbp. Het Cbp houdt toezicht op de naleving van de Wgba.[237]

Wet Bevordering integriteitbeoordelingen door het openbaar bestuur
Op basis van de Wet Bevordering integriteitbeoordelingen door het openbaar bestuur (hierna: Wet Bibob) hebben bestuursorganen een instrument om de integriteit van aanvragers van vergunningen en subsidies te toetsen. Het bestuursorgaan kan de aanvrager allerlei informatie vragen over de bedrijfsstructuur, zeggenschap en financiering van de gevraagde beschikking of overheidsopdracht (art. 30 Wet Bibob). In de Wet Bibob is een streng regime opgenomen ten aanzien van de verstrekking van persoonsgegevens. Verder zijn in de wet bepalingen opgenomen die ertoe strekken de verspreiding van de gegevens van het Bureau BIBOB tot het noodzakelijke minimum te beperken. Bovendien is in artikel 27 nadrukkelijk bepaald dat een ieder die op grond van de voorliggende regeling persoonsgegevens inzake een derde verkrijgt, tot geheimhouding verplicht is, behoudens de in het wetsvoorstel geregelde uitzonderingsgevallen. De Wbp is niet van toepassing op de uitwisseling van gegevens wanneer de Wet Bibob van toepassing is.

Wet op de jeugdzorg
Het Bureau Jeugdzorg (hierna: BJZ) vormt sinds de invoering van de Wet op de jeugdzorg (hierna: Wjz) de toegang tot de jeugdzorg. Qua verwerking van persoonsgegevens bevat de Wjz op een aantal punten concretiseringen van de algemene normen van de Wbp. Deze bijzondere regels derogeren aan de bepalingen van de Wbp. Op de gebieden die niet in de Wjz zijn geregeld, geldt de Wbp als algemene wet.[238] Zo is in artikel 53 van de Wjz bepaald dat het BJZ in bepaalde gevallen (bijzondere) persoonsgegevens mag verwerken zonder toestemming van de betrokkene.

Het BJZ verwerkt voor haar uiteenlopende taken persoonsgegevens, waaronder bijzondere gegevens, voor uiteenlopende doeluiteinden. In de memorie van toelichting is aangegeven dat de artikelen 8, 9 en 21 van de Wbp de grondslag bieden voor de verwerking van (bijzondere) persoonsgegevens voor de uitoefening van de taken. De wetgever geeft aan dat de persoonsgegevens uitsluitend mogen worden verwerkt voor het doel waarvoor ze zijn verzameld of een daarmee verenigbaar doel. Gegevens die in het kader van een bepaalde taak worden verzameld mogen niet zonder meer worden gebruikt voor de uitoefening van een andere taak.[239]

[237] Cbp 2006, p. 1
[238] *Kamerstukken II 2001-2002*, 28 168, nr. 3, p. 40
[239] Idem, p. 40 en 41

7.3.3.2 Zelfregulering

Het onderzochte veiligheidshuis is van start gegaan terwijl het proces om de gegevensuitwisseling rechtmatig te laten verlopen nog niet was afgerond. Het stappenplan, zoals genoemd in paragraaf 7.2 is niet (volledig) doorlopen. Voor een aantal casusoverleggen zijn in het verleden, vóór het operationeel worden van het veiligheidshuis, al schriftelijke afspraken gemaakt over de uitwisseling van persoonsgegevens. Het verwerken van de persoonsgegevens in de verschillende casusoverleggen van het veiligheidshuis is echter nog niet gemeld aan het Cbp. Ook moet nog worden onderzocht of een voorafgaand onderzoek of een algemene ontheffing voor het verwerken van bijzondere persoonsgegevens nodig is.[240] Landelijke systemen (zoals Viadesk veelplegers) zijn overigens wel aangemeld.

Beleidsmedewerkers van het OM, de politie en de gemeente zijn belast met de taak ervoor te zorgen dat de gegevensuitwisseling in het veiligheidshuis conform de privacywetgeving geschiedt. Er is inmiddels een conceptprivacyreglement opgesteld. Dit privacyreglement zal een bijlage vormen van het samenwerkingsconvenant dat wordt afgesloten tussen de verschillende samenwerkingspartners. De gegevensuitwisseling in elk casusoverleg zal vervolgens worden gemeld bij het Cbp. Deze meldingen zullen deel uitmaken van het privacyreglement.

Het conceptprivacyreglement gaat in op de samenwerking, de gegevensuitwisseling, de informatieverstrekking aan betrokkenen en de rechten van betrokkenen. Op bepaalde punten worden de bepalingen van de Wbp geconcretiseerd, terwijl op andere punten de betreffende bepaling uit de Wbp is overgenomen.

In het concept wordt aangegeven dat er in het kader van de samenwerking persoonsgegevens worden uitgewisseld en dat hiervoor bestanden worden aangelegd en bijgehouden. De gegevensuitwisseling heeft het doel in gezamenlijkheid een (veelal persoonsgerichte) aanpak af te spreken ter voorkoming of terugdringing van overlast of criminaliteit, het handhaven van de openbare orde dan wel het verlenen van (na)zorg aan slachtoffers. Bepaald is dat de persoonsgegevens uitsluitend mogen worden verwerkt voor zover dat noodzakelijk is voor deze doelstellingen en in overeenstemming met de wettelijke regelingen, waaronder de geldende geheimhoudingsplichten. De persoonsgegevens mogen verder worden verwerkt als die verdere verwerking verenigbaar is met het doel en voor zover noodzakelijk voor de goede uitoefening van de taak van de desbetreffende samenwerkingspartner.

De hoofdofficier van justitie van het betreffende arrondissement wordt als verantwoordelijke voor de verwerking van persoonsgegevens aangemerkt.

Volgens het conceptreglement moeten de samenwerkingspartners aan de medewerkers een geheimhoudingsplicht opleggen en mogen strafrechtelijke persoonsgegevens niet verstrekt worden tenzij daarvoor een rechtmatige verstrekkingsgrond en een uitzondering op het verbod van verwerking van bijzondere persoonsgegeven is aan te wijzen. Daarnaast wordt de officier van justitie geraadpleegd om te voorkomen dat een eventuele strafvervolging gevaar loopt.

[240] Voor het verwerken van persoonsgegevens betreffende het ras in het casusoverleg criminele en overlastgevende Antillianen heeft het Cbp een ontheffing afgegeven. Het Cbp heeft deze ontheffing echter ingetrokken nadat een daartegen ingesteld beroep door de rechtbank Den Haag gegrond was verklaard (Rechtbank Den Haag, 27 juli 2007, LJN BB0711). In zijn uitspraak van 3 september 2008 heeft de Raad van State (zaaknummer 200706325/1) bepaald dat de overheid een databank mag aanleggen met persoonsgegevens van Antilliaanse en Arubaanse probleemjongeren.

In het conceptreglement wordt een limitatieve opsomming gegeven van de persoonsgegevens die in het bestand kunnen worden vastgelegd. Aangegeven is dat voor de verwerking van bijzondere persoonsgegevens een wettelijke uitzonderingsgrond aan de orde dient te zijn en dat deze gegevens uitsluitend worden verwerkt door instanties die krachtens de wet zijn belast met het strafrecht of krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens bevoegd zijn deze te verwerken. Eventuele gezondheids- en hulpverlenings-gegevens worden verwerkt door daartoe in de wet aangewezen instanties of zijn noodzakelijk in aanvulling op de verwerking van de strafrechtelijke gegevens voor de doeleinden van deze gegevensverwerking. Gegevens omtrent nationaliteit en een eventuele foto worden uitsluitend opgenomen in de noodzakelijke aanvulling op de strafrechtelijke of gezondheidsgegevens, gelet op het doel van verwerking. Voor het al dan niet mogen uitwisselen van justitiële en strafvorderlijke gegevens dient de Aanwijzing Wet justitiële en strafvorderlijke gegevens als leidraad. Voor de politionele gegevens wordt verwezen naar de Wet politiegegevens en het daarbij behorende Besluit politiegegevens.

Bepaald is dat de persoonsgegevens alleen aan ondertekenaars van het samenwerkings-convenant verstrekt worden. Alleen als de betrokkene hiermee heeft ingestemd of de verstrekking noodzakelijk is op grond van een wettelijke verplichting of uit de taak van de samenwerkingspartner de noodzaak voortvloeit, vindt verstrekking aan derden plaats.

In het conceptreglement is bepaald dat maatregelen met betrekking tot de toegang tot persoonsgegevens, de lees- en schrijfbevoegdheden van samenwerkingspartners en het vereiste niveau van beveiliging moeten worden getroffen. Aangegeven is dat de persoonsgegevens niet langer dan noodzakelijk mogen worden bewaard, maar dat ze in ieder geval verwijderd en vernietigd worden vijf jaar nadat de betrokkene voor het laatst is besproken. Voor de dagelijkse zorg, het bewaren, verwijderen en verstrekken van persoonsgegevens is een beheerder aangewezen.

Volgens het conceptreglement moeten betrokkenen schriftelijk geïnformeerd worden over de verwerking van hun persoonsgegevens. Ook is in het conceptreglement een regeling getroffen waarmee de betrokkene in staat wordt gesteld zijn rechten uit te oefenen. Hierbij wordt aangesloten bij de bepalingen van de Wbp; zo nu en dan worden de wettelijke normen geconcretiseerd. Zo is ter concretisering van artikel 36 lid 3 van de Wbp bepaald dat een beslissing tot correctie in ieder geval binnen vier weken wordt uitgevoerd.

7.3.4 Gegevensuitwisseling in het veiligheidshuis

In het knelpuntenonderzoek is geconstateerd dat zich verschillende knelpunten voordoen bij de gegevensuitwisseling in samenwerkingsverbanden. Opvallend is dat uit het onderzoek bij het veiligheidshuis blijkt dat zich bij de daadwerkelijke uitwisseling van persoonsgegevens geen knelpunten voordoen. Wel doen zich knelpunten voor op beleidsmatig niveau, bij het opstellen van het privacyreglement.

7.3.4.1 Privacyreglement

De beleidsmedewerkers ervaren de nodige knelpunten bij het opstellen van het privacyreglement. De privacyregelgeving wordt vanwege de abstractheid als ingewikkeld ervaren. Daarnaast zijn er veel verschillende wetten van toepassing op de gegevensuitwisseling in het veiligheidshuis en worden er bijzondere gegevens verwerkt. Elders in Nederland zijn ook veiligheidshuizen operationeel, sommige al langere tijd. Ook bij

deze veiligheidshuizen is het eerder uitzondering dan regel dat er een vastgesteld convenant is voor gegevensuitwisseling. De beleidsmedewerkers geven aan dat alle mensen die betrokken zijn bij veiligheidshuizen dezelfde vragen over gegevensuitwisseling hebben. Er is contact gezocht met het Cbp en het Ministerie van Justitie, maar deze contacten hebben niet voor de gewenste duidelijkheid gezorgd. Tijdens de interviews is aangegeven dat de behoefte bestaat aan een landelijk model voor gegevensuitwisseling in veiligheidshuizen. Het wordt als vreemd ervaren dat een dergelijk model niet beschikbaar is, terwijl het opzetten van veiligheidshuizen door het Ministerie van Justitie gepromoot wordt. Medio 2008 is echter een modelprivacyconvenant voor veiligheidshuizen beschikbaar gekomen van de Helpdesk Privacy van het Ministerie van Justitie. Bij het opstellen van het conceptprivacyreglement is nu gebruik gemaakt van een convenant van een ander veiligheidshuis. Dat convenant ligt nog bij het Cbp ter goedkeuring. Ten slotte vinden de beleidsmedewerkers het moeilijk te bepalen hoe omgegaan moet worden met het uitwisselen van persoonsgegevens tussen het samenwerkingsverband veiligheidshuis en andere organisaties of samenwerkingsverbanden zoals het sociaal team en het meldpunt overlast. Het doel is om deze partijen het privacyreglement ook te laten ondertekenen.

Om ongewenste vertraging te voorkomen is besloten het veiligheidshuis van start te laten gaan zonder dat aan de wettelijke verplichtingen is voldaan. Het opstellen van een privacyreglement is een langdurig proces. In het besluit om het veiligheidshuis van start te laten gaan zonder dat aan de wettelijke verplichtingen is voldaan, heeft ook meegewogen dat er in het land al meer dan 20 veiligheidshuizen operationeel zijn, die, voor zover wij weten, ook nog niet over een goedgekeurd samenwerkingsconvenant en privacyreglement beschikken.

Alle medewerkers van het veiligheidshuis zijn tijdens een startbijeenkomst gewezen op het feit dat zij in het veiligheidshuis te maken hebben met privacygevoelige gegevens. Er zijn geen afzonderlijke afspraken gemaakt over geheimhouding. Volgens de projectleider en de beleidsmedewerkers geldt voor alle medewerkers al een geheimhoudingsplicht op grond van bijzondere wetten of gedragscodes. Zij weten niet of de medewerkers zich hiervan wel bewust zijn. Hiervoor is aangegeven dat in het conceptprivacyreglement een geheimhoudingsbepaling is opgenomen: voor zover de samenwerkingspartners daartoe niet al verplicht zijn, leggen zij aan die medewerkers die inzage hebben in of op andere wijze persoonsgegevens verkrijgen uit een overleg of een bestand een plicht tot geheimhouding op. Een aantal geïnterviewden heeft aangegeven dat zij bij de start van het veiligheidshuis niet zijn geïnstrueerd over privacybescherming door de organisatie waarvoor ze werkzaam zijn.

De projectleider en de beleidsmedewerkers zien het belang van privacybescherming in en zijn zich bewust van de risico's van het verwerken van persoonsgegevens. Een beleidsmedewerker gaf tijdens het interview aan dat organisaties vaak geen belang hechten aan privacybescherming en dat het daarom goed is dat het Cbp zich op toezicht en handhaving richt.

7.3.4.2 Gegevensuitwisseling tussen samenwerkingspartners

Uit de gesprekken die zijn gevoerd met deelnemers aan de casusoverleggen blijkt dat zich geen knelpunten voordoen bij het werkelijk uitwisselen van persoonsgegevens.

Een van de geïnterviewden heeft aangegeven dat toestemming van de betrokkene de basis is voor gegevensuitwisseling in het casusoverleg huiselijk geweld. De GGZ, de DJI, de RvdK en

het sociaal team vragen in beginsel ook altijd toestemming voor de gegevensuitwisseling. Zonder toestemming zijn er ook mogelijkheden om persoonsgegevens uit te wisselen.

In de casusoverleggen is privacybescherming geen onderwerp van gesprek. De deelnemers aan de casusoverleggen geven aan dat het uitwisselen van gegevens noodzakelijk is om een bepaald maatschappelijk doel te bereiken. Op basis van professionaliteit wordt beslist of gegevens moeten worden uitgewisseld om het uiteindelijke doel te bereiken. Sommige geïnterviewden lijken privacybescherming als negatief, als een belemmering te zien. Volgens hen moet het niet zo zijn dat het maatschappelijk doel (bijvoorbeeld veiligheid of resocialisatie) niet kan worden bereikt omdat bepaalde gegevens niet mogen worden uitgewisseld.

De deelnemers van de casusoverleggen gaan er vanuit dat vragen over de toelaatbaarheid van het uitwisselen van persoonsgegevens op beleidsmatig niveau zijn beantwoord. Er wordt dan ook vanuit gegaan dat de gegevensuitwisseling in de casusoverleggen is toegestaan.

Uit de afgenomen interviews blijkt dat de samenwerking in het veiligheidshuis de gegevensuitwisseling soepeler doet verlopen. Er ontstaat begrip voor elkaars werkwijze en het vertrouwen in elkaar is toegenomen (namen krijgen een gezicht), waardoor er sneller en meer persoonsgegevens worden uitgewisseld dan voorheen het geval was. Volgens de projectleider speelt ook het enthousiasme van de betrokken medewerkers een rol; men wil het uiteindelijke doel zo graag realiseren dat mogelijk meer gegevens dan noodzakelijk worden uitgewisseld. De geïnterviewde vertegenwoordigers van de gemeente, de RvdK, de GGZ en DJI geven aan dat er in de casusoverleggen teveel gegevens worden uitgewisseld of dat gegevens worden uitgewisseld die niet voor alle deelnemers relevant zijn. Ook mag bijvoorbeeld ‘over het schouder’ worden meegekeken in het registratiesysteem van een samenwerkingspartner. De geïnterviewde vertegenwoordigers van de gemeente, de politie, het OM, de DJI en de RvdK geven aan dat de GGZ terughoudender omgaat met de gegevensuitwisseling dan de andere samenwerkingspartners. Ook het BJZ en de RvdK worden genoemd als terughoudender samenwerkingspartners voor wat betreft de gegevensuitwisseling. Dit hangt wellicht samen met het medisch beroepsgeheim. De medewerkers van de betreffende organisaties ervaren dit geheim niet als belemmerend voor de gegevensuitwisseling. Er wordt zorgvuldig bepaald welke gegevens uitgewisseld kunnen worden. De psychiater van de GGZ gaat uit van toestemming van de betrokkene. Hij adviseert of het strafrechtelijk traject of het zorgtraject moet worden ingezet en gaat daarbij niet of slechts in het algemeen in op het ziektebeeld van de betrokkene. Professionele waarden, zoals de geheimhoudingsplicht, hebben wel een temperende werking op een volledige onbelemmerde gegevensuitwisseling.

Aan de convenanten voor gegevensuitwisseling die gelden voor sommige casusoverleggen, wordt in de praktijk niet altijd evenveel waarde gehecht. Een geïnterviewde gaf aan dat het vaststellen van het convenant een formaliteit was op basis waarvan vervolgens toegang kon worden verkregen tot een landelijk geautomatiseerd systeem; in de praktijk werd met dit convenant niets gedaan. Een andere deelnemer van hetzelfde casusoverleg was van de inhoud van het convenant überhaupt niet op de hoogte.

7.3.4.3 Klachten en verzet

Sinds het operationeel worden van het veiligheidshuis hebben betrokkenen nog geen gebruik gemaakt van hun rechten tot inzage, correctie en verzet. Ook bij de casusoverleggen die vóór de start van het veiligheidshuis al bestonden, heeft zich dit zelden voorgedaan. Bij

bijvoorbeeld het veelplegersoverleg heeft zich slechts eenmaal een betrokkene beklaagd over het feit dat hij als veelpleger werd aangemerkt. Bij de samenwerkingsverbanden waarmee het veiligheidshuis een relatie heeft, het meldpunt overlast en het sociaal team, maken betrokkenen ook zelden gebruik van hun rechten. Het sociaal team heeft nog nooit een verzoek om inzage of correctie of een klacht ontvangen. Bij het meldpunt overlast, dat sinds 2003 van start is, zijn ongeveer vijf verzoeken om informatie ontvangen van betrokkenen of hun gemachtigden.

Volgens de geïnterviewden is de oorzaak van het geringe gebruik van de rechten te vinden in het feit dat veel personen van wie in het veiligheidshuis gegevens worden verwerkt zich aan de onderkant van de samenleving bevinden. Het betreft niet het type burger dat zich in eerste instantie druk maakt over schending van hun privacy. Sommige geïnterviewden geven aan dat juist vanwege de kwetsbaarheid van de doelgroep van het veiligheidshuis extra zorgvuldigheid bij de verwerking van persoonsgegevens is geboden.

7.3.5 Conclusies

De gegevensuitwisseling in het onderzochte veiligheidshuis vindt niet geheel conform de Wbp plaats. Er is niet voldaan aan de meldingsverplichting en er zijn geen afspraken gemaakt ten aanzien van de rechten van betrokkenen, beveiliging en bewaren. Wellicht zou de gegevensuitwisseling kunnen voldoen aan de wet als aan deze verplichtingen voldaan zou zijn, maar het antwoord op de vraag of dit het geval is, was in dit onderzoek niet vast te stellen. Daarvoor zou diepgaander onderzoek moeten plaatsvinden. Per casusoverleg zou moeten worden beoordeeld welke wettelijke regelingen van toepassing zijn en welke bepalingen over de uitwisseling van persoonsgegevens deze wetten bevatten.

Gelet op het feit dat is aangegeven dat de gegevensuitwisseling is vergemakkelijkt doordat het vertrouwen in elkaar is toegenomen, is de kans echter aanwezig dat in strijd met de artikelen 8, 9 en 11 van de Wbp wordt gehandeld.

Binnen het veiligheidshuis is wel een verantwoordelijke aangewezen als bedoeld in de Wbp. In het knelpuntenonderzoek was vastgesteld dat dit als een knelpunt werd ervaren maar binnen het veiligheidshuis is men er wel in geslaagd een verantwoordelijke aan te wijzen.

Op beleidsmatig niveau doet zich een aantal van de in het knelpuntenonderzoek geconstateerde knelpunten voor. De privacyregelgeving wordt als ingewikkeld ervaren door de abstractheid ervan. Daarnaast doen zich knelpunten voor omdat er sprake is van samenloop van verschillende wetten en er bijzondere gegevens worden verwerkt. Het feit dat er geen landelijk model beschikbaar is voor de gegevensuitwisseling in een veiligheidshuis wordt als gemis ervaren.

