ACHTERGRONDSTUDIES EN VERKENNINGEN 25

INHOUD

dr. J.A.G. Versmissen
mr. drs. A.C.M. de Heij

Elektronische overheid en privacy

Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid

COLLEGE BESCHERMING PERSOONSGEGEVENS

dr. J.A.G. Versmissen
mr. drs. A.C.M. de Heij

Elektronische overheid en privacy

Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid

Publicaties in de serie Achtergrondstudies en verkenningen zijn het resultaat van onderzoeken uitgevoerd door of in opdracht van het College bescherming persoonsgegevens (CBP). Met het uitbrengen van deze publicaties beoogt het CBP de discussie en de meningsvorming te stimuleren over ontwikkelingen in de samenleving waarbij de persoonlijke levenssfeer van de burger in het geding is. In veel gevallen wordt in de publicaties het normatieve kader zoveel mogelijk praktisch uitgewerkt voor het onderwerp van de studie. Het CBP wil hiermee een handreiking geven voor het realiseren van de eigen verantwoordelijkheid die de wet een ieder geeft voor de bescherming van persoonsgegevens.

COLOFON

Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid, College bescherming persoonsgegevens,
Den Haag, juli 2002

COLLEGE BESCHERMING
PERSOONSGEGEVENS

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag
TELEFOON 070 381 13 00
FAX 070 381 13 01
E-MAIL info@cbpweb.nl
INTERNET www.cbpweb.nl

ISBN 90 74087 31 0

Ontwerp: Proforma, strategie, ontwerp en management (M. Monster)
Druk: Sdu Grafisch Bedrijf bv

Voorwoord

De overheid brengt steeds meer structuur aan in haar informatiehuishouding. Langzaam maar zeker creëert zij zo een elektronische identiteits- en informatie-infrastructuur.

Deze ontwikkeling brengt belangrijke kansen en bedreigingen met zich mee voor de bescherming van persoonsgegevens. Met het voorliggende rapport geeft het CBP invulling aan zijn rol als toezichthouder op dat terrein: in een vroeg stadium meedenken en adviseren is daarvan een belangrijk onderdeel.

De doelstelling van het rapport is tweeledig: richting geven aan de ontwikkeling van een informatie-infrastructuur voor de overheid, en aannemelijk maken dat de privacyregels doorgaans meer dan voldoende speelruimte laten om de ambities op het terrein van elektronische overheid te realiseren.

Privacyregels hoeven aan weinig legitieme overheidsdoelstellingen in de weg te staan. Daarvoor is het wel van belang om er vanaf het begin rekening mee te houden. Dat geldt zowel voor het opstellen van beleid als voor het ontwerpen van organisatiestructuren, informatiesystemen en procedures. Een privacy-vriendelijke infrastructuur schept mede de voorwaarden om dat mogelijk te maken.

Het rapport bespreekt de informatie-infrastructuur van de overheid aan de hand van de thema's identiteitsmanagement en regie over de eigen persoonsgegevens. Vanuit deze visie op elektronische overheid en privacy reikt het vier ontwerpprincipes aan voor die infrastructuur: niet-kenbaarheid, differentiatie, optimale transparantie en doelbinding.

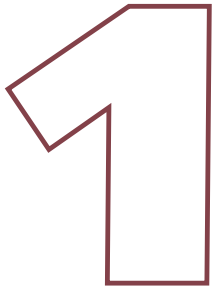
Waarmee moeten overheidsorganisaties in de praktijk rekening houden als gevolg van de Wet bescherming persoonsgegevens? Als leidraad voor het beantwoorden van deze vraag in concrete gevallen geeft het rapport een WBP-analyse van twee actuele thema's op het gebied van elektronische overheid: pro-actieve dienstverlening en de verdeling van overheidsdienstverlening over een front-office en een backoffice.

Het CBP rekent erop met dit rapport een bijdrage te leveren aan de totstandkoming van een informatie-infrastructuur voor de overheid die terecht het vertrouwen van de burger geniet.

mr. P.J. Hustinx
voorzitter

Inhoud

Inleiding



Net als andere partijen is de overheid al decennialang bezig met automatisering. Tot eind jaren tachtig was daarbij voornamelijk sprake van zogenaamde 'eiland-automatisering'. Hierbij wordt lokaal naar de beste oplossing van een automatiseringsvraagstuk gezocht zonder veel rekening te houden met de omgeving. Het laatste decennium hebben beleidsmakers bij de rijksoverheid – in het bijzonder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) – steeds meer aandacht gekregen voor het grotere geheel. Dat blijkt uit de opeenvolgende BIOS-nota's, het actieprogramma Elektronische Overheid en de nota Contract met de Toekomst. Gezien de buitengewoon ingewikkelde problematiek is het niet verwonderlijk dat de uitvoering van het beleid flink achter loopt op de formulering ervan. Een periode van begripsvorming en het creëren van draagvlak door beleidsmakers ging in de uitvoering aanvankelijk vooral vergezeld van pilotprojecten en een 'laat duizend bloemen bloeien'-aanpak. Momenteel worden echter de eerste gerichte stappen gezet naar het tot stand komen van een informatie-infrastructuur.

De bescherming van persoonsgegevens vindt haar oorsprong in het grondrecht van de burger op eerbiediging en bescherming van zijn persoonlijke levenssfeer. Ook andere grondrechten kunnen hier echter bij gebaat zijn, zoals het recht op gelijke behandeling, vrijheid van meningsuiting en 'fair play' van de overheid in het algemeen. Vanuit deze oorsprong heeft zich sinds 1970 een stelsel ontwikkeld van principes voor de behoorlijke omgang met persoonsgegevens. De wet- en regelgeving waarin deze principes zijn verankerd, heeft in de laatste decennia een ontwikkeling doorgemaakt die tot op zekere hoogte parallel loopt aan die op het gebied van automatisering.

De Wet persoonsregistraties (WPR) van 1988 sloot aan bij de toen heersende kijk op automatisering door het begrip 'persoonsregistratie' als uitgangspunt te nemen. Met de sterke opkomst van computernetwerken werd steeds onduidelijker waar de grenzen van een persoonsregistratie lagen. Daarmee nam het belang van verwerkingen van persoonsgegevens die niet direct samenhingen met opname in een bestand, sterk toe. Ook de EU heeft dit probleem onderkend. Zij vaardigde in 1995 een richtlijn uit die het begrip 'verwerken van persoonsgegevens' als uitgangspunt heeft en daarmee beter toepasbaar is in de huidige netwerkomgevingen. Deze richtlijn is in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens (WBP)[1]. Doordat de uitgangspunten van beide wetten overeenkomen, zijn er overigens geen fundamentele materiële verschillen tussen de WBP en de WPR. De WBP is op 1 september 2001 van kracht geworden.

Deze ontwikkelingen bieden een mooi moment voor een verkenning van privacyaspecten van de elektronische overheid.

1.1 Elektronische overheid

Als startpunt van het overkoepelende beleid bij de rijksoverheid op het gebied van informatie- en communicatietechnologie kan gekozen worden de eerste Beleidsnota Informatievoorziening Openbare Sector (BIOS 1[2]). Deze concentreerde zich op de organisatie van de informatievoorziening in de relaties tussen de departementen en tussen de bestuurslagen. In BIOS 2, *De computer gestuurd*[3], kwam daarbij de inzet van informatiebeleid en informatietechnologie om de relatie tussen burgers en overheid te verbeteren. BIOS 3, *Terug naar de toekomst*[4], borduurt voort op deze twee kernthema's: communicatie en interactie tussen burger en overheid enerzijds[5], en de informatiehuishouding van de overheid anderzijds. De beleidsmakers van BZK introduceren daarbij de notie van een informatie-infrastructuur.

[1] Wet van 6 juli 2000, Stb. 302, houdende regels inzake de bescherming van persoonsgegevens.
[2] Kamerstukken II, 1987–1988, 20644, nr. 2.
[3] Kamerstukken II, 1990–1991, 20644, nr. 15.
[4] Kamerstukken II, 1994-1995, 20644, nr. 23.
[5] Zij het nu opgesplitst in twee aparte thema's, te weten een goede elektronische toegankelijkheid van de overheid en een betere publieke dienstverlening.

Doelmatige en doeltreffende inzet van informatie en informatie- en communicatietechnologie bij de uitvoering van opdrachten van het politiek bestuur vereist dat de overheid beschikt over een goede infrastructuur, dat wil zeggen over generieke, relatief permanente basisvoorzieningen en -afspraken voor en over gegevensverwerking, gegevensopslag en gegevenstransport. De literatuur duidt zo'n stelsel van voorzieningen en afspraken aan als een 'informatie-infrastructuur'.

Uit: Ministerie van BZK. BIOS 3: Terug naar de toekomst. (blz. 49)

De ontwikkeling van de informatie-infrastructuur voor de overheid staat in feite nog in de kinderschoenen. Dat deze ontwikkeling niet te stuiten is, lijkt duidelijk. Het is echter onmogelijk om al in detail te voorspellen waarheen zij zal leiden.[6] In dit rapport concentreren we ons daarom op een aantal belangwekkende ontwikkelingen in de richting van een dergelijke infrastructuur, zonder daarbij een heel precies beeld voor ogen te hebben hoe die infrastructuur al deze elementen met elkaar in samenhang zal verenigen. Dit is ook in lijn met de opvolgers van de BIOS-nota's, het *Actieprogramma Elektronische Overheid*[7] en de nota *Contract met de toekomst*[8].

De afgelopen tijd hebben verschillende commissies zich gebogen over thema's die veel raakvlakken hebben met de elektronische overheid, zoals de commissies Snellen (modernisering GBA)[9], Wallage (toekomst overheidscommunicatie)[10] en Docters van Leeuwen (ICT en overheid)[11]. Te verwachten valt dan ook dat de beleidsontwikkeling op het terrein van de elektronische overheid voorlopig nog niet tot rust zal komen.

Is de richting waarin de informatie-infrastructuur van de overheid zich gaat ontwikkelen nog onduidelijk, de problemen die deze het hoofd moet bieden zijn beter gearticuleerd (zie onder). Bijlage 1 bevat een overzicht van de belangrijkste beleidsinitiatieven op het gebied van de elektronische overheid die een infrastructureel karakter hebben.

In toenemende mate blijkt dat de gegevenshuishouding van de overheid tekortschiet en welke problemen dit geeft. Het manifesteert zich:

- bij de handhaving, doordat gegevens niet voor alle betrokken partijen beschikbaar zijn, onvolledig zijn, niet actueel zijn of onderling strijdig zijn.
- bij fraudebestrijding, doordat objecten (personen, bedrijven, gebouwen e.d.) niet uniek identificeerbaar zijn, doordat gegevens over deze objecten onjuist blijken, of doordat gewenste gegevenskoppelingen falen door gebrek aan standaardisatie.
- bij het verminderen van de administratieve lastendruk voor burgers en bedrijven, i.e. bij het door het kabinet gevoerde beleid om burgers en bedrijven niet steeds opnieuw dezelfde gegevens aan de overheid te laten verstrekken.
- bij de modernisering van de publieke dienstverlening, waar invoering van de (g)één-loketgedachte via het programma Overheidsloket 2000 en pro-actieve dienstverlening slechts gedeeltelijk kunnen worden gerealiseerd zolang de daarvoor benodigde gegevens in de backoffice van de overheid her en der verspreid blijven liggen.
- bij het zo efficiënt mogelijk inrichten van de interne bedrijfsvoering van de overheid, doordat dezelfde gegevens door meerdere organisaties worden verzameld en

[6] Wel lijkt al duidelijk dat een *identiteits-infrastructuur* voor de overheid er een fundamenteel onderdeel van zal vormen. Zie hiervoor hoofdstuk 2.
[7] Kamerstukken II, 1998–1999, 26387, nr. 1.
[8] Kamerstukken II, 1999–2000, 26387, nr. 8.
[9] Adviescommissie Modernisering GBA (2001). *GBA in de toekomst: Gemeentelijke basisadministratie persoonsgegevens als spil voor toekomstige identiteits-infrastructuur*. Den Haag.
[10] Commissie Toekomst overheidscommunicatie (2001). *In dienst van de democratie*. Den Haag.
[11] Commissie ICT en overheid. *Burger en overheid in de informatiesamenleving*: De noodzaak van institutionele innovatie. Den Haag.

beheerd, waardoor onnodig hoge kosten worden gemaakt en schaarse ICT-deskundigheid onvoldoende efficiënt wordt ingezet.
– bij beleidsvorming, -monitoring en -verantwoording (VBTB[12]), waar betrouwbare en breed geaccepteerde sturingsgegevens en kengetallen nog (te) vaak ontbreken.

Uit: Voortgangsrapportage aan de Tweede Kamer over het programma Stroomlijning basisgegevens. Kamerstukken II, 2001–2002, 26387, nr. 11.

1.2 Rol en positie van privacybescherming

De wet- en regelgeving ter bescherming van persoonsgegevens vindt haar oorsprong in het grondrecht van de burger op eerbiediging van zijn persoonlijke levenssfeer. *Privacy* is de gangbare term om te verwijzen naar de mogelijkheid van mensen om ongestoord zichzelf te kunnen zijn. Hoewel er een sterke verbinding bestaat tussen de privacy enerzijds en persoonsgegevens anderzijds, is er wel degelijk een onderscheid.

In de eerste plaats bestrijkt privacy een breder gebied dan persoonsgegevens. Naast deze *informationele privacy* worden vaak de *fysieke* en de *relationele privacy* onderscheiden. Denk bij fysieke privacy aan de eerbiediging van het menselijk lichaam en de woning, bij relationele privacy aan de vrijheid om naar believen met anderen te communiceren en om te gaan. Informationele privacy is ten dele een afgeleid principe dat kan bijdragen aan indirecte bescherming van de fysieke en relationele privacy. Een voorbeeld is het geheim blijven van gegevens over telefoongesprekken als voorwaarde om je vrij te kunnen voelen om te bellen met wie je wilt.

In de tweede plaats dienen principes ten aanzien van een behoorlijke omgang met persoonsgegevens, zoals juistheid en vertrouwelijkheid, een breder doel dan privacy alleen. Andere belangrijke argumenten voor zorgvuldigheid zijn het voorkomen van schade door misbruik (bijv. identiteitsfraude), de economische waarde (de burger is een 'sitting duck', hij weet niet wat er met zijn persoonsgegevens gebeurt en kent de werkelijke waarde er niet van) en het voorkomen van discriminatie.[13] Dat leidt er toe dat regels over een behoorlijke omgang met persoonsgegevens óók van toepassing kunnen zijn als het recht op privacy zelf niet of nauwelijks een rol speelt. In dit rapport concentreren we ons op aspecten van het verwerken van persoonsgegevens die samenhangen met informationele privacy.

Het grondrecht op eerbiediging van de persoonlijke levenssfeer is verankerd in onder meer artikel 8 van het EVRM[14] en artikel 10 van onze Grondwet. Beide artikelen staan beperkingen van het recht op privacy toe, maar alleen onder een aantal voorwaarden: de maatregel moet in een democratische samenleving *noodzakelijk* zijn voor bepaalde legitieme doelen en bij of krachtens de wet zijn voorzien. Dat betekent dat de maatregel in een juiste verhouding moet staan tot het beoogde doel (*proportionaliteit*), waarbij het minst ingrijpende middel voorgaat (*subsidiariteit*), en met de nodige waarborgen moet zijn omgeven.

De uitgangspunten voor de bescherming van persoonsgegevens zijn in Europa vastgelegd in het Verdrag van Straatsburg[15]. Deze zijn in EU-verband verder uitgewerkt in Richtlijn 95/46/EG[16]. De WBP is de Nederlandse implementatie daarvan. De WBP bevat niet alleen richtlijnen voor concrete situaties. Zij biedt ook houvast voor langetermijnbeslissingen zoals over de inrichting van een informatie-infrastructuur.

[12] Van beleidsbegroting tot beleidsverantwoording.
[13] Zie Van den Hoven (2000).
[14] Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (1951).
[15] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoons-gegevens (1981).
[16] Richtlijn 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281).

Privacywetgeving bevat niet zoveel regels die dwingend voorschrijven hoe precies met persoonsgegevens moet worden omgegaan. De WBP gaat uit van de eigen verantwoordelijkheid van organisaties voor een goede privacybescherming en geeft de maatstaven daarvoor aan in een stelsel van rechten en verplichtingen. Het gaat daarbij vooral om randvoorwaarden waarbinnen persoonsgegevens verwerkt mogen worden. Hierbij spelen ook een aantal 'zachte' normen een rol. Zo moet er bijvoorbeeld soms een afweging gemaakt worden tussen het gerechtvaardigd belang van degene die persoonsgegevens wil verwerken en het privacybelang van de persoon in kwestie.

Om een goede invulling te kunnen geven aan de normen uit de privacywetgeving komt het daarom vaak aan op het bereiken of in stand houden van een situatie waarin niet alleen aan specifieke regels is voldaan, maar ook meer in het algemeen het privacybelang in balans is met andere belangen. Er is daarbij sprake van balanceren rondom een steeds verschuivend evenwichtspunt. Maatschappelijke en technologische ontwikkelingen kunnen de bestaande balans bedreigen, maar bieden tegelijkertijd vaak ook kansen om een nieuw evenwicht tot stand te brengen.

Het creëren van voldoende vertrouwen bij burgers is een essentiële voorwaarde voor het welslagen van de plannen op het gebied van elektronische overheid. Het belang daarbij van een goede bescherming van de persoonlijke levenssfeer wordt algemeen erkend. Er zijn mogelijkheden om de handelingsruimte van de overheid te vergroten zonder dat het de privacy van de burgers aantast.[17] In de praktijk ontstaan er echter nog wel eens problemen doordat de consequenties van de privacywetgeving in een te laat stadium worden onderkend. Zij kunnen dan moeilijk worden ingepast en worden als knellend ervaren. Dit is eenvoudig te ondervangen door bij het ontwerpen van structuren, processen en systemen al vanaf het prille begin rekening te houden met privacyaspecten.
Wanneer er dan afgewogen beslissingen worden genomen en deze ook in de organisatiesfeer zorgvuldig worden uitgewerkt, staat de privacywetgeving aan weinig legitieme doelstellingen in de weg. *Privacy by design* is de manier bij uitstek om optimaal gebruik te maken van de meer dan voldoende speelruimte bij het verwerken van persoonsgegevens die de wettelijke randvoorwaarden in de regel bieden.

[17] Ook de conclusie van de Raad voor het openbaar bestuur in haar advies ICT en het recht om anoniem te zijn (januari 2000).

De burger en zijn identiteit

Al sinds mensenheugenis spelen identiteit en de verificatie daarvan een rol in het maatschappelijk verkeer.

In vroeger tijden was de kring van personen waarin iemand verkeerde overzichtelijk en kon hij erop vertrouwen dat Jan Jan was. Verificatie van identiteit was meestal een kwestie van directe herkenning. Het is nog geen twee eeuwen geleden dat Napoleon het systeem van de burgerlijke stand in de Lage Landen introduceerde. En nog tientallen jaren na Phileas Fogg's expeditie van 1872 was het mogelijk om zonder reisdocumenten de wereld rond te trekken.