Voor de deelnemers aan de casusoverleggen is privacybescherming minder belangrijk dan het bereiken van het maatschappelijk doel (veiligheid, reïntegratie en resocialisatie). Het beeld bestaat dat privacyregelgeving een randvoorwaardelijke belemmering kan opleveren.

Opvallend is verder dat de meeste geïnterviewden aangegeven dat de uitwisseling van persoonsgegevens gemakkelijker verloopt sinds wordt samengewerkt in het veiligheidhuis. Het vertrouwen in elkaar is door de samenwerking vergroot. Door het onderlinge vertrouwen wordt de waakzaamheid minder. De inhoudelijke doelstelling wordt gehaald en het privacybelang wordt niet altijd gediend.

Voor een aantal casusoverleggen zijn privacyregels opgesteld. Er zijn aanwijzingen dat in de praktijk niet conform deze convenanten die voor de casusoverleggen zijn opgesteld, wordt gewerkt. Door geïnterviewden is bijvoorbeeld aangegeven dat het convenant in hun ogen alleen een formaliteit is.

7.4 Casestudy II: Geestelijke gezondheidszorg

7.4.1 Inleiding

Begin 2007 zijn een organisatie voor de geestelijke gezondheidszorg (GGZ) en een stichting voor verslavingszorg (VZ) gestart met de ontwikkeling van een behandelvoorziening en een woonvoorziening voor personen die dakloos zijn, afhankelijk zijn van (verschillende) verdovende middelen, in ieder geval lijden aan psychiatrische stoornissen en veelal ook somatische aandoeningen hebben. Bij velen van hen hebben diverse zorgtrajecten in het verleden niet geleid tot een humaan bestaan.

De gesloten buitenstedelijke voorziening is bedoeld voor personen die afkomstig zijn uit twee van de vier grote steden. De opname is gedwongen en is een voorziening in de ketenzorg die is ontwikkeld voor de grote steden. Het project is een direct uitvloeisel van de doelstellingen van het kabinet Balkenende II om de overlast in de grote steden te beperken. De GGZ beschikt over een Erkenning van het Ministerie van Volksgezondheid, Welzijn en Sport voor dit project.

Het casestudyonderzoek is verricht in juli en augustus 2008 en bestond uit een dossieronderzoek en een interviewronde. In het kader van het dossieronderzoek zijn verschillende relevante documenten bestudeerd, waaronder de uitvoeringsovereenkomst en de privacyreglementen van de samenwerkingspartners. Vervolgens is met een zestal vertegenwoordigers van de samenwerkingspartners een interview gehouden. In verband met de anonimiteit van de casus zijn enkel de functies van de geïnterviewde personen genoemd in bijlage 2.

7.4.2 Doel en organisatie

Als schakel in de ketenzorg heeft de GGZ instelling zich bereid verklaard een opname- en behandelkliniek te exploiteren.

De structuur van het project is als volgt. Tussen de gemeentelijke gezondheidsdiensten (GGD-en) van de twee grote steden en de GGZ is een uitvoeringsovereenkomst gesloten. De twee GGD-en zijn verantwoordelijk voor de selectie van de personen uit de doelgroep. De GGZ is verantwoordelijk voor een psychiatrische behandeling, de (somatische) zorg en begeleiding ten tijde van het verblijf in de instelling. Naast deze overeenkomst is de GGZ een overeenkomst aangegaan met een stichting voor VZ om de specifieke behandel- en zorgdeskundigheid te waarborgen.

Bij de selectie van de patiënten zijn ook de (psychiatrische) instellingen in de twee grote steden betrokken. De meeste patiënten van het project zijn afkomstig uit deze instellingen, of waren daar al in behandeling. Met hen zijn geen afspraken vastgelegd over participatie in het

project. De GGD-en fungeren als intermediair tussen de GGZ-instelling en de instellingen in de grote steden.

Voorts vinden nog contacten plaats met de gemeente waarin de instelling is gevestigd.

Van het totale voor het project benodigde personeel stelt VZ 25% en de GGZ 75% ter beschikking. Verwacht wordt dat bij een exploitatie van de maximaal beoogde capaciteit de totale inzet voor het project 200 tot 240 fte zal omvatten. Uiteindelijk moeten er in februari 2010 120 bedden beschikbaar zijn, waarvan steeds 50% voor elk van de grote steden bestemd is.

Het verblijf in de instelling vindt plaats op basis van een door de rechter uitgesproken Rechterlijke Machtiging (hierna: RM) en wordt daarna besproken in de gemeentelijke toeleidingscommissie. Voor beide grote steden bestaat een toeleidingscommissie die ongeveer eens per twee maanden bijeenkomt. In deze toeleidingscommissie fungeert een medewerker van de GGD als voorzitter en is altijd de psychiater van de GGZ-instelling aanwezig. Daarnaast is bij iedere toeleidingscommissie een aantal psychiaters van instellingen in de grote steden aanwezig. Deze psychiaters melden een aantal patiënten aan bij de toeleidingscommissie die zij geschikt achten voor behandeling in de buitenstedelijke instelling van de GGZ. Niet alle patiënten die worden besproken in de toeleidingscommissie worden ook daadwerkelijk geplaatst in de instelling. De GGD-en zijn verantwoordelijk voor de aanlevering van een compleet medisch dossier aan de leden van de toeleidingscommissie.

De RM wordt aangevraagd door de psychiater van de instelling waaruit de patiënt afkomstig is, nadat deze is besproken in de toeleidingscommissie. Andere patiënten hebben al een RM en kunnen na bespreking in de toeleidingscommissie zonder tussenkomst van de rechter in de GGZ-instelling worden opgenomen.

De GGZ is verplicht de GGD-en volgens een vastgelegd reglement te informeren over het verloop van de behandeling. De uitvoering van de behandeling en de begeleiding is per patiënt vastgelegd in een behandelingsplan verbonden aan een behandelovereenkomst.

Vanaf het begin van het project in februari 2007 tot september 2008 zijn in totaal 75 patiënten behandeld in de instelling. Enkele daarvan zijn weer vertrokken en twee zijn overleden. Op dit moment verblijven er 66 personen in de instelling.

7.4.3 Wettelijk kader en zelfregulering

7.4.3.1 Wettelijk kader

Het medisch beroepsgeheim vloeit voort uit artikel 88 van de Wet op de Beroepen in de Individuele Gezondheidszorg (hierna: Wet BIG). In dit artikel is bepaald dat een ieder verplicht is geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of wat daarbij te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen. De Wet BIG geldt voor (tand)artsen, apothekers, gezondheidszorgpsychologen, psychotherapeuten, fysiotherapeuten, verloskundigen en verpleegkundigen.[241]

[241] Cbp 2005, p. 1

Aan het medisch beroepsgeheim is nadere invulling gegeven in de Wgbo. De Wgbo is opgenomen in afdeling 5 van boek 7 van het Burgerlijk Wetboek (hierna: BW). In artikel 7:457 van het BW is bepaald dat de hulverlener ervoor moet zorgen dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden worden verstrekt dan met toestemming van de patiënt. Naast de Wgbo zijn de Wbp en de Wet Bopz van belang.

In de Wgbo zijn de rechten en plichten over en weer van patiënten en hulpverleners geregeld. De relatie tussen de GGZ als instelling en de patiënt wordt gezien als een contractuele relatie, de zogenaamde behandelovereenkomst. Ook in de Wet Bopz zijn bepalingen opgenomen over het verstrekken van informatie over patiënten en bewaartermijnen.

Omdat in de Wgbo en de Wet Bopz bepalingen zijn vastgelegd over privacybescherming, zijn de consequenties van de Wbp voor de gezondheidszorg beperkt. Dit neemt niet weg dat organisaties in de gezondheidszorg zich moeten houden aan de regels in de Wbp. De Wet Bopz is een bijzondere wet en de Wgbo geeft algemene regels. De Wet Bopz gaat daarom voor de Wgbo. Daarnaast biedt de Wgbo in de meeste gevallen meer bescherming voor de patiënt dan de Wbp en in die gevallen gaat de Wgbo voor op de Wbp.

Alle patiënten worden gedwongen opgenomen en dat houdt in dat een RM is afgegeven voor deze opname, op grond van artikel 2 van de Wet Bopz. De familie van de patiënt of de patiënt zelf kan een dergelijke rechterlijke machtiging vragen en daarnaast kan de officier van justitie dat ambtshalve doen, doorgaans gebeurt dit laatste op aangeven van hulpverleners. Het verzoek moet vergezeld gaan van een geneeskundige verklaring. Hierin moet worden aangetoond dat de betrokkene een stoornis heeft en gevaar veroorzaakt (of dreigt te veroorzaken), en dat voortkomt uit die stoornis en dat gevaar kan niet zonder personen of instellingen buiten het psychiatrisch ziekenhuis worden afgewend. Deze verklaring moet van een onafhankelijk arts of psychiater komen, een deskundige die niet bij de behandeling van de patiënt is betrokken**.** Deze overlegt zo mogelijk eerst met de huisarts en de behandelend psychiater. Als dat niet mogelijk is, vermeldt hij de reden daarvan in de verklaring.

De opname via een RM kan maximaal zes maanden duren (de rechter kan ook een kortere termijn voorschrijven). Daarna of eerder kan ontslag volgen, of krijgt de behandeling een vrijwillig karakter. De periode kan echter ook worden verlengd, mits de criteria nog steeds van toepassing zijn. Zo'n eventuele machtiging tot voortgezet verblijf heeft een geldigheidsduur van maximaal een jaar.

Op grond van de Wgbo en de Wbp is verwerking en uitwisseling van gegevens in beginsel enkel toegestaan met toestemming van de patiënt. Deze toestemming wordt schriftelijk vastgelegd. Er bestaat wel een aantal uitzonderingen. Toestemming is niet vereist als een wettelijk voorschrift de verstrekking van informatie eist.

De Wet Bopz bevat een aantal verplichtingen tot het verstrekken van (persoons)gegevens. De wet bevat een informatieverplichting aan familie en wettelijke vertegenwoordigers. Daarnaast is de voor de behandeling verantwoordelijke persoon op grond van artikel 38, lid 2, Wet Bopz verplicht om voor het opstellen van het behandelingsplan overleg te plegen met de instelling of de psychiater die de patiënt voorafgaande aan zijn opneming behandelde of begeleidde, alsmede met de huisarts van de patiënt. Indien de behandelende persoon beslist dat de patiënt niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake van de

voorgestelde behandeling, pleegt hij over de behandeling overleg met de wettelijke vertegenwoordiger van de patiënt of, indien deze ontbreekt, met de persoon die daartoe door de patiënt schriftelijk is gemachtigd.

Voorts kunnen op grond van het Besluit Patiëntendossier Bopz zonder toestemming van de patiënt gegevens worden overgedragen aan de hulpverlener die de behandeling overneemt. Dit is een uitzondering op artikel 7:457 BW.

Op gegevensuitwisseling over patiënten met anderen dan de in de voorgaande alinea's genoemde personen is de WGBO van toepassing. In de Wgbo is het medisch beroepsgeheim vastgelegd, dat inhoudt dat een hulpverlener geen gegevens van een patiënt aan anderen mag verstrekken. Doorbreking van het medisch beroepsgeheim is alleen toegestaan als de patiënt hiervoor toestemming heeft gegeven, dit is toegestaan aan personen die direct bij de behandeling betrokken zijn en indien er een conflict van plichten bestaat. Een conflict van plichten kan zich voordoen wanneer een zwaarwegend belang van de patiënt of een ander dan de patiënt de doorbreking van de geheimhoudingsplicht rechtvaardigt, omdat het bewaren van het geheim voor de patiënt of de ander ernstig nadeel of gevaar oplevert.

Naast de Wet Bopz en de Wgbo is ook de Wbp van toepassing op de gegevensuitwisseling en -verwerking binnen een samenwerkingsverband. Op grond van de Wbp hebben de patiënten recht op informatie, inzage, correctie en verzet. Daarnaast bestaat voor de verantwoordelijke de plicht de verwerking van persoonsgegevens binnen het samenwerkingsverband te melden bij het Cbp.

7.4.3.2 Zelfregulering en afspraken

In de uitvoeringsovereenkomst tussen de GGD-en en de GGZ is opgenomen dat de GGD-en verantwoordelijk zijn voor de aanlevering van een volledig medisch dossier. In de samenwerkingsovereenkomst tussen de GGZ en VZ zijn geen bepalingen opgenomen over gegevensuitwisseling. Geen van beide overeenkomsten bevat bepalingen over welke gegevens wel en niet mogen worden uitgewisseld. Ook zijn er geen bepalingen opgenomen over de uitwisseling van de gegevens met derden. Tijdens de interviews is aangegeven dat voor het aangaan van het samenwerkingsverband geen contact is geweest met het Cbp of een andere deskundige op het gebied van de uitwisseling van persoonsgegevens. De gegevens-uitwisseling is ook niet gemeld bij het Cbp.

Bij de uitwisseling met derden wordt door de GGZ en VZ gehandeld volgens het privacyreglement van de GGZ. Dit reglement is vastgesteld door de Raad van bestuur van de GGZ en inhoudelijk geactualiseerd tot en met 22 juni 2007. Dit document is een vervanging van het document dat intern vanaf mei 2006 heeft gediend als privacyregelement GGZ en dat voornamelijk toezag op de werking en toepassing van de Wet bescherming persoonsgegevens. In het privacyreglement van de GGZ is opgenomen dat geen patiëntgegevens via de e-mail mogen worden uitgewisseld. Het privacyreglement bepaalt dat de toepassing van de Wbp nog nader zal worden beschreven in de notitie "Toepassing Wet bescherming persoonsgegevens binnen GGZ".

De beide betrokken GGD-en hebben een eigen privacyreglement. Daarnaast wordt in de praktijk veel gebruik gemaakt van de Handreiking gegevensuitwisseling in het kader van bemoeizorg die is opgesteld door de GGD Nederland samen met de GGZ Nederland en de

Koninklijke Nederlandse Maatschappij tot bevordering van Geneeskunde.[242] In deze handreiking wordt gesteld dat de richtlijnen die daarin zijn genoemd in overeenstemming zijn met de bepalingen in de Wbp.[243] Juist binnen de ketensamenwerking is het voor een effectieve behandeling noodzakelijk dat gegevens worden uitgewisseld.

7.4.4 Gegevensuitwisseling binnen het samenwerkingsverband

7.4.4.1 Toeleidingscommissie

Binnen het samenwerkingsverband vindt de meeste uitwisseling van persoonsgegevens plaats binnen de toeleidingscommissie. Nadat een patiënt is geplaatst in de GGZ-instelling vindt ook nog regulier overleg plaats tussen de GGD en de GGZ over het verloop van de behandeling van de patiënten. Het informeren van de GGD door de GGZ vindt plaats via een vastgelegd reglement.

De dossiers worden per koerier bezorgd aan de leden van de toeleidingscommissie. In de uitvoeringsovereenkomst is niet vastgelegd dat de verschillende instellingen in de grote steden onderdeel uitmaken van de toeleidingscommissie, terwijl dat in de praktijk wel zo is. Alle leden van de toeleidingscommissie krijgen de dossiers van alle patiënten die worden besproken toegestuurd.

De patiënten van de verschillende psychiaters worden vervolgens in aanwezigheid van alle andere psychiaters besproken. Dit betekent dat de andere psychiaters informatie verkrijgen over personen die niet hun patiënt zijn en waarmee zij geen behandelovereenkomst hebben gesloten.

Af en toe neemt een psychiater van een van de instellingen in de grote steden contact op met de psychiater van de GGZ om te overleggen of een bepaalde casus kans van slagen heeft in de toeleidingscommissie.

Als een patiënt afkomstig is uit een instelling uit een van de grote steden bestaat voorafgaand aan de behandelovereenkomst met de psychiater van de GGZ een behandelovereenkomst met de psychiater van die instelling. In de toeleidingscommissie worden ook patiënten besproken die in het geheel geen behandelovereenkomst hebben. Deze zijn bijvoorbeeld afkomstig uit een huis van bewaring waar besloten is dat deze persoon door een psychiater moet worden gezien. Deze psychiater kan de betrokken persoon vervolgens voordragen aan de toeleidingscommissie. De politie is nooit aanwezig bij een toeleidingscommissie.

Tussen de GGD en de patiënt bestaat geen behandelovereenkomst of andere relatie. De GGD functioneert als intermediair tussen de psychiaters en de buitenstedelijke instelling van de GGZ. Wel beschikt de GGD over het volledige patiëntdossier zoals dat ook aanwezig is binnen de GGZ-instelling.

[242] GGD Nederland e.a. 2005
[243] GGD Nederland e.a. 2005, p. 9

7.4.4.2 Plichten op basis van de Wbp

Tot op heden zijn geen gegevens vernietigd binnen het project en heeft ook nog geen enkele (voormalige) patiënt om verwijdering of vernietiging van gegevens verzocht. Een enkele keer verzoekt een patiënt om inzage in zijn dossier en die inzage is in alle gevallen verleend.

Over het bewaren van de gegevens zijn geen afspraken gemaakt en de verwerking van de persoonsgegevens binnen het samenwerkingsverband is niet gemeld aan het Cbp. Dit laatste kan onder meer veroorzaakt worden door het gegeven dat binnen het samenwerkingsverband geen verantwoordelijke is aangewezen. De patiëntbestanden van de twee GGD'en zijn wel gemeld bij het Cbp. In deze patiëntbestanden zijn ook de gegevens van de patiënten opgenomen die in de GGZ-instelling verblijven.

7.4.4.3 Gegevensuitwisseling tussen samenwerkingspartners

De GGZ-instelling werkt met een elektronisch patiëntdossier. Daarnaast is er van iedere patiënt een papieren dossier beschikbaar. Alleen de behandelend psychiater en de psychiatrisch verpleegkundige hebben toegang tot het elektronisch patiëntdossier. Zij zijn daarvoor geautoriseerd. De papieren dossiers worden bewaard in een kast op het secretariaat van de GGZ instelling. Deze kast wordt 's nachts afgesloten. De secretariaatsmedewerkers hebben inzage in de papieren dossiers en zullen aan anderen dan GGZ of GGD-medewerkers niet toestaan dat zij een dossier uit de kast nemen. Over de inzage in de papieren dossiers zijn geen afspraken gemaakt.

In bepaalde gevallen wordt besloten dat sommige informatie over een patiënt niet aan alle medewerkers die bij de behandeling zijn betrokken, moet worden verstrekt. Bijvoorbeeld als een patiënt in een ver verleden een delict heeft gepleegd dat een belemmering kan vormen in de omgang met de patiënt. Dit zijn echter werkafspraken om de werkzaamheden goed te laten verlopen en wordt niet gedaan met het oog op privacy.

Tussen de partners van het samenwerkingsverband worden zonder belemmering gegevens uitgewisseld. Dit gebeurt zowel schriftelijk, telefonisch als via de e-mail. Het is niet voorgekomen dat de GGZ weigerde gegevens te verstrekken aan de GGD en andersom is dit ook niet gebeurd. De geheimhoudingsplicht heeft tot nu toe ook niet geleid tot problemen bij de uitwisseling van gegevens tussen de samenwerkingspartners. Alle geïnterviewden hebben wel aangegeven dat het belang van privacy (binnen het samenwerkingsverband) groot is.

7.4.4.4 Gegevensuitwisseling met derden

In het privacyreglement van de GGZ is bepaald dat zonder toestemming van de patiënt geen gegevens over patiënten mogen worden opgevraagd bij derden en dat ook niet zonder toestemming gegevens mogen worden verstrekt aan derden.

Aan de patiënten die zijn opgenomen in de GGZ-instelling wordt nooit toestemming gevraagd voor de verstrekking van gegevens aan derden. De psychiater van de GGZ maakt bij ieder dossier een afweging of hij de gegevens kan doorgeven aan iemand anders en daarbij het beroepsgeheim kan doorbreken.

Het voorgaande betekent niet dat door de instelling aan iedere willekeurige persoon gegevens worden verstrekt. In de interviews is aangegeven dat bepaalde organisaties en bedrijven zoals de politie en incassobureaus bijzonder gemakkelijk denken over privacy. Het is voorgekomen

dat medewerkers van de politie aan de balie van de instelling vragen stelden over de aanwezigheid van een bepaalde persoon in de instelling. Daarover is geen informatie verstrekt.

De enige derden aan wie informatie over de patiënt wordt verstrekt zijn de rechterlijke macht, de officier van justitie, de advocaat van een patiënt en een ziekenhuis waarin een patiënt wordt opgenomen voor de behandeling van een somatische aandoening. In die gevallen worden enkel de voor de instelling of organisatie relevante gegevens verstrekt.

Als gegevens bij andere instanties worden opgevraagd leidt dat wel eens tot problemen. Of de gegevens worden verkregen is vaak afhankelijk van de persoon die de telefoon opneemt.

Met de gemeente waarin de instelling is gevestigd worden alleen NAW gegevens uitgewisseld ten behoeve van de bijstandsuitkering voor de patiënten. Hierover zijn geen afspraken gemaakt. De kosten van de bijstanduitkering worden vervolgens weer door de stad waaruit de patiënt afkomstig is, terugbetaald aan de gemeente waarin de instelling gevestigd is.

7.4.4.5 Klachten en verzet

Als een patiënt een klacht heeft over de gegevensverwerking, dan kan hij deze indienen bij de klachtencommissie van de GGZ. Daarnaast kan een patiënt een klacht indienen bij de tuchtrechter en een schadeclaim indienen bij de civiele rechter. Voorts kan strafvervolging plaatsvinden als de schending van het beroepsgeheim opzettelijk heeft plaatsgevonden. Tot op heden is binnen het project geen van deze procedures gevolgd. Daarbij moet in aanmerking worden genomen dat het project nog maar kort loopt. De behandelend psychiater gaf aan dat hij in zijn vorige baan veelvuldig met klachten te maken heeft gehad en dat deze zeker geen bijzonderheid zijn in de geestelijke gezondheidszorg.

Naast de formele klachtenprocedure kan een patiënt zich wenden tot de patientenvertrouwens-persoon. Patiënten worden geïnformeerd over hun rechten door middel van een informatiemap die op de kamer van de patiënt ligt.

7.4.5 Conclusies

Binnen het onderzochte samenwerkingsverband in de geestelijke gezondheidszorg wordt de normering van de Wbp niet ervaren als een knelpunt in samenwerking. Overigens betekent dit niet dat in het geheel niet in strijd met de Wbp wordt gehandeld. Ten aanzien van de casus kan enkel worden gesteld of dit als knelpunt wordt ervaren door de betrokkenen. Aan de ervaren knelpunten ligt een aantal redenen ten grondslag.

Ten eerste is de Wbp niet de enige wettelijke regeling die van toepassing is op de uitwisseling van persoonsgegevens in dit samenwerkingsverband. Meer nog dan de Wbp spelen de Wgbo en de Wet Bopz een rol bij de uitwisseling. In het knelpuntenonderzoek werd de samenloop van de Wbp met andere wetten gezien als een knelpunt, maar binnen deze casus levert die samenloop vrijwel geen knelpunten op. Het betrokken personeel van de verschillende instellingen en de gemeentelijke gezondheidsdiensten handelen op basis van de Wgbo en de Wet Bopz. Het is voor hen duidelijk dat de bepalingen die in die twee wetten zijn opgenomen voorgaan op de Wbp waar het de uitwisseling van persoonsgegevens ten behoeve van de behandeling van de patiënten betreft.

Wanneer de behandeling van een patiënt door een psychiater van één van de instellingen in de grote steden wordt overgedragen aan de psychiater van de GGZ-instelling, is die uitwisseling toegestaan op basis van de Wet Bopz en het Besluit Patiëntendossier Bopz. Dit geldt ook voor de verplichte consultatie van de huisarts van de patiënt en het raadplegen van de familie over een behandelplan, als de patiënt zich daar zelf geen oordeel over kan vormen.

De Wet Bopz staat niet toe dat met anderen dan de in die wet genoemde personen gegevens worden uitgewisseld over de patiënt die wordt behandeld op basis van een RM. In de praktijk worden de gegevens over een patiënt echter ook verstrekt aan de GGD en de psychiaters van andere instellingen in de grote steden die zitting hebben in de toeleidingscommissie. Zij hebben beide geen behandelovereenkomst gesloten met de patiënt maar zijn wel op de hoogte van alle gegevens van aan patiënt. Deze uitwisseling van persoonsgegevens is in ieder geval deels mogelijk op basis van de Wgbo. Daarnaast is de handreiking bemoeizorg van belang bij de uitwisseling.

Een arts kan immers het beroepsgeheim zonder toestemming van de patiënt verbreken indien de persoon aan wie de gegevens worden verstrekt rechtstreeks bij de behandeling betrokken is of er een conflict van plichten bestaat. Deze afweging wordt door de psychiater van de GGZ instelling wel gemaakt.

Tot nu toe zijn door of namens patiënten geen klachten ingediend over de manier waarop de gegevens binnen het samenwerkingsverband worden uitgewisseld. Ook de bestaande jurisprudentie is voor de betrokken psychiaters geen reden om terughoudend te zijn met uitwisseling van gegevens binnen het samenwerkingsverband. Of deze uitwisseling daadwerkelijk niet in strijd is met de Wgbo kan enkel in individuele zaken beoordeeld worden, omdat dit afhankelijk is van de omstandigheden van het geval.

Door alle geïnterviewden wordt een groot belang aan privacy gehecht. Dit belang wordt nog versterkt door de kwetsbare groep waar zij verantwoordelijk voor zijn. Zij hebben allemaal aangegeven dat nauwelijks gegevens worden uitgewisseld met derden.

Dat aan privacy veel belang wordt gehecht, betekent echter niet dat ook alle toepasselijke bepalingen uit de Wbp worden nageleefd. Het Cbp of een andere deskundige heeft geen rol gespeeld bij de totstandkoming van de samenwerking en de gegevensuitwisseling binnen het samenwerkingsverband is niet gemeld bij het Cbp. Voor beide grote steden geldt wel dat de patiënten die worden behandeld door de GGZ-instelling ook in een eigen bestand van de GGD zijn opgenomen en dat bestand is wel gemeld. Dat de gegevensuitwisseling niet is gemeld, betekent overigens niet per definitie dat in strijd met de wet wordt gehandeld, omdat een groot aantal gegevensverwerkingen is vrijgesteld van de meldplicht.

In het knelpuntenonderzoek is aangegeven dat het lastig is om binnen samenwerkings-verbanden een verantwoordelijke aan te wijzen. Binnen deze casus leidt dat echter niet tot een knelpunt omdat in het geheel geen verantwoordelijke is aangewezen. Er is dus ook niet een expliciet een doel geformuleerd voor de gegevensuitwisseling ten behoeve van het doen van een melding. Het doel van de gegevensuitwisseling blijkt uiteraard wel uit de overeenkomsten die zijn gesloten tussen de GGZ en de GGD'en en de organisatie voor VZ.

Het knelpunt van de onbekendheid met de interpretatieruimte van de Wbp komt niet voor binnen deze casus. De afwegingen die moeten worden gemaakt, worden gemaakt binnen het

kader van de Wgbo en de Wet Bopz, waarbij de Handreiking bemoeizorg als leiddraad wordt gehanteerd.

De patiënten worden door de behandelend psychiater wel geïnformeerd over de verwerking van hun gegevens en indien van toepassing, hun wettelijke vertegenwoordigers. Ook worden de patiënten geïnformeerd over hun rechten door middel van een informatiemap op hun kamer. Tot op heden is ieder verzoek om inzage gehonoreerd en zijn nog geen verzets- of klachtprocedures gevolgd.

7.5 Vergelijking en algemene conclusies

In deze paragraaf worden de twee casus vergeleken aan de hand van de knelpunten die in het voorgaande onderzoek zijn geïdentificeerd. Aan de hand van die vergelijking worden enkele algemene conclusies over de uitwisseling van persoonsgegevens in samenwerkingsverbanden getrokken.

7.5.1 Samenloop van de Wbp met andere wetten

Zowel binnen het veiligheidshuis als het samenwerkingsverband in de geestelijke gezondheidszorg is sprake van samenloop van de Wbp met andere wetten.

Het feit dat naast de Wbp zoveel andere wetten van toepassing kunnen zijn, wordt wel als knelpunt ervaren in het veiligheidshuis, maar dan met name op beleidsniveau en niet door de medewerkers die de gegevens dagelijks uitwisselen. Binnen de casus over de geestelijke gezondheidszorg wordt vrijwel geen aandacht besteed aan de toepasselijkheid van de Wbp en wordt er in de meeste gevallen terecht van uitgegaan dat de bijzondere wetten waar men zich aan houdt, de uitwisseling afdoende regelen.

Uit het voorgaande kan worden afgeleid dat de samenloop van wetgeving eerder tot een knelpunt leidt als de partners in een samenwerkingsverband meer verscheiden zijn en met de samenwerking verschillende, deels wellicht conflicterende, doelen worden nagestreefd. Daarbij lijkt de verscheidenheid van de partners een doorslaggevende factor te zijn. Het veiligheidshuis heeft onder meer tot doel het voorkomen van strafbare feiten en het terugdringen van recidive, het terugbrengen en voorkomen van overlast en het verlenen van passende zorg aan het slachtoffer. De samenwerking in de geestelijke gezondheidszorg is gericht op de behandeling van de patiënt maar heeft tot doel criminaliteit en overlast te voorkomen. De partners binnen het samenwerkingsverband in de geestelijke gezondheidszorg vallen echter alle onder de werking van de Wgbo terwijl voor iedere samenwerkingspartners in het veiligheidshuis een andere wettelijke regeling van toepassing is.

Voorts kan nog worden opgemerkt dat samenloop van wetgeving eerder tot een knelpunt leidt als er mogelijk spanning bestaat tussen het belang van de betrokkenen en het belang dat met het samenwerkingsverband wordt nagestreefd. Binnen de gemeentelijke gezondheidszorg kan het belang van de behandelaar zeer wel overeenkomen met het belang van de patiënt. Beide zullen in beginsel gericht zijn op genezing. Daar moet als kanttekening bij worden geplaatst dat een groot aantal patiënten gedwongen verblijft in de buitenstedelijke instelling. Een verdachte die binnen het veiligheidshuis wordt besproken heeft een ander belang dan het veiligheidshuis en privacy kan daarom nadrukkelijker een rol spelen.

7.5.2 Aanwijzen verantwoordelijke

Binnen het samenwerkingsverband in de geestelijke gezondheidszorg is geen verantwoordelijke in de zin van de Wbp aangewezen. Binnen dat samenwerkingsverband wordt het bepalen van de verantwoordelijke in de praktijk dan ook niet ervaren als een knelpunt.

Binnen het veiligheidshuis is de hoofdofficier van justitie aangewezen als verantwoordelijke voor de verwerking van persoonsgegevens. Tijdens de totstandkoming van het veiligheidshuis heeft dit niet tot knelpunten geleid. Dat de hoofdofficier is aangewezen kan verklaard worden door het gegeven dat de officier van justitie een regietaak vervult en een beleidsvormende taak heeft. Daarnaast is het veiligheidshuis een initiatief dat vanuit het ministerie van Justitie wordt gepromoot.

Concluderend kan worden gesteld dat het aanwijzen van een verantwoordelijke in de onderzochte casus in de ogen van de geïnterviewden niet tot knelpunten heeft geleid. In het ene geval omdat men zich daar niet mee bezig heeft gehouden en in het andere geval omdat één van de samenwerkingspartners het initiatief heeft genomen en het aanwijzen van die partner als verantwoordelijke daarom voor de hand lag.

7.5.3 Onbekendheid met interpretatieruimte Wbp

In het onderzochte veiligheidshuis wordt de onbekendheid met de interpretatieruimte van de Wbp met name door de betrokken juristen en beleidsmedewerkers als een knelpunt ervaren. In de praktijk speelt de interpretatieruimte van de Wbp geen rol omdat gegevens worden uitgewisseld als de betrokkenen van mening zijn dat dit ten goede komt aan het bereiken van de doelstellingen van het veiligheidshuis.

Binnen de GGZ levert de onbekendheid met de interpretatieruimte van de Wbp geen knelpunt op omdat de Wbp bij de uitwisseling in de praktijk nauwelijks een rol speelt door de toepasselijkheid van andere wetgeving. De bepalingen uit de Wbp die wel van toepassing zijn, zoals de meldplicht in artikel 27 Wbp, zijn enerzijds minder lastig te interpreteren dan de open normen elders in de Wbp en hebben daarnaast binnen het GGZ samenwerkingsverband nog geen rol gespeeld omdat geen melding is gemaakt van de verwerking.

Uit het voorgaande kan worden geconcludeerd dat personen die de wettekst bestuderen in hun dagelijkse werk de onbekendheid met de interpretatieruimte als een knelpunt ervaren. Waar gegevens feitelijk worden uitgewisseld, speelt deze interpretatieruimte geen rol.

7.5.4 Voorafgaand onderzoek

De verwerking van persoonsgegevens in beide samenwerkingsverbanden is niet gemeld bij het Cbp. Van een voorafgaand onderzoek kan daarom ook nog geen sprake zijn. De lange doorlooptijd is daarom niet als een knelpunt ervaren.

7.5.5 Gegevensuitwisseling in strijd met de Wbp

In het knelpuntenonderzoek is het vermoeden uitgesproken dat deelnemers aan samenwerkingsverbanden informatie krijgen over betrokkenen waarmee zij niets te maken

hebben of, als het gaat om een betrokkene waarmee ze wel een relatie hebben, informatie krijgen die voor de uitvoering van hun taak niet noodzakelijk is.

Op de uitwisseling binnen de GGZ-casus zijn de Wgbo en de Wet Bopz van toepassing en wordt daarnaast de Handreiking bemoeizorg gehanteerd die naar het oordeel van de opstellers in overeenstemming met de bepalingen van de Wbp is. De geestelijke gezondheidszorg neemt in bescherming van privacy ook historisch een bijzondere positie in omdat zij al vele jaren werken met privacywetgeving in de vorm van de voorgangers van de Wgbo en de Wet Bopz. Daarnaast beschikte de sector reeds over een klachtenregeling voordat deze was opgenomen in de Algemene wet bestuursrecht. Zoals in de inleiding al is gesteld wordt in dit onderzoek echter niet de vraag beantwoord of de gegevensuitwisseling conform dan wel in strijd met de Wbp plaatsvindt.

Ten aanzien van het veiligheidshuis kan ook niet worden uitgesloten dat in strijd met de Wbp gegevens worden uitgewisseld. Met name is het de vraag of informatie wordt verkregen die voor de uitvoering van een bepaalde taak niet noodzakelijk is. Toch kan deze vraag enkel in algemene zin worden beantwoord. Dit geldt zowel voor de GGZ als voor het veiligheidshuis. Of de uitwisseling van gegevens over een bepaalde betrokkene rechtmatig is, is altijd afhankelijk van de omstandigheden van het geval van de betrokkene.

7.5.6 Afsluitend

Als de twee casestudies met elkaar worden vergeleken blijkt dat het privacybewustzijn in de twee cases sterk van elkaar verschilt. Binnen de casus in de geestelijke gezondheidszorg is men zich zeer bewust van het belang van privacy en is men zeer terughoudend met het uitwisselen van gegevens aan partners buiten degenen die direct betrokken zijn bij de behandeling van een patiënt. Dit wordt ook bevestigd door de casus van het veiligheidshuis waarin door de geïnterviewden is gesteld dat de GGZ terughoudender omgaat met de uitwisseling van persoonsgegevens dan de andere samenwerkingspartners. Daar staat tegenover dat de samenwerkingspartners binnen de geestelijke gezondheidszorg ook minder oog hebben voor de weinige bepalingen uit de Wbp die wel van toepassing kunnen zijn, terwijl daar op beleidsniveau binnen het veiligheidshuis wel aandacht voor bestaat. Concluderend kan worden gesteld dat de Wbp niet als een knelpunt wordt ervaren maar dat dit niet betekent dat er, positiefrechtelijk bezien, geen knelpunten zouden zijn.

Hoofdstuk 8 Slotbeschouwing

8.1 Inleiding

In dit hoofdstuk worden de bevindingen van het onderzoek waarvan hiervoor verslag is gedaan met elkaar in verband gebracht en nader beschouwd. In hoofdstuk 3 is het beschrijvingskader van het onderzoek geschetst. Op basis daarvan zijn vragenlijsten opgesteld en is enquêteonderzoek uitgevoerd. In de hoofdstukken 4 en 5 zijn de uitkomsten van de drie uitgevoerde enquêteonderzoeken weergegeven. In hoofdstuk 6 hebben we verslag gedaan van onderzoek onder 'betrokkenen' die een geschil aanhangig hebben gemaakt bij een rechterlijk college, het Cbp of de Nationale ombudsman. In hoofdstuk 7 zijn de resultaten weergegeven van casestudies die we hebben uitgevoerd naar de uitwisseling van persoonsgegevens in twee situaties van ketensamenwerking. De bevindingen die we opdeden in interviews en tijdens expertmeetings met vertegenwoordigers van belangenbehartigingsorganisaties, met juridisch experts, met Functionarissen Gegevensbescherming, met medewerkers van bedrijven en overheden en het Cbp, zijn behalve voor het opstellen van vragenlijsten vooral gebruikt voor de interpretatie van de onderzoeksuitkomsten. Die bevindingen gebruiken we ook bij de afsluitende beschouwingen in dit laatste hoofdstuk .

Bij het trekken van algemene conclusies in dit hoofdstuk onderstrepen we nogmaals het gegeven dat we niet bij alle uitgevoerde enquêtes een bevredigende respons konden behalen. De respons op de enquête onder de FG's is voldoende, die op de enquête onder meldende organisaties matig, terwijl de respons op de enquête onder organisaties in het algemeen onvoldoende is. Dat brengt beperkingen met zich mee voor de wijze waarop de bevindingen uit het enquêteonderzoek kunnen worden veralgemeniseerd. Daarover is in hoofdstuk 4 en 5 dan ook met enige terughoudendheid gerapporteerd. Daar staat tegenover dat de resultaten van de drie enquêtes onderling redelijk consistent lijken te zijn. De drie groepen verschillen van elkaar waar het gaat om hun mate van betrokkenheid bij de wet. Bij de FG's is die het grootst, bij de organisaties die in de algemene enquête zijn bevraagd is die – gemiddeld genomen – het kleinst. Wanneer de bevindingen tegen die achtergrond worden bezien komt daaruit een duidelijk en consistent beeld naar voren. En hoewel niet bij elke enquête de respons bevredigend was, stelt nadere interpretatie van de bevindingen van het vragenlijstenonderzoek op basis van de interviews en de expertmeetings ons niettemin wel in staat tot het trekken van enkele algemene concluderende lijnen in dit slothoofdstuk.

In paragraaf 8.2 worden de onderzoeksvragen die in hoofdstuk 1 zijn geformuleerd voorzien van een antwoord. De probleemstelling van het evaluatieonderzoek, die er op was gericht de bevindingen uit het knelpuntenonderzoek empirisch te onderzoeken, komt in paragraaf 8.3 aan de orde.

8.2 Beantwoording van de onderzoeksvragen

8.2.1 Inleiding

In deze paragraaf worden de onderzoeksvragen uit hoofdstuk 1 beantwoord. Die onderzoeksvragen vallen in drie delen uiteen, die in afzonderlijke subparagrafen centraal staan. Paragraaf 8.2.2 gaat over de normen uit de Wbp, paragraaf 8.2.3 betreft de

informatievoorziening over de wet, terwijl in paragraaf 8.2.4 toezicht en rechtsbescherming centraal staan.

8.2.2 Normeren

1. Wat zijn de voor- en nadelen van open normen, in het algemeen en specifiek voor de Wbp? Hoe werkbaar zijn de open normen uit de Wbp? Is altijd duidelijk wanneer gegevens mogen worden uitgewisseld?

De kern van de Wbp bestaat uit open normen. Bij de toepassing van de wet in concrete situaties moeten die normen nader worden ingevuld. Uit het knelpuntenonderzoek kwam naar voren dat de wet mede daardoor moeilijk hanteerbaar zou zijn in de praktijk. Tegen die achtergrond is het van belang vast te stellen dat vrijwel iedereen die we in het kader van het evaluatieonderzoek hebben geraadpleegd van oordeel is dat het onderwerp privacy niet anders dan met open normen kan worden geregeld. Daarbij worden als algemene voordelen van open normen genoemd dat open normen een nadere invulling kunnen krijgen in een bepaalde context, zoals een regeling per sector of branche. De wet en de regelingen per branche maken vervolgens een meer casusspecifieke beoordeling mogelijk en ook wordt gesteld dat op die manier beter rekening kan worden gehouden met onvoorziene omstandigheden. Specifiek voor de Wbp wordt benadrukt dat technologische ontwikkelingen van groot belang zijn voor privacybescherming en dat daarop alleen door middel van open normstelling flexibel kan worden ingespeeld.

Hoewel de keuze van de wetgever voor het stellen van open normen dus breed wordt gedeeld, blijkt de veronderstelling over de wijze waarop die normen in de praktijk zouden gaan functioneren deels niet uit te komen. De wetgever hoopte dat de open normen in de wet zouden leiden tot de ontwikkeling van nadere normstelling binnen de sectoren waarop de wet van toepassing is. Die nadere normen zijn wel tot stand gekomen, maar niet over de hele breedte van de praktijk waarin de wet van toepassing is. Gedragscodes in de zin van artikel 25 van de wet zijn slechts in zeer beperkte mate ontwikkeld. Uit de enquêtes blijkt anderzijds wel dat bij ruim de helft van de organisaties en branches normenkaders tot stand zijn gekomen, zoals een afzonderlijk privacyprotocol of een branchecode, waarvan privacynormen deel uitmaken. Rechtsontwikkeling door middel van geschilbeslechting komt nauwelijks van de grond. Het Cbp doet wel het nodige aan het bevorderen van bekendheid met de wet en het verduidelijken van de wijze waarop die in bepaalde gevallen moet worden toegepast. Dat geschiedt onder meer door het uitgeven van informatiebladen, het publiceren van richtsnoeren en het bemiddelen in concrete geschillen die burgers opwerpen over de toepassing van de wet. Het college brengt naar verluidt eind 2008 een jurisprudentiebundel uit waarin de eigen ‘jurisprudentie’ en die van rechterlijke colleges gebundeld is.