Nu is het zo dat er van een geboorte binnen enkele dagen aangifte moet worden gedaan in de betreffende gemeente. De naam en enkele andere gegevens van de nieuwgeborene worden genoteerd. Daarmee bestaat deze 'echt' voor de overheid. Hij heeft een officiële, administratieve identiteit gekregen. Deze is alleen in zeer uitzonderlijke gevallen nog te wijzigen.

Burgers hebben een identiteit nodig om zich te kunnen onderscheiden van anderen. Ook kunnen zij ermee bewijzen een bevoegdheid te hebben of gerechtigd te zijn om te handelen, toegang te krijgen, te ontvangen. Soms gaat het daarbij om bovengenoemde 'echte' identiteit, dan weer om een identiteit die iemand zelf heeft gekozen of die hoort bij zijn hoedanigheid in een bepaalde situatie. Een persoon kan dus meerdere, soms ook tijdelijke identiteiten hebben.

Dit levert problemen op voor een gefragmenteerde en geautomatiseerde overheid die – uiteraard binnen redelijke grenzen – een goed en actueel beeld moet hebben van haar burgers. Het vaststellen en opslaan van de 'echte' identiteit van een persoon is een typische overheidstaak. Identiteitsbewijzen kunnen door de overheid en anderen verschaft worden, al dan niet direct verbonden met de 'echte' identiteit.

2.1 Identiteitsmanagement

De opkomst van moderne communicatietechnologie, in het bijzonder internet, heeft een grote invloed op de omgang met identiteiten. Er bestaat een grote behoefte aan niet-fysieke manieren om identiteit te kunnen aantonen of verifiëren. Steeds meer is er daarom naast de fysieke en de administratieve identiteit ook sprake van een digitale identiteit.

De digitale identiteit zal in veel gevallen aan een fysieke identiteit te koppelen moeten zijn. Daarvoor zijn technieken als de digitale handtekening en biometrie geschikt. Er wordt hard gewerkt aan het tot stand brengen van een PKI – de ondersteunende infrastructuur voor de digitale handtekening – voor communicatie met de overheid. Het is de bedoeling dat de elektronische Nederlandse identiteitskaart eNIK op termijn biometrische identificatie gaat ondersteunen. Daarnaast wordt de GBA gemoderniseerd, waarmee ook gegevens over de 'echte' identiteit eenvoudig en real-time beschikbaar zullen komen. Deze ontwikkelingen samen bieden het beeld van een zich ontwikkelende identiteitsinfrastructuur voor de overheid. Die zal het fundament vormen van de informatie-infrastructuur van de overheid.

De overheid heeft behoefte aan een goed functionerende identiteitsinfrastructuur omdat zij in tal van gevallen zekerheid moet hebben over de identiteit van haar burgers. Het is echter geenszins noodzakelijk dat burgers altijd en overal voor de overheid kenbaar zijn. Vanuit privacyperspectief is dit ook niet wenselijk. Het loont daarom om na te denken over waar, wanneer en voor wie kenbaarheid al dan niet een vereiste is, en over de consequenties van keuzes op

dit gebied. Waar mogelijk verdient niet-kenbaarheid de voorkeur. In infrastructurele termen: niet-kenbaarheid is een belangrijk ontwerpprincipe.

Niet-kenbaarheid als ontwerpprincipe

Bescherming van persoonsgegevens komt voor een belangrijk deel neer op het zorgen voor een juiste en behoorlijke omgang met zulke gegevens. Daarnaast is echter een meer fundamentele benadering mogelijk. Geen betere manier tenslotte om onjuist of onbehoorlijk gebruik van persoonsgegevens te voorkomen dan door te zorgen dat er helemaal geen persoonsgegevens zijn.

De meest radicale manier om verwerking van persoonsgegevens te voorkomen, is helemaal geen gegevens vast te leggen: volledige anonimiteit. De belangrijkste toepassingen daarvan liggen in de sfeer van het verschaffen van toegang tot openbare informatie. Het is in het algemeen voor de overheid niet nodig om te weten wie dergelijke informatie heeft opgevraagd of geraadpleegd.

Wanneer het wel nodig is om gegevens vast te leggen, is het vaak mogelijk om ervoor te zorgen dat het geen persoonsgegevens zijn, dat wil zeggen ervoor zorgen dat de gegevens niet herleidbaar zijn tot identificeerbare personen. Er zijn in essentie twee methoden om dit te bereiken. De eerste is het gebruik van pseudo-identiteiten. De tweede is het werken met eigenschappen, rechten of bevoegdheden.

De identiteit van de persoon die achter een pseudo-identiteit schuil gaat is wel bekend, maar in de specifieke situatie of door de specifieke partij niet vast te stellen. Onder bijzondere omstandigheden kan de verbinding tussen pseudo-identiteit en persoon toch gelegd worden. Het kiessysteem in een aantal landen van het Gemenebest biedt een duidelijk voorbeeld. Dat is niet volledig anoniem. Stembiljetten zijn voorzien van een nummer dat de stemmer uniek identificeert. De verbinding tussen nummer en kiezer is echter alleen te leggen onder zeer bijzondere omstandigheden en na rechterlijke toetsing.

Identiteiten worden vaak gebruikt wanneer het in feite gaat om eigenschappen, rechten of bevoegdheden die iemand heeft. Koops (2001) noemt als voorbeeld de deelname van burgers aan een digitaal forum over de toekomst van hun wijk. De identiteit van de discussiedeelnemers hoeft de overheid daarbij niet te kennen. Wel zal zij zeker willen weten dat alleen belanghebbenden mee discussiëren.

Privacy-enhancing technologies (PET) vormen de technische neerslag van de hierboven geschetste ideeën.[18] Voor het afschermen van identiteiten in een informatiesysteem kan gebruik gemaakt worden van een zogenaamde *identiteitsbeschermer*. Dit systeemelement converteert de identiteit van de betrokkene in één of meerdere pseudo-identiteiten. Het plaatsen van de identiteitsbeschermer creëert twee soorten domeinen binnen het informatiesysteem. In het identiteitsdomein is de identiteit bekend en toegankelijk. In de pseudo-identiteitsdomeinen is dit niet het geval.

Een wijdverbreid misverstand is dat niet-kenbaarheid een eigenschap is van een gegevensverwerkend proces als geheel. Zij zou daarom niet in aanmerking komen voor processen waarin op enig moment identiteiten bekend moeten zijn. Overal in het informatiesysteem kunnen echter identiteitsbeschermers geplaatst worden. Neem als voorbeeld de aanvraag van een vergunning, uitkering of subsidie. In het begin en aan het eind van de procedure zal het daarbij meestal nodig zijn om de identiteit van de aanvrager te kennen. Daartussen echter juist meestal niet. Identiteitsbeschermers kunnen voor het hele traject tussen intake

[18] Meer in het algemeen omvat PET ook klassieke informatiebeveiliging en alle overige technologieën die waarborgen inhouden tegen onrechtmatige verwerking van persoonsgegevens. Zie ook paragraaf 5.5.

en toekenning of uitbetaling, maar ook onderdelen daarvan, een pseudo-identiteitsdomein maken.

Verplaatsen we ons naar het infrastructurele niveau, dan neemt het belang van niet-kenbaarheid alleen maar toe. Dit is helder en overtuigend beargumenteerd door Koops:

Wanneer identiteitsvaststelling het uitgangspunt is bij alle maatschappelijke relaties en dat gebeurt met één uniek identificatiemiddel (een supersofi-nummer), wordt het technisch een peulenschil om een bijzonder gedetailleerd beeld van iemand op te stellen. Dat mag weliswaar niet zo maar van de WBP en het CBP, maar dat wil niet zeggen dat het niet in bepaalde gevallen toch gebeurt en, belangrijker, dat wil niet zeggen dat in de toekomst [niet] andere keuzes kunnen worden gemaakt. Als de infrastructuur er ligt, wordt het makkelijker voor de politiek om, op basis van ad hoc-argumenten, besluiten te nemen die diep indringen in de persoonlijke levenssfeer van mensen. Dat hóéft niet, maar het kán wel.
De vraag die ik hiermee wil opwerpen is of we een dergelijke maatschappij – een identiteitsmaatschappij – tot stand willen brengen, waarin technologie alles vermag en het alleen van politieke besluitvorming *achteraf* afhangt hoe fundamentele waarden zoals privacy in de maatschappij worden gewaarborgd. Of willen we een maatschappij die vooraf de ontwikkeling van technologie normeert en beperkt en daar als het ware fundamentele waarden inbouwt, door identificatie alleen toe te staan wanneer dat echt noodzakelijk is en door in andere gevallen met pseudonieme of anonieme bevoegdheidsvaststelling te volstaan? In een identiteitsmaatschappij dreigt het gevaar van een sluipende uitholling van fundamentele waarden als privacy (er mag steeds een klein beetje meer worden gekoppeld door net iets meer instanties), totdat je, gechargeerd gezegd, op een gegeven moment 's ochtends wakker wordt en merkt dat je transparant bent geworden voor overheid en bedrijfsleven. In een pseudonimiteits-maatschappij kan de politiek alleen ingrijpende maatschappelijke wijzigingen door-voeren door de technische infrastructuur grootschalig te wijzigen – met alle kosten van dien – hetgeen vermoedelijk in elk geval een beter maatschappelijk debat zal uit-lokken. Belangrijk is dat er nu een maatschappelijke discussie wordt gevoerd over de toekomst van de informatiemaatschappij: willen we als samenleving een identiteits-infrastructuur of een pseudonimiteitsinfrastructuur?

Uit: Bert-Jaap Koops. 'Een nieuwe GBA, digitale kluisjes en identificatiedrang'. Nederlands Juristenblad 2001, afl. 32, blz. 1555-1561.

Koops stelt als afsluiting de vraag: willen we als samenleving een identiteits-infrastructuur of een pseudonimiteitsinfrastructuur? Het behoeft geen betoog dat het CBP de laatste optie voorstaat. Essentieel is daarbij de infrastructurele dimensie. Het is niet voldoende dat iedere overheidsinstantie voor zich deze lijn volgt. Ook op het overkoepelende niveau dienen hiervoor adequate voor-zieningen te worden getroffen. Alleen dan is ook in ketens van verwerkingen door meerdere overheidsinstanties niet-kenbaarheid een reëel en praktisch toepasbaar uitgangspunt.

De terroristische aanslagen in de Verenigde Staten hebben de discussie over veiligheid versus privacy opnieuw aangejaagd. Duidelijk moge nu zijn dat dit grotendeels een schijndiscussie is. Van pseudoniemen kan weldoordacht gebruik gemaakt worden. Niet-kenbaarheid als uitgangspunt is dan prima te verenigen met kenbaarheid wanneer de omstandigheden daartoe noodzaken. Bij het ontwerpen van informatiesystemen dient niet-kenbaarheid dan ook het uitgangspunt te zijn. Het motto luidt: kenbaarheid waar nodig, niet-kenbaarheid waar mogelijk.

2.2 Persoonsnummerbeleid

Een natuurlijk en veel toegepast hulpmiddel bij identiteitsmanagement zijn persoonsnummers of andere uniek identificerende codes. Bekende door de overheid gehanteerde persoonsnummers zijn het sofi-nummer en het A-nummer uit de GBA.

Een nummer als het A-nummer heeft weinig invloed op de manier waarop met administratieve identiteiten wordt omgegaan. Het is een intern administratienummer, dat niet bij de burger bekend is. En belangrijker: zelfs al zou de burger zijn A-nummer wel kennen (hij kan het gewoon bij de gemeente opvragen), dan kan hij er nauwelijks iets mee. Het A-nummer wordt immers niet gebruikt in het contact tussen overheid en burger.

Voor het interne persoonsnummer van de belastingdienst gold twintig jaar geleden hetzelfde. Dit veranderde echter toen dat nummer eerst aan burgers bekend werd gemaakt en later uitgebreid werd tot het sofi-nummer. Deze uitbreiding hield onder meer in dat het nummer voortaan door meerdere instanties gebruikt werd. Niet alleen in hun eigen administraties, maar ook voor het uitwisselen en koppelen van gegevens. Het sofi-nummer kwam bovendien op paspoort en rijbewijs te staan. Als compensatie kwamen er strikte regels voor het gebruik[19], die echter niet altijd even duidelijk zijn.

Ten gevolge van dit alles nam het belang van het sofi-nummer allengs toe. Hoewel er formeel aan het hebben van een sofi-nummer geen rechten te ontlenen zijn, is de perceptie doorgaans anders. Het nummer is uitgegroeid tot een soort pseudo-identiteit. Het is voor burgers interessant en relatief eenvoudig om creatief met hun administratieve identiteit(en) om te gaan. De laatste tijd worden dan ook steeds meer problemen onderkend met het sofi-nummer. Het blijkt in de praktijk moeilijk te beheren. Tegelijkertijd neemt de roep van allerlei organisaties om het sofi-nummer te mogen gebruiken toe. Er is daarom alle aanleiding voor herbezinning.

Grijpink (2001) analyseert de problematiek van het beheer van nummerstelsels. Aansluitend op zijn aanbevelingen pleit het CBP voor differentiatie, niet uniformiteit als ontwerpprincipe voor het persoonsnummerbeleid.

Differentiatie als ontwerpprincipe

Grijpink stelt vast dat nummerbeheer dat (mede) afhankelijk is van samenwerking tussen onafhankelijke partijen, slechts kans van slagen heeft als het gebruik van het nummer bijdraagt aan de oplossing van een probleem dat alle betrokken partijen als belangrijk ervaren. Wanneer het gebruik in de praktijk te ver verwijderd is van dit probleem, bijvoorbeeld doordat veel niet direct daarbij betrokken partijen ook van het nummer gebruik maken, blijkt het zo goed als onmogelijk om een voldoende hoge kwaliteit van de bij het nummer vastgelegde gegevens te waarborgen.[20]

[19] Het Besluit gebruik sofi-nummer.

[20] Een lage gegevenskwaliteit is niet alleen bezwaarlijk voor degene die de gegevens verwerkt. Zo kan fraude met sofi-nummers voor de slachtoffers ervan ernstige en langdurige gevolgen hebben. Het kan soms zeer veel tijd, moeite en zelfs overredingskracht kosten om eenmaal als gevolg hiervan onjuist vastgelegde gegevens gecorrigeerd te krijgen.

Dit bezwaar geldt bijna per definitie voor een uniform nummerstelsel, gebaseerd op een enkel algemeen persoonsnummer. Deze conclusie wordt niet alleen gesteund door de hierboven aangestipte problemen met het sofi-nummer, maar ook door ervaringen in onder meer Zweden en de Verenigde Staten. Deze landen worden vaak aangehaald als voorbeelden dat een algemeen persoonsnummer wel degelijk goed kan functioneren. In beide landen is men echter ook met de grenzen ervan geconfronteerd. In Zweden is in 1993 een regeringscommissie ingesteld met als opdracht om maatregelen voor te stellen om het gebruik van nationale persoonsnummers aanzienlijk te beperken. Een regeringswisseling kort na het verschijnen van het rapport van deze commissie,[21] heeft het in een bureaula doen verdwijnen. Er zijn echter nog altijd geregeld discussies over de negatieve aspecten van het nummer, maar die lijken vooralsnog weinig praktische gevolgen te hebben voor het nummergebruik. In de Verenigde Staten heeft de toezichthouder op het Social Security Number in verband met de identiteitsfraude die met dat nummer gepleegd wordt, gesproken van een nationale crisis.[22]

Een gedifferentieerde aanpak, waarbij diverse nummers naast elkaar bestaan, biedt in veel gevallen voordelen. Grijpink beveelt op basis van zijn analyse dan ook aan dat de overheid haar gegevenshuishouding baseert op een meervoudige nummerstrategie. Daarin is een belangrijke rol weggelegd voor sector- en ketengebonden nummerstelsels. Waar mogelijk en wenselijk kunnen algemene persoonsnummers een aanvullende rol spelen. Deze bestaat vooral uit het mogelijk maken van vergelijkingen tussen de verschillende sectorale nummers. Daarmee kan de gegevenskwaliteit gewaarborgd worden en fraude bestreden.

Keten- of sectorgebonden nummers zijn gemakkelijker te beheren en leiden daardoor tot hogere gegevenskwaliteit. Dat is een belangrijk voordeel vanuit het oogpunt van gegevensbescherming. Een gedifferentieerd systeem van nummerstelsels heeft nog een voordeel. Het maakt het moeilijker om ongecontroleerd allerlei gegevens aan elkaar te koppelen en zo gedetailleerde profielen van burgers op te stellen. Zoals we in de vorige paragraaf al betoogden is een systeem dat naar zijn aard minder mogelijkheden tot misbruik van persoonsgegevens biedt, te verkiezen boven een waarin de beperkingen vooral van juridische aard zijn.[23]

2.3 Conclusie

Een infrastructurele aanpak is onontbeerlijk om fundamentele waarden als privacy op lange termijn te garanderen.

Er ontwikkelt zich een identiteitsinfrastructuur voor de overheid, die de basis zal vormen voor haar informatie-infrastructuur. Pseudo-identiteiten zijn onmisbaar gereedschap bij privacybescherming in informatiesystemen. Niet-kenbaarheid is daarom een essentieel ontwerpprincipe voor de identiteitsinfrastructuur van de overheid.

Persoonsnummers spelen een belangrijke rol bij identiteitsmanagement. Nummerstelsels zonder onderliggend gedeeld probleem blijken moeilijk te beheren. Vanuit informatiekundig perspectief valt er daarom veel te zeggen voor een gedifferentieerde aanpak waarin verschillende keten- en sectornummers naast elkaar bestaan. Zo'n aanpak kan tegelijkertijd gezien worden als een bijdrage aan infrastructurele privacyborging.

[21] *Personal Identification Numbers – Privacy and efficiency*. Personal Identification Number Enquiry. Zweden, voorjaar 1994.

[22] The Social Security Administration's inspector general says the power of the Social Security number makes it a valuable asset subject to limitless abuse, and calls that misuse has developed into "a national crisis." (Washington Post, 31 mei 2001).

[23] Zie ook Lessig (1999) voor een uitvoerige bespreking van deze these.

De burger en zijn gegevens

Overheidsinstanties verwerken persoonsgegevens niet in een vacuüm. Zij kunnen die gegevens verkrijgen uit eigen waarneming of van derden. Vaak ook zal de burger de gegevens zelf aanleveren. Omgekeerd is er druk persoonsgegevensverkeer van de overheid naar burgers. Het is hierom geen toeval dat de informatierelatie burger-overheid sterk in de belangstelling staat. Een belangrijk thema daarbij is de mogelijkheid om de burger de regie te geven over zijn eigen persoonsgegevens.

De invulling van het begrip 'regie' is in de loop der tijd wat verschoven. Aanvankelijk ging het vooral om transparantie. De burger heeft er recht op om te weten wat de overheid met zijn persoonsgegevens doet. Hij kan dan in de gaten houden wat ermee gebeurt en eventueel bezwaar aantekenen of om correctie verzoeken. Regie over de eigen persoonsgegevens wil dan in feite zeggen: zicht op (de verwerking van) de eigen persoonsgegevens.