De open normen van de wet moeten dus in een specifieke context (sector, branche) nader worden ingevuld en in concrete situaties worden geïnterpreteerd. Dat brengt noodzakelijkerwijs administratieve lasten met zich mee. Het verbaast dan ook niet dat verantwoordelijken melden dat de wet aanleiding geeft tot administratieve lasten en dat de tevredenheid over de wet varieert met de hoogte van de administratieve lasten bij de toepassing van de wet. In paragraaf 5.9 is verslag gedaan van een statistische analyse die is uitgevoerd op de gegevens uit het bestand organisaties met een FG. Uit die analyse blijkt dat de hoogte van het rapportcijfer dat FG’s geven aan de Wbp in sterke mate wordt bepaald door drie factoren: de duidelijkheid die zij zeggen te hebben over de wijze waarop de open normen moeten worden geïnterpreteerd, de hoogte van de administratieve lasten en het geconstateerde

aantal onrechtmatige verwerkingen. Meer dan zestig procent van de variatie in de hoogte van het rapportcijfer over de tevredenheid over de wet kan hierdoor worden verklaard, hetgeen een hoog percentage kan worden genoemd. De onzekerheid over de wijze waarop de open normen moeten worden toegepast is veruit de sterkste factor in de vergelijking. Onduidelijkheid over de invulling van de open normen leidt tot onzekerheid over de toepassing van de wet en heeft een negatief effect op de tevredenheid over de wet. In de eerste plaats ontstaan niet goed in te schatten juridische risico's voor de organisatie wanneer gegevens worden verwerkt. In de tweede plaats leidt ook het niet verwerken van gegevens tot een ongewenste uitkomst, namelijk tot onderbenutting van gegevens. De administratieve lasten die de toepassing van de wet met zich meebrengt worden bepaald door de verplichtingen die de wet voorschrijft (zoals de meldingsplicht), de nadere invulling van de wet in sectorale regelingen en de toepassing van die normen in concrete situaties. Wellicht weinig verrassend, blijkt uit de enquête onder de FG's dat hoe groter de administratieve lasten, des te minder tevreden de FG over de wet is. Het geconstateerde aantal foute verwerkingen is een interessante factor, die er op lijkt te wijzen dat wanneer een FG een onrechtmatige gegevensverwerking constateert, daarmee het belang van de wet wordt onderstreept. Hoewel er weinig onrechtmatige verwerkingen worden geconstateerd, blijkt uit de enquête onder FG's dat hoe vaker een FG een onrechtmatige verwerking waarneemt, hoe meer tevreden hij is over de wet.

Opvallend is dat uit het verslag van het enquêteonderzoek in hoofdstuk 5 (onder meer tabel 34 en 35) blijkt dat hoe minder organisaties met de Wbp te maken hebben, des te meer ze zeggen duidelijkheid te hebben over de vraag welke persoonsgegevens mogen worden verwerkt. Hoewel we met die gegevens terughoudend moeten omgaan, gelet op de geringe respons op de enquête onder de organisaties in het algemeen, laat de vergelijking van de drie enquêtes wel een duidelijk beeld zien. Dat lijkt er op te wijzen dat de Wbp vooral niet als een lastige wet wordt beschouwd door diegenen die weinig van de wet weten. En omgekeerd betekent het dat de organisaties die relatief het meest intensief met de wet te maken hebben, in ons onderzoek de organisaties met een FG, aangeven de meeste problemen te hebben met de toepassing van de wet. Meer dan de helft van de FG's gaf immers aan onvoldoende informatie te hebben om de wet goed uit te kunnen voeren. De organisaties die een melding hebben gedaan bij het Cbp nemen een tussenpositie in, ook wat betreft de kennis die zij van de wet hebben. 'Wat niet weet, wat niet deert', kan uit de onderlinge vergelijking van de enquêteresultaten worden afgeleid. Dat duidelijke signaal komt uit het hele onderzoek naar voren.

Ook in de twee uitgevoerde casestudies waar situaties van gegevensuitwisseling aan de orde waren, is gebleken dat de open normen van de wet voor problemen zorgen. De meest opvallende bevinding in de uitgevoerde casestudies is dat men aan de vraag hoe de normen moeten worden geïnterpreteerd vaak niet eens toekomt. Onbekendheid van de normen en onzekerheid over de wijze waarop deze moeten worden toegepast, blijkt in de praktijk een probleem. In de uitgevoerde casestudies bleek dat dit kan leiden tot onrechtmatige gegevensuitwisselingen.

2. Wat is de achtergrond van het ontbreken van sectorale regelgeving en/of gedragscodes? Vervulde het Cbp hierbij een 'ontwikkelende' en stimulerende rol?

Uit onderzoek onder organisaties in het algemeen kan worden afgeleid dat een deel van de geënquêteerde organisaties beschikt over een privacycode (zie paragraaf 4.3). Dat is vaak een privacycode die de organisatie zelf heeft ontwikkeld, maar het kan ook gaan om een branchecode waarvan privacynormen deel uitmaken. Uit de antwoorden op de vragenlijst

blijkt dat betrekkelijk veel respondenten het antwoord op deze vraag niet wisten. Bij deze bevindingen moeten we aantekenen dat we een gestratificeerde steekproef uit het handelsregister hebben genomen. De enquête is ingevuld door relatief grote organisaties, vooral uit branches die met de wet te maken hebben. Dat zou kunnen betekenen dat voor het totaal van alle bedrijven die in Nederland persoonsgegevens verwerken minder (branche)codes worden gehanteerd dan uit dit onderzoek is gebleken. Dat betrekkelijk veel organisaties zeggen te beschikken over een of andere regeling over privacy, betekent niet dat die gedragscodes ook bij het Cbp ter goedkeuring zijn aangemeld ex artikel 25 Wbp. De experts die we hebben geraadpleegd geven aan dat die goedkeuringsprocedure tijdrovend is en dat onder meer daarom vaak van goedkeuring wordt afgezien. Dat sluit aan bij de bevindingen van het knelpuntenonderzoek (zie ook paragraaf 3.2.2).

De respondenten die wij in het kader van het onderzoek hebben gesproken menen dat van een sterk stimulerende rol van het Cbp met het oog op de normontwikkeling niet kan worden gesproken. Het Cbp geeft zelf wel met enige regelmaat 'richtsnoeren' uit, recent over Internet en privacybescherming ('Publicatie van persoonsgegevens op Internet', december 2007), maar we kunnen niet vaststellen dat hiervan een sterke stimulans op branches en sectoren uitgaat om regelingen en codes op te stellen.

3. Op welke wijze kan worden voorzien in de ontwikkeling van sectorale normen en door wie?

Uit de enquêteresultaten en uit veel van de gevoerde gesprekken komt als beeld naar voren dat er op het terrein van de bescherming van persoonsgegevens een gebrek is aan duidelijke en toepasbare normen. Dat is niet aan de Wbp toe te schrijven, want – zoals hiervoor is benadrukt – breed wordt de keuze voor open normen onderschreven, maar wel aan de nog niet erg ontwikkelde nadere regelgeving, het gemis aan jurisprudentie en wellicht ook aan duidelijke informatievoorziening. De meeste van onze respondenten hebben overigens begrip voor de keuze die het Cbp in 2007 heeft gemaakt voor een accentverschuiving richting toezicht, waardoor advisering en informatievoorziening minder nadruk krijgen. Uiteraard moet de organisatie gelet op zijn beperkte capaciteit prioriteiten stellen. Tegelijkertijd lijkt het een groot manco dat er in ons land op dit moment geen organisatie is die een stimulerende en ontwikkelende rol vervult op het terrein van de bescherming van persoonsgegevens. Er is ook geen duidelijke gemeenschap van experts of belangenbehartigers die zich hard maakt voor het privacybelang van de burger. Er is wel een genootschap van FG's, maar omdat er bij slechts ca 250 organisaties FG's zijn aangesteld, ongeveer 0,3 promille van het totaal aantal organisaties in ons land, zijn de mogelijkheden van dat NGFG, waarbij slechts 80 FG's zijn aangesloten, niet erg groot. De relaties tussen het Cbp en het NGFG zijn overigens uitstekend; de voorzitter van het college voert regelmatig overleg met het genootschap en de lijnen zijn kort. De conclusie is dat het privacybelang behoefte heeft aan professionele behartigers, maar die zijn op dit moment nog onvoldoende in aantal en in kracht.

Hoewel de meeste respondenten van mening zijn dat nadere normstelling in branches sectoraal moet worden ontwikkeld, heeft een enkele gesprekspartner daar weinig vertrouwen in. Volgens deze gesprekspartner zou een meer actieve houding van de wetgever, door het stellen van normen in ministeriële regelingen of amvb's, een alternatief kunnen zijn. Tegelijkertijd moet worden vastgesteld dat voor diverse overheidssectoren dergelijke normen in lagere regelgeving (beleidsregels en aanwijzingen) wel degelijk reeds tot stand zijn gekomen.

4. Wat kan worden gezegd over de mate waarin technologische ontwikkelingen een rol spelen bij de toepassing van de wet?

Er zijn verschillende technologische ontwikkelingen die relevant zijn voor de bescherming van het recht op privacy. Onze respondenten menen dat het Cbp goed werk verricht door nu al aandacht te vragen voor 'de technologie van de toekomst'. Een aantal van die ontwikkelingen, zoals RFID en biometrie, gaat namelijk enorm snel. Aan de andere kant zijn die technologische innovaties zodanig ingrijpend dat nog onvoldoende bepaald kan worden wat daarvan precies de gevolgen zullen zijn voor de bescherming van persoonsgegevens. Van de toepassing van technieken als RFID en biometrie bij de door ons onderzochte populatie in de enquêtes is nog maar zeer beperkt sprake (zie hoofdstuk 4, tabel 29 en 30). Toch zijn er verschillende voorbeelden die het actuele belang daarvan onderschrijven, zoals de OV-chipkaart, de vingerafdruk die supermarkten voor transacties willen gaan gebruiken en de vele toepassingen van cameratoezicht. Voor veel van deze technieken geldt dat ze zeer gebruiksvriendelijk zijn en daarom ook door burgers worden gewaardeerd. Een goed beeld van de wijze waarop het grote publiek de afweging maakt tussen de privacyrisico's van deze technologische ontwikkelingen en het gebruiksgemak daarvan bestaat echter niet en is door ons ook niet in kaart gebracht.

In vergelijking met RFID en biometrie baren al langer bekende technieken veel van onze respondenten meer zorgen. Daarbij worden met name het Internet (webbeacons, cookies) en het koppelen van bestanden vaak genoemd. Bij meer dan de helft van de organisaties is de omgang met persoonsgegevens veranderd als gevolg van technologische ontwikkelingen. Bijna de helft van de organisaties met een FG heeft het privacybeleid aangepast onder invloed van deze technieken (zie paragraaf 4.9). Die bevindingen wijzen er op dat deze technologische ontwikkelingen wel degelijk van belang zijn in de praktijk van de bescherming van het privacybelang. Het belang van de technologische innovaties blijkt ook uit het feit dat het steeds vaker voorkomt dat burgers op Internet elkaars privacy schenden. Denk aan filmpjes gemaakt met mobiele telefoons die via sites als You Tube en Hyves hun weg vinden. De wet is hierop minder goed toegesneden. Hierbij moet wel worden opgemerkt dat de Wbp persoonsgegevens beschermt en niet elk filmpje dat op een dergelijke site wordt geplaatst als een vorm van verwerking van persoonsgegevens kan worden aangemerkt. Voor zover de Wbp hiertegen geen bescherming kan bieden, kan het strafrecht dat mogelijk wel doen. Hoewel de term 'verantwoordelijke' zich ook tot de burger richt, wordt dat begrip vooral geïnterpreteerd als een functionaris binnen een organisatie die gegevensbestanden beheert. Handhaving van de wet ten aanzien van de burger als 'verantwoordelijke' moet vrijwel onmogelijk worden geacht door de massaliteit en de anonimiteit van de privacyschendingen door burgers.

5. Op welke manier vormt de normering van de Wbp een knelpunt in de (keten)samenwerking?

Uit de door ons uitgevoerde casestudies, waarvan in hoofdstuk 7 verslag is gedaan, blijkt niet dat de respondenten die we binnen de betrokken organisaties hebben geraadpleegd van mening zijn dat de normen van de wet problemen met zich mee brengen voor de ketensamenwerking. Dat wil echter niet zeggen dat er zich geen knelpunten zouden voordoen wanneer de wet conform de bedoeling wordt toegepast. In de GGZ-case staat de Wbp bij de samenwerkende partijen niet scherp op het netvlies. Dat wordt deels veroorzaakt door de nadruk die de op de psychiatrie specifiek toepasselijke privacywetgeving krijgt. Bij het bestudeerde veiligheidshuis lijkt bij de afweging tussen het privacybelang en het beleidsdoel dat met de samenwerking en de uitwisseling van gegevens wordt gediend (bijvoorbeeld meer

veiligheid, of preventieve handhaving) het belang van privacy het onderspit te delven. Deze opvallende bevindingen kunnen echter niet zo maar worden veralgemeniseerd naar andere of alle gevallen van gegevensuitwisseling bij ketensamenwerking. Het is in dat verband goed te beklemtonen dat de door ons bestudeerde gevallen van ketensamenwerking relatief nieuw zijn. Bij het onderzochte veiligheidshuis zijn privacyregels nog volop in ontwikkeling. In beide cases zijn er bovendien verschillende andere wettelijke regelingen van toepassing die ook het privacybelang beschermen. Opvallend is dat door de samenwerkende partijen in de GGZ-case het privacybelang zwaarwegend wordt geacht, maar dat de Wbp daaraan niet of nauwelijks heeft bijgedragen.

8.2.3 Informeren

6. Hoe duidelijk is de wet en op welke wijze en in welke mate worden normen verduidelijkt door het Cbp en de jurisprudentie?

Uit het enquêteonderzoek (zie paragraaf 5.3) blijkt – zoals hierboven ook al werd gerapporteerd – dat de moeite die respondenten zeggen te hebben met de duidelijkheid van de wet, toeneemt naarmate ze vaker met de wet te maken hebben. Dat is op zich verklaarbaar omdat de wet open normen bevat, die in concrete situaties moeten worden ingevuld. Vragen over de toepassing van de wet zouden onder 'het bevorderen van bewustwording' en 'het bevorderen van normontwikkeling' kunnen worden geschaard, beide onderdeel van het 'viersporenbeleid' dat Cbp en voorheen de Registratiekamer sinds 1998 volgden. In 2007 maakte het Cbp een bewuste keuze de prioriteit te verleggen naar toezicht en handhaving. In dat jaar ontving het Cbp bijna 6.000 verzoeken om algemene voorlichting. Er waren bijna 400 klachtzaken en verzoeken om bemiddeling. Het college besloot bij verzoeken om hulp en bijstand de prioriteit te leggen bij ernstige overtredingen met een structureel karakter en met grote gevolgen voor een groot aantal burgers of groepen burgers. De verwachting is dat door het intensiveren van het toezicht op de naleving van de normen, die naleving grotere prioriteit zal krijgen. En wellicht zullen als gevolg van het afsluiten van de mogelijkheid het Cbp om advies te vragen andere organisaties gaan investeren in normontwikkeling en advisering. Anderzijds weten we uit rechtssociologische literatuur dat wanneer normen in een veld ingang vinden en worden geaccepteerd, die normen ook meer worden nageleefd. Dat zou juist pleiten voor een meer actieve adviesrol van het Cbp. De respondenten die we hebben geraadpleegd hebben over het algemeen begrip voor de keuze die het college heeft gemaakt. Gelet op de omvang van de organisatie en de breedte van het takenpakket is het stellen van prioriteiten onontkoombaar. Daarbij komt dat er binnen het takenpakket een inherente spanning zit tussen toezicht houden, ontwikkelen en uitvoeren. Niet alleen compliceert het geven van adviezen over de toepassing van de wet de handhavingstaak, beide taken vragen ook verschillende competenties. Een toezichthouder kiest immers vaak een veel passievere rol dan een ontwikkelaar. Overigens is het goed vast te stellen dat de wet geen verplichte adviestaak aan het Cbp heeft opgedragen, behoudens het adviseren over wetgeving, zoals bedoeld in artikel 51 lid 2 Wbp.

Het voorgaande neemt niet weg dat onze respondenten een intermediaire rol bij de ontwikkeling en uitwerking van de wet node zeggen te missen. Dat geldt – wellicht niet toevallig – bij uitstek (maar niet uitsluitend) voor de vertegenwoordigers van burgerbelangen. Gedurende het onderzoek zijn in dit verband door onze gesprekspartners verschillende voorbeelden genoemd van vragen waarop geen antwoord kon worden verkregen. Dat het Cbp de adviserende en informerende rol niet (langer) wenst te spelen wordt des te klemmender doordat ook de rechtsontwikkeling in de jurisprudentie achterblijft. Burgers werpen niet vaak

een geschil op over privacyaangelegenheden. Voor zover een privacybelang in een concreet geschil aan de orde is, speelt dat vrijwel steeds een rol in het kader van een geschil over een andere aangelegenheid, en komt de privacyvraag niet in zijn zuivere vorm aan de orde.

7. Welke informatie wordt, onder meer door het Cbp, aan de doelgroepen van de wet (verantwoordelijken, professionele gebruikers en burgers) gegeven? Is die informatie voldoende? Welke verbeteringen zijn mogelijk?

Algemene informatie over de wet wordt door het Cbp verschaft via richtsnoeren, informatiebladen, handleidingen en checklists. Via de sites mijnprivacy.nl en cbpweb.nl is veel informatie gemakkelijk toegankelijk. Specifieke informatie kon tot 2007 bij het Cbp worden ingewonnen, maar zoals gezegd heeft het college in dat jaar besloten in beginsel niet meer op dergelijke verzoeken in te gaan.

Uit het onderzoek komt naar voren dat de informatievoorziening in de ogen van de gebruikers van de wet te kort schiet. De voorlichtende en interpreterende functie, die het Cbp voorheen uitoefende, wordt gemist. Er lijken wel initiatieven, zoals van VNO/NCW, FME/CWM en ECP.nl, te ontstaan om dat 'gat' te vullen, maar die komen slechts langzaam op gang. Er is behoefte aan instanties die zich op gezaghebbende wijze op wetsinterpretatie, normuitlegging en –ontwikkeling toeleggen. Die randvoorwaarde moet worden vervuld, willen de normen uit de wet bij het publiek en bij verantwoordelijken gaan leven.

8. Hoe is de naleving van de informatieplicht en leidt dat er toe dat de burger regie voert over zijn gegevens?

De burger heeft diverse rechten die door de Wbp worden gewaarborgd. Om te beginnen moet hij worden geïnformeerd dat zijn persoonsgegevens worden verwerkt. Verder heeft hij het recht op inzage en kan hij verzoeken om correctie of aanvulling van de gegevens. Wanneer gebruikmaking van die rechten niet leidt tot het gewenste resultaat, kan een burger een geschil aanhangig maken. Daarvoor zijn verschillende wegen te bewandelen: het indienen van een klacht bij de Nationale ombudsman, de weg naar de civiele rechter, de bestuursrechter (al dan niet voorafgegaan door bezwaar) of een geschillencommissie. Ook kan een verzoek om bemiddeling worden voorgelegd aan het Cbp.

Over de op hen rustende informatieplicht rapporteren de geënquêteerde organisaties dat deze taak ertoe heeft geleid dat hun organisatie zorgvuldiger omgaat met persoonsgegevens en privacy. Dat leidt er toe dat de meeste organisaties (van de organisaties in het algemeen 72 procent en van de meldende organisaties drie kwart) de betrokkene informeren over de verwerking van zijn persoonsgegevens. Daarvoor worden verschillende methoden gehanteerd, waarbij de website, het aanvraagformulier en de algemene voorwaarden vaak worden genoemd (hoofdstuk 4, tabel 23).

Betrokkenen maken niet vaak gebruik van de mogelijkheden die de Wbp biedt om inzage te krijgen in de over hen verzamelde gegevens (tabel 26, hoofdstuk 4). Bijna de helft van de organisaties in het algemeen geeft aan nooit verzoeken om inzage te krijgen. Bij circa een derde van de organisaties komt dit soms voor. Correctie en aanvulling van gegevens komen iets vaker voor (bij een op de vijf regelmatig, bij de helft soms, bij een op de vijf nooit). We hebben geen opinieonderzoek gedaan onder betrokkenen en dus hebben we niet kunnen achterhalen in hoeverre er ongearticuleerde behoeften aan inzage, correctie en aanvulling bestaan en of er drempels zijn die aan het hanteren van die rechten in de weg staan. Via

populaire media wordt niet of nauwelijks bekendheid gegeven aan de mogelijkheden die burgers ter beschikking staan ter bescherming van hun eigen privacy.

Een opvallende bevinding is dat hoewel betrokkenen niet vaak gebruik lijken te maken van hun recht tot inzage, correctie of aanvulling, organisaties toch nog redelijk vaak (ruim een op de drie) een procedure hebben vastgesteld voor de wijze waarop ze op dergelijke verzoeken moeten reageren (tabel 27, hoofdstuk 4).

Uit diverse bronnen blijkt dat burgers een veel groter vertrouwen hebben in overheden, dan in bedrijven als het gaat om de wijze waarop organisaties met hun persoonsgegevens omgaan. Daarbij speelt volgens een respondent mogelijk een rol de gedachte dat wanneer de overheid gegevens verzamelt, dat voor een hoger doel, het algemeen belang is en dat het dan wel goed zit met het belang van privacybescherming. Daarentegen wordt door de experts die we hebben geraadpleegd vrij algemeen de wijze waarop overheden met persoonsgegevens omgaan juist kritischer bejegend dan de manier waarop bedrijven dat doen. Bedrijven hebben vaak een kwetsbare klantrelatie, die kan worden verbroken bij ontevredenheid over de wijze waarop persoonsgegevens worden verwerkt. Daarbij is van belang dat klanten naar de concurrent kunnen gaan. Die mogelijkheid hebben burgers bij de overheid vaak niet. Om die reden geven bedrijven in de enquête aan dat het behoud van het vertrouwen van de klant een cruciale rol speelt bij de bescherming van het privacybelang. Dat is de belangrijkste reden waarom bedrijven een melding doen bij het Cbp. Bedrijven (twee derde) geven net als semi-overheidsinstellingen (drie kwart) aan privacybescherming te zien als een belangrijk marketinginstrument richting klanten en gebruikers (tabel 3, hoofdstuk 5).

9. Hoe groot is de naleving van de meldingsplicht (bij Cbp en FG)?

In 2007 waren er ruim 32.000 meldingen in het register bij het Cbp aanwezig. Wanneer we de resultaten van de enquête onder FG's extrapoleren, dan komen we tot de conclusie dat in 2007 ruim 2.600 nieuwe meldingen bij de FG's zijn gedaan, tegenover 4.000 nieuwe meldingen bij het Cbp-register. Jaarlijks worden er in het Cbp-register 1.700 meldingen ingetrokken of geactualiseerd.

Over de naleving van de meldingsplicht kunnen op basis van het onderzoek strikt genomen geen mededelingen worden gedaan. We weten immers niet hoeveel verwerkingen voor melding in aanmerking komen. Wel kan met enige terughoudendheid worden gesteld dat de respons van de organisaties in het algemeen er op wijst dat er op dit punt geen sprake is van een groot gebrek aan kennis. Het merendeel van de organisaties kent de verplichting en zegt zich er aan te houden. Een beperkt deel van de organisaties in de steekproef geeft aan de verplichting niet te kennen. Een nog kleinere groep kent de verplichting wel, maar wenst zich daaraan niet te houden (paragraaf 4.6.1). Bij deze beschrijving moet worden aangetekend dat de steekproef gericht was op de wat grotere organisaties binnen sectoren waar relatief vaak met bestanden met persoonsgegevens wordt gewerkt. Verwacht mag worden dat het kennisniveau binnen kleinere organisaties, althans het type organisatie dat niet in de enquête was betrokken, lager zal zijn, waardoor niet uitgesloten kan worden dat de meldingsplicht daar minder goed wordt nageleefd. Tegelijkertijd zal er gemiddeld genomen bij die organisaties ook minder vaak sprake zijn van verwerkingen die gemeld moeten worden.

De meldende organisaties hebben volgens de enquête gemiddeld genomen één verwerking van persoonsgegevens die onder het Vrijstellingsbesluit Wbp valt, en daarom niet hoeft te worden gemeld, en twee verwerkingen van persoonsgegevens die bij het Cbp zijn gemeld. De helft van de meldende organisaties geeft aan de wettelijke ontwikkelingen goed in de gaten te

houden. De brancheverenigingen, het Cbp en collega-bedrijven spelen daarbij ook een rol (tabel 17, hoofdstuk 4).

Binnen de organisaties met een FG wordt gesteld dat drie kwart van de personen die met persoonsgegevens werken op de hoogte is van de meldingsplicht. De FG's schatten zelf in dat in ongeveer tachtig procent van de gevallen waarin een melding bij hen moet worden gedaan, die melding ook daadwerkelijk volgt (paragraaf 4.6.1).

10. Tot welke administratieve lasten leidt de naleving van de meldingsplicht?

We hebben de organisaties die melden bij het Cbp gevraagd naar de door hen ervaren complexiteit van de meldingsprocedure. Uit de bevindingen blijkt dat de procedure niet als erg ingewikkeld wordt gezien (paragraaf 4.6.8). Gemiddeld kost een melding ongeveer zes uur (mediaan), maar er zijn grote verschillen in het tijdsbeslag dat wordt gerapporteerd en omdat men zich de tijdsbesteding niet altijd goed meer voor de geest kon halen is dat cijfer indicatief. Anderzijds moet worden opgemerkt dat de tijdsbesteding die in ons onderzoek wordt gerapporteerd, redelijk overeen lijkt te komen met de schatting die in 2006 is opgesteld door adviesbureau EIM in opdracht van ACTAL (zie ook paragraaf 4.6.8). Enkele FG's die we hebben gesproken, geven aan dat weliswaar de melding zelf niet veel tijd hoeft te kosten, maar dat veel tijd gaat zitten in het beantwoorden van de voorvraag wanneer een verwerking moet worden gemeld. Dat komt overeen met de bevinding uit de enquête dat bijna veertig procent van de respondenten het niet altijd duidelijk vindt wanneer moet worden gemeld.

11. Heeft de meldingsplicht de omgang met persoonsgegevens beïnvloed? Is de bescherming van de privacy daardoor verbeterd?

De organisaties met een FG en ook de organisaties die bij het Cbp melden geven aan dat de meldingsplicht een positief effect heeft op de privacy van burgers. Dat is niet toe te schrijven aan acties die het Cbp onderneemt naar aanleiding van de melding. Het effect zit vooral in het feit dat organisaties als gevolg van de op hun rustende meldingsplicht beter gaan nadenken over de doelen van de verwerking en daarbij een afweging maken tussen het privacybelang en het doel van de registratie, dus het belang dat de organisatie heeft bij de verwerking van de gegevens. Het is ook niet zo dat de melding bij het Cbp er aan bijdraagt dat betrokkenen meer zicht hebben op de gegevens die over hen worden verwerkt (paragraaf 4.6.7). Slechts één op de vier organisaties die meldt, meent dat de melding verbetering brengt in de kennis die betrokkenen hebben van de over hen verzamelde gegevens. Dat gegeven wordt bevestigd door de interviews met belangenbehartigingsorganisaties die stellen dat betrokkenen de weg naar het meldingenregister niet weten te vinden. Over de toegankelijkheid van het meldingenregister wordt nog wel eens geklaagd. Al met al is het merendeel van de geraadpleegde organisaties en respondenten kritisch over de positieve effecten van het melden voor de mogelijkheden van burgers om de verwerking van hun persoonsgegevens te beïnvloeden.

12. Wat is de rol van de FG's en het Cbp bij de meldingsplicht?

De rol van het Cbp bij de meldingsplicht lijkt niet erg groot. Uit ons materiaal kan worden afgeleid dat het Cbp bijna nooit inhoudelijk reageert op een ingediende melding (paragraaf 4.6.6). Die waarneming wordt bevestigd in de gevoerde gesprekken, onder andere met het Cbp. De respondenten van de enquête onder meldende organisaties geven aan niet te zijn geconfronteerd met een voorafgaand onderzoek in de zin van artikel 31 van de wet.

De wijze waarop het Cbp reageert op meldingen contrasteert sterk met de wijze waarop wordt omgesprongen met meldingen binnen organisaties met een FG. Daar geven de enquêteresultaten aan dat meldingen meestal wél worden gecontroleerd (tabel 20, hoofdstuk 4). Daarbij past dat bijna vijftig procent van de FG's aangeeft behoefte te hebben aan controle door het Cbp van de rechtmatigheid van de gegevensverwerking (paragraaf 5.4). Het is overigens geen wettelijke taak van het Cbp om ieder melding te controleren, maar controle van meldingen is wel een middel ten behoeve van het uitoefenen van toezicht.

13. Welke rol spelen FG's en Cbp bij voorlichting over en controle op het doelbindingsprincipe? Is een afweging tussen het privacybelang en het doel van de registratie voldoende gewaarborgd?

Een meerderheid van de FG's geeft in het enquêteonderzoek aan dat de meldingsplicht als positief effect heeft dat een serieuze afweging tussen het doel van de registratie en het privacybelang is gewaarborgd (tabel 9, hoofdstuk 5). Daarbij past dat de FG's tijdens de expertmeeting tegen die achtergrond het belang van de functie van het interne toezicht benadrukken. Juist door de interne positie kan de FG proactief en stimulerend werken, maar ook toezicht houden. Het Cbp is niet tot meer in staat dan marginale toetsing van de ingediende meldingen. Sporadisch wordt in acties gecontroleerd of er wel is gemeld. Een FG kan in potentie een meer intensieve rol spelen binnen zijn organisatie. De FG kent de context en casuïstiek meer van binnen uit.

Door de respondenten wordt gemeld dat doelbinding, een afweging van privacybelang tegen het doel van de verwerking, wordt bevorderd door de meldingsplicht. De informatieplicht heeft volgens de FG's een minder sterk geprononceerde betekenis (tabel 10, hoofdstuk 5). Dat heeft ongetwijfeld ook te maken met het feit dat reacties van betrokkenen veelal achterwege blijven. Het privacyrecht wordt slechts in beperkte mate 'geactiveerd', waardoor de informatieplicht onvoldoende het privacybelang kan waarborgen. Veel van de door ons geïnterviewde respondenten menen dat de meeste betrokkenen betrekkelijk luchthartig met hun privacy omspringen, zolang dat privacybelang niet in negatieve zin wordt geraakt. Dat neemt niet weg dat de organisaties die een melding bij Cbp hebben gedaan en de organisaties die in de enquête onder organisaties in het algemeen zijn bevraagd in meerderheid van mening zijn dat betrokkenen precies weten welke gegevens over hen worden bijgehouden (tabel 10, hoofdstuk 5).

14. Welke verbeteringen zijn mogelijk rond meldingsplicht en informatieplicht?

Uit de enquêteresultaten en onze gesprekken met vertegenwoordigers van verantwoordelijken maken we op dat de meldingsplicht redelijk goed functioneert. De administratieve lasten blijven binnen de perken. Hoewel het nut van het meldingenregister wordt betwijfeld, gaat van de meldingsplicht een zekere disciplinerende werking uit. Een enkele gesprekspartner is van mening dat het computerprogramma dat moet worden gehanteerd voor het doorgeven van de meldingen zou kunnen worden vereenvoudigd. Ruim een kwart van de FG's vindt het meldingenprogramma of het –formulier van het Cbp in meer of mindere mate onduidelijk (paragraaf 5.4).

De informatieplicht heeft als doel betrokkenen te informeren over de mogelijkheid die ze hebben tot inzage, verwijdering of correctie van hun geregistreerde persoonsgegevens. Van die rechten wordt slechts beperkt gebruik gemaakt hoewel de bevraagde organisaties stellen dat betrokkenen wel worden geïnformeerd. Mogelijk zien betrokkenen geen risico's verbonden aan de registratie van hun persoonsgegevens. Tegen die achtergrond lijkt het

verstandig onderzoek te doen naar de mate waarin betrokkenen hun rechten kennen. Dat zou mogelijk tot de conclusie kunnen leiden dat de bewustwording van de privacyrisico's die betrokkenen lopen verder moet worden versterkt.

8.2.4 Toezicht en rechtsbescherming

15. Waarom gaan verantwoordelijken (niet) over tot benoeming van een FG?

Zoals gezegd, zijn er 250 organisaties die een FG hebben aangesteld, ongeveer 0,3 promille van het totaal aantal organisaties in ons land. Veel, ook grotere en internationaal opererende bedrijven, hebben er van afgezien een FG te benoemen. De achtergrond daarvan is dat ze de meerwaarde van die functionaris niet zien. Dat ze geen FG aanwijzen betekent niet dat ze het belang van privacybescherming niet zien. Integendeel. Vaak hebben deze bedrijven een privacy officer, waarvan door onze informanten wordt gesteld dat het doorgaans gaat om invloedrijke functionarissen. Veelal zijn privacy officers staffunctionarissen, verantwoordelijk voor risicomanagement en kwaliteitssystemen rond de bescherming van privacy in de organisatie. De bescherming van privacy wordt door bedrijven met een privacy officer gezien als een 'asset', een kwaliteitsvereiste, dat in de richting van klanten van groot belang wordt geacht. Wanneer een bedrijf op dat punt een steek laat vallen, kan dat snel leiden tot imagoschade en dus een verliespost opleveren.

Dat organisaties een privacy officer aanstellen in plaats van een FG wordt in sommige gevallen ook veroorzaakt doordat het bedrijf opereert op een consumentenmarkt en onderdeel is van een holding met vestigingen in andere landen. Uit het oogpunt van uniformiteit wordt dan voor het benoemen van een privacy officer gekozen met dezelfde bevoegdheden en plaats binnen de organisatie, ongeacht het land waarin de bedrijfsonderdelen gevestigd zijn. Daarbij speelt ook een rol dat de functie van FG binnen het kader van de Europese richtlijn in verschillende Europese landen op een uiteenlopende wijze is vormgegeven. Mede als gevolg daarvan is de figuur van de FG in Nederland vooral te vinden bij overheden en semi-overheden (zie tabel 4, hoofdstuk 4).

Bedrijven die wel een FG benoemen geven aan daartoe over te gaan omdat daardoor de toezichtslast vanwege het Cbp vermindert, maar vooral omdat op die manier het privacybelang wordt onderstreept. Het marketingbelang, de mogelijkheid je als organisatie te onderscheiden door de zorgvuldige behandeling van persoonsgegevens, wordt ook vaak genoemd als reden om een FG aan te stellen (zie tabel 3, hoofdstuk 5).

16. Welke invulling geven het Cbp en de FG's aan de wettelijk aan hen toegekende functies bij het toezicht en hoe vaak doen ze dat?

Sinds 1998 hebben de Registratiekamer en het Cbp, om te komen tot een uitoefening van de toezichthoudende taak met maximaal resultaat, gehandeld op basis van het zogenaamde 'viersporenbeleid'. De volgende vier sporen zijn bewandeld:

1. het bevorderen van bewustwording;
2. het bevorderen van normontwikkeling;
3. het op de voet volgen van technologische ontwikkelingen;
4. het in voorkomende gevallen handhavend optreden.

De inkomsten uit opgelegde boetes en dwangsommen bedroegen in 2005 bijna 17.000 euro (9 boetes, 2 dwangsommen), in 2006 ruim 12.000 euro (3 boetes, 0 dwangsommen) en in 2007

ruim 20.000 euro (0 boetes, 39 dwangsommen). In 2007 heeft het college besloten geen prioriteit te geven aan onderzoek naar de meldingsplicht.

Volgens het Cbp hebben voorlichting en advisering er niet toe geleid dat de Wbp voldoende wordt nageleefd. Het Cbp heeft daarom het accent binnen zijn takenpakket in 2007 verlegd naar de toezichtstaak. Het Cbp wil komen tot een 'high trust benadering' in het toezicht. Daarbij neemt het Cbp een voorbeeld aan de NMa en de OPTA. Ook bij deze toezichthouders vindt een combinatie plaats van taken op het gebied van voorlichting en taken op het gebied van toezicht en handhaving. Een groot verschil tussen het Cbp en de NMa en OPTA lijkt echter te zijn dat de NMa en OPTA toezicht houden op professionals, terwijl het overgrote deel van de verantwoordelijken in de zin van de Wbp geen professional op het gebied van bescherming van persoonsgegevens is.

De FG's gaven tijdens de expertmeeting aan dat zij een stevige positie hebben binnen de bedrijven waarbinnen ze werkzaam zijn. De combinatie van een adviserende en een toezichthoudende taak wordt daarbij door hen als een effectief instrument genoemd. Ze beschouwen zichzelf in de eerste plaats als adviseur, maar die rol kan vooral goed uit de verf komen doordat de geadviseerde weet dat de FG ook toezichthouder is. De FG heeft eigenlijk als enig wettelijk instrument het geven van een aanbeveling aan de verantwoordelijke. In de praktijk wordt dat instrument echter niet toegepast. Zij oefenen hun adviesfunctie vooral op informele wijze uit door onder meer voorlichting, overleg en het rechtstreeks aanspreken van collega's. Uit het enquêteonderzoek blijkt dat FG's vrijwel allemaal rechtstreeks toegang hebben tot het management van de organisatie. Vaak is de FG onderdeel van de juridische staf of de centrale directie. De FG's zijn niet verplicht aanwijzingen van de leiding van de organisatie op te volgen voor zover die betrekking hebben op de uitoefening van hun functie (art. 63, lid 2, Wbp). Toch meldt een kwart van de FG's ons dat dit bij hun organisatie anders is (paragraaf 4.4). Het is niet uit te sluiten dat dit komt omdat de FG-taak veelal slechts een deel van het totale takenpakket van de betreffende medewerker omvat. Tijdens de expertmeeting meldden de aanwezige FG's dat zij in hun functioneren als FG volstrekt autonoom te werk kunnen gaan. Daarbij tekenen we aan dat we tijdens de expertmeeting vermoedelijk wel een bijzondere groep FG's hebben gesproken. Deze FG's zijn allen aangesloten bij het genootschap van FG's en enkelen bekleden daarbinnen een bestuurlijke functie.

De FG-taak is meestal slechts een onderdeel van een groter takenpakket. Het staat een organisatie (met een enkele uitzondering, waarin de benoeming wettelijk verplicht is) vrij een FG te benoemen. Wanneer een FG wordt benoemd, treedt het Cbp terug als eerstelijns toezichthouder. Overigens rapporteren de FG's aan ons dat het Cbp naar hun inschatting inderdaad een meer terughoudende rol speelt bij het toezicht op de privacybescherming binnen hun organisatie (tabel 11, hoofdstuk 5). Het contact dat FG's met het Cbp hebben is niet erg intensief. Bijna de helft meldt bijna nooit contact te hebben met de contactpersoon bij het college. Dat neemt niet weg dat de FG's gematigd positief zijn over de inhoudelijke ondersteuning door het Cbp.

17. Wat zijn overwegingen voor betrokkene al dan niet te klagen en te procederen?

Uit hoofdstuk 6 blijkt dat het grote moeite kostte betrokkenen te vinden die hebben geklaagd of een geschil aanhangig hebben gemaakt. Uit diverse bronnen blijkt dat hierbij de drempel voor burgers te hoog ligt. Onbekendheid met de mogelijkheden speelt hierbij een rol, evengoed als het ontbreken van intermediairen die hier een verbindende rol kunnen spelen. De op dit vlak gespecialiseerde rechtshulpverleners zijn doorgaans werkzaam bij de grotere

kantoren, waardoor de financiële drempel voor een betrokkene aanzienlijk is. Als we het privacybelang tegenkomen in geschillen, speelt dat veelal in de context van een ander geschil, bijvoorbeeld over ontslag of een financiële kwestie. Er doet zich een soort NIMBY-effect voor: privacy in het algemeen wordt door burgers niet zo van belang geacht, maar als in enig conflict de privacy van het individu aan de orde is, is het onderwerp opeens hoogst relevant.

18. In hoeverre heeft de jurisprudentie preventieve werking en hoe zou deze kunnen worden vergroot?

Uit hoofdstuk 6 blijkt dat er nog niet veel jurisprudentie is over de wet en voor zover die er wel is, is die slecht ontsloten. Daarin komt eind 2008 verandering doordat het Cbp een jurisprudentiebundel publiceert waarin behalve de uitspraken van het college, ook rechterlijke uitspraken zijn opgenomen. Bij de Nationale ombudsman worden wel met enige regelmaat klachten aanhangig gemaakt, maar omdat de ombudsman alleen bevoegd is ten aanzien van overheden levert dat geen compleet beeld op.

8.3 Conclusie

De probleemstelling van het onderzoek, zoals die in hoofdstuk 1 is geformuleerd, luidt:

> In hoeverre voldoet de werking van de Wbp in de praktijk aan de doelstellingen van de wet, in het bijzonder gelet op de in de literatuur gesignaleerde knelpunten en welke aanpassingen zijn mogelijk en wenselijk binnen het kader van de EU-richtlijn?