Recente adviezen aan de regering, zoals de rapporten van de commissies Snellen (modernisering GBA) en Docters van Leeuwen (ICT en overheid), verschuiven de focus naar een actievere invulling van de term. De burger moet in grote mate zelf kunnen bepalen wat de overheid wel en niet met zijn persoonsgegevens mag doen. Regie over de eigen persoonsgegevens staat in dat geval voor: zeggenschap over (de verwerking van) de eigen persoonsgegevens.

Hieronder bespreken we achtereenvolgens de informatierelatie burger-overheid en de noties van zicht op en zeggenschap over de eigen persoonsgegevens.

De burger en zijn gegevens

3.1 De informatierelatie burger-overheid

We bespreken de informatierelatie tussen burger en overheid aan de hand van drie typen burgers. Deze zijn ontleend aan Biesboer (1998). Een vergelijkbare analyse is overigens te vinden in het rapport van de commissie Wallage[24].

De *loyale* burger is enthousiast over nieuwe mogelijkheden van elektronische dienstverlening. Hij stelt een groot vertrouwen in de overheid. Die krijgt carte blanche voor het verwerken van zijn gegevens, en mag hem daarbij ook op zijn plichten wijzen. Hij is wel navenant verbolgen als de overheid zijn rechten toch blijkt te schenden.

De *inzage*-burger laat de overheid op zich ook graag haar gang gaan. Voorwaarde daarvoor is wel dat hij de mogelijkheid heeft om een oogje in het zeil te houden: eerst zien, dan geloven. Zonodig moet hij ook aan de bel kunnen trekken.

De *contract*-burger wil zoveel mogelijk zelf de controle behouden. Het liefst beheert hij zelf een elektronisch kluisje met daarin zijn persoonsgegevens. Informatiestromen tussen overheidsinstanties zijn niet vanzelfsprekend. Hij wil weten hoe die lopen en waarvoor ze nodig zijn. Ook moeten er procedures zijn om gegevensverwerkingen aan te vechten.

Uiteraard zijn dit ideaaltypen, waaraan geen enkele burger geheel voldoet. Ze zijn dan ook bedoeld als illustratie van manieren waarop de burger invulling kan geven aan zijn informatierelatie met de overheid. Welke informatierelatie een burger in een concreet geval kiest, kan hij onder meer laten afhangen van het soort informatie, de aangeboden dienst en de overheidsinstantie in kwestie.[25] Het sleutelwoord is echter vertrouwen. Hoe meer vertrouwen de burger heeft in wat de overheid met zijn persoonsgegevens doet, des te meer zal hij geneigd zijn om zich als loyale burger op te stellen. Ironisch genoeg is transparantie een belangrijke voorwaarde voor dit vertrouwen.

[24] Commissie Toekomst overheidscommunicatie. In dienst van de democratie. Den Haag, 2001, paragraaf 6.1.4.

[25] Onderzoek suggereert dat het model van de inzage-burger het populairst is. Zie hiervoor bijvoorbeeld het rapport van de commissie Wallage.

Er ontstaat zo in eerste instantie het beeld van een burger die bewust kiest hoe nauw hij op verschillende gebieden betrokken wil zijn bij de verwerking van zijn persoonsgegevens. In de volgende twee paragrafen, over zicht op en zeggenschap over de eigen persoonsgegevens, zullen we zien dat dit beeld enige nuancering behoeft.

3.2 Zicht op de eigen persoonsgegevens

De burger heeft er recht op om te weten wat er met zijn persoonsgegevens gebeurt. Dat is de gedachte achter regie over de eigen persoonsgegevens in de zin van: zicht daarop. Tegen dit beleidsuitgangspunt is vanuit privacyoptiek geen enkel bezwaar. Integendeel, transparantie is juist een principe van gegevensbescherming. Het is echter wel belangrijk om het in het juiste perspectief te blijven zien.

Hierboven stelden we al vast dat de burger lang niet altijd alles wil weten. Behalve van niet willen is het vaak ook een kwestie van niet kunnen. Bekkers (2001) spreekt in het kader van de digitale dienstverlening door de overheid van de 'mythe van de intelligente en mondige burger'. Beleidsmakers schetsen het beeld van de intelligente burger die beschikt over zekere bureaucratische en digitale competenties. Hij waarschuwt terecht voor het toenemen van de kloof tussen overheid en burger doordat veel burgers in onvoldoende mate over deze competenties beschikken.

Bekkers' analyse gaat ook op voor het thema van zicht op de eigen persoonsgegevens. De BZK-modelburger die actief zicht houdt op en waakt over de manier waarop de overheid met zijn persoonsgegevens omgaat, moet waarschijnlijk nog geboren worden. Sterker nog: deze zal nooit geboren worden. De overheid als conglomeraat van instanties met talloze gegevensverwerkingen is eenvoudig te complex voor een burger om geheel te doorgronden.

De burger kan en wil de overheid niet altijd tot in detail in de gaten houden. Integendeel, hoe minder last hij heeft van de overheid, hoe beter. De overheid streeft er daarom terecht ook naar om burgers zoveel mogelijk met één gezicht tegemoet te treden, bijvoorbeeld door gezamenlijk of gemeenschappelijk gebruik van gegevens. (Paradoxaal genoeg wordt dit ene gezicht in de context van informatiesystemen overigens 'transparantie' genoemd.)

De kunst voor de overheid is om de juiste balans te vinden tussen deze twee deels tegenstrijdige doelstellingen. Zij beschikt daarbij over twee complementaire strategieën. De ene is om de burger zo duidelijk mogelijke informatie te verschaffen over hoe zij met zijn persoonsgegevens omgaat. De andere is om zo duidelijk en vertrouwenwekkend te werken dat de burger niet steeds de noodzaak voelt om die informatie ook daadwerkelijk tot zich te nemen.

Optimale transparantie

Zo duidelijk mogelijke informatie verschaffen gaat verder dan het bieden van maximale transparantie. Een parallel is te trekken met de beleidslijn van BZK met betrekking tot openbaarheid van overheidsinformatie[26]. Daarin wordt aangegeven dat openbaarheid van die informatie alleen niet voldoende is. Zij moet ook op een toegankelijke manier beschikbaar zijn. Voor informatie over gegevensverwerkingen door de overheid geldt iets soortgelijks. Er moet sprake zijn van actieve openheid, niet alleen maar van passieve. Het moet voor de burger niet alleen in principe mogelijk zijn om achter de informatie te komen waar hij naar op zoek is. De overheid dient ook gericht in te spelen op zijn concrete informatiebehoefte en het hem zo gemakkelijk mogelijk maken. Dat kan bijvoor-

[26] Beleidslijn "Naar optimale beschikbaarheid van overheidsinformatie". Kamerstukken II, 1999-2000, 26387, nr. 7.

beeld door te laten zien welke belangrijke registraties er zijn in overheidsland en hoe de informatiestromen daartussen lopen. Het devies luidt dus *optimale* transparantie in plaats van *maximale* transparantie. Zo krijgt de burger niet alleen *zicht* op, maar ook *inzicht* in de verwerkingen van zijn persoonsgegevens. En alleen zo kan transparantie ook daadwerkelijk de haar toegedichte rol vervullen als 'trigger' voor de burger om zijn rechten uit te oefenen, en voor de toezichthouder om zonodig op te treden.

Doelbinding als ontwerpprincipe

Duidelijk en vertrouwenwekkend werken met persoonsgegevens kent vele facetten. Voor het scheppen van een inzichtelijk functionerende infrastructuur is met name het beginsel van *doelbinding* van belang. Doelbinding betekent dat persoonsgegevens altijd voor duidelijk omschreven en specifieke doeleinden moeten worden verzameld. Ook moet verder gebruik van de gegevens daarmee verenigbaar zijn. De redelijke verwachting die burgers ten aanzien van gegevensverwerkingen door de overheid hebben, speelt bij het bepalen daarvan een belangrijke rol.

Hierboven is betoogd dat een infrastructuur zonder specifieke regels gebaseerd op transparantie en controle door de burger niet werkbaar is. Alles tot in het kleinste detail regelen is geen alternatief. Dat zou evenmin werkbaar zijn, maar bovenal biedt het de burger geen inzicht, en daardoor geen vertrouwen. Doelbinding als ontwerpprincipe voor de gegevenshuishouding kan daaraan wel een belangrijke bijdrage leveren.

De burger en zijn gegevens

3.3 Zeggenschap over de eigen persoonsgegevens

De burger heeft er recht op om zelf te bepalen wat er wel en niet met zijn persoonsgegevens gebeurt. Dat is de gedachte achter regie over de eigen persoonsgegevens in de zin van: zeggenschap daarover.

Zeggenschap over de eigen persoonsgegevens bestaat in feite uit twee aan elkaar tegengestelde delen:
- het recht van de burger om zich te verzetten tegen bepaalde op zich wel toegestane verwerkingen van zijn persoonsgegevens ('opt out'), en
- de mogelijkheid voor de burger om toestemming te verlenen voor bepaalde op zich niet toegestane verwerkingen van zijn gegevens ('opt in').

Overheidsinstanties verwerken persoonsgegevens omdat zij dat wettelijk verplicht zijn of omdat het noodzakelijk is voor de uitvoering van een publiekrechtelijke taak.[27] Er is daarbij niet zoveel ruimte voor een recht op verzet. De overheid moet nu eenmaal het een en ander van haar burgers weten. Als de burger naar eigen goeddunken gegevens voor de overheid verborgen mocht houden, kon de belastingdienst haar deuren wel sluiten. Overigens kan er wel sprake zijn van persoonlijke omstandigheden op grond waarvan een burger zich met recht kan verzetten tegen een verwerking van zijn gegevens door een overheidsorgaan.[28] Dat doet echter niets af aan de noodzaak van het betreffende gegevensverwerkende proces in het algemeen.

De mogelijkheid om toestemming te verlenen staat de laatste tijd het meest in de belangstelling. 'Het is toch eigenlijk betuttelend en niet meer van deze tijd dat de overheid voor de burger bepaalt wat er allemaal wel en – vooral – niet met zijn persoonsgegevens mag gebeuren; die burger is mans genoeg om dat zelf te beslissen.' Dat is de teneur van rapporten als die van de commissies Snellen (modernisering GBA) en Docters van Leeuwen (ICT en overheid). Snellen c.s. pleiten voor een gegevenskluisje voor de burger. Daarin kan deze –

[27] Zie paragraaf 6.3.
[28] Zie paragraaf 7.4.

als hij dat wil – naast de altijd aanwezige GBA-informatie nog extra gegevens stoppen. Hij bepaalt vervolgens zelf welke publieke en private partijen er toegang toe krijgen. Docters van Leeuwen c.s. zitten op een vergelijkbare lijn als zij ervoor pleiten de burger zelf de doelbinding van zijn persoonsgegevens te laten bepalen.

Hierboven wezen we al op de mythe van de intelligente en mondige burger. De aanname dat de burger voldoende overzicht heeft om dit soort zaken zelf te kunnen beslissen – als hij dat überhaupt zou willen – is niet realistisch. Om deze reden zal zeggenschap van de burger over zijn eigen persoonsgegevens slechts een corrigerende rol kunnen spelen binnen een algemeen kader voor wat toelaatbare verwerkingen van persoonsgegevens door de overheid zijn. Voor zover de burger deze zeggenschap wel krijgt, doet de overheid er goed aan om eerst te zorgen voor de hierboven bepleite optimale transparantie. Alleen dan kan de burger in voorkomende gevallen ook werkelijk en in vrijheid zijn toestemming verlenen.

Veel belangrijker zijn de talrijke situaties waarin de burger van zijn recht op zeggenschap, voor zover hij het al heeft, geen gebruik kan of wil maken. Dan is het van belang dat wat er gebeurt, aansluit bij wat hij redelijkerwijs kan verwachten. Wil het systeem als geheel aanvaardbaar zijn, dan moet dat zeker gelden voor de manier waarop het zonder regie-aanwijzingen van de burger werkt.[29]

Informationele zelfbeschikking

Voortbouwend op het bovenstaande vallen er principiële kanttekeningen te zetten bij informationele zelfbeschikking. Een recht daarop is niet in strijd met de uitgangspunten van de nationale en Europese regels omtrent gegevensbescherming. Zo heeft Duitsland een recht op informationele zelfbeschikking. Dat kent echter zeer veel uitzonderingen en is daardoor sterk verwaterd.

Verzet is lang niet altijd mogelijk. Veel gegevensverwerkingen moeten nu eenmaal plaatsvinden. Ook toestemming kent haar beperkingen. Tot op zekere hoogte dient de burger tegen zichzelf in bescherming te worden genomen. Niet voor niets is er in de discussies bij het opstellen van de Wet bescherming persoonsgegevens en het EU Handvest expliciet voor gekozen om geen recht op informationele zelfbeschikking te formuleren.

De Europese privacyrichtlijn en de WBP verkiezen een minder vergaand recht op informationele privacy en bescherming van persoonsgegevens. Dat kent bijgevolg veel minder uitzonderingen. In essentie gaat het om een afgewogen systeem van 'checks and balances'. Verzet en toestemming spelen daarin een corrigerende rol. Toestemming moet aan enkele belangrijke voorwaarden voldoen. Zij moet vrij gegeven en specifiek zijn, gebaseerd zijn op voldoende en juiste informatie en kan altijd weer worden ingetrokken.[30]

3.3 Conclusie

De burger kan zijn informatierelatie met de overheid op meerdere manieren inkleuren. Hoe meer hij de overheid vertrouwt, hoe kleiner zijn behoefte zal zijn om haar in de gaten te houden.

Regie over de eigen persoonsgegevens heeft twee facetten: zicht en zeggenschap. De overheid moet zorgen voor *optimale* transparantie. Zo krijgt de burger niet alleen *zicht op*, maar ook *inzicht* in de verwerkingen van zijn persoonsgegevens. Pas wanneer burgers inzicht hebben in de verwerkingen van hun persoonsgegevens is de tijd rijp om ze daar ook zeggenschap over te geven.

[29] Vergelijk het eerdere betoog voor doelbinding als ontwerpprincipe.

[30] Zie Hustinx (2001) voor een diepgaande bespreking van deze thematiek.

Informationele zelfbeschikking kent echter haar grenzen. Bewust is in onder meer de Wet bescherming persoonsgegevens gekozen voor een systeem van ‘checks and balances’ waarin toestemming en verzet slechts een corrigerende rol spelen. Belangrijker is dat de overheid ook zonder regie-aanwijzingen van de burger duidelijk en vertrouwenwekkend werkt. Doelbinding als ontwerp-principe van haar informatie-infrastructuur kan daaraan een belangrijke bijdrage leveren.

Informatie-infrastructuur en privacy

Voortbouwend op de ingrediënten uit de eerste drie hoofstukken kunnen we nu een visie neerzetten op de bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid.

4.1 Privacy by design

In het beleid en de uitvoering op het gebied van de elektronische overheid tekent zich een gestage ontwikkeling af naar een informatie-infrastructuur voor de overheid. Veel van de informatie in deze infrastructuur bestaat uit persoonsgegevens. Wat moet er gedaan worden om de bescherming van deze persoonsgegevens te waarborgen?

Het kenmerkende van een infrastructuur is dat het gaat om generieke basisvoorzieningen met een relatief permanent karakter. Om maatregelen ter bescherming van persoonsgegevens werkelijk in zo'n infrastructuur te verankeren is het nodig dat zij aan dezelfde karakteristieken voldoen. Alleen wanneer privacy op een robuuste manier wordt ingebouwd is zij ook op langere termijn te garanderen. Wat we daarom zoeken zijn ontwerpprincipes voor informatie-infrastructuren die de bescherming van persoonsgegevens tot een organisch onderdeel ervan maken.

Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Ontwerpprincipes die de bescherming van persoonsgegevens op zich ondersteunen zijn daarom niet voldoende. Eveneens moeten in de infrastructuur mechanismen verankerd worden die actief het vertrouwen van de burger in het privacy-vriendelijk functioneren ervan bevorderen.

4.2 Identiteitsinfrastructuur

Een informatie-infrastructuur waarin veel persoonsgegevens worden verwerkt kan niet zonder een adequate identiteitsinfrastructuur als basis. Het lijkt voor de hand te liggen om hiervoor, analoog aan de bestaande identiteitsinfrastructuur, kenbaarheid als uitgangspunt te nemen. Een kenmerk van elektronische omgevingen is echter dat wie ze gebruikt gemakkelijk allerlei digitale sporen achterlaat. Wanneer deze sporen op een eenduidige manier te identificeren zijn, is het eenvoudig om ze aan elkaar te koppelen. Dat geeft de overheid de mogelijkheid om een gedetailleerd beeld van burgers op te bouwen. Regels en procedures kunnen daaraan weliswaar in de weg staan, maar beter is het om de infrastructuur zo in te richten dat deze het ongecontroleerd koppelen van persoonsgegevens verhindert. Niet-kenbaarheid is daarvoor een belangrijk ontwerpprincipe.

Bij niet-kenbaarheid als ontwerpprincipe zijn twee belangrijke kanttekeningen te maken. De eerste is dat niet-kenbaarheid niet noodzakelijk een eigenschap is van een gegevensverwerkend proces als geheel. De tweede is dat niet-kenbaarheid niet aan identificatie in de weg moet staan waar deze noodzakelijk is. Het motto luidt: kenbaarheid waar nodig, niet-kenbaarheid waar mogelijk.

Niet-kenbaarheid als ontwerpprincipe kent twee complementaire uitwerkingen. De eerste manier om niet-kenbaarheid vorm te geven is door het gebruik van pseudo-identiteiten. Informatie is daarbij wel gekoppeld aan een identificeerbare persoon, maar slechts onder bijzondere omstandigheden ook tot die persoon te herleiden.
De tweede manier om niet-kenbaarheid vorm te geven is door het gebruik van bewijzen van eigenschappen, rechten of bevoegdheden. Die zullen doorgaans op basis van een identiteit worden verstrekt. Voor gebruik zullen ze ook aan de

betreffende persoon gekoppeld moeten kunnen worden, maar deze persoon hoeft niet langer identificeerbaar te zijn. In beide gevallen kunnen er wel digitale sporen ontstaan, maar deze zullen niet of zeer moeilijk ongecontroleerd samen te voegen zijn tot gedetailleerde profielen van identificeerbare personen.

Persoonsnummers spelen een belangrijke rol bij identiteitsmanagement. Nummerstelsels zonder onderliggend gedeeld probleem blijken moeilijk te beheren. Vanuit informatiekundig perspectief valt er daarom veel te zeggen voor een gedifferentieerde aanpak waarin verschillende sector- en ketennummers naast elkaar bestaan. Differentiatie als ontwerpprincipe is tegelijkertijd een bijdrage aan infrastructurele privacyborging. Het is het analogon op identiteitsniveau van het gebruik van pseudo-identiteiten, en daarom ook relevant buiten de specifieke context van persoonsnummers.