Alles overziend is de conclusie van dit evaluatieonderzoek dat de doelstellingen van de Wbp, het waarborgen van evenwicht tussen het privacybelang en andere belangen en het versterken van de positie van personen van wie gegevens worden verwerkt, nog niet ten volle worden gerealiseerd. Uit het enquêteonderzoek, interviews met experts, FG's, vertegenwoordigers van burgerbelangen, casestudies en interviews met burgers die een geschil aanhangig hebben gemaakt komt het beeld naar voren van een wet die in de rechtspraktijk nog niet erg leeft, betrekkelijk lastig hanteerbaar wordt geacht en waarbij een op de toepassing gerichte privacygemeenschap en –cultuur nog niet in de volle breedte tot ontwikkeling is gekomen. We proeven een sfeer van rechtssubjecten die zich met enige terughoudendheid in de wet verdiepen. Over het algemeen stelt men dat het allemaal wel goed zit en dat er geen problemen zijn met privacy.

Tegelijkertijd is van belang dat de Wbp nog niet erg lang bestaat, hoewel ze in de Wpr een verwante rechtsvoorganger had. Kenmerkend voor de Wbp is dat het gaat om een wettelijke regeling met open normen die nadere invulling behoeven. Dat kost tijd. En – zo luidt een rode draad van de onderzoeksbevindingen – de rechtsontwikkeling in de zin van sectorale normen en jurisprudentie, die vraagt om contextspecifieke kennis (branche, sector, technologie), is nog niet over de hele linie uitgekristalliseerd.

Open normen

Dat de wet bestaat uit open normen die in de rechtspraktijk nadere invulling behoeven is op zichzelf geen knelpunt. Het wordt pas een knelpunt als blijkt dat nadere normering door middel van gedragscodes en regelingen per branche of sector niet tot ontwikkeling komt. Ruim de helft van de organisaties en branches beschikt over een privacycode, maar daar staat dus tegenover dat veel organisaties nog geen nadere regelingen kennen.

Rechten betrokkenen
Waar een doelstelling van de wet is het toekennen van een inzage- en correctierecht aan betrokkenen, is het van belang op te merken dat uit het onderzoek naar voren komt dat betrokkenen slechts in zeer beperkte mate van die rechten gebruik maken. De meeste in de enquête betrokken organisaties stellen dat ze betrokkenen via allerlei kanalen informeren over de verwerking van hun persoonsgegevens. Niettemin kan de conclusie dat betrokkenen maar weinig van hun inzage- en correctierechten gebruik maken erop wijzen dat zij onvoldoende bekend zijn met de rechten van inzage, correctie en verwijdering. Nader onderzoek zou dat aan het licht kunnen brengen.

De functie van FG
Organisaties kunnen – meestal op vrijwillige basis – een FG benoemen. De activiteiten van een dergelijke functionaris lijken in de praktijk bij te dragen aan een bewuste omgang met persoonsgegevens binnen die organisaties. Toch is er bij slechts 0,3 promille van de organisaties in ons land een FG aangesteld. Aanstelling van een dergelijke functionaris zou voor veel organisaties ook een te zwaar middel zijn om privacybescherming te waarborgen. Daarom is het wenselijk dat meer dan tot op heden praktijk is organisaties gezamenlijk, branchegewijs, overgaan tot de aanstelling van een FG, zoals artikel 62 van de wet mogelijk maakt. Het belang van de functie zou ook verder kunnen toenemen door daaraan meer dan op dit moment eisen te stellen op het vlak van kwaliteit, opleiding en vaardigheden.

De meldingen en het meldingenregister
De bedoeling van de verplichting om in beginsel alle verwerkingen van persoonsgegevens te melden is om de bewustwording van de omgang met die gegevens te versterken en de naleving van het doelbindingsprincipe te bevorderen. De praktijk bij de onderzochte organisaties die een melding hebben gedaan laat inderdaad een zekere terughoudendheid zien bij het gebruik van persoonsgegevens voor andere doelen dan waarvoor zij oorspronkelijk zijn verzameld. Tegelijkertijd lijkt er in veel organisaties ook sprake van onbekendheid met de normen van de wet. De melding lijkt inderdaad een preventief effect te hebben op het ongebreidelde gebruik van persoonsgegevens binnen de desbetreffende organisaties, maar minder dan 25 procent van de organisaties doet een melding. Opnemen van een melding in het meldingenregister bij het Cbp lijkt op zichzelf niet erg zinvol. Uit de door ons afgenomen interviews maken wij op dat het register slechts in (zeer) beperkte mate door betrokkenen wordt geraadpleegd. Daar staat tegenover dat het Cbp aangeeft dat het meldingenregister jaarlijks ruim 20.000 maal wordt geraadpleegd. Het Cbp weet niet door wie dat gebeurt. Onze respondenten geven verder nog aan dat de transparantie van het meldingenregister te wensen over laat.

De taken van het Cbp, advies en toezicht
Over de taakuitoefening door het Cbp bestaat wisselende tevredenheid. Aan de ene kant worden de richtsnoeren, adviezen en bemiddelingen door het Cbp op prijs gesteld. Aan de andere kant wordt nog meer van het Cbp verwacht op het vlak van 'compliance assistance': informatievoorziening en advisering. Er is veel behoefte aan uitleg en interpretatie van de wet, juist waar een op privacybescherming gerichte gemeenschap van vakgenoten of belangenbehartigingsorganisaties nog niet bestaat. Investeringen in de kennisfunctie rond de privacybescherming lijken dringend noodzakelijk. Tegelijkertijd bestaat er breed begrip voor de noodzaak voor het Cbp keuzes te maken. En er moet ook worden vastgesteld dat het Cbp niet belast is met een wettelijk voorgeschreven adviestaak (behoudens advisering over wetgeving). Hoewel het Cbp keuzes moet maken, gelet op de beperkt beschikbare mensen en middelen, zeggen sommige van onze gesprekspartners dat de keuze voor toezicht, tegen de

achtergrond van de achterblijvende rechtsontwikkeling te vroeg is gemaakt. Voortgaande investeringen in ontwikkeling en kennisbevordering zouden op (middel)lange termijn mogelijk beter renderen en op den duur een accent op toezicht kunnen rechtvaardigen. Maar er is ook een ander gedachtegang mogelijk waarin die keuze voor toezicht en handhaving juist leidt tot het ontstaan van initiatieven elders rond voorlichting, bewustwording en normontwikkeling.

Administratieve lasten
De bevindingen over de administratieve lasten die de wet met zich meebrengt op het punt van de meldingsplicht, passen bij de schattingen die in eerder door EIM uitgevoerd onderzoek zijn opgesteld. Administratieve lasten zijn er volgens onze gesprekspartners met name rond vragen over dataverkeer met derde landen. De vergunningplicht die daarbij geldt stuit op bezwaren, maar de EU-richtlijn geeft hiervoor een verplichtend kader.

Kennis van de wet
Veel bedrijven zeggen de wet te kennen, maar het is de vraag of ze zichzelf daarbij niet overschatten. Privacy is voor burgers wel een onderwerp, maar de gevoelige plek zit 'diep'. Burgers maken onderscheid tussen privacy in het algemeen, die in dat denkkader aan andere belangen, zoals veiligheid, ondergeschikt kan zijn, en de eigen privacy. Wanneer het persoonlijk wordt is er sneller sprake van een issue van grote zorg.

Wat we al langer weten, en wat in veel evaluatiestudies naar de werking van wetgeving wordt bevestigd, blijkt ook uit dit verslag waarin de werking van de Wbp in de praktijk is beschreven: het kost tijd voordat wettelijke normen ingang vinden in de praktijk. Dat geldt zeker voor de Wet bescherming persoonsgegevens. Juist omdat de wet veel open normen bevat moet de rechtsontwikkeling in de vorm van nadere normstelling en jurisprudentie tijd worden gegund. Hoewel in ruim de helft van de organisaties een privacyregeling van kracht is, zijn er (dus) ook veel organisaties die nog steeds een nadere regeling ontberen. De kennis over de wet moet groter worden en de bewustwording bij verantwoordelijken en betrokkenen moet nog groeien. Mede door technologische ontwikkelingen zal het belang van privacybescherming toenemen. Het intensiveren van de toezichtsinspanningen kan daarbij een rol spelen, maar ook zouden betrokkenen kunnen worden geactiveerd inspanningen te leveren ten behoeve van het privacybelang. Normontwikkeling, voorlichting en advisering op maat behoeven nadrukkelijk aandacht.

Summary

The Act
The Personal Data Protection Act (hereafter: Wbp) came into force on September 1, 2001. The Wbp is the successor of the Personal Data Files Act. The Wbp implements the European Directive on Privacy (hereafter: the Privacy Directive).[244]

The Wbp regulates the most important rules for the registration and use of personal data. The aim of the act is to arrange for safeguards, so that a balance between privacy protection and other interests is realized. Furthermore, the act strengthens the position of individual persons by assigning rights when their data are being processed. In correspondence with these rights, controllers (the organisations determining the purpose and means of the data processing) are confronted with obligations. Strengthening the position of the individuals concerned is also arranged for by notification and the assignment of an inspector (hereafter: Cbp).

Research framework
Article 80 of the Wbp is the basis of this evaluation. This article implies that both the Ministers of Justice and of Home Affairs within five years after the coming into force of the Wbp send a report on the effectiveness and efficiency of the functioning of the act to the Houses of Parliament. In this report possible bottlenecks in the functioning of the act must be addressed, as well as the degree into which the act serves the privacy of individual persons. The evaluation started with a research of possible bottlenecks about which a report was issued in 2007. Different from that study this research, that focuses on the question whether or not the supposed bottlenecks do occur in practice, is an empirical research.

Research question
The central question is:

> *To which degree meets the functioning of the Wbp in practice the standards of the act, in particular related to the bottlenecks formulated in literature, and which adjustments are possible and desirable within the framework of the Directive on Privacy?*

When elaborating this central question 18 different specific questions were formulated and answered, distributed over three categories: regulation, information and inspection and legal protection.

Research plan
Different research methods were used. Next to the study of relevant literature, three questionnaires were send out. The first survey was executed under a sample of public authorities and organisations enlisted in the commercial register. The second questionnaire was mailed at organisations selected by means of a sample drawn from the notification register at the Cbp. The third questionnaire was send to all officials for data protection (hereafter: FG's). The questionnaires are based on the description frame of the research, presented in chapter 3. This description frame was established on the basis of some pilot interviews and literature study. The results of the surveys were interpreted with the help of several experts, gathered in a few expert meetings. Also, a few in-depth interviews were

[244] Directive 95/46/EG, PbEG L 281, p. 0031-0050.

undertaken with privacy officers, legal experts and the president of the Cbp. To understand more of the consequences of the act on data exchange in case of cooperation between several organisations, two case studies were carried out. Finally we spoke to several civilians and legal aid officers who brought a conflict over a case concerning the processing of personal data to a court or to the Cbp.

Results
When interpreting the results of this study it is important to stress that the response of one of the surveys (the FG's survey) was sufficient, while at the same time the response of another survey (send to a sample of organisations enlisted in the notification register) was moderate and the response of the third survey (send to a sample of organisations enlisted in the commercial register) was insufficient. This induces some caution while presenting and generalising the results. On the other hand, through the combination of the results of the surveys and the comparison with the information gathered with qualitative research methods, a fairly consistent picture appears.

The general conclusion of the evaluation research is that the standards of the Wbp, safeguarding the balance between privacy interests and other fundamental rights and strengthening the position of persons whose data are processed, are not fully realised. The research findings indicate that the Wbp is not yet a very significant act in legal practise. The act seems to be relatively hard to handle. Until now a clear-cut community of privacy experts did not yet develop. Neither did a pronunciated privacy culture originate.

Because of the open standards of the Wbp, development of standards in lower regulation is desirable in sectors and organisations. The research shows that on the one hand more than half of the organisations do have a privacy code. At the same time a lot of organisations do not have such codes and regulations. Next to that the surveys and the results of the interviews and expert meetings, do point out that the knowledge different target-groups have of the act must increase. Not all the controllers and individuals concerned are aware of the importance of privacy interest. This is illustrated by the very limited use the individuals concerned make of their rights to inspect, correct, complement and remove the information concerning them. The limited awareness of the importance of privacy can also appear from the very minimal number of conflicts brought to courts and the Cbp concerning privacy issues. Privacy is an important topic for individuals, but the sensitive spot is not easily touched. Individuals do make a distinction between privacy in general, which can be subordinate to other interests, such as safety, and their own privacy. When the processing concerns more personal data, privacy is considered a much more delicate matter by the individuals involved.

Organisations have the authority to appoint a FG. This official seems to contribute to a greater awareness in the processing of personal data within the organisation. But only 0,3 promille of all organisations in The Netherlands did appoint a FG. For many organisations the appointment of such an official would not be a proportionate mean to safeguard privacy protection. Therefore, appointing FG's in sectors, together with other organisations (according art. 62 of the Wbp), should be stimulated. The status of the position can also increase through the assessment of requirements concerning quality, education and skills. The requirement to notify the processing of personal data is meant to strengthen the awareness of the privacy interest, to improve the check of the proportionality of the processing of personal data and to inform the individual concerned about the identity of the controller. The research findings do show a certain reservation in using personal data. The notification procedure indeed seems to have a preventive effect, but the registration of a notification at the Cbp does not seem to

contribute to that. Interviews with individuals concerned and their legal aid officers seem to point out that the register is not very known. The interviews also indicate that the register is not very transparent.

A central result of the research is that the further development of standards, enlightenment, and specific advice need attention. Intensifying the inspection as the Cbp announced in 2007 can be helpful, but needs to be supported by compliance assistance. Individuals concerned can be activated to promote their privacy interests. The need for the further development of standards and specific interpretation of the Wbp can be understood against the background of the relatively short existence of the Wbp. The Wbp is an act with open standards, which needs to be interpreted. That takes up a great deal of time. And – as a continuous thread which runs through this findings – development of sectoral standards and jurisprudence asks for specific knowledge (sector, technology) which is not yet available on the whole.

Literatuurlijst

ACT-II 2004
Ambtelijke commissie toezicht II, *Rapport van bevindingen betreffende de zelfevaluatie door het College Bescherming Persoonsgegevens (Cbp) van het toezicht op de verwerking van persoonsgegevens*, 16 december 2004

Alberdingk Thijm 2001
Chr. A. Alberdingk Thijm, *Privacy vs. Auteursrecht in een digitale omgeving*, ITeR 49, eJure: 2001

Alberdingk Thijm 2004
Chr. A. Alberdingk Thijm, *Het nieuwe informatierecht*, Den Haag 2004

Arentsen
M.J. Arentsen, *Beleidsorganisatie en beleidsuitvoering*, Enschede 1991

Boog e.a 2006
J.J. Boog, P.A. van der Hauw, M.M.M. Linssen, M.J. Overweel, Administratieve lasten in het privacydomein, reductievoorstellen nader bekeken, Zoetermeer: EIM 2006

Consumentenbond 2005
Consumentenbond, *Wie kijkt er mee?*, Consumentengids augustus/september 2005, p. 74-79

Cuijpers 2006
C. Cuijpers, *Verschillen tussen de Wbp en Richtlijn 95/46/EG en de invloed op de administratieve lasten- en regeldruk*, Tilburg: TILT/Universiteit van Tilburg, 2006

Dorbeck-Jung e.a. 2005
B.R. Dorbeck-Jung, M.J. Oude Vrielink-van Heffen en G.H. Reussing, *Open normen en regeldruk. Een onderzoek naar de kosten en oorzaken van irritaties bij open normen in de kwaliteitszorg*, Enschede: Universiteit Twente/IGS, 2005

Dubbeld 2007
L. Dubbeld, *Functionarissen voor de gegevensbescherming: onzichtbare privacybeschermers*, Privacy & Informatie 2007, aflevering 2, p. 69-70

Van Erp 2007
J.G. van Erp, *Informatie en communicatie in het handhavingsbeleid. Inzichten uit wetenschappelijk onderzoek*, Den Haag: Boom uitgevers, 2007

Field 2000
A. Field, Discovering Statistics Using SPSS for Windows: Advanced Techniques for Beginners, London: Sage Publications, 2000

Van Geest e.a.
J. van Geest en A. Ringeling (red.), *Evalueren met beleid: de Evaluatiecommissie Wet milieubeheer in bedrijf,* Den Haag, Sdu Uitgevers, 1998

GGD Nederland e.a. 2005
GGD Nederland, GGZ Nederland en KNMG, *Handreiking gegevensuitwisseling in het kader van bemoeizorg*, april 2005

Van den Heuvel e.a.
E. van den Heuvel, K. Nagel, C. van 't Hof en B. Schermer, *RFID-bewustzijn van consumenten: Hoe denken Nederlanders over Radio Frequency Identification?,* Een publieksonderzoek van het Rathenau Instituut, de Consumentenbond en ECP.nl, 2007

Holvast 2005
J. Holvast, *Interview met Jacob Kohnstamm*, P&I 2005, 3, p. 114-119

Holvast 2005a
J. Holvast, *De aanmeldingsplicht, een overbodige bepaling?,* P&I 2005, 5, p. 208-211

Holvast 2006
J. Holvast, G. Michels en J.P. van Schoonhoven, *De staat van de privacybescherming van de burger 2005-2006,* P&I 2006, 311, p. 262-269

Hooghiemstra en Nouwt 2004
T. Hooghiemstra en S. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers, 2007

Koorn e.a. 2004
R. Koorn, H. van Gils, J. ter Hart, P. Overbeek en R. Tellegen, *Privacy Enhancing Technologies. Witboek voor beslissers*, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, december 2004

Mol Lous 2008
L. Mol Mous, *De Wet politiegegevens: herziening van de Wet politieregisters*, Ars Aequi, april 2008, p. 303-307

Muller e.a. 2007
E.R. Muller, H.R.B.M. Kummeling en R.P. Bron, *Veiligheid en privacy. Een zoektocht naar een nieuwe balans*, Den Haag: Boom Juridische uitgevers, 2007

Nationale ombudsman
Jaarverslag 2007

Overkleeft-Verburg 1995
G. Overkleeft-Verburg, *De Wet persoonsregistraties: norm, toepassing en evaluatie (diss. Tilburg),* Zwolle: Tjeenk Willink 1995.

Prins e.a. 1995
J.E.J. Prins e.a., *In het licht van de Wet persoonsregistraties: zon, maan of ster?*, ITeR nr. 1, Deventer: Kluwer 1995. De belangrijkste conclusies werden als afzonderlijk rapport opgenomen in de tweede ITeR-bundel (Deventer: Kluwer 1996).

Prins en Berkvens 2002
J.E.J. Prins en J.M.A. Berkvens, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer, 2002

Rodrigues 2006
P.R. Rodrigues en A.H. Vedder, *De staat van de privacybescherming van de burger 2005-2006*, P&I 2006 , 312, p. 270-277

Sauerwein 2003
L.B. Sauerwijn, *Handreiking voor gemeenten over privacyaspecten bij criminaliteitspreventie,* uitgave Ministerie van Justitie, herziene versie december 2003

Snippe 2006
J. Snippe, R. van der Stoep, M. van Zwieten en B. Bieleman, *Lokale aanpak zeer actieve veelplegers: nazorgtraject,* Groningen-Rotterdam: Intraval, 2006

Terstegge 2000
J.H.J. Terstegge, *De nieuwe Wet bescherming persoonsgegevens: handleiding voor de praktijk,* Alphen aan den Rijn: Samsom 2000

TNS NIPO 2005
TNS NIPO, *Burgers en hun privacy. Opinie onder burgers,* februari 2005 (onderzoek in opdracht van het Cbp)

TNS NIPO 2006
TNS NIPO, *De naleving en beleving van de informatieplicht onder organisaties in Nederland. Onderzoek onder huisartsen, onderwijsinstellingen en woningbouwcorporaties,* februari 2006 (onderzoek in opdracht van het Cbp)

Vedder e.a. 2007
A. Vedder, L. van der Wees, B.J. Koops en P. de Hert, *Van privacyparadijs tot controlestaat. Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag: Rathenau Instituut/TILT, 2007, studie 49

De Vries en Rutgers 2001
H.H. de Vries en D.J. Rutgers, *Wet bescherming persoonsgegevens, toepassing in arbeidsverhoudingen,* Deventer: Kluwer, 2001

Westerman 2006
P.C. Westerman, *De onmogelijkheid van deregulering*, Nederlands Juristenblad 2006/3, p. 132-137

Zwenne e.a. 2007
G.J. Zwenne, A.W. Duthler, M. Groothuis, H. Kielman, W. Koelewijn en L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens.* Literatuuronderzoek en knelpuntenanalyse, Leiden/Den Haag: WODC 2007

College bescherming persoonsgegevens

Cbp 2002
Brief van het College bescherming d.d. 14 januari 2002, kenmerk z2001-1575, over het omgaan met persoonsgegevens binnen het Bureau Jeugdzorg

Cbp 2003
Nieuwsbericht: oproep tot naleving meldingsplicht
http://www.cbpweb.nl/documenten/med_20030121_handhaving.stm?refer=true&
refurl=http%3A// www.cbpweb .nl/indexen/ind_melden_publ.stm&theme=purple

Cbp 2004
Informatieblad College bescherming persoonsgegevens, *De functionaris voor de gegevensbescherming*, nummer 16, 2004

Cbp 2004a
'Boetes voor gemeenten en bedrijven na controle meldingsplicht 2003', 26 juli 2004, te vinden op: http://www.cbpweb.nl/documenten/med_20040726_mo2003.stm, geraadpleegd op 24 augustus 2008

Cbp 2005
Informatieblad College bescherming persoonsgegevens, *Geheimhouding van medische gegevens*, nummer 33A, juni 2005

Cbp 2006
Informatieblad College bescherming persoonsgegevens, *De GBA en het gebruik daarvan*, nummer 21A, februari 2006

Cbp
Jaarverslagen College bescherming persoonsgegevens 2001 tot en met 2007

Cbp 2007a
Informatieblad College bescherming persoonsgegevens, *Informatie delen in samenwerkingsverbanden*, nummer 31A, oktober 2007

Cbp 2007b
College bescherming persoonsgegevens, *Tien gouden regels voor verwerking van persoonsgegevens door de sociale dienst*, januari 2007

Cbp 2007c
Verslag van een Rondetafelconferentie over uitwisseling van gegevens in hulpverlening en zorg op 23 april 2007, georganiseerd door de Inspectie jeugdzorg en het College bescherming persoonsgegevens

Cbp 2007d
Cbp Richtsnoeren, *Publicatie van persoonsgegevens op Internet*, december 2007

Cbp 2008
Jaarverslag Cbp 2008

Cbp 2008a
Advies van het College bescherming persoonsgegevens inzake het conceptwetsvoorstel Wet herziening kinderbeschermingsmaatregelen d.d. 21 februari 2008, kenmerk z2007-01417

Ministerie van Justitie

MvJ 2007
Persbericht: Minister wil meer Veiligheidshuizen
http://www.ministerievanjustitie.nl/organisatie/minister_hirsch_ballin/fotoalbum/hirsch-ballin-wil-meer-veiligheidshuizen.aspx

MvJ 2008
Persbericht installatie Commissie Veiligheid en Privacy,
http://www.justitie.nl/actueel/persberichten/archief-2008/80117commissie-veiligheid-en-persoonlijke-levenssfeer-geinstalleerd.aspx

MvJ 2008a
Nieuwsbericht bezoek Veiligheidshuis Bergen op Zoom
http://www.ministerievanjustitie.nl/organisatie/staatssecretaris_albayrak/Fotoalbum/Fotos-Staatssecretaris-Albayrak-bezoekt-Veiligheidshuis-Bergen-op-Zoom.aspx

Bits of Freedom

Bits of Freedom 2006
Nieuwsbericht over staken activiteiten per 1 september 2006.
http://www.bof.nl/opheffing.html

Kamerstukken

Kamerstukken II 1997-1998, 25 892, nr. 3 (Memorie van Toelichting Wet bescherming persoonsgegevens)

Kamerstukken II 1999–2000, 26 883, nr. 3 (Memorie van Toelichting Wet Bevordering integriteitbeoordelingen door het openbaar bestuur)

Kamerstukken II 2001-2002, 28 168, nr. 3 (Memorie van Toelichting Wet op de jeugdzorg)

Kamerstukken II 2005-2006, 30 327, nr. 3 (Memorie van Toelichting Wet politiegegevens)

Kamerstukken II 2007-2008, 31 051, nr. 2 (Verslag van een algemeen overleg)

Kamerstukken II 2007-2008, 31 200 XIII, nr. 51 (Bevindingen van de Minister van Economische Zaken bij het NMa-jaarverslag 2007)

Coalitieakkoord 2007 (akkoord tussen de Tweede Kamerfracties van CDA, PvdA en ChristenUnie, 7 februari 2007)

Richtlijnen

Richtlijn 95/46/EG, PbEG L 281, p. 0031-0050 (Privacyrichtlijn)

Artikel 29 Werkgroep

Artikel 29 Werkgroep 2006
Artikel 29 Werkgroep, *Werkprogramma 2006-2007, WP 120*, goedgekeurd op 5 april 2006

Artikel 29 Werkgroep 2007
Artikel 29 Werkgroep, *Advies 4/2007 over het begrip persoonsgegeven*, WP 136, goedgekeurd op 20 juni 2007

Artikel 29 Werkgroep 2008
Artikel 29 Werkgroep, *Werkprogramma 2008-2009, WP 146*, goedgekeurd op 18 februari 2008

Europese Commissie

Europese Commissie 2003
Europese Commissie, *Eerste verslag over de toepassing van de Richtlijn gegevensbescherming* (95/46/EG) /* COM/2003/0265 def.

Europese Commissie 2007
Europese Commissie, *Mededeling van de commissie aan het Europees Parlement en de Raad over de follow-up van het Werkprogramma voor een betere toepassing van de Richtlijn gegevensbescherming*, COM (2007) 87 definitief

OPTA

Website OPTA
www.opta.nl

OPTA 2008
Richtsnoer Opta, Visie op toezicht en handhaving, 12 maart 2008

Nederlandse Vereniging Voor Burgerzaken

NVVB
Nederlandse Vereniging Voor Burgerzaken, *Verstrekking uit en geheimhouding van persoonsgegevens in de Gemeentelijke basisadministratie persoonsgegevens*

Bijlage 1 Samenstelling begeleidingscommissie

prof. mr. L.F.M Verhey (voorzitter), Universiteit Maastricht

mr. dr. P. Blok, rechtbank Den Haag

mw mr. A.C.J.M. Emmaneel, College bescherming persoonsgegevens

mw dr. H.L. Janssen, ministerie van BZK – directie Constitutionele Zaken en Wetgeving

mr. dr. J.P. de Jong, ministerie van Justitie – directie Wetgeving

mw mr. W.M. de Jongste, ministerie van Justitie – WODC

mr. dr. A.J. Nieuwenhuis, Universiteit van Amsterdam

drs. J. Swank, ministerie van Justitie – directie Rechtshandhaving en Criminaliteitsbestrijding

Bijlage 2 Geïnterviewde personen

Geïnterviewde personen

- De heer A.A.M. Jean Pierre, IB-Groep
- De heer J. Holvast, adviesbureau Holvast & Partner
- De heer mr. dr. J.P. de Jong, Ministerie van Justitie
- Mevrouw dr. H.L. Janssen, ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- De heer mr. J. Kohnstamm, voorzitter College bescherming persoonsgegevens
- De heer dr. J.A.G. Versmissen, College bescherming persoonsgegevens
- Mevrouw mr. A.C.J.M. Emmaneel, College bescherming persoonsgegevens
- De heer mr. drs. J.H.J. Terstegge, Philips International B.V. en voorzitter van de werkgroep privacy van VNO-NCW
- De heer L. Linssen, secretaris informatiebeleid VNO-NCW
- De heer M. Bolhuis, Google
- de heer K. Bruin, privacy officer KLM
- mevrouw mr. T.E. van Dijk, College bescherming persoonsgegevens
- mevrouw dr. J. van Erp, Erasmus Universiteit Rotterdam
- de heer mr. drs. T. Hooghiemstra, HEC voor ICT en bestuur in de publieke sector
- de heer R. Kolthek, UPC
- de heer mr. dr. S. Nouwt, Universiteit van Tilburg

Deelnemers expertmeetings

Expertmeeting FG's
- De heer H.L.D. Fernald
- De heer drs. P.P.R. d'Hondt, gemeente Almelo
- De heer C.P. Kaastra, gemeente Arnhem
- De heer Korremans, Randwijk Holding
- De heer prof. dr. Peters
- Mevrouw Scheuing, privacy officer Action
- Mevrouw mr. J.M. Titulaer-Meddens
- Mevrouw mr. W.K.M. Uytdehaage, Groene Hartziekenhuis
- De heer mr. J. de Zeeuw, Ministerie van LNV

Expertmeeting organisaties die belangen van burgers behartigen:
- mevrouw Dekker, Nationale ombudsman
- de heer dr. M. Heldoorn, Nederlandse Patiënten Consumenten Federatie
- mevrouw drs. P. Lam, ANWB
- mevrouw Lavell, Ouders Online
- mevrouw mr. M. Markenstein, KNMG
- mevrouw Versluis, Nederlandse Patiënten Consumenten Federatie
- de heer drs. M. van der Vlis, Rover
- de heer M. Wessling, Consumentenbond

Expertmeeting advocaten:
- de heer mr. C. Alberdingk Thijm, SOLV advocaten
- mevrouw mr. L. Moerel, De Brauw Blackstone Westbroek
- mevrouw mr. H. de Vries, Kennedy Van der Laan

Casestudyonderzoek Veiligheidshuis

Hieronder is aangegeven met welke functionarissen is gesproken.

Openbaar Ministerie
- projectleider
- procesmanager gegevensuitwisseling
- beleidsmedewerker belast met het opstellen van een privacyconvenant
- coördinerend officier van justitie

Politie
- beleidsmedewerker belast met het opstellen van een privacyconvenant
- beleidsmedewerker slachtofferzaken en regionaal coördinator huiselijk geweld

Gemeente
- senior beleidsadviseur openbare orde en veiligheid

Dienst Justitiële Inrichtingen
- medewerker maatschappelijke dienstverlening

Raad voor de Kinderbescherming
- casusregisseur, afdeling strafzaken

GGZ
- psychiater

Bureau Jeugdzorg
- teammanager

Sociaal team
- voorzitter

Casestudyonderzoek GGZ

Hieronder is aangegeven met welke functionarissen is gesproken.

GGZ
- juridisch beleidsmedewerker
- projectleider
- psychiater
- clusterhoofd bedrijfsvoering

GGD
- hoofd afdeling persoonsgerichte aanpak
- teamleider/sociaal psychiatrisch verpleegkundige

Bijlage 3 Casusoverleggen veiligheidshuis

Naam	Meerderjarige veelplegers
Doelgroep	Delinquenten die over een periode van vijf jaar (waarvan het laatste jaar het peiljaar vormt) meer dan tien processen-verbaal tegen zich zagen opmaken, waarvan ten minste één in het peiljaar.
Doelstelling	• Een gezamenlijke inspanning leveren aan het verminderen van criminaliteit en overlast voor burgers in het arrondissement Leeuwarden en het terugdringen van recidive door een geïntegreerde aanpak van meerderjarige veelplegers. • Een integrale en intensieve samenwerking door middel van een gezamenlijke ketensturing en een persoonsgebonden aanpak van veelplegers, die leidt tot: - Vermindering van recidive; - een effectieve, sluitende en efficiënte aanpak binnen de politie- en justitieketen, gericht op preventie en repressie; - realisatie van een sluitende en effectieve samenwerking tussen de politie- en justitieketen en de gemeenten/sociale teams, die een bijdrage kunnen leveren aan een succesvolle reïntegratie; - het beschikbaar stellen van voldoende menskracht, deskundigheid en informatie aan de kerngroep veelplegers en het casusoverleg veelplegers.
Deelnemers	• Openbaar Ministerie • Politie • Dienst Justitiële Inrichtingen • Reclasseringsinstellingen • Gemeente • GGZ • Sociale teams ook deelnemer?
Regeling privacy	• Sinds september 2007 is een convenant gegevensuitwisseling van kracht. Dit convenant is opgesteld conform het model van het Ministerie van Justitie. • Tussen het OM en de GGZ is een afspraak gemaakt over gegevensuitwisseling en het medisch beroepsgeheim. Afgesproken is dat de GGZ adviseert op basis van het medisch dossier zonder op de inhoud in te gaan.

Naam	**Jeugd:** • **Casusoverleg risicojongeren** • **Justitieel Casus Overleg** • **Casusoverleg nazorg**
Doelgroep	• Jeugdigen van 0 tot 18 jaar die een strafbaar feit hebben gepleegd of die risico lopen met justitie in aanraking te komen omdat zij bijvoorbeeld overlast geven of spijbelen. • Jeugdigen ouder dan 18 jaar behoren ook tot de doelgroep als zij in het kader van de toepassing van het jeugdstrafrecht een jeugddetentie of PJI-maatregel opgelegd hebben gekregen in verband met strafbare feiten begaan voor het bereiken van de leeftijd van 18 jaar. Voor deze groep jongeren moet nazorg geregeld worden.
Doelstelling	*Casusoverleg risicojongeren* Het doel van dit overleg is te voorkomen dat jongeren die in de fout gaan in herhaling vallen of in de criminaliteit terecht komen. *Justitieel Casus Overleg (JCO)* Het JCO heeft tot doel een kwalitatieve verbetering van de afdoeningsbeslissing te realiseren doordat de voornaamste ketenpartners hun informatie over de jongere bijeenbrengen op grond waarvan de officier een afdoeningsbeslissing kan nemen. *Casusoverleg nazorg* Het doel van dit overleg is door middel van samenwerkingsafspraken een sluitende aanpak te realiseren voor nazorg voor jeugdigen die na of tijdens een vrijheidsbenemende straf of maatregel terugkomen in de maatschappij.
Deelnemers	*Casusoverleg risicojongeren* • Politie • Bureau Jeugdzorg • Gemeente • Voorliggende voorzieningen • Regionaal Meld- en Coördinatiepunt • Halt • Verslavingszorg • GGZ • algemeen maatschappelijk werk *Justitieel Casus Overleg* • Openbaar Ministerie • Politie • Raad voor de Kinderbescherming *Casusoverleg nazorg* • Raad voor de Kinderbescherming • Bureau Jeugdzorg/Jeugdreclassering • Dienst Justitiële Inrichtingen • Gemeente • Regionaal Meld- en Coördinatiepunt
Regeling privacy	Voor de gegevensuitwisseling in het JCO is een convenant opgesteld volgens het model van het Ministerie van Justitie.

Naam	Criminele en overlastgevende Antillianen
Doelgroep	60 criminele en 150 overlastgevende Antillianen
Doelstelling	• Terugdringen criminaliteit door persoonsgerichte aanpak; • Aanpak criminaliteit en vermindering schietincidenten; • Aanpak nazorg na detentie; • Preventieve aanpak: minimaal 15 Antillianen gaan per jaar in een traject • Nader door politie in te vullen concrete doelstellingen voor de projectperiode 1 oktober – 1 april 2008 (specifieke actie op criminele Antillianen)
Deelnemers	• Politie • Openbaar Ministerie • Reclassering • Regionaal Meld- en Coördinatiepunt 12-23 • Sociaal team • Buro Saris • GGZ • Gemeente
Regeling privacy	Voor de gegevensuitwisseling in het casusoverleg is een convenant opgesteld volgens het model van het Ministerie van Justitie. Ook is een voorafgaand onderzoek aangevraagd bij het Cbp. Tegen de positieve beslissing van het Cbp is beroep aangetekend door belangenorganisaties. Dit beroep is gegrond verklaard. De afloop van het hoger beroep is nog onbekend.

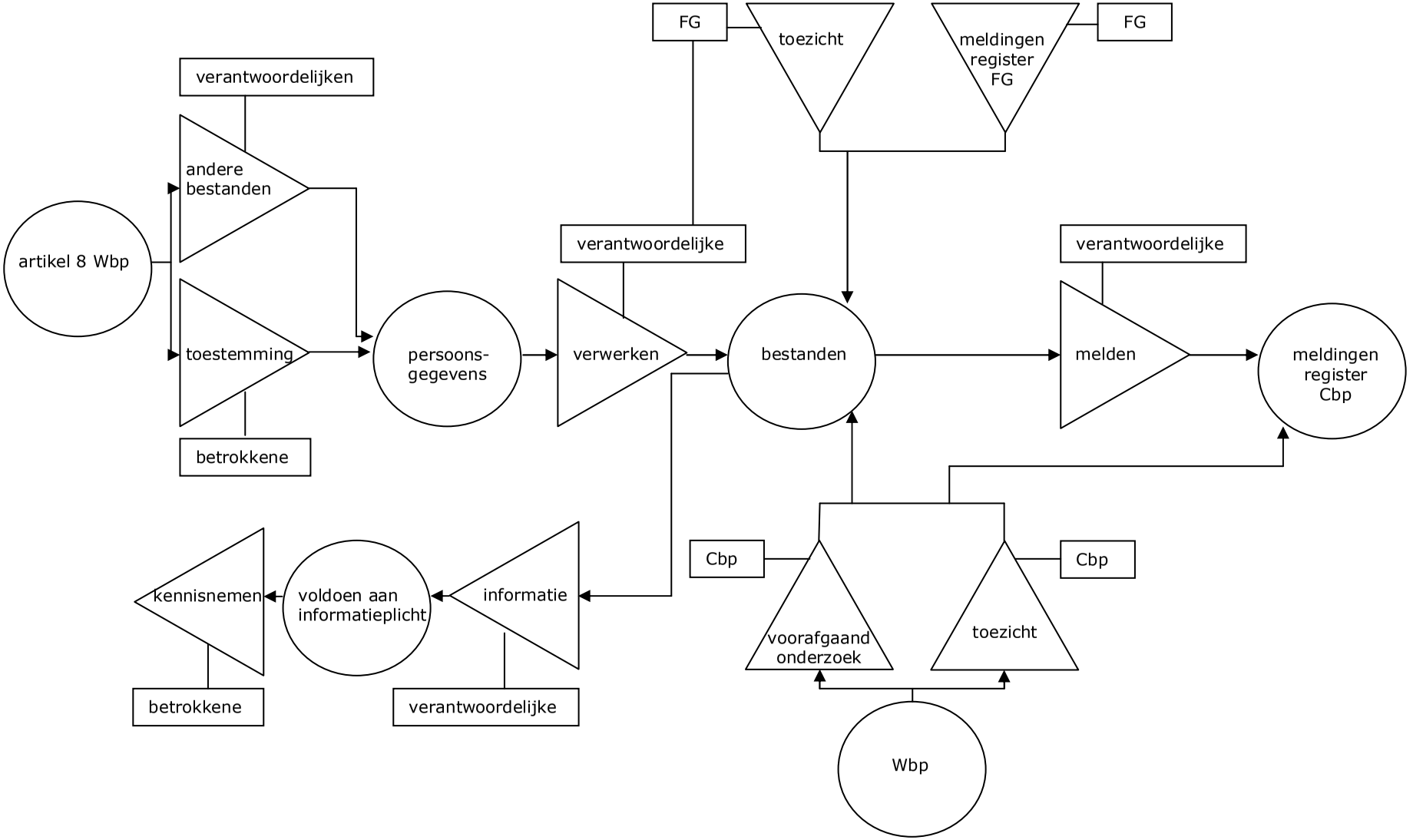
Naam	Huiselijk geweld
Doelgroep	Plegers van huiselijk gewel
Doelstelling	• stoppen van huiselijk geweld; • het voorkomen van recidive door middel van gerichte interventies; • het herstellen van de rechtsnorm; • de coördinatie van begeleiding in het strafrechtelijk traject bij huiselijk geweld; • nauwe samenwerking met de coördinatie 1ste Hulp bij Huiselijk Geweld; • het zo goed mogelijk adviseren van de rechtbank in strafrechtelijke trajecten; • terugbrengen en voorkomen van overlast; • verlenen van passende zorg aan slachtoffer; • ouders motiveren hulp voor hun kinderen te organiseren; • zijn van een betrouwbaar informatieknooppunt voor partners in veiligheid; • verlenen van nazorg; • versterken van de ketenregie.