We hebben twee ontwerpprincipes voor de identiteitsinfrastructuur onderscheiden: niet-kenbaarheid en differentiatie. Beide hebben als belangrijk voordeel dat zij het alternatief niet uitsluiten, terwijl dat omgekeerd in veel grotere mate het geval is. In een gedifferentieerd stelsel is het relatief eenvoudig om, waar en wanneer dat wenselijk of noodzakelijk is, meer uniformiteit aan te brengen. In een uniform stelsel differentiatie aanbrengen is veel lastiger. Evenzo is het relatief eenvoudig om, waar en wanneer dat wenselijk of noodzakelijk is, pseudoniemen door identiteiten te vervangen, maar veel lastiger is het om een op identiteit gebaseerd systeem weer te pseudonimiseren.[31]

4.3 Vertrouwen

Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Recent is er herhaaldelijk voor gepleit om dit vertrouwen te verankeren door de burger zoveel mogelijk de regie over zijn eigen persoonsgegevens in handen te geven. De burger kan zijn informatierelatie met de overheid op meerdere manieren inkleuren. Hoe meer hij de overheid vertrouwt, hoe kleiner zijn behoefte zal zijn om haar in de gaten te houden.

Regie over de eigen persoonsgegevens heeft twee facetten: zicht en zeggenschap. De overheid moet zorgen voor optimale transparantie. Zo krijgt de burger niet alleen zicht op, maar ook inzicht in de verwerkingen van zijn persoonsgegevens. Pas wanneer burgers inzicht hebben in de verwerkingen van hun persoonsgegevens is de tijd rijp om ze daar ook zeggenschap over te geven. Zelfs dan zullen zij echter niet alles wat de overheid met hun persoonsgegevens doet in detail kunnen of willen volgen. Informationele zelfbeschikking kent daarom haar grenzen. Bewust is in onder meer de Wet bescherming persoonsgegevens gekozen voor een systeem van 'checks and balances' waarin toestemming en verzet slechts een corrigerende rol spelen. Belangrijker is dat de overheid ook zonder regie-aanwijzingen van de burger duidelijk en vertrouwenwekkend te werk gaat. Doelbinding als ontwerpprincipe van haar informatie-infrastructuur kan daaraan een belangrijke bijdrage leveren.

4.4 Resumerend

Het *Leitmotiv* is 'privacy by design'. Bescherming van persoonsgegevens in een informatie-infrastructuur begint bij de ontwerpprincipes. Vier belangrijke daarvan zijn:

- niet-kenbaarheid;
- differentiatie;
- optimale transparantie;
- doelbinding.

[31] Zie Goldberg (2000).

De Wet bescherming persoonsgegevens

5

Dit hoofdstuk behandelt de hoofdpunten van de Wet bescherming persoonsgegevens (WBP), toegespitst op de elektronische overheid. Eerst bespreken we de bestuursrechtelijke context waarin de WBP in dit verband bezien moet worden. Vervolgens zetten we kort de belangrijkste uitgangspunten van de WBP uiteen. Voor een algemene beschouwing over de rol en positie van privacybescherming zij verwezen naar paragraaf 1.2.

De Wet bescherming persoonsgegevens

5.1 Bestuursrechtelijke context

De overheid is geen eenvormig geheel. Rijksoverheid, provincies, gemeenten en waterschappen hebben alle hun eigen organisatie. Zeker op het niveau van het rijk is sprake van een conglomeraat van organen, diensten, instellingen en functies die onderling weer allerlei vormen van afhankelijkheid en samenwerking vertonen. In het perspectief van de rechtsstaat staat echter nog steeds voorop, dat taken en bevoegdheden voor specifieke doeleinden zijn toegekend aan bestuursorganen die bij de uitoefening daarvan gebruik kunnen maken van de onder hen ressorterende ambtenaren en diensten. Gaat er in het overheidsapparaat iets mis, dan kan de betrokken minister daarop in veel gevallen worden aangesproken in het parlement of bij de administratieve rechter. Een soortgelijke reactie is mogelijk bij provincies en gemeenten, al komen de meeste lijnen daar – anders dan bij het rijk – samen bij één bestuursorgaan.

De privacywetgeving sluit bij deze bestuursrechtelijke benadering aan. Zo bevat de WBP gedragsregels voor het bestuursorgaan dat voor een verwerking van persoonsgegevens[32] verantwoordelijk[33] is, ongeacht waar en op welke wijze die verwerking feitelijk plaatsvindt. In de praktijk is het van belang om eerst vast te stellen of er sprake is van een verwerking van persoonsgegevens in de zin van de wet, en om dan na te gaan wie als verantwoordelijke voor deze verwerking kan worden aangemerkt. Dat is óók van belang, omdat de inhoud van de gedragsregels in de regel nauw aansluit bij de specifieke taken en bevoegdheden ten dienste waarvan de verwerking plaatsvindt.

Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele invulling van het begrip. Het laatste criterium speelt met name een rol als er verschillende actoren bij de verwerking betrokken zijn en de juridische bevoegdheid onvoldoende helder is geregeld om te kunnen bepalen wie van de betrokken actoren als verantwoordelijke in de zin van de wet moet worden aangemerkt. In dat geval moet bij de overheid dus worden nagegaan aan welk bestuursorgaan de verwerking redelijkerwijs moet worden toegerekend.

Niet alleen de WBP bevat gedragsregels voor een bestuursorgaan. De regels van de WBP staan naast of gaan samen met andere wet- en regelgeving waaraan het desbetreffende bestuursorgaan onderworpen is. Het complex van toepasselijke regelgeving zal derhalve steeds in onderlinge samenhang moeten worden bezien. Zo bepaalt artikel 6 WBP dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt moeten worden. Deze zorgvuldigheidsnorm zal voor bestuursorganen mede worden ingevuld door de algemene beginselen van behoorlijk bestuur van de Algemene wet bestuursrecht. Artikel 6 WBP brengt tot uitdrukking dat geen gegevensverwerking mogelijk is die niet in overeenstemming is met de wet. Het woord ‘wet’ heeft mede betrekking op andere wetgeving inzake de verwerking van persoonsgegevens.

[32] Verwerking van persoonsgegevens is volgens de definitie van artikel 1, onder b, WBP: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Als persoonsgegeven geldt volgens artikel 1, onder a, WBP: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

[33] Een verantwoordelijke is volgens de definitie daarvan in artikel 1, onder d, WBP: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Het gaat hier dus om een schakelbepaling die verzekert dat de betrokken regelingen in onderling verband van toepassing zijn. Een voorbeeld om dit te illustreren. Het verzamelen van persoonsgegevens met als doel om op basis van die gegevens een met de Algemene wet gelijke behandeling (Awgb) strijdig onderscheid te maken[34], is niet toegestaan. Of er voor de verwerking wel een grondslag is te vinden in artikel 8 van de WBP is in dat geval niet relevant. De verwerking is onrechtmatig omdat het doel waarvoor gegevens worden verzameld in strijd is met een wettelijke bepaling, te weten de Awgb.

5.2 Verantwoordelijkheid

De WBP bevat regels voor het verwerken van persoonsgegevens. *Persoonsgegevens* zijn kort gezegd alle gegevens over een identificeerbare natuurlijke persoon. Verwerken kan alle handelingen omvatten tussen het verzamelen van persoonsgegevens en het vernietigen daarvan. Een belangrijk uitgangspunt van de wet is dat er altijd een instantie verantwoordelijk is voor de gegevensverwerking, die in voorkomende gevallen ook in rechte aansprakelijk kan worden gehouden voor situaties die in strijd zijn met de wet.
De wettelijke regels richten zich in de eerste plaats tot deze *verantwoordelijke*. Bij de overheid is dat steeds het betrokken bestuursorgaan, ook als het feitelijke handelen of nalaten zich buiten het directe zicht van het bestuursorgaan afspeelt. Dat laatste kan zich gemakkelijk voordoen bij uitbesteding aan externe dienstverleners, of bij samenwerkingsverbanden die in de praktijk min of meer een eigen leven leiden of waarvan de structuur onduidelijk is.

5.3 Doelbinding en rechtmatigheid

De WBP stelt voorop dat persoonsgegevens alleen voor vooraf nauwkeurig omschreven en gerechtvaardigde doeleinden mogen worden verzameld, en niet mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor de gegevens zijn verkregen (artikelen 7-9 WBP).

De WBP kent verschillende grondslagen voor het verwerken van persoonsgegevens. Bij bestuursorganen zal het in de regel gaan om die van artikel 8, onder e. Zij mogen op grond daarvan persoonsgegevens verzamelen als dat noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak.[35] Ook kan het gaan om een gegevensverwerking die noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke is onderworpen (artikel 8, onder c). Steeds dienen bestuursorganen bij het verwerken van persoonsgegevens terughoudendheid te betrachten: minimalistisch gegevensgebruik is het uitgangspunt.

Als persoonsgegevens voor verschillende doeleinden verwerkt worden, moeten deze doeleinden met elkaar verenigbaar zijn. Uitzonderingen op het principe van de doelbinding bij verdere verwerking zijn mogelijk, maar slechts zeer beperkt en zonder wettelijke basis niet structureel (artikel 43 WBP). Een registratie die als doel heeft het verstrekken van persoonsgegevens aan diverse soorten afnemers, zoals de GBA, dient om deze reden beperkt te blijven tot algemene basisgegevens en een wettelijke grondslag te krijgen.

In bepaalde gevallen gelden ten slotte additionele of strengere regels. Zo kunnen wettelijke en andere geheimhoudingsverplichtingen een overigens geoorloofde verstrekking blokkeren (artikel 9 WBP). Voor *bijzondere gegevens*[36] geldt een omgekeerd regime: zij mogen niet verwerkt worden, behoudens in een aantal specifiek in de WBP omschreven gevallen (artikelen 16-23 WBP).

[34] Hiervan is bijvoorbeeld sprake bij het registreren van gegevens omtrent iemands ras door een uitzendbureau teneinde cliënten van dit gegeven op de hoogte te stellen ten behoeve van de selectie van 'geschikte' kandidaten voor een baan.

[35] Meestal van het betreffende bestuursorgaan zelf, maar het kan ook gaan om een publiekrechtelijke taak van een bestuursorgaan waaraan gegevens verstrekt worden.

[36] Bijzondere gegevens zijn gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging, alsmede strafrechtelijke gegevens en bepaalde gegevens over hinderlijk gedrag.

5.4 Transparantie, de rechten van de burger, gegevenskwaliteit

Bij het verzamelen van persoonsgegevens dient het bestuursorgaan de betrokkene te informeren over de doeleinden waarvoor het de gegevens gaat gebruiken, tenzij deze daarvan al op de hoogte is. In sommige gevallen moeten ook andere bijzonderheden worden vermeld. Dit geldt ook als de persoonsgegevens uit andere bronnen zijn verkregen (artikelen 33-34 WBP). Bovendien mogen burgers verzoeken om inzage in en verbetering, aanvulling, verwijdering of afscherming van hun gegevens (artikelen 35-36 WBP). Ook kunnen zij zich op basis van bijzondere persoonlijke omstandigheden tegen een verwerking van hun gegevens verzetten (artikel 40 WBP). Het bestuursorgaan neemt in al deze gevallen een besluit dat vatbaar is voor bezwaar en beroep bij de rechter (artikel 45 WBP). Het bestuursorgaan dient er overigens ook zelf voor te zorgen dat de gegevens, gelet op de doeleinden van de verwerking, juist en nauwkeurig zijn (artikel 11 WBP).

Steeds vaker werken verschillende bestuursorganen samen in ketens waarbinnen gegevensuitwisseling plaatsvindt. Alle bestuursorganen in een keten hebben in principe dezelfde verplichtingen. Dat geldt bijvoorbeeld ook als de gegevens elders zijn verkregen, als een en ander bij wet geregeld wordt, of als er een geïntegreerd loket in het leven wordt geroepen om invulling aan de samenwerking te geven.

5.5 Informatiebeveiliging en Privacy-Enhancing Technologies

Informatiebeveiligingsexpert Bruce Schneier (1999) stelt terecht dat beveiliging geen product is, maar een proces. Daarmee wil hij aangeven dat vele componenten van een systeem of omgeving een rol spelen bij de beveiliging. Behalve de componenten zelf zijn hun onderlinge samenhang en interacties van belang. Bovendien geldt ook voor de beveiligingsketen dat deze slechts zo sterk is als de zwakste schakel.

Wanneer organisaties wordt gevraagd welke maatregelen zij hebben getroffen om de privacy te beschermen, wijzen zij er steevast op dat zij zich hebben ingespannen om de persoonsgegevens te beveiligen tegen ongeautoriseerde toegang. Daarmee is de bescherming van de privacy vrijwel geheel afhankelijk van het correct uitvoeren en functioneren van die beveiligingsmaatregelen. Beveiliging van persoonsgegevens is echter meer dan klassieke informatiebeveiliging.

Artikel 13

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De extra aan de beveiliging van persoonsgegevens te stellen eisen zijn opgenomen in artikel 13 van de WBP (zie kader). Informatiebeveiliging als een voortdurend proces omvat ook de beveiliging van persoonsgegevens als onderdeel van een duidelijk en actief privacybeleid.

Een goede manier voor het realiseren en in stand te houden van een duidelijk en actief privacybeleid is het opnemen ervan in de managementscyclus. Er kunnen dan drie belangrijke fasen worden onderscheiden, te weten het vaststellen, implementeren en evalueren van het privacybeleid. In de eerste fase ontwikkelt de organisatie een privacybeleid, op basis waarvan een beleid voor de verwerking van persoonsgegevens kan worden geformuleerd. In de tweede fase wordt het geformuleerde beleid geconcretiseerd naar specifieke maatregelen en procedures voor de verwerkingscyclus van persoonsgegevens. Gelet op de eisen van artikel 13 moeten hierbij zowel technische als organisatorische aspecten worden meegenomen. De derde fase betreft het evalueren en waar nodig bijstellen van het beleid en de maatregelen uit de andere twee fasen.

Artikel 13 WBP verlangt van de verantwoordelijke dat deze passende technische en organisatorische maatregelen neemt tegen verlies of onrechtmatige verwerking van persoonsgegevens. Daarbij gaat het niet alleen om traditionele beveiligingsaspecten als het garanderen van de integriteit en exclusiviteit van bestanden en berichten. Technische en organisatorische maatregelen kunnen het bestuursorgaan ook ondersteunen bij het voldoen aan de materiële voorwaarden voor gegevensverwerking en andere plichten uit de WBP.
Ketenafhankelijkheden brengen een zwaardere verplichting voor de betrokken bestuursorganen met zich mee.

Privacy-enhancing technologies (PET) kunnen in het bijzonder een bijdrage leveren aan het niet onnodig verzamelen of verder verwerken van persoonsgegevens. De Tweede Kamer heeft bij de behandeling van de WBP de regering bij motie opgeroepen om de toepassing van PET in haar eigen systemen voortvarend ter hand te nemen. De algemene lijn hierbij is dat gegevensverwerkende systemen bij voorkeur zodanig moeten zijn ingericht, dat de wettelijke randvoorwaarden daarin zoveel mogelijk zijn verankerd.

Bij het ontwerpen van structuren, processen en systemen is het nodig om al vanaf het prille begin rekening te houden met privacyaspecten. Het bewerkstelligen van een goede omgang met persoonsgegevens is dan naar verhouding eenvoudig, terwijl het hanteren van privacybepalingen in een niet daarop toegesneden omgeving vaak moeizaam blijkt. Op systeemniveau geldt net als op het infrastructurele niveau dat 'privacy by design' de manier bij uitstek is om optimaal gebruik te maken van de meer dan voldoende speelruimte voor het verwerken van persoonsgegevens die de wettelijke randvoorwaarden in de regel nog laten.

In bijlage 2 is van een aantal bouwstenen van informatie-infrastructuren aangegeven op welke manier zij als PET kunnen worden ingezet.

5.6 Tot slot

De hierboven behandelde privacyrandvoorwaarden vloeien direct of indirect voort uit Europese regelgeving. Ook specifieke wetgeving die in het leven wordt geroepen om de ontwikkeling naar een elektronische overheid te faciliteren, zal in overeenstemming met deze Europese regelgeving moeten zijn. In een complexe omgeving waarin meerdere partijen opereren, zijn goede procedures voor het onderhouden en bewaken van randvoorwaarden en waarborgen essentieel. Heldere protocollen, checklists, privacyreglementen en auditafspraken kunnen daartoe dienstig zijn, evenals het aanstellen van functionarissen voor de gegevensbescherming.[37] De randvoorwaarden gelden a fortiori voor (doorgaans complexe) gevallen van publiek-private samenwerking en hybride organisaties.

[37] Zie hiervoor Bijlage 3: Raamwerk privacy-audits en Bijlage 4: De functionaris voor de gegevensbescherming.

In de laatste twee hoofdstukken diepen we de privacyaspecten uit van twee belangrijke trends op het gebied van elektronische overheid. Hoofdstuk 6 gaat over pro-actieve dienstverlening, hoofdstuk 7 over de verdeling van overheidsdienstverlening over een frontoffice en een backoffice.

De overheid: pro-actieve dienstverlening

Pro-actieve dienstverlening is die vorm van dienstverlening waarbij de overheid op eigen initiatief het dienstverleningsproces naar de burger start. Er zijn twee hoofdvormen te onderscheiden, die ook in combinatie kunnen voorkomen:
– het gericht benaderen van de burger met een dienstverleningsaanbod;
– het automatisch uitvoeren van regelingen zonder tussenkomst van de burger.
Bij het gericht benaderen van burgers wordt vaak gebruik gemaakt van de persoonsgegevens waarover het bestuursorgaan in diverse administraties reeds beschikt. Soms is er een uitgebreidere verzameling persoonsgegevens voor nodig. De gegevens moeten dan bijeen worden gebracht door het koppelen van de bestanden van eigen diensten of andere bestuursorganen om een profiel van de betrokken burgers te verkrijgen. Deze aanpak wordt vaak gevolgd bij armoedebestrijding en kwijtschelding van gemeentelijke belastingen.

Voor het automatisch uitvoeren van regelingen heeft een overheidsdienst veelal persoonsgegevens nodig. Die worden dan niet direct van de burger verkregen, maar langs een andere weg. Dit kan door gegevens op te halen van andere diensten of bestuursorganen of door te koppelen met andere beschikbare bestanden bij de overheid. Deze werkwijze wordt gevolgd bij de prolongatie van kinderbijslag. Eenmaal aangevraagd wordt de kinderbijslag automatisch uitgekeerd aan de ouder zolang het recht daarop blijft bestaan.

Het uitwisselen van gegevens tussen instanties met een publiekrechtelijke taak is op zichzelf geen nieuw verschijnsel. ‘Publiekrechtelijke burenhulp’ in die vorm vindt al op grote schaal plaats. Meestal richt die zich op controle van de door de burger overgelegde gegevens en het elkaar inlichten over geconstateerde fraudegevallen. Bij pro-actieve dienstverlening is het doel anders, namelijk een meer externe oriëntatie van de overheid om de burger zoveel mogelijk met één gezicht tegemoet te treden.

Er zijn verschillende vormen van pro-actieve dienstverlening. In veel gevallen zal het tot de normale taakuitoefening van het bestuursorgaan behoren om de burger te wijzen op bepaalde rechten of nieuwe regelingen. Pro-actieve dienstverlening in die zin behoort tot de taak van het bestuursorgaan of ligt in het verlengde van uitvoering van een wettelijke regeling.