Deelnemers	• Politie • Openbaar Ministerie • Advies- en Steunpunt Huiselijk Geweld • Reclassering • Bureau Jeugdzorg
Regeling privacy	In het verleden is een regeling Huiselijk Geweld en Privacy opgesteld over de verstrekking van politiegegevens. Het doel is te gaan werken conform het modelconvenant gegevensuitwisseling van het Ministerie van Justitie

Naam	**Ex-gedetineerden**
Doelgroep	Gedetineerden die op vrije voeten komen (ongeveer 1000 per jaar in de provincie)
Doelstelling	Het opstellen van een plan van aanpak op maat m.b.t.: • Pas (ID-kaart) • Poen (uitkering of voorschot) • Bed (huisvesting) • Brood (werk, dagbesteding etc.) Als deze aanpak werkt, zal de recidive met 20% afnemen.
Deelnemers	• Gemeente • Dienst Justitiële Inrichtingen • Reclasseringsinstellingen
Regeling privacy	-

Naam	**Overlastgevende personen**
Doelgroep	Personen die door psychische stoornissen, verslaving, of een combinatie van deze factoren overlast veroorzaken en waarbij – tijdelijk – de mogelijkheden van een betrokken organisatie of een sociaal team te boven worden gegaan. Ook verslaafde overlastplegers behoren tot deze doelgroep.
Doelstelling	• Voorzien in adequate maatregelen voor de betrokken persoon en omgeving; • Doorbreken van impasses in de persoonsgebonden plannen van aanpak; • Realiseren van een koppeling tussen de hulpverlenings- en justitiële keten; • Voorkomen van escalaties van overlastsituaties (plegen van strafbare feiten door betreffende overlastpleger of omgeving).
Deelnemers	• Openbaar Ministerie • Politie • GGZ • Gemeente • Reclassering • Verslavingszorg • Wellicht in de toekomst: maatschappelijke opvang
Regeling privacy	-

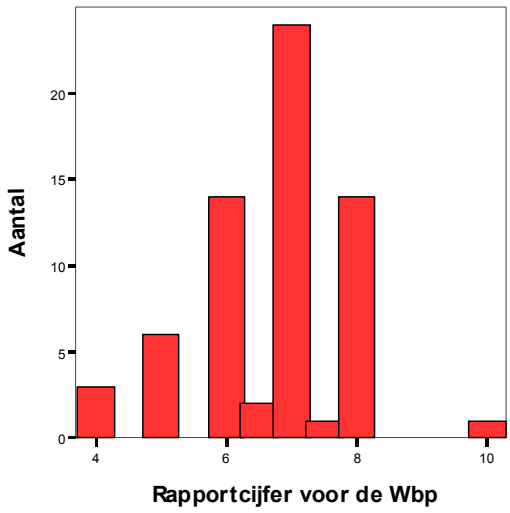
Bijlage 4 Schema Wbp



Bijlage 5 Regressieanalyse

Afhankelijke variabele: tevredenheid met de Wbp
Aan de FG's is gevraagd om als algemeen kwaliteitsoordeel een rapportcijfer te geven voor de Wbp, het Cbp en de eigen organisatie. De Wbp scoort een 6,7, het Cbp scoort een 6,6 en ten slotte de eigen organisatie van de FG krijgt het hoogste cijfer; een 6,8. In het regressiemodel dat zal worden opgesteld is het rapportcijfer voor de Wbp de afhankelijke variabele. De tevredenheid met het functioneren van de eigen organisatie is de vierde onafhankelijke variabele. Om deze reden worden beide rapportcijfers nader uitgewerkt.

We hebben om een totaalbeeld te creëren aan de FG's gevraagd een rapportcijfer te geven voor de Wbp, het Cbp en de eigen organisatie. Het lijkt er op dat de FG's gematigd tevreden zijn over de uitvoering van het privacybeleid, want in alle drie gevallen wordt gemiddeld uitgekomen op een kleine voldoende. De Wbp scoort een 6,7, het Cbp scoort een 6,6 en ten slotte de eigen organisatie van de FG krijgt het hoogste cijfer; een 6,8.



Figuur 9 Verdeling rapportcijfer (van 0 tot 10) voor de Wbp

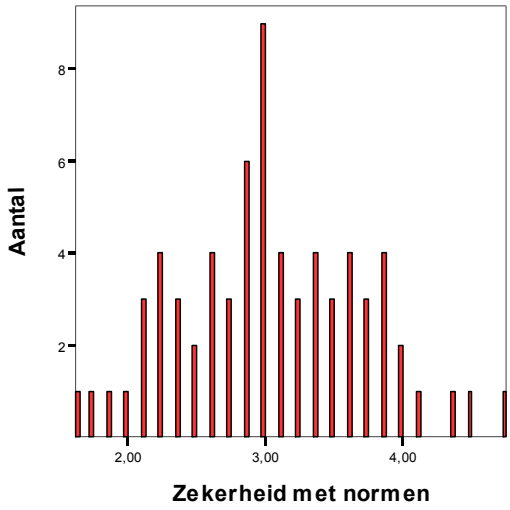
De belangrijkste score is in het licht van de evaluatie van de Wbp het rapportcijfer voor de Wbp. Dit cijfer geeft de over-all tevredenheid over deze wet aan. Figuur 9 laat de verdeling van het rapportcijfer voor de Wbp zien. Een vraag die kan worden gesteld is door welke factoren verschillen in de totale tevredenheid over de Wbp tussen de afzonderlijke organisaties worden bepaald. De verdeling van het rapportcijfer voor de Wbp laat een redelijk symmetrische verdeling rondom het gemiddelde van 6,7 zien. Een dergelijke verdeling kan zonder problemen als afhankelijke variabele in een regressieanalyse dienen.

Onafhankelijke variabelen

Duidelijkheid over open normen
De omgang met de open normen door FG's is een variabele die in het model zal worden getoetst. Voor het construeren van een indicator voor duidelijkheid over de open normen, zijn de volgende items opgenomen:

1. Hoe wij de meldplicht in de Wbp moeten interpreteren is altijd volstrekt duidelijk
2. Het is ons altijd volledig duidelijk welke persoonsgegevens we mogen verwerken
3. Het is ons altijd goed helder welke gegevens wij aan derden mogen verstrekken
4. Het ministerie van Justitie vult de open normen goed in
5. Het Cbp vult de open normen goed in
6. De open normen worden goed verduidelijkt door de jurisprudentie
7. De regels van de Wbp sluiten goed aan op de in onze organisatie en branche geldende privacynormen
8. Er zijn voldoende handleidingen en best practices te vinden om de Wbp goed te kunnen toepassen

Deze items zijn bijzonder consequent door de FG's ingevuld. Dit resulteert in een Cronbach's alfa van 0,864. Verwijdering van één van deze items levert geen substantiële verhoging van de alfa op. De scores van deze items worden bij elkaar opgeteld en om ze vergelijkbaar te maken met de scores van de andere indicatoren gedeeld door 8. Zo ontstaat een indicator die varieert tussen 1 (zeer veel onzekerheid over de open normen) tot 5 (zeer weinig onzekerheid over de open normen). De verdeling van deze indicator is weergegeven in Figuur 10.



Figuur 10 Verdeling van de zekerheid van FG's over de open normen

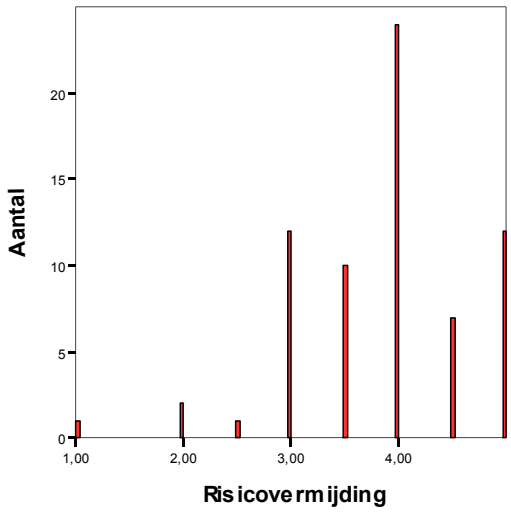
We zien in Figuur 10 dat de indicator voor onzekerheid zich verdeelt tussen 1 en 5. De verdeling ziet er redelijk normaal uit, met een duidelijke piek in het midden. Er zijn ongeveer even veel organisaties met veel (score lager dan 3) als met weinig onzekerheid (score hoger dan 3). Deze verdeling biedt een goede basis voor opname in een regressieanalyse.

Risicovermijding

Voor het construeren van een variabele voor risicovermijding zijn de volgende items opgenomen.

1. Als andere organisaties ons vragen persoonsgegevens te verstrekken en het is ons niet helemaal duidelijk of we die op grond van de Wbp mogen verstrekken, verstrekken we ze niet
2. Als we persoonsgegevens willen verwerken en het is ons niet helemaal duidelijk of dat van de Wbp mag, verwerken we ze niet

Deze stellingen zijn redelijk consistent ingevuld door de FG's. Cronbach's alfa is 0,626. Dit is voldoende consistentie voor het samennemen van de beide items in een Lickertschaal. Hiertoe zijn de scores van beide stellingen bij elkaar opgeteld en gedeeld door 2. Zo ontstond een indicator die varieert tussen 1 (bereid om risico's te accepteren) en 5 (risicomijdend). De verdeling is weergegeven in Figuur 11.



Figuur 11 Verdeling van de risicomijding van organisaties met een FG

We zien dat veruit de meeste FG's risicomijdend zijn. Bij twijfel worden geen gegevens verwerkt of verstrekt. Een klein aantal FG's is echter bereid om ook bij twijfel over de juridische mogelijkheden gegevens te verwerken. Deze verdeling biedt een voldoende normale spreiding om op te kunnen nemen in de regressieanalyse.

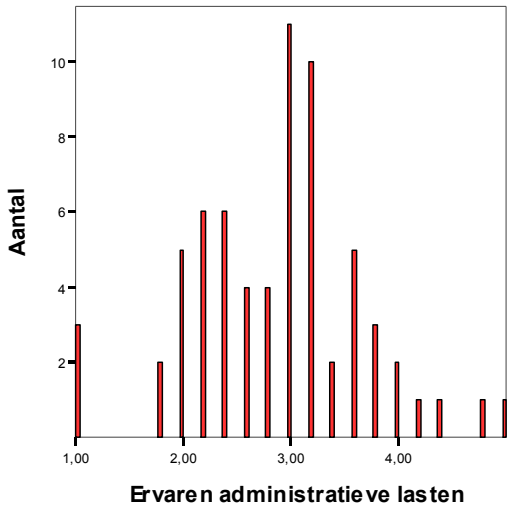
Hoogte administratieve lasten

Voor het construeren van een indicator voor de administratieve lasten zijn de volgende items opgenomen:

1. De administratieve lasten van de plicht om betrokkenen te informeren en hun toestemming te vragen zijn veel te hoog
2. De administratieve lasten van de meldplicht zijn veel te hoog
3. het actueel houden van de meldingen is een grote administratieve last
4. De administratieve lasten van het inzagerecht zijn veel te hoog
5. De administratieve lasten van de Wbp zijn hoog door de open normen

De bovengenoemde items beslaan verschillende aspecten van administratieve lasten. Deze items over administratieve lasten zijn zeer consistent door de FG's ingevuld. Dat betekent dat een hoge score op één van deze items sterk samenhangt met een hoge score op de andere items. Cronbach's alfa is 0,891 en verwijdering van één van deze items leidt niet tot een substantiële verhoging van deze alfa. De scores op deze items kunnen daarom bij elkaar worden opgeteld. Vervolgens zijn is de totaalscore gedeeld door vijf om de indicator voor administratieve lasten vergelijkbaar te maken met de hierna volgende indicatoren voor

onzekerheid en risicomijding. Er ontstaat zo een nieuwe indicator die varieert tussen 1 en 5, waarbij 1 staat voor zeer weinig ervaren administratieve lasten en 5 voor administratieve lasten die zeer hoog worden ervaren. Figuur 12 geeft de verdeling van de indicator voor administratieve lasten weer.

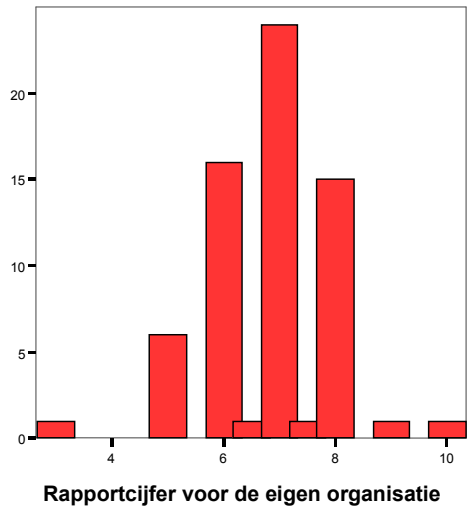


Figuur 12 De verdeling van de ervaren administratieve lasten

We zien dat de indicator voor de ervaren administratieve lasten een spreiding heeft tussen de 1 en 5. Verder zien we dat de meeste organisaties een gemiddelde administratieve last ervaren. Ten slotte hebben ongeveer even veel organisaties te maken met lage als met hoge administratieve lasten. De waarnemingen zijn redelijk normaal verdeeld en de indicator vormt daarmee een goede basis voor een regressieanalyse.

Tevredenheid met het functioneren van de eigen organisatie

Naast de geconstrueerde indicatoren voor administratieve lasten, onzekerheid over de open normen en risicovermijding wordt nog een vierde variabele in de regressieanalyse meegenomen. Verwacht kan worden dat een hoge tevredenheid over het functioneren van de eigen organisatie op het gebied van privacybescherming leidt tot een grotere tevredenheid over de Wbp. Het ‘rapportcijfer’ dat betrekking heeft op het eigen functioneren van de organisatie op het gebied van de Wbp loopt daarom mee in de regressieanalyse. Dit rapportcijfer loopt van 0 tot 10, waarbij 0 betekent dat de organisatie de Wbp zeer slecht uitvoert en 10 staat voor een zeer goede uitvoering. Figuur 13 toont de verdeling van de tevredenheid over de uitvoering van de Wbp door de eigen organisatie.

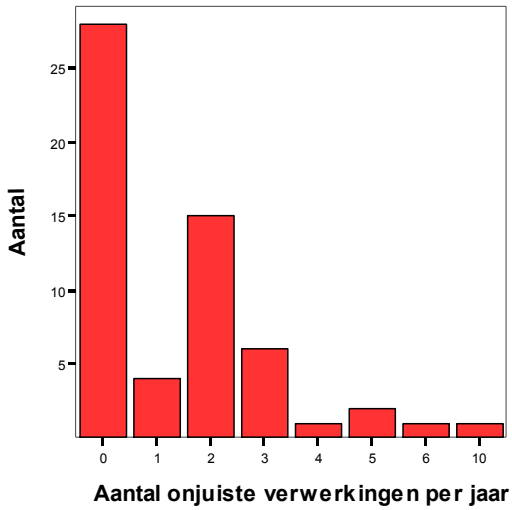


Figuur 13 Verdeling van het rapportcijfer voor de eigen organisatie

We zien de meeste FG's hun eigen organisatie een 7 geven. De grafiek laat een redelijk normale verdeling zien. De verdeling is redelijk symmetrisch rond het gemiddelde en de meeste waarnemingen zitten in de buurt van het gemiddelde. Deze variabele kan daarom zonder problemen worden opgenomen in de regressieanalyse.

Aantal geconstateerde onjuiste verwerkingen

Het aantal geconstateerde onjuiste verwerkingen door de FG is een variabele die niet uit het stellingendeel van de enquête komt, maar is te beschouwen als een feitelijke waarneming (zie paragraaf 4.4). Deze variabele is als vijfde onafhankelijke variabele opgenomen in het model dat de tevredenheid van de FG over de Wbp verklaart, omdat het te verwachten is dat het aantal geconstateerde onjuiste gegevensverwerkingen van invloed kan zijn op de tevredenheid met de Wbp. Wanneer een FG regelmatig onjuiste gegevensverwerkingen constateert, zal dit het belang van de Wbp kunnen onderstrepen. In de enquête die onder FG's is uitgezet is gevraagd naar het aantal geconstateerde onjuiste gegevensverwerkingen per jaar. Over het algemeen worden weinig overtredingen van de Wbp geconstateerd, maar er zijn FG's die hier vaker mee worden geconfronteerd. Figuur 14 geeft de verdeling van het aantal geconstateerde onjuiste verwerkingen weer.



Figuur 14 Verdeling aantal geconstateerde onjuiste verwerkingen per jaar

De meeste FG's constateren geen onjuiste gegevensverwekingen. Maximaal worden 10 onjuiste gegevensverwerkingen geconstateerd door de FG. De verdeling is niet normaal verdeeld, maar laat voldoende spreiding zien om in de regressieanalyse te worden meegenomen.

Regressieanalyse

Er is een regressieanalyse uitgevoerd op het bestand van de *organisaties met een FG*. Het rapportcijfer voor de Wbp is de afhankelijke variabele. Er zijn vijf onafhankelijke variabelen, te weten het rapportcijfer voor de eigen organisatie, de hoogte van de administratieve lasten, de mate van zekerheid over de invulling van de open normen en de mate van risicovermijding van de organisatie. In eerste instantie wordt een regressieanalyse uitgevoerd met alle onderscheiden variabelen. Op basis van deze waarneming zijn indicatoren samengesteld voor:

1. De administratieve lasten;
2. De onzekerheid over de open normen;
3. De voorzichtigheid waarmee men optreedt bij onzekerheid

Daarnaast lijken ook het aantal geconstateerde overtredingen en de tevredenheid over het functioneren van de eigen organisatie verklarende variabelen te kunnen zijn. Omdat de vragenlijst voor de FG's veruit de meeste relevante vragen bevat die de tevredenheid met de Wbp kunnen verklaren, wordt een analyse gemaakt op basis van dit bestand. De vragenlijsten voor de *organisaties in het algemeen* en de *meldende organisaties* hebben elk te veel beperkingen voor een dergelijke over-all analyse. Bovendien is de kennis van deze respondenten met betrekking tot de Wbp vermoedelijk geringer dan van de FG's, waardoor zij zich waarschijnlijk geen goed geïnformeerd oordeel over deze wet kunnen vormen.

Dit leidt tot een model dat 64 procent van de variantie verklaart, maar twee variabelen hebben geen statistisch significante bijdrage aan het model, te weten de voorzichtigheidsscore en het rapportcijfer voor de eigen organisatie. Deze variabelen worden vervolgens uit het model verwijderd. Wanneer een regressieanalyse wordt uitgevoerd met het 'rapportcijfer' voor de

Wbp als afhankelijke variabele, blijken drie onafhankelijke variabelen een substantiële en statistisch significante bijdrage te leveren in het model.

Het model doorstaat de tests voor multicollineariteit en seriële correlatie. Bij een tolerantiewaarde van minder dan 0,1 en een VIF waarde groter dan 10 wordt de collineariteit als probleem beschouwd (Field 2000). De collineariteitsstatistiek laat zien dat multicollineariteit in dit model geen problemen oplevert (zie Tabel 50). Bij een Durbin-Watsonscore (D-W-score) kleiner dan 1,67 kan er sprake zijn van seriële correlatie (kritieke score bij 3 onafhankelijke variabelen, N = 50 en alfa = 0,05). Bij een D-W-score kleiner dan 1,42 is er zeker sprake van seriële correlatie. In dit model bedraagt de D-W-score 1,8. Dit toont aan dat er geen sprake is van seriële correlatie.

De belangrijkste bron van ontevredenheid over de Wbp blijkt de duidelijkheid over de toepassing van de open normen in de wet te zijn. Daarnaast zijn het de hoogte van de ervaren administratieve lasten en het aantal geconstateerde onjuiste verwerkingen. De mate van risicovermijding door de organisatie en de tevredenheid over de eigen organsatie blijken geen effect op de tevredenheid met de Wbp te hebben. Risicomijdende organisaties zijn dus even tevreden als de organisaties die wel risico's nemen. Dat zelfde geldt voor organisaties die vinden dat ze Wbp-conform handelen in vergelijking met organisaties die dat niet vinden. Met deze drie indicatoren kan 61 procent van de variantie in de tevredenheid over de Wbp worden verklaard. In Tabel 50 is het model samengevat.

Tabel 50 Regressieparameters en collineariteitstatistiek voor algemene tevredenheid over de Wbp

	B	**Bèta**	**Sign.**	**Collineariteitstatistiek**	
				Tolerance	*VIF*
Constante	4,726	-	0,000	-	-
Duidelijkheid over open normen	1,067	0,636	0,000	0,901	1,110
Hoogte administratieve lasten	-0,537	-0,364	0,000	0,896	1,116
Aantal geconstateerde onjuiste verwerkingen	0,174	0,278	0,004	0,912	1,097

De uitkomsten van bovenstaande analyse zijn goed te interpreteren. Kort samengevat leiden de volgende zaken tot een ***hoge waardering*** voor de Wbp:

1. Er is duidelijkheid over de manier waarop de open normen in de Wbp moeten worden toegepast. Deze factor is grofweg twee maal zo sterk als de andere twee factoren. Duidelijkheid over de manier waarop de open normen moeten worden ingevuld leidt tot zekerheid over een juiste uitvoering van de Wbp. Wanneer deze duidelijkheid er onvoldoende is en men de gegevens toch gaat verwerken, heeft men te maken met niet goed in te schatten juridische risico's voor de organisatie, zoals het risico op constatering van normschending door het Cbp en juridische acties van betrokkenen. Maar ook het door de onduidelijkheid niet verwerken van de gegevens leidt voor de organisatie tot een ongewenste uitkomst, namelijk tot een onderbenutting van gegevens die men niet durft te verwerken of uit te wisselen. Duidelijkheid over hoe de wet moet worden uitgevoerd blijkt zowel bij organisaties die risico's accepteren als bij organisaties die risico's mijden een positieve uitwerking te hebben. Dit zou een verklaring kunnen zijn waarom de indicator voor risicovermijding geen verschil laat zien tussen deze twee groepen.
2. De administratieve lasten van de Wbp worden als laag ervaren. Lage administratieve lasten leiden tot een hoge waardering voor de wet omdat het de organisatie weinig tijd, geld of moeite kost om de wet uit te voeren.

3. De FG constateert jaarlijks veel onjuiste verwerkingen van persoonsgegevens. Wanneer de FG jaarlijks veel overtredingen constateert, betekent dit dat de FG er keer op keer aan wordt herinnerd dat de Wbp een nuttige functie vervult. Dat draagt bij aan de tevredenheid over de Wbp.