Van pro-actieve dienstverlening is daarnaast sprake bij het benaderen van burgers voor *andere* wettelijke regelingen. Diverse vormen kunnen hierbij onderscheiden worden. Het bestuursorgaan waarmee de burger reeds een rechtsverhouding heeft, wijst op eventuele aanspraken op andere regelingen die worden uitgevoerd door *hetzelfde* bestuursorgaan. Of het bestuursorgaan waarmee de burger reeds een rechtsverhouding heeft, wijst op eventuele aanspraken op regelingen die een *ander* bestuursorgaan uitvoert. Of een bestuursorgaan wijst de burger waarmee het *nog geen* rechtsverhouding heeft op eventuele aanspraken.

Pro-actieve dienstverlening heeft voor de burger ook minder aantrekkelijke kanten. Zo kan het zijn dat hem duidelijk wordt gemaakt dat hij niet voor bepaalde aanspraken in aanmerking komt, of aan bepaalde verplichtingen moet voldoen. Pro-actieve dienstverlening op basis van onjuiste of onvolledige gegevens kan bovendien leiden tot het niet benaderen van burgers die wel degelijk voor een dienst in aanmerking komen.

6.1 Algemeen kader

De kernvraag bij pro-actieve dienstverlening is of overheidsorganisaties de door hen geregistreerde persoonsgegevens mogen gebruiken om burgers gericht te

benaderen teneinde hen te wijzen op bepaalde rechten of verplichtingen. Om die te kunnen beantwoorden is het allereerst van belang om vast te stellen of er een wettelijke grondslag voor is. Als dat het geval is, dan is te bezien met welke nadere eisen of beperkingen in dat kader moet worden rekening gehouden.

6.2 Verzamelen

Artikel 7 WBP bepaalt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De doeleinden waarvoor de gegevens worden verzameld, moeten voorafgaand aan de verkrijging nauwkeurig vastgesteld zijn. Artikel 8 WBP bevat een limitatieve opsomming van gronden voor toelaatbare gegevensverwerking. Van gerechtvaardigde doeleinden van het verzamelen en vastleggen van persoonsgegevens kan alleen sprake zijn als deze met inachtneming van artikel 8 kunnen worden bereikt. Indien op grond van artikel 8 kan worden gesproken van een gerechtvaardigd doel, is daarmee ook voldaan aan het vereiste van artikel 7 dat persoonsgegevens voor een gerechtvaardigd doel moeten zijn verzameld.

In de sfeer van de overheid worden persoonsgegevens doorgaans in eerste instantie verzameld ter uitvoering van een specifieke publiekrechtelijke taak. Een gemeentelijke sociale dienst verkrijgt bijvoorbeeld persoonsgegevens over degene die een aanvraag doet voor een uitkering op grond van de Algemene bijstandswet (ABW). Een gemeente houdt een administratie van drank- en horecavergunningen bij. Artikel 8, onder e, WBP geeft aan dat een bestuursorgaan persoonsgegevens kan verwerken indien dat noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan. Bij het verzamelen van gegevens zal het bestuursorgaan doorgaans gebruik maken van de bevoegdheden die met het oog op de uitoefening van de desbetreffende taak zijn toegekend. De burger is in de regel verplicht om daaraan zijn medewerking te verlenen.

6.3 Verder gebruik

Zoals gezegd kunnen bepaalde vormen van pro-actieve dienstverlening rechtstreeks samenhangen met het doel waarvoor persoonsgegevens zijn verzameld. De WBP staat daaraan niet in de weg. Interessanter is de vraag of gegevens die zijn verzameld voor de uitvoering van een bepaalde wettelijke regeling verwerkt mogen worden voor *verdergaande* vormen van pro-actieve dienstverlening. Dat hangt af van de vraag of die verwerking eveneens berust op een wettelijke grondslag, en voorts of dat gebruik niet onverenigbaar is met het doel waarvoor de gegevens in eerste instantie zijn verzameld.

De WBP maakt geen onderscheid tussen het intern gebruiken van gegevens en het verstrekken van gegevens aan derden. Of gegevens die voor een bepaald doel zijn verkregen ook mogen worden verwerkt voor andere doeleinden, dient in alle gevallen beoordeeld te worden aan de hand van artikel 8 en 9 WBP. Het is niet waarschijnlijk dat persoonsgegevens die vastgelegd zijn in de meeste administraties, mede zijn verzameld met het doel om de betrokken burgers te benaderen over andere wettelijke regelingen. Het verzamelen zal doorgaans tot doel hebben om de uitvoering van bepaalde wettelijke taken mogelijk te maken.

Als een overheidsinstelling persoonsgegevens uit haar bestanden wil gaan gebruiken om een selectie te maken van bepaalde personen om deze mensen in opdracht van een andere instelling te wijzen op bepaalde rechten, of wanneer er een selectie gemaakt wordt om persoonsgegevens te verstrekken aan die andere instelling, moet dit dus van geval tot geval beoordeeld worden aan de hand van de zojuist genoemde algemene bepalingen.

Voor het verwerken van persoonsgegevens in het kader van pro-actieve dienstverlening dient dus eerst een grondslag gevonden te worden in artikel 8 WBP. In het algemeen kan er slechts een beroep worden gedaan op de grondslag genoemd onder c dan wel onder e. Artikel 8, onder c, WBP vereist dat de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is. De gegevensverwerking moet in dat geval noodzakelijk zijn ter uitvoering van een wettelijke verplichting. De verantwoordelijke moet ook aan die verplichting gebonden zijn. Een algemene wettelijke taakstelling valt niet onder deze bepaling. Voor bestuursorganen zal de grondslag onder e dan ook het meest in aanmerking komen. Dit onderdeel vereist dat de verwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan, dan wel door het bestuursorgaan waaraan de gegevens worden verstrekt. De gegevensverwerking moet derhalve zijn toegespitst op de goede vervulling van een publiekrechtelijke taak van het verstrekkende of ontvangende bestuursorgaan en de verwerking moet daarvoor noodzakelijk zijn.

Met de term 'noodzakelijk' wordt uitvoering gegeven aan het proportionaliteitsbeginsel, dat rechtstreeks voortvloeit uit artikel 8 EVRM. Het is een toetssteen voor de mate van inbreuk op de persoonlijke levenssfeer in gevallen waarin deze op zich gerechtvaardigd is.

Deze bepaling leidt er toe dat aandacht moet worden besteed aan de vraag in hoeverre de verschillende vormen van pro-actieve dienstverlening onderdeel uitmaken van een publiekrechtelijke taak van het desbetreffende bestuursorgaan. Ook zal bekeken moeten worden wat het effect is van deze dienstverlening: in hoeverre wordt het doel werkelijk bereikt? De inbreuk op de belangen van de betrokkene mag immers niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

Het subsidiariteitsbeginsel vloeit eveneens voort uit artikel 8 EVRM. Het doel waarvoor de gegevens worden verwerkt, dient in redelijkheid niet op een andere, voor de betrokkene minder ingrijpende wijze te kunnen worden verwezenlijkt. Kan bijvoorbeeld bekendheid worden gegeven aan een regeling door middel van algemene voorlichting? Kan de beoogde dienstverlening worden gerealiseerd door het (mee)zenden van informatie aan een doelgroep gelijktijdig met andere dienstverlening?

Een goed alternatief voor het verstrekken van gegevens aan derden is in veel gevallen het gebruik maken van gegevens binnen een organisatie. De organisatie die de gegevens verwerkt, maakt dan zelf een selectie en stuurt deze personen informatie van een andere organisatie mee. De selectie die de organisatie maakt, mag echter niet te ingrijpend zijn of gebaseerd zijn op allerlei gevoelige informatie. Zoals reeds is vermeld is ook het intern gebruik van gegevens aan regels gebonden.

6.4 Onverenigbaar gebruik

Indien een toereikende grondslag voor de gegevensverwerking bestaat, moet deze op grond van artikel 9 WBP niet onverenigbaar zijn met het doel waarvoor de gegevens in eerste instantie zijn verkregen. In artikel 9, tweede lid, staat met welke factoren hierbij in ieder geval rekening moet worden gehouden.

Van belang is bijvoorbeeld de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen. Een voorbeeld van een nauwe verwantschap is de verwerking van gegevens door een water-

schap van verzoeken om kwijtschelding en het gebruik van deze gegevens om kwijtschelding te verlenen voor volgende jaren. Ook kwijtscheldingen binnen gemeentelijke heffingenstelsels van verschillende aard kunnen op een dergelijke manier worden gerealiseerd. De verwantschap in de grondslag van de heffing, de benodigde gegevens en de rechtspositie van de betrokkenen zijn hierbij van belang. Ook het verwachtingspatroon van de burger speelt een belangrijke rol.

Verder moet rekening worden gehouden met de aard van de gegevens. Hoe gevoeliger het gegeven, hoe minder snel mag worden aangenomen dat er sprake is van verenigbaar gebruik indien bij enige verwerking wordt afgeweken van het oorspronkelijke doel. Voor gevoelige gegevens zijn bovendien specifieke regels opgenomen in de WBP. Voorts zijn de gevolgen van de beoogde verwerking voor de betrokkene van belang, de wijze waarop de gegevens zijn verkregen en de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Een niet verenigbare verwerking is bijvoorbeeld die wanneer een bestuursorgaan in het kader van pro-actieve dienstverlening allerlei voor verschillende doeleinden verkregen persoonsgegevens uit diverse bronnen met elkaar in verband brengt om een beeld te krijgen van de armoede van zijn burgers.

Wel verenigbaar is bijvoorbeeld de verstrekking door het ministerie van VROM van de NAW-gegevens van personen die huursubsidie ontvangen aan een gemeente ten behoeve van een bijdrage uit het woonlastenfonds. Het gaat in dit laatste geval om weinig gegevens en de doelen zijn aan elkaar verwant, namelijk het voorzien in de woonlasten van betrokkenen.

Artikel 43 WBP maakt het mogelijk om het verbod van onverenigbaar gebruik in artikel 9, eerste lid, in bijzondere gevallen buiten toepassing te laten voor zover dat noodzakelijk is in het belang van bijvoorbeeld de voorkoming, opsporing en vervolging van strafbare feiten. Het gaat hierbij om een uitzondering die alleen van geval tot geval en naar zijn aard restrictief kan worden toegepast. De wetgever kan in bijzondere wetten wel andere voorzieningen treffen, maar is daarbij gebonden aan de beperkingen van artikel 8 EVRM en Richtlijn 95/46/EG.

6.5 Geheimhouding en gesloten verstrekkingenregime

Indien er geen sprake is van onverenigbaar gebruik, kunnen toch andere blokkeringen bestaan voor pro-actieve dienstverlening. In artikel 9, vierde lid, WBP staat dat de verwerking van persoonsgegevens achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat.

Naast de algemene regels die hiervoor zijn genoemd, bestaat er voor overheidsinstanties soms specifieke wetgeving ten aanzien van de bescherming van persoonsgegevens. Denk daarbij aan de SUWI-wetgeving[38] en de Algemene bijstandswet (Abw). De Algemene bijstandswet kent bijvoorbeeld een gesloten verstrekkingenregime. Limitatief is in de wet opgenomen aan welke instanties sociale diensten gegevens mogen verstrekken (artikel 125 Abw). Verder kent de wet een stringente geheimhoudingsbepaling (artikel 123 Abw). Indien een instantie niet wordt genoemd in artikel 125 mag de sociale dienst slechts gegevens verstrekken indien een wettelijk voorschrift tot bekendmaking verplicht of indien degene op wie de gegevens betrekking hebben schriftelijk heeft verklaard tegen de verstrekking van deze gegevens geen bezwaar te hebben. Dit betekent overigens niet dat er een ongebreidelde gegevensuitwisseling mogelijk

[38] Zie bijlage 1.

is tussen de wel in artikel 125 genoemde instanties. Steeds wordt aangegeven voor de uitvoering van welke wetten gegevensverkeer mogelijk is.[39]

6.6 Conclusie

Pro-actieve dienstverlening door de overheid heeft vele verschijningsvormen. De WBP geeft in samenhang met sectorale wetgeving spelregels voor gegevensverwerking in het kader van pro-actieve dienstverlening. Deze vormen op zichzelf geen beletsel voor pro-actieve dienstverlening, maar zijn wel mede bepalend voor de vorm waarin deze kan worden uitgevoerd.

Vaak vormt het koppelen van bestanden met persoonsgegevens de basis voor pro-actieve dienstverlening. Daarbij is het van belang om van meet af aan een duidelijk beeld te hebben welke instanties welke gegevens gaan verstrekken en op grond van welke wettelijke bepalingen. Ook zal pro-actieve dienstverlening slechts effectief zijn als de gegevens die worden gebruikt voldoende actueel en van voldoende kwaliteit zijn voor koppeling. Bij gebreke daarvan kunnen in de praktijk de lasten van bestandskoppeling voor overheid en burger niet onaanzienlijk oplopen.

[39] Een bijzondere rol speelt de Belastingdienst als spin in het web van de informatiehuishouding van de overheid. In twee rapporten heeft de toenmalige Registratiekamer aandacht gevraagd voor het vergaren en verstrekken van gegevens door de Belastingdienst (De Zeeuw 1998, 1999).

De overheid: frontoffice en backoffice

7

De overheid heeft een veelheid aan taken. Deze taken variëren van klassieke activiteiten zoals het handhaven van de openbare orde en veiligheid, en het heffen van belastingen, tot het verlenen van vergunningen, het doen van uitkeringen, het geven van subsidie voor activiteiten die zij wil bevorderen zoals sport- en vrije tijdsbesteding, en het in stand houden van een infrastructuur. Bij een aantal van deze activiteiten heeft de overheid geen rechtstreeks contact met de burger. Voor andere activiteiten is contact met de burger wel noodzakelijk. De burger wenst iets van de overheid, de overheid moet presteren. Soms heeft de overheid persoonsgegevens nodig om de haar opgedragen taak uit te voeren, in andere gevallen is dat niet nodig.

Binnen het beeld van een presterende overheid valt een ontwikkeling waar te nemen. De uitvoering van taken wordt opgedeeld in twee fasen, namelijk een intake en een eerste deel van dienstverlening door een frontoffice en de verdere afwikkeling daarvan indien nodig door een backoffice.Het frontoffice verzamelt veelal een set basisgegevens voor de dienstverlening die de burger van de overheid wenst. Het backoffice beoordeelt of de burger voor de gevraagde dienstverlening in aanmerking komt. Afhankelijk van de situatie verifieert en controleert het de door de burger opgegeven gegevens bij andere instellingen of verstrekt het die gegevens juist aan ze.

De variëteiten van de werkwijze van een frontoffice en een backoffice kunnen in uitwerking verschillen van deze hoofdlijnen. Kern is evenwel dat de overheid de burger steeds vaker een loket op één locatie biedt voor verschillende vormen van dienstverlening. Dit loket kan ook een virtueel loket zijn. De dienstverlening wordt in dat geval aangeboden via internet.

Bij deze werkwijze van een frontoffice en een backoffice kan het gaan om een en hetzelfde bestuursorgaan met verschillende diensten of om een samenwerkingsverband van verschillende bestuursorganen. Een gevolg kan hoe dan ook zijn dat steeds meer onderdelen van de overheid via hun backoffices gaan samenwerken en informatie gaan uitwisselen. De backoffices kunnen daardoor versmelten tot één groot geheel dat over meer informatie over de burger beschikt dan elk van de backoffices afzonderlijk nodig heeft. Ook kan een taakverdeling ontstaan waarbij de kwaliteit van bepaalde gegevens vanuit authentieke bronnen wordt bewaakt en andere gebruikers daarop min of meer vertrouwen.

Doel van deze werkwijze is enerzijds onder meer klantvriendelijkheid voor de burger. Hij hoeft zich voortaan slechts te wenden tot één loket met zijn vraag. De overheid gaat van aanbodsturing naar een meer vraaggerichte wijze van functioneren. Voor de overheid is anderzijds ook efficiencyverbetering van de eigen werkprocessen beoogd. Door standaardisering en stroomlijning van gegevenssets wordt een betere en snellere informatie-uitwisseling tot stand gebracht. Dit moet onder meer leiden tot vermindering van de administratieve lasten voor het bedrijfsleven. Ook kunnen door deze wijze van werken fraude en misbruik beter worden bestreden. In bijlage 5 is schematisch weergeven in diverse modellen hoe de informatiehuishouding en de gegevensstromen in dit verband er in een aantal stadia van ontwikkeling uit kunnen zien.

Op verschillende momenten worden in de periode tussen de intake en het verlenen van de dienst aan de burger gegevens verzameld en vastgelegd, op basis waarvan nieuwe informatie wordt gegenereerd en gegevens worden verstrekt door diensten en bestuursorganen. Voor zover het in dit proces gaat om persoonsgegevens, is daarop de WBP van toepassing.

Deze wet bepaalt dat met de verzamelde gegevens zorgvuldig moet worden omgegaan. Van de betrokkene worden immers (vertrouwelijke) persoonsgegevens verzameld en verder verwerkt en op grond daarvan kunnen bestuursorganen voor de burger belangrijke beslissingen nemen. Voorkomen moet worden dat door de gegevensverwerking een onjuist beeld van de burger ontstaat. Verder moet worden voorkomen dat de betrokkene het zicht op de gegevensverwerking verliest doordat hij niet weet welke instantie zijn gegevens heeft of waarvoor ze worden gebruikt. Deze verschillende aspecten raken de privacy van betrokkene.

In het navolgende wordt nader ingegaan op de regels van de WBP alsmede op de beginselen die aan die regels ten grondslag liggen. Dit slechts voor zover deze van belang zijn in de context van een verdeling van overheidsdienstverlening over een frontoffice en een backoffice en de verschuivingen die zich in dat kader voordoen. Het gaat daarbij om in hoofdstuk 5 genoemde beginselen als doelbinding, transparantie, gegevenskwaliteit, rechten van betrokkene en beveiliging.

Bijzondere aandacht is op zijn plaats voor de vraag wie nu precies waarvoor verantwoordelijk is. De dynamiek van organisaties en technische hulpmiddelen mag niet tot gevolg hebben dat de verantwoordelijkheid en aansprakelijkheid voor het overheidshandelen langzaam minder duidelijk worden en gaandeweg dreigen te verdwijnen. Duidelijk moet zijn welk bestuursorgaan verantwoordelijk is voor welke verwerkingen van persoonsgegevens. Hoe complexer het samenwerkingsverband, des te meer is helderheid over taakverdeling en verantwoordelijkheidsverdeling noodzakelijk.

7.1 Verantwoordelijke

Voor gegevensverwerkingen in een frontoffice ligt de verantwoordelijkheid in de regel bij het bestuursorgaan dat belast is met de taak ten dienste waarvan de desbetreffende verwerkingen plaatsvinden. Dat bestuursorgaan is immers bevoegd om te beslissen over het doel en de middelen van de verwerking. Dat is ook het geval als het bestuursorgaan de uitvoering van verschillende taken via hetzelfde frontoffice laat verlopen. In situaties waarin meerdere personen, rechtspersonen of bestuursorganen betrokken zijn bij een keten van gegevensverwerkingen én in verband met de aard van die relatie ook in aanmerking komen om als verantwoordelijke te worden aangemerkt, is er behoefte aan een aanvullend criterium. Aan de hand van in het maatschappelijk verkeer geldende maatstaven moet in dergelijke gevallen worden bezien aan welke persoon, rechtspersoon of bestuursorgaan een bepaalde verwerking moet worden toegerekend.

Bij de verwerking van persoonsgegevens door een gemeenschappelijk frontoffice kan het problematisch zijn om de verantwoordelijkheid vast te stellen. Is er sprake van een gezamenlijke verantwoordelijkheid, dus alle betrokken bestuursorganen te samen voor het geheel? Een gedeelde verantwoordelijkheid, dus ieder bestuursorgaan voor zijn eigen deel? Of is het frontoffice zelf in staat om als verantwoordelijke in rechte op te treden? Richtinggevend voor de beantwoording van de vraag wie verantwoordelijke is, is de bestuursrechtelijke organisatie: maken frontoffice en backoffice deel uit van hetzelfde bestuursorgaan, gaat het om meerdere bestuursorganen, of is voor de uitvoering een aparte publiekrechtelijke of privaatrechtelijke rechtspersoon opgericht?

Vooraf kan in zijn algemeenheid niet duidelijk gesteld worden wie de verantwoordelijke is. Wel zullen in dergelijke samenwerkingsverbanden keuzen moe-

ten worden gemaakt die aanvaardbaar zijn met het oog op de doeleinden van het verzamelen, de transparantie en de uitoefening van de rechten van de betrokkenen. Een uitdrukkelijke regeling van de onderlinge verhoudingen verdient hierbij uiteraard de voorkeur.

Wat hiervoor is gesteld over de verwerkingen in het frontoffice, geldt in het algemeen ook voor die in het backoffice. Wel zal de verantwoordelijkheid voor verwerkingen in dat geval doorgaans eerder uit de bestaande zeggenschapsverhoudingen voortvloeien.

7.2 Doelbinding

Ook bij het verwerken van persoonsgegevens in situaties waarin sprake is van een frontoffice en een backoffice, moeten deze gegevens op grond van artikel 7 WBP voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en moeten de doeleinden voorafgaand aan de verkrijging bekend zijn.

Voor de verwerking van persoonsgegevens door het frontoffice is een precieze omschrijving van de doeleinden derhalve een eerste vereiste. Het uitgangspunt is daarbij dat de gegevens ook in deze situatie worden verzameld voor de uitvoering van een specifieke publiekrechtelijke taak. Indien bepaalde gegevens voor meer taken benodigd zijn, ligt het voor de hand om die gegevens slechts één keer te verzamelen en vast te leggen. Daarbij kan het gaan om verschillende taken van hetzelfde bestuursorgaan, maar ook om situaties waarbij het ene bestuursorgaan de intake verzorgt voor het andere. In al deze gevallen is het van belang ervoor te zorgen dat een bestuursorgaan alleen de beschikking krijgt over die persoonsgegevens die voor de goede vervulling van een aan dat bestuursorgaan opgedragen publiekrechtelijke taak noodzakelijk zijn.

Indien een bestuursorgaan op deze wijze – al dan niet ook voor een ander bestuursorgaan – persoonsgegevens verzamelt voor de uitvoering van verschillende publiekrechtelijke taken, zal de omschrijving van de doeleinden waarvoor de gegevens worden verzameld ruimer zijn dan anders. Dit kan bijvoorbeeld door het specificeren van meerdere doeleinden of subdoeleinden die corresponderen met de publiekrechtelijke taken voor de goede vervulling waarvan het verzamelen en vastleggen van de betrokken persoonsgegevens noodzakelijk is. Het is dan wel nodig dat de omschreven doeleinden in het verlengde liggen van elkaar of anderszins een zekere verwantschap vertonen.

In het licht van het voorgaande is net als bij pro-actieve dienstverlening artikel 9 WBP van belang. Dit artikel bepaalt dat gegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen. De vraag naar de verenigbaarheid van de verdere verwerking van persoonsgegevens dient zich bij de werkwijze van een frontoffice en een backoffice direct aan bij het moment van het verzamelen en de doeleinden daarvan. Een frontoffice kan dus niet zomaar alle persoonsgegevens verzamelen die nodig zijn voor de taakvervulling van alle verschillende daarop aangesloten bestuursorganen, zonder nadere beperking. Hier ligt een begrenzing van de één-loketgedachte. Wel is het mogelijk dat samenhangende taken - op een gestructureerde wijze en met behoud van het eigen karakter van die taken – vanuit één frontoffice worden ondersteund.

Ook bij het verdere gebruik van de aldus verkregen persoonsgegevens dient met de in hoofdstuk 5 behandelde algemene voorwaarden te worden rekening gehouden. Er dient dus steeds een toereikende grondslag gevonden te worden

in artikel 8 WBP. Daarbij zal in de regel gedacht kunnen worden aan de onderdelen c en e, die onderscheidenlijk betrekking hebben op gegevensverwerkingen die noodzakelijk zijn om een wettelijke verplichting na te komen waaraan de verantwoordelijke is onderworpen, en verwerkingen die noodzakelijk zijn voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan, dan wel door het bestuursorgaan waaraan de gegevens worden verstrekt. Daarnaast zal het in artikel 9 WBP gestelde verbod van onverenigbaar gebruik niet mogen worden overtreden, tenzij daarvoor hetzij een toereikende grondslag kan worden gevonden in specifieke wetgeving, hetzij in bijzondere gevallen een beroep kan worden gedaan op artikel 43 WBP.

Een en ander geldt dus ook voor de uitwisseling van persoonsgegevens met andere bestuursorganen vanuit de backoffices en voor het gegevensverkeer met authentieke registraties. In het laatste geval betekent dit dat in veel gevallen specifieke wetgeving nodig zal zijn die op de aard van de betrokken persoonsgegevens is toegesneden. Zoals eerder vermeld is de wetgever daarbij gebonden aan de beperkingen van artikel 8 EVRM en Richtlijn 95/46/EG.

7.3 Transparantie

Het beginsel van transparantie impliceert dat de verwerking van persoonsgegevens voor een ieder inzichtelijk moet zijn. Bijzondere aandacht verdient daarbij de transparantie voor de betrokken personen zelf. Deze transparantie wordt op verschillende niveaus bewerkstelligd.

In de eerste plaats is dit het geval door de melding van de verwerking bij het CBP of de functionaris voor de gegevensbescherming. In de melding wordt de gegevensverwerking geconcretiseerd zoals deze feitelijk geschiedt. De meldingen vinden plaats op grond van artikel 27 en 28 WBP en komen bij het CBP in een openbaar register. Ingevolge artikel 30, tweede lid, WBP kan een ieder dit register kosteloos raadplegen. Ingevolge artikel 30, derde lid, WBP is de verantwoordelijke verplicht om een ieder inlichtingen te verstrekken over de verwerking en informatie te verschaffen over die onderwerpen die in de melding moeten worden beschreven. Voor de verwerking van persoonsgegevens door een frontoffice of backoffice betekent dit dat deze zal moeten worden gemeld, tenzij deze verwerking is vrijgesteld van die verplichting op grond van het Vrijstellingsbesluit. Omdat dit besluit alleen betrekking heeft op eenvoudige en veel voorkomende standaardverwerkingen, ligt het niet voor de hand dat voor de bestaande praktijk van samenwerking tussen een frontoffice en backoffices anders dan bij uitzondering een vrijstelling zal bestaan van de meldingsplicht.

In de tweede plaats voorzien de artikelen 33 en 34 WBP in een verplichting om de betrokkene te informeren over de verwerking van persoonsgegevens door de verantwoordelijke. Deze bepalingen brengen met zich mee dat betrokkene bij de verkrijging van persoonsgegevens door het frontoffice onder meer moet worden geïnformeerd over het doel van de verwerking en de identiteit van de verantwoordelijke. Dat houdt in elk geval in dat een doel van de verwerking tevens is de verzameling van gegevens voor het backoffice van het betrokken of een ander bestuursorgaan. Afhankelijk van de situatie kan deze informatieplicht meer omvatten, als dat nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige gegevensverwerking te waarborgen en deze niet op een andere wijze op de hoogte is gebracht.

Deze informatieplicht geldt in principe ook bij verkrijging van persoonsgegevens door het backoffice, zij het dat er dan eerder sprake zal kunnen zijn van een uitzondering. Zo kan in deze situatie artikel 34, vijfde lid, WBP een rol

spelen. De informatieverplichting geldt volgens deze bepaling niet indien de vastlegging of de verstrekking is voorgeschreven bij of krachtens de wet. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

In paragraaf 3.2 hebben we betoogd dat het nodig is om aan de informatieplicht een actieve invulling te geven.

7.4 Rechten van betrokkene

De betrokkene moet te weten kunnen komen waarom zijn gegevens worden verzameld en welk gebruik ervan wordt gemaakt. De WBP geeft de betrokkene daartoe een aantal rechten naast het zojuist bedoelde recht om geïnformeerd te worden over de identiteit van de verantwoordelijke en het doel van de vastlegging van gegevens.

Ingevolge artikel 35, eerste lid, WBP heeft de betrokkene het recht om te weten of over hem gegevens worden verwerkt. Wanneer dit het geval is kan hij inzage vragen in zijn gegevens op grond van artikel 35, tweede lid, WBP. Wanneer zijn gegevens niet correct zijn kan hij verbetering vragen. Ook kan hij verzoeken om aanvulling, verwijdering of afscherming van zijn gegevens. Dit is geregeld in artikel 36, eerste lid, WBP.

Verder kan een betrokkene zich verzetten tegen bepaalde verwerkingen. Het relatieve recht van verzet dat de verantwoordelijke verplicht tot hernieuwde afweging, is geregeld in artikel 40 WBP. Het absolute recht van verzet dat met name geldt bij direct marketing, staat in artikel 41 WBP. Bij het verwerken van gegevens binnen een frontoffice en een backoffice van de overheid kan het relatieve recht van verzet een rol spelen. Het moet dan gaan om een verwerking die is gebaseerd op artikel 8, onder e of f, WBP. Hiervoor is er reeds op gewezen dat bij bestuursorganen de grondslag voor de verwerking veelal die van artikel 8, onder e, WBP zal zijn. De persoonlijke omstandigheden van betrokkene kunnen zich verzetten tegen een bepaalde verwerking door een bestuursorgaan. Dit moet dan een hernieuwde afweging maken en een besluit nemen, dat vatbaar is voor bezwaar en beroep op de rechter. Wil het verwerken behoorlijk en zorgvuldig zijn, dan kan het in bepaalde gevallen geboden zijn dat het bestuursorgaan de betrokkene wijst op dit relatieve recht van verzet. Alertheid van het bestuursorgaan lijkt op dit punt geboden.

De rechten van betrokkenen kunnen worden uitgeoefend tegenover het bestuursorgaan dat verantwoordelijk is voor de verwerking. Dat betekent dat een bestuursorgaan in de praktijk door betrokkenen kan worden aangesproken op alle verwerkingen waarover het zeggenschap heeft. Voor de behandeling van verzoeken om inzage of correctie, of voor de uitoefening van het recht op verzet bij overheidsdienstverlening via een frontoffice en een backoffice, zal een zorgvuldige procedure moeten worden ontwikkeld, waarbij de betrokkenen hun rechten op een eenvoudige manier kunnen uitoefenen en het bevoegde bestuursorgaan in voorkomende gevallen een juiste beslissing neemt. Bij samenwerking van verschillende bestuursorganen in ketens zal het bevoegde orgaan de betrokkene niet kunnen verwijzen naar een ander orgaan en zich ook niet zonder meer kunnen beroepen op het standpunt van een bestuursorgaan dat verantwoordelijk is voor de kwaliteit van de persoonsgegevens in een authentieke bron. Bij een goede regeling van de onderlinge relaties zal elk bestuursorgaan in de keten in staat zijn om de eigen verantwoordelijkheid te dragen en waar te maken.

De uitoefening van deze rechten kan in het gedrang komen als de verantwoordelijkheid binnen het samenwerkingsverband tussen een frontoffice en een backoffice onduidelijk is. Tot wie moet betrokkene zich dan wenden? Kan hij zijn rechten ook doen gelden bij het frontoffice voor de verwerking van de hem betreffende gegevens in het backoffice? Het contact verloopt via het frontoffice, dus het lijkt voor de hand te liggen dat hij zich daartoe wendt. Het frontoffice beschikt echter niet over alle gegevens in het backoffice. Moet het frontoffice het verzoek of betrokkene dan doorsturen naar het backoffice? Wanneer hierover geen duidelijke afspraken worden gemaakt die aan de betrokkenen worden medegedeeld, ontstaat er een onwerkbare situatie. Transparantie is ook op dit punt nu net een van de beginselen van een behoorlijke en zorgvuldige omgang met persoonsgegevens.

7.5 Gegevenskwaliteit

Het beginsel van de zorgplicht voor gegevenskwaliteit houdt in dat persoonsgegevens rechtmatig moeten zijn verkregen, en zoveel mogelijk juist en up-to-date moeten zijn. Artikel 6 WBP stelt voorop dat persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze moeten worden verwerkt. Dit artikel keert zich tegen die vormen van gegevensverwerking die als unfair of onbetamelijk moeten worden beschouwd.

Voorwaarde voor een eerlijke verwerking is onder meer dat de betrokkene van het bestaan van de verwerking kennis kan hebben en dat, wanneer van hem gegevens worden verkregen, deze daadwerkelijk en volledig wordt ingelicht over de omstandigheden waaronder deze verkrijging plaatsvindt. Voor samenwerkingsverbanden met een frontoffice en een backoffice betekent dit dat de betrokkene moet worden geïnformeerd over de samenwerking en in het bijzonder wat de rol van het frontoffice in dit geheel is.

Een ander aspect van de zorgplicht betreft de juistheid en volledigheid van de te verwerken persoonsgegevens. Artikel 11, eerste lid, WBP bepaalt dat persoonsgegevens slechts worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn. Het tweede lid van dit artikel bepaalt voorts dat de verantwoordelijke de nodige maatregelen treft dat de gegevens juist en nauwkeurig zijn. Het artikel legt op degene die gegevens verwerkt een verplichting op tot toetsing. Deze toetsing betreft zowel de aard van de gegevens als de hoeveelheid van de gegevens met betrekking tot de doeleinden van de verwerking. De toetsing van de juistheid van de gegevens is een inspanningsverplichting voor de verantwoordelijke. Een garantie van de juistheid van de gegevens kan niet in alle gevallen worden gevergd. De juistheid van de gegevens wordt mede bepaald door de context waarin ze worden gebruikt.

Binnen de context van een front- en backoffice zullen de gegevens in eerste instantie van de betrokkene zelf worden verkregen. Het frontoffice zal er meestal van uit moeten gaan dat de door de betrokkene verstrekte gegevens juist zijn. Het frontoffice kan afhankelijk van de aard van de gevraagde dienstverlening verlangen dat de burger ter ondersteuning van zijn verzoek documenten overlegt. De uiteindelijke controle van de juistheid van de opgegeven gegevens zal veelal plaatsvinden in het backoffice. Het bestuursorgaan dat daarvoor verantwoordelijk is heeft in de regel immers de bevoegdheid dan wel de wettelijke verplichting om deze gegevens te controleren en te verifiëren bij andere instanties.

Binnen een samenwerkingsverband met een frontoffice en een of meerdere backoffices kan in dit kader een situatie ontstaan waarin voor een gedeelte van de

controle van de juistheid van de gegevens bevoegdheden worden overgedragen aan het frontoffice. De controle vindt dan in een eerdere fase plaats. De precieze consequenties daarvan voor de verdeling van verantwoordelijkheden tussen de betrokken bestuursorganen zijn niet altijd even duidelijk.

7.6 Beveiliging

Binnen de samenwerking tussen een front- en een backoffice van bestuursorganen zullen hoge eisen worden gesteld aan de beveiliging vanwege de aanwezige risico's en de aard en omvang van de persoonsgegevens waar het om gaat. De beveiliging moet niet alleen zijn gericht op de doorgifte van de gegevens, maar ook op de inrichting van de informatiehuishouding en op het voorkomen van onnodige verzameling bij het frontoffice en verdere verwerking van persoonsgegevens bij het backoffice. Bij grootschalige vormen van samenwerking zal het beheer van de infrastructuur veelal zijn toevertrouwd aan een aparte rechtspersoon, die op zijn beurt vaak weer gebruik maakt van de diensten van uiteenlopende derden. De verantwoordelijkheid voor een juiste gang van zaken blijft ook dan steeds berusten bij het bestuursorgaan dat verantwoordelijk is voor de verwerking van de persoonsgegevens. Wel zal een dienstverlener in bepaalde gevallen als bewerker mede aansprakelijk kunnen zijn voor de schade die ontstaat door zijn werkzaamheid. De WBP vereist dan ook eveneens een goede regeling van de verhouding met voorkomende bewerkers (artikelen 14, 49 en 50 WBP).

Bezien van het gezichtspunt van beveiliging vraagt het virtuele loket bijzondere aandacht. Wanneer de burger zich aan het virtuele loket meldt, dient hij zich vaak te identificeren en te legitimeren. Het bestuursorgaan dient in veel gevallen met zekerheid te weten met wie het te maken heeft voor het verlenen van een dienst of voor de goede vervulling van zijn publiekrechtelijke taak. Een uittreksel, een vergunning, een uitkering etc. moet wel bij de persoon komen die daar recht op heeft. In de praktijk vindt de controle van de identiteit van de burger bij het virtuele loket plaats door hem unieke gegevens te laten opgeven waarover in het algemeen de burger alleen zelf beschikt en deze te controleren aan de hand van informatie die het bestuursorgaan over de burger heeft. In de toekomst zal de te ontwikkelen elektronische identiteitskaart hierbij een prominente rol gaan spelen.

7.7 Conclusie

Een samenwerkingsverband tussen bestuursorganen met een (gemeenschappelijk) frontoffice en verschillende backoffices leidt vanuit de optiek van de bescherming van persoonsgegevens tot verschillende aandachtspunten op uiteenlopende niveaus.

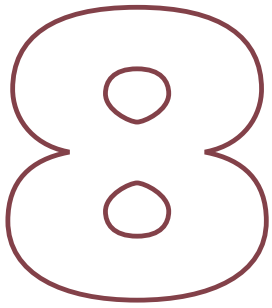
Voorop staat dat de verantwoordelijkheden van de betrokken bestuursorganen vooraf zo duidelijk mogelijk moeten worden afgebakend en verhelderd. Daarbij wordt ook duidelijk aan welke verplichtingen en randvoorwaarden deze bestuursorganen bij het inrichten van hun samenwerking gebonden zijn. Ook wordt zo voorkomen dat de betrokken burgers bij de uitoefening van hun rechten van het kastje naar de muur worden gestuurd, en dat de verantwoordelijkheid voor bepaalde onderdelen van het proces in de praktijk zoek raakt.

In de praktijk ontstaan nog wel eens problemen doordat de consequenties van de privacywetgeving pas in een te laat stadium worden onderkend, dan moeilijk kunnen worden ingepast en als knellend worden ervaren. Dit is eenvoudig te ondervangen door al in een vroeg stadium met deze consequenties rekening

te houden. Wanneer er dan afgewogen beslissingen worden genomen en deze ook in de organisatiesfeer zorgvuldig worden uitgewerkt, staat de privacywetgeving aan weinig legitieme doelstellingen in de weg.

De WBP stelt dus wel grenzen aan een samenwerkingsverband maar stuurt vooral de wijze waarop er samengewerkt kan worden. Waar deze grenzen precies liggen, hangt af van welke bestuursorganen zijn betrokken, welke publiekrechtelijke taken er worden uitgevoerd en het terrein waarop de samenwerking plaatsvindt.

Samenvatting



Deze studie is een bewerking van een notitie van het CBP uit december 2001. Het richt zich met name op diegenen bij de overheid die betrokken zijn bij de beleidsvorming op het gebied van elektronische overheid. De doelstelling van de studie is tweeledig:

- **een richting aangeven voor de ontwikkeling van een informatie-infrastructuur aan de hand van ontwerpprincipes die de bescherming van persoonsgegevens bevorderen;**
- **de speelruimte die de privacyregels laten illustreren aan de hand van een analyse van twee actuele thema's op het gebied van de elektronische overheid.**

Samenvatting

Infrastructuur

Binnen de elektronische overheid tekent zich een beweging af in de richting van het tot stand komen van een informatie-infrastructuur. Wil deze goed functioneren dan is het essentieel dat burgers er vertrouwen in hebben. De bescherming van persoonsgegevens verdient daarom ook op het infrastructurele niveau aandacht. Het gaat daarbij om het binnen de wettelijke randvoorwaarden vinden van een balans tussen privacy en andere belangen. Achteraf privacy inbouwen blijkt erg lastig, er dient daarom vanaf het prille begin rekening mee te worden gehouden. *Privacy by design* is het motto.

Identiteit

Er ontwikkelt zich een identiteitsinfrastructuur voor de overheid, die de basis zal vormen voor haar informatie-infrastructuur. Naast identiteiten zijn ook pseudo-identiteiten onmisbaar gereedschap bij privacybescherming in informatiesystemen. Niet-kenbaarheid is daarom een essentieel ontwerpprincipe voor de identiteitsinfrastructuur van de overheid.

Persoonsnummers spelen een belangrijke rol bij identiteitsmanagement. Nummerstelsels zonder onderliggend gedeeld probleem blijken moeilijk te beheren. Vanuit informatiekundig perspectief valt er daarom veel te zeggen voor een gedifferentieerde aanpak waarin verschillende sector- en ketennummers naast elkaar bestaan. Zo'n aanpak kan tegelijkertijd gezien worden als een bijdrage aan infrastructurele privacyborging.

Regie

Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Recent is er herhaaldelijk voor gepleit om dit vertrouwen te verankeren door de burger zoveel mogelijk de regie over zijn eigen persoonsgegevens in handen te geven. De burger kan zijn informatierelatie met de overheid op meerdere manieren inkleuren. Hoe meer hij de overheid vertrouwt, hoe kleiner zijn behoefte zal zijn om haar in de gaten te houden.

Regie over de eigen persoonsgegevens heeft twee facetten: zicht en zeggenschap. De overheid moet zorgen voor optimale transparantie. Zo krijgt de burger niet alleen zicht op, maar ook inzicht in de verwerkingen van zijn persoonsgegevens. Pas wanneer burgers inzicht hebben in de verwerkingen van hun persoonsgegevens is de tijd rijp om ze daar ook zeggenschap over te geven. Zelfs dan zullen zij echter niet alles wat de overheid met hun persoonsgegevens doet in detail kunnen of willen volgen. Informationele zelfbeschikking kent daarom haar grenzen. Bewust is in onder meer de Wet bescherming persoonsgegevens gekozen voor een systeem van 'checks and balances' waarin toestemming en verzet slechts een corrigerende rol spelen. Belangrijker is dat de overheid ook zonder regieaanwijzingen van de burger duidelijk en vertrouwenwekkend werkt. Doelbinding als ontwerpprincipe van haar informatie-infrastructuur kan daaraan een belangrijke bijdrage leveren.

Privacy by design
Het kenmerkende van een infrastructuur is dat het gaat om generieke basisvoorzieningen met een relatief permanent karakter. Om maatregelen ter bescherming van persoonsgegevens werkelijk in zo'n infrastructuur te verankeren is het nodig dat zij aan dezelfde karakteristieken voldoen. Alleen wanneer privacy op een robuuste manier wordt ingebouwd is zij ook op langere termijn te garanderen. Dit geeft het belang aan van ontwerpprincipes voor informatie-infrastructuren die de bescherming van persoonsgegevens tot een organisch onderdeel ervan maken.

Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Ontwerpprincipes die de bescherming van persoonsgegevens op zich ondersteunen zijn daarom niet voldoende. Eveneens moeten in de infrastructuur mechanismen verankerd worden die actief het vertrouwen van de burger in het privacyvriendelijk functioneren ervan bevorderen.

Analyses

Pro-actieve dienstverlening
Bij pro-actieve dienstverlening benadert de overheid de burger gericht met een dienstverleningsaanbod of voert zij regelingen zonder zijn tussenkomst automatisch uit.
- Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.
- Voor verder gebruik dat niet rechtstreeks samenhangt met deze doeleinden is een wettelijke grondslag nodig. Die zal er meestal in bestaan dat de gegevens noodzakelijk zijn voor het voldoen aan een wettelijke verplichting of het goed vervullen van een publiekrechtelijke taak.
- Een randvoorwaarde daarbij is dat dit niet ook op een minder ingrijpende manier mogelijk is.
- Ook moet het verder gebruik verenigbaar zijn met het doel waarvoor de gegevens zijn verkregen. Voor de beoordeling daarvan is onder meer van belang hoe nauw de oude en nieuwe doeleinden verwant zijn, de aard van de gegevens en het verwachtingspatroon van de burger.
- Tot slot kan een specifieke wettelijke geheimhoudingsplicht roet in het eten gooien.

De spelregels van de WBP in samenhang met sectorale wetgeving vormen op zichzelf geen beletsel voor pro-actieve dienstverlening, maar zijn wel mede bepalend voor de vorm waarin deze kan worden uitgevoerd. Pro-actieve dienstverlening zal slechts effectief zijn als de gegevens die worden gebruikt voldoende actueel zijn en geschikt zijn voor koppeling. Bij gebreke daarvan kunnen in de praktijk de lasten van bestandskoppeling voor overheid en burger niet onaanzienlijk oplopen. Tenslotte dient onder ogen te worden gezien of de beoogde positieve effecten voor de burger niet ook een schaduwzijde hebben.

Frontoffice/backoffice
Meer en meer deelt de overheid de uitvoering van haar taken op in twee fasen, namelijk een intake en een eerste deel van dienstverlening door een frontoffice en de verdere afwikkeling daarvan indien nodig door een backoffice. Het frontoffice verzamelt veelal een set basisgegevens voor de dienstverlening die de burger van de overheid wenst. Het backoffice beoordeelt of de burger voor de gevraagde dienstverlening in aanmerking komt. De overheid biedt de burger zo één, soms virtueel, loket voor verschillende vormen van dienstverlening.
- De verantwoordelijkheden van de betrokken bestuursorganen moeten hierbij vooraf zo duidelijk mogelijk worden afgebakend en verhelderd.

- Daarbij wordt ook duidelijk aan welke verplichtingen en randvoorwaarden zij bij het inrichten van hun samenwerking gebonden zijn.
- Ook wordt zo voorkomen dat de betrokken burgers bij de uitoefening van hun rechten van het kastje naar de muur worden gestuurd, en dat de verantwoordelijkheid voor bepaalde onderdelen van het proces in de praktijk zoek raakt.

In de praktijk ontstaan nog wel eens problemen doordat de consequenties van de privacywetgeving pas in een te laat stadium worden onderkend, dan moeilijk kunnen worden ingepast en als knellend worden ervaren. Dit is eenvoudig te ondervangen door al in een vroeg stadium met deze consequenties rekening te houden. Wanneer er dan afgewogen beslissingen worden genomen en deze ook in de organisatiesfeer zorgvuldig worden uitgewerkt, staat de privacywetgeving aan weinig legitieme doelstellingen in de weg.

De WBP stelt dus wel grenzen aan een samenwerkingsverband maar stuurt vooral de wijze waarop er samengewerkt kan worden. Waar deze grenzen precies liggen, hangt af van welke bestuursorganen zijn betrokken, welke publiekrechtelijke taken er worden uitgevoerd en het terrein waarop de samenwerking plaatsvindt.

Bijlagen

Bijlagen

Elektronische overheid: wat gebeurt er?

Bijlage 1

Hieronder schetsen we kort enkele van de talrijke ontwikkelingen op het gebied van elektronische overheid. De focus is gelegd bij initiatieven met een infrastructureel karakter. Zoveel mogelijk is aangesloten bij onderwerpen uit dit rapport: identiteitsmanagement, frontoffice en backoffice, en gegevensuitwisseling in de backoffice van de overheid (de basis voor pro-actieve dienstverlening). Daarnaast noemen we enkele initiatieven van algemene infrastructurele aard en op het gebied van administratieve lastenverlichting voor het bedrijfsleven.

Identiteitsmanagement

PKI overheid

www.pkioverheid.nl

PKI is een infrastructuur die ervoor zorgt dat mensen verzekerd kunnen zijn van de vertrouwelijkheid van elektronische communicatie en transacties. Twee belangrijke functies die met behulp van de PKI-infrastructuur kunnen worden gerealiseerd zijn het zetten van een elektronische handtekening en het versturen van beveiligde e-mail.

De doelstelling van de taskforce PKI overheid luidt:

"Het realiseren van een werkbare en betrouwbare infrastructuur voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers".

Nog dit jaar moet van een situatie bereikt worden waarbij voor vrijwel alle vormen van communicatie en transactie gebruik kan worden gemaakt van de infrastructuur die de taskforce heeft vastgesteld.

Elektronische identificatie

Onderdeel van het project Nieuwe Generatie Reisdocumenten is naast het nieuwe papieren paspoort de invoering een elektronische nationale identiteitskaart, de eNIK. Deze zal worden uitgerust met een elektronische handtekening. Het doel is gebruik te maken van technieken zoals PKI, biometrie en smartcards. De eNIK moet bijdragen aan betrouwbare identiteitsvastelling op de elektronische snelweg.

Modernisering GBA

http://www.bprbzk.nl

In maart 2001 publiceerde de tijdelijke Adviescommissie Modernisering GBA haar rapport GBA in de toekomst: *Gemeentelijke basisadministratie persoonsgegevens als spil voor toekomstige identiteits-infrastructuur*. De commissie onderkent daarin de ontwikkeling die gaande is in de richting van een overheidsinformatie-infrastructuur, waarbinnen identiteitsvragen een belangrijke rol zullen spelen. Een gemoderniseerde GBA zou in de toekomst een belangrijke faciliterende rol kunnen spelen bij het gebruik van geverifieerde en gelatiniseerde persoonsgegevens in het maatschappelijk verkeer. Daarbij kiest de commissie ervoor om de regie over deze persoonsgegevens zoveel mogelijk bij de burger zelf te leggen. Dat kan volgens haar door middel van de digitale kluis, die de burger een overzicht biedt van de over hem in de GBA opgeslagen gegevens. Daarnaast kan de burger zelf extra gegevens toevoegen, en deze naar eigen goeddunken ook aan derden ter beschikking stellen.

Basisregister Reisdocumenten

http://www.bprbzk.nl

Om fraude en misbruik met reisdocumenten tegen te gaan heeft het agentschap BPR een Basisregister Reisdocumenten ontwikkeld. Het systeem bestaat uit twee delen:

– Het Basisregister Reisdocumenten. De bedoeling is dat overheidsorganisaties die verantwoordelijk zijn voor de uitgifte van identiteitsdocumenten zelf een basisregister over die uitgegeven documenten moeten bijhouden.

– Het Verificatieregister. Hierin worden enkel reisdocumentennummers en het soort reisdocument opgenomen. Bij het opgeven van de nummers wordt de geldigheid van het document weergegeven.

Gebruikers die het verificatieregister willen raadplegen dienen eerst door BPR geautoriseerd te worden als gebruiker, na het maken van autorisatieafspraken kunnen de deelnemende organisaties de geldigheid van de reisdocumenten controleren.

Kiezen op afstand
http://www.ministervanboxtel.nl
In het project Kiezen op Afstand onderzoekt het ministerie van BZK of verkiezingen eenvoudiger en toegankelijker gemaakt kunnen worden door de toepassing van moderne informatie- en communicatietechnologie. Het doel van het project is het stemmen te moderniseren, aantrekkelijker te maken, mogelijke drempels om te gaan stemmen te verlagen en de betrokkenheid van de burger bij het democratisch proces te vergroten. Het eerste doel van het project is het mogelijk te maken dat de kiezer voor het uitbrengen van zijn stem niet langer gebonden is aan een bepaald stemlokaal, maar ook zonder daarvoor een kiezerspas te hoeven aanvragen zijn stem op een willekeurige stemlocatie kan uitbrengen. Hiervoor wordt een systeem van 'elektronisch stemmen op afstand' ontwikkeld. Daarnaast wordt onderzocht of het in de toekomst mogelijk zal zijn om 'internetstemmen' in te voeren, waardoor de kiezer via de computer thuis zou kunnen stemmen.
De hindernissen blijken in de praktijk tegen te vallen. In februari besloot het kabinet om het project voorlopig in de ijskast te zetten. Onduidelijk is of een geplande grootscheepse proef bij de Provinciale-Statenverkiezingen maart volgend jaar doorgang zal vinden.

Frontoffice en backoffice

Overheidsloket 2000
http://www.ol2000.nl
Onder motto's als "denken en werken vanuit de burger" en "burgers en bedrijven beter aan bod" wordt de een-loketgedachte verder uitgewerkt. Binnen het organisatieconcept OL2000 staan de realisatie van het vraaggericht aanbieden van diensten en de integratie van gefragmenteerde loketten centraal. De redenering hierachter is dat de totstandkoming van een fysiek of virtueel geïntegreerd loket de communicatie tussen overheid en burgers aanzienlijk zal verbeteren. Op drie domeinen (Bedrijven; Bouwen en Wonen; Zorg en Welzijn) wordt er gewerkt aan geïntegreerde loketten. Daarnaast wordt een generieke loketmodel ontwikkeld.

Sociale As
Burgers die inkomensondersteunende voorzieningen (zoals huursubsidie, bijzondere bijstand of thuiszorg) aanvragen moeten vaak herhaaldelijk gegevens verstrekken aan verschillende instanties. In het kader hiervan wordt onderzocht hoe de verbindingen tussen de verschillende loketten en backoffice met inzet van vraaggerichte methoden en andere ICT technieken tot stand kunnen komen. Door het uitvoeren van pilots wordt nagegaan of dienstverlening inderdaad vanuit een klantcontactpunt te realiseren is. Het doel is daarbij dat vanuit dat klantcontactpunt zowel het informeren/ bevragen van de burger kan plaatsvinden als het verlenen van de toegang tot het feitelijke administratieve, dienstverlenende proces.

SUWI
www.suwi.nl
De sector van de sociale zekerheid is sterk in beweging. De conclusie van de politieke en maatschappelijke discussie laat zich vertalen in de doelstelling: mensen sneller aan (betaalde) baan helpen waardoor de arbeidsparticipatie vergroot wordt zodat de kosten van de sociale zekerheid kunnen worden teruggedrongen. Via een doelgerichte, efficiënte en klantgerichte uitvoering van de wet- en regelgeving wordt er gewerkt aan de realisatie van het gestelde doel. Uiteindelijk heeft dit geleid tot de huidige Structuur Uitvoering Werk en Inkomen, beter bekend als SUWI. Hierbij blijven alle eerste klantcontacten, de behandeling van aanspraken op uitkeringen en het feitelijk verzorgen van uitkeringen binnen het publieke domein. De reïntegratie – activiteiten worden aan commerciële bedrijven overgelaten.
De gemeenten blijven verantwoordelijk voor de uitvoering van de Algemene bijstandswet (Abw). De vijf uitvoeringsinstellingen (Cadans, GAK, USZO, SFB en GUO) gaan samen in de Uitvoeringsinstelling werknemers verzekeringen (UWV). Centra voor Werk en Inkomen (CWI's) vormen het hart van de dienstverlening en zijn o.a verantwoordelijk voor de eerste intake ten behoeve van de gemeente en het UWV.
Ook is gewerkt aan een nieuwe ICT-infrastuctuur: SUWInet. SUWInet maakt de koppeling van decentraal opgeslagen elektronische gegevens mogelijk. Daarnaast is er beperkt sprake van 'nieuwbouw'.
Het bureau Keteninformatie Werk en Inkomen (BKWI) is per 2 januari 2002 opgericht en houdt zich bezig met het stroomlijnen en faciliteren van de informatiestromen binnen het SUWI cluster. Het bureau regelt afspraken betreft gegevensuitwisseling en ziet er toe dat die afspraken ook nageleefd worden.

Gegevensuitwisseling

Pro-actieve dienstverlening
Pro-actieve dienstverlening is die vorm van dienstverlening waarbij de overheid op eigen initiatief het dienstverleningsproces richting de burger start op basis van de informatie die reeds bij de overheid bekend staat. Anders dan een responsieve overheid neemt de overheid het initiatief richting de klant. Hierbij staat 'klant' voor burger, bedrijf, instelling of organisatie.
Pro-actieve dienstverlening beoogt onder meer om de rechtsgelijkheid te vergroten doordat burgers ontvangen waar zij aanspraak op kunnen maken. Burgers die er moeite mee hebben om de overheid op eigen initiatief te benaderen vormen een belangrijke doelgroep. Ook kan pro-actieve dienstverlening helpen om de werkprocessen bij de overheid beter te organiseren mede daardoor de beeldvorming over de overheid verbeteren.
In november 2001 heeft BZK een "Handboek pro-actieve dienstverlening" uitgegeven waarin de resultaten staan van het onderzoek naar welke overheidsdiensten zich voor pro-actieve dienstverlening lenen en aan welke randvoorwaarden die dan moet voldoen.

Stroomlijning Basisgegevens
www.stroomlijningbasisgegevens.nl
Het programma Stroomlijning Basisgegevens heeft tot doel om een belangrijke impuls te geven aan de totstandkoming van een stelsel van authentieke registraties, die door verschillende overheidsorganisaties worden of moeten worden opgezet. Met als uitgangspunt dat een bepaald gegeven slechts eenmaal door de overheid wordt verzameld en vervolgens verplicht door alle andere overheidsorgani-

saties wordt gebruikt. Voorwaarde voor iedere authentieke registratie is onder andere dat deze bij wet de enig officieel erkende registratie is voor de gegevens die erin voorkomen.
Er zijn twee actielijnen geformuleerd. Een actielijn beleidsontwikkeling, die gericht is op de ontwikkeling van een kader voor authentieke registraties. Voor de actielijn implementatie stuurt ieder ministerie zelf een deel van de activiteiten aan, bijvoorbeeld de ontwikkeling en invoering van een of meerdere authentieke registraties. Overheidsorganisaties kunnen een beroep doen op een stimuleringsregeling voor het op kleine schaal realiseren van het hergebruik van gegevens. Het programmabureau doet op deze wijze leerervaringen op.

Inlichtingenbureau
www.inlichtingenbureau.nl
Het Inlichtingenbureau maakt het mogelijk geautomatiseerd gegevens uit te wisselen tussen sociale diensten en de UWV, de Informatie Beheer Groep en de Belastingdienst. De ontvangen gegevens worden vervolgens onderling vergeleken. De vergelijking is erop gericht na te gaan of een persoon in dezelfde periode naast een Abw-uitkering een ander vorm van inkomen heeft, is ingeschreven bij een instelling van wetenschappelijk of hoger onderwijs of beschikt over vermogen.

De gegevensvergelijking binnen het Inlichtingenbureau vindt plaats op basis van het sofi-nummer. De gegevensvergelijking wordt uitgevoerd zowel voor de hoofduitkeringsgerechtigde als voor zijn of haar partner. Dit betekent dat ook eventuele inkomsten van een partner kunnen leiden tot een samenloopsignaal. Een samenloopsignaal is een indicatie dat er naast een uitkering sprake is van:
– een uitkering op basis van de WAO, ZW, WW, Wajong en WAZ;
– een inkomen uit een dienstverband.

Infrastructuur

RINIS
www.rinis.nl
RINIS realiseert een gestroomlijnde communicatie tussen de Sociale Zekerheid en gelieerde sectoren. Dat gebeurt door de inzet van gestandaardiseerde communicatie tussen de sectoren. Alle binnen een sector gebruikte definities en bestandsformaten hoeven daarom niet direct overboord.
Bij de uitwisseling van gegevens binnen het RINIS-concept zijn steeds drie partijen actief. Naast de sector die gegevens aanvraagt en de sector die gegevens aanlevert is dat de RINIS-organisatie. Die zorgt als intermediair voor de juiste routering, voor beheersbare software, voor standaardisatie, beveiliging, privacybescherming, helpdesk en coördinatie.
RINIS wisselt zelf geen gegevens uit en slaat deze ook niet centraal op. De RINIS-organisatie bewaakt uitsluitend de onderling gemaakte afspraken en ondersteunt het uitwisselingsproces, zowel technisch als organisatorisch.

Digitale Duurzaamheid
www.digitaleduurzaamheid.nl
De Taskforce Digitale Duurzaamheid brengt kennis en ervaring van overheidsorganisaties op het van digitaal informatiebeheer en kwaliteitszorg bij elkaar. Dit met het oog op de transparantie en toegankelijkheid van overheidsinformatie. Het geheugen van de overheid bestaande uit een verantwoorde efficiënte en kwalitatief goede digitale bedrijfsvoering, verantwoording naar de maatschappij en het culturele erfgoed. Daarvoor is het essentieel om de informatiehuishouding van de overheid in de backoffice op orde te krijgen en te houden.

Administratieve lastenverlichting

ICT en administratieve lasten

Als reactie op het rapport van de Commissie Administratieve Lasten startte de minister van Economische Zaken in juni 2000 een actieprogramma waarbij wordt beoogd door het inzetten van internet de administratieve lasten voor het bedrijfsleven terug te dringen. In het kader hiervan zijn verschillend projecten gestart gericht op het definiëren en implementeren van een gegevens- en procesarchitectuur ter ondersteuning van een online bedrijvenloket, vereenvoudigde uitwisseling van berichten en ontsluiting van wet- en regelgeving, formulieren en beslis- en rekenregels.

Elektronische Heerendiensten

http://213.160.207.40/ehd.php

De drie grootste gegevensvragers van de overheid zijn de Belastingdienst, het CBS en het UWV. In het programma Elektronische Heerendiensten (EHD) hebben zij een gemeenschappelijk model ontwikkeld door middel waarvan de meest gevraagde gegevens van bedrijven in een handomdraai uit de elektronisch opgeslagen administratieve gegevens van een bedrijf worden afgeleid. Vervolgens worden deze met één druk op de knop via internet beveiligd verzonden. In een test is aangetoond dat toepassing van het EHD-concept een aanzienlijke lastenverlichting oplevert.

Infrastructurele bouwstenen

bijlage 2

Een belangrijke bijdrage aan het informatie-infrastructurele denken is geleverd door Grijpink (1999). Hij constateert dat veel informatieproblemen in bedrijfsketens en organisatienetwerken communicatie met anderen betreffen. Daardoor zijn deze met klassieke informatisering niet op te lossen. Als alternatief stelt hij *keteninformatisering* voor. Deze benadering benadrukt het belang van de scheiding tussen registratie en communicatie, van afsprakenstelsels en van een 'kale' informatie-infrastructuur. Dit zijn eigenschappen die ook vanuit privacyoptiek waardevol kunnen zijn. Dat is geen toeval. Vaak blijken principes die bijdragen aan een juiste en behoorlijke omgang met persoonsgegevens ook vanuit algemeen informatiekundig perspectief zinnig.
Projecten als RINIS en Stroomlijning Basisgegevens vullen een gedeelte van de informatie-infrastructuur gedetailleerd in. Zij zal echter ook voor een groot deel bestaan uit een aantal lossere bouwstenen in de vorm van min of meer algemeen aanvaarde en beschikbare methoden en technieken.[42] Hieronder bespreken we privacyaspecten van enkele daarvan.

Definiëren, standaardiseren
Binnen één informatiesysteem of zelfs één organisatie is het weliswaar nodig om definities te hebben van de verwerkte gegevens, maar die kunnen vaak impliciet blijven, en er is vrijheid ten aanzien van hoe ze gedefinieerd worden. Wel valt er uit informatiekundig perspectief veel te zeggen voor expliciete en systematische gegevensdefinities. Voor gegevensuitwisseling tussen organisaties is het echter essentieel dat gegevens duidelijk gedefinieerd zijn. Gegevensuitwisseling verloopt moeizamer naarmate iedere organisatie meer haar eigen definities hanteert.

Er valt een grof onderscheid te maken tussen basisgegevens enerzijds en daarvan afgeleide gegevens anderzijds. Wanneer basisgegevens gedeeld worden, kan iedere organisatie haar eigen afgeleide gegevens daaruit bepalen. Uit basisgegevens als bruto salaris, overige inkomsten, bijzondere kosten en wat dies meer zij kan ieder organisatie volgens haar eigen definitie het afgeleide gegeven 'inkomen' bepalen. Wil dit goed werken, dan is het wel nodig dat voor alle basisgegevens een brede consensus bestaat over de definitie ervan.

Een alternatief is dat er een brede consensus wordt gevormd over een te hanteren definitie van een afgeleid gegeven. Eén instantie kan dit gegeven bepalen en het vervolgens verstrekken aan andere instanties die er ook recht op hebben. Wanneer bijvoorbeeld het belastbaar inkomen als standaard aanvaard wordt, kan de Belastingdienst dit uitrekenen en het vervolgens verstrekken aan andere instanties die het nodig hebben.[43]

Vanuit privacyperspectief is niet in het algemeen een voorkeur uit te spreken; beide opties hebben nadelen. De eerste mogelijkheid betekent dat er veel gedetailleerde gegevens op grote schaal verspreid worden. De tweede kan het een stuk eenvoudiger maken om gegevens uit verschillende registraties aan elkaar te koppelen.

Verwijzen
Wie binnen een informatie-infrastructuur een gegeven van elders wil betrekken krijgt niet alleen te maken met de vraag of het verstrekken en het verkrijgen van dat gegeven wel rechtmatig zijn, maar zal vaak ook niet op voorhand weten waar dat gegeven te halen is. Om tegemoet te komen aan dit laatste probleem dient de informatie-infrastructuur verwijsfaciliteiten te bieden. Verwijsinformatie bestaat uit identificerende gegevens (bijvoorbeeld NAW-gegevens of een sofi-nummer) met een verwijzing naar waar meer gegevens over de persoon in kwestie te vinden zijn. Hoewel verwijsgegevens dus in beginsel geen inhoudelijke gegevens zijn, kunnen ze indirect toch vaak bijdragen aan een beeld van iemand. Dat betekent dat niet zomaar iedereen toegang tot verwijsindexen mag krijgen. Die moet in beginsel beperkt worden tot

[42] Zie Grijpink (1999), blz. 92.

[43] Vaak zal dit zelfs kunnen via 'ontkoppeld koppelen' (zie hieronder bij 'verifiëren'). Daarbij beantwoordt de Belastingdienst slechts de vraag of iemands belastbaar inkomen al dan niet boven of onder een bepaalde grens zit.

verwijzingen naar informatie waar diegene ook toegang toe heeft. Helemaal oppassen wordt het als de informatie waarnaar verwezen wordt automatisch op te vragen is. Er dient dan voldoende aandacht te zijn voor de juiste autorisatieprocedures.

Verifiëren
Bij verificatie wordt er een vooraf gedefinieerde, gesloten vraag gesteld aan een informatiesysteem. Het systeem antwoordt eenvoudig met ja of nee. Andere benamingen voor deze techniek zijn 'hit/no hit-systeem' en 'ontkoppeld koppelen'. Een eenvoudig voorbeeld is dat een instantie de GBA bevraagt of een persoon al dan niet 18 jaar of ouder is. Verifiëren is op deze manier een privacyvriendelijk alternatief voor koppelen. Daarbij zou de geboortedatum opgevraagd worden om na te gaan of deze al dan niet 18 jaar in het verleden ligt.

Autorisatie
Toegangscontrole tot gegevens is een soort 'negatieve' bouwsteen, maar daarmee geen onbelangrijke. Om de kwaliteit van gegevens voldoende hoog te houden is het belangrijk dat alleen geautoriseerde personen ze mogen wijzigen. Als teveel mensen toegang zouden hebben tot bepaalde gegevens zou er aarzeling kunnen ontstaan om deze nog in het systeem op te nemen. Afgezien daarvan zijn er natuurlijk de regels over toegang tot persoonsgegevens die nageleefd moeten worden. Ook binnen organisaties geldt het doelbindingsprincipe: gegevens mogen alleen toegankelijk zijn voor diegenen voor wie dat uit hoofde van hun functie noodzakelijk is.
Autorisatie zou men kunnen zien als een privacy-enhancing technology, die naleving van de privacywetgeving bevordert: het is veel moeilijker om onbevoegd van gegevens kennis te nemen als het systeem je er gewoon niet bij laat komen. Bij PET in engere zin zou het systeem zo gebouwd worden dat zo min mogelijk sprake is van identificerende gegevens. Dit heeft als voordeel dat met veel eenvoudigere autorisatieprocedures kan worden volstaan. Zie verder paragraaf 5.4.

Signaleren
Grijpink omschrijft signaleren als 'het voortdurend vergelijken van twee gegevens op het voorkomen van een bepaald patroon en waarschuwen dat een gegeven een bepaalde waarde heeft'. Een soort koppelen in real-time dus. Een eenvoudigere vorm van signaleren, die uit het oogpunt van de behoorlijke omgang met persoonsgegevens echter ook belangrijk is, is het eenvoudig actief verstrekken van de informatie dat een bepaald gegeven gewijzigd is.
Wanneer deze mogelijkheid beschikbaar is als infrastructurele bouwsteen kan zij gebruikt worden om te bevorderen dat informatie actueel blijft, zodat een voldoende kwaliteit van de gegevens gewaarborgd kan blijven. In de praktijk blijkt dit soms een groot probleem te zijn, bijvoorbeeld bij het verzenden van afloopberichten in de strafrechtsketen en het voldoen aan de terugmeldplicht voor de GBA.

Raamwerk privacy-audit

bijlage 3

Ter ondersteuning van het proces voor het vaststellen, implementeren en evalueren van het privacybeleid is onder auspiciën van het CBP een productenset ontwikkeld bestaande uit de *Quickscan*, de *WBP Zelfevaluatie* en het *Raamwerk Privacy Audit*.

De *Quickscan* is een door elke medewerker in te vullen lijst met 13 vragen over de privacybescherming in de organisatie. De uitkomsten ervan geven een globaal beeld van hoe het met de privacybescherming in een organisatie is gesteld.

De *WBP Zelfevaluatie* is een instrument ten behoeve van het management van organisaties voor het verkrijgen van een oordeel over de implementatie en/of naleving van de bepalingen van de WBP. In de WBP Zelfevaluatie worden het ambitieniveau en de feitelijke stand van zaken met betrekking tot implementatie van de WBP in de organisatie met elkaar vergeleken. Desgewenst kan het management besluiten tot het laten uitvoeren van een (onafhankelijke) review op de uitgevoerde zelfevaluatie.

Het *Raamwerk Privacy Audit* is gemaakt voor het uitvoeren van een privacy audit in een organisatie door een gecertificeerde auditor. De uitkomst van een privacy audit geeft het management van een organisatie een hoge mate van zekerheid hoe het met de bescherming van de persoonsgegevens in de organisatie is gesteld.

Zie voor meer informatie: www.cbpweb.nl onder audit.

Bijlagen

Bijlage 4

De functionaris voor de gegevensbescherming

De WBP biedt overheidsorganisaties de mogelijkheid om een functionaris voor de gegevensbescherming aan te stellen. Deze houdt binnen de organisatie toezicht op de verwerking van persoonsgegevens en daarmee op de toepassing en naleving van de WBP. Meldingen van verwerkingen van persoonsgegevens kunnen bij deze functionaris worden gedaan. Tevens is hij een deskundig aanspreekpunt voor de verantwoordelijke. Ook kan hij als contactfunctionaris optreden voor de personen over wie persoonsgegevens worden verwerkt: burgers, personeelsleden en klanten.

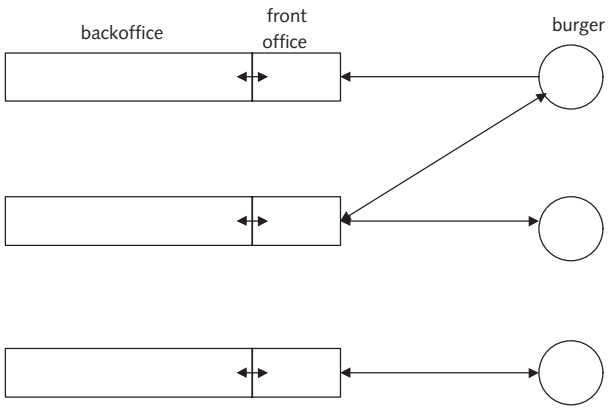
Het uitoefenen van toezicht door de FG kan meebrengen dat deze de verwerkingsprocessen binnen de organisatie inventariseert, dit met het oog op het nakomen van de meldingsverplichting. Van meldingen legt de FG een bestand aan. Klachten die betrekking hebben op het gebruik van persoonsgegevens kunnen door hem worden behandeld. Jaarlijks dient hij verslag te doen aan de verantwoordelijke van zijn werkzaamheden en bevindingen. Binnen de organisatie waarin hij werkzaam is, kan hij functioneren als vraagbaak. Collega's en de leiding kan hij adviseren inzake de toepassing van de WBP of een gedragscode die voor de branche geldt. Ook kan hij adviseren over het passende niveau van beveiliging van de informatiehuishouding in de organisatie en over maatregelen die zijn gericht op het beperken van de verwerking van persoonsgegevens.

Zijn positie en taak stellen de functionaris voor de gegevensbescherming er dus bij uitstek toe in staat om een belangrijke rol te spelen bij het vaststellen, implementeren en evalueren van het privacybeleid van de organisatie. Benoeming van zo'n functionaris zal – mits deze uiteraard naar behoren werkzaam is – ertoe leiden dat het CBP zich als nationale toezichthouder terughoudend opstelt ten aanzien van de betreffende organisatie.

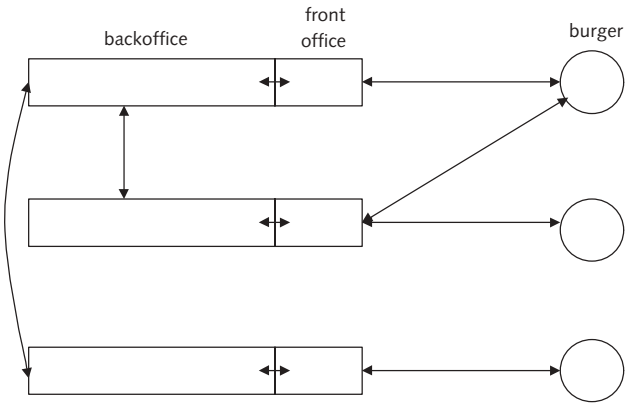
Zie voor meer informatie: www.cbpweb.nl onder FG

Modellen voor inrichting frontoffice en backoffice

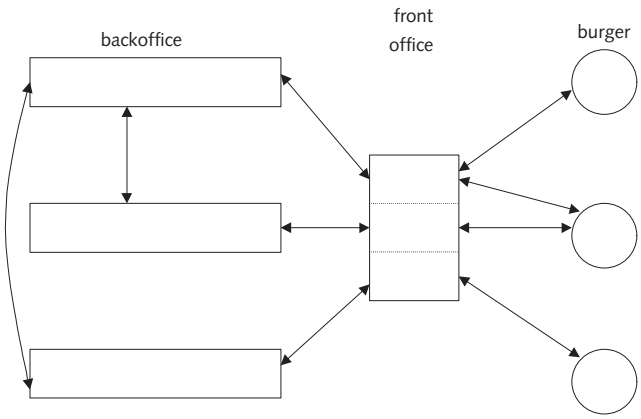
Bijlage 5



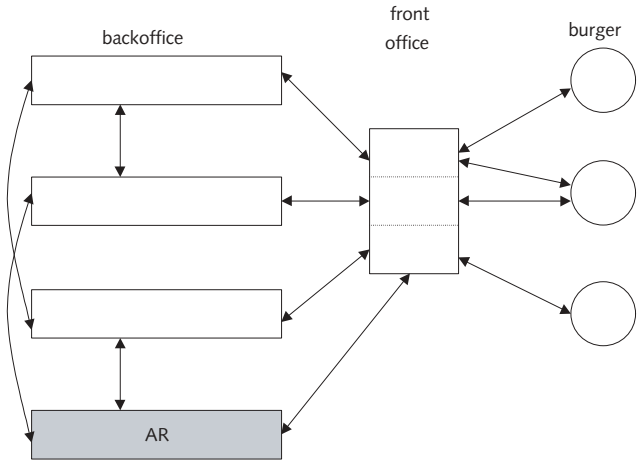
Model 1: **overheidsinstanties met gescheiden backoffice en frontoffice die onderling geen gegevens uitwisselen.**



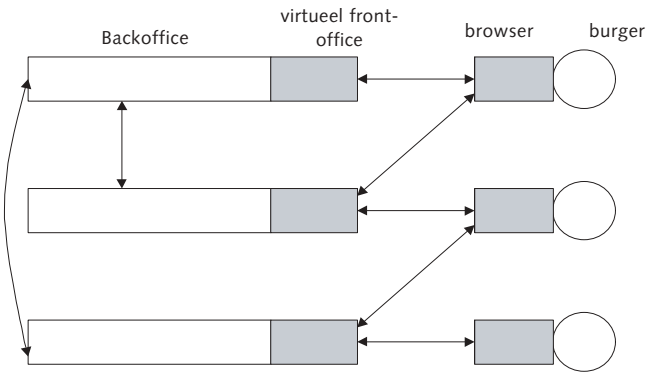
Model 2: **als model 1, maar nu wisselen sommige backoffices informatie met elkaar uit.**



Model 3: **als model 2, maar nu zijn ook de frontoffices (fysiek of operationeel) geïntegreerd (een-loketgedachte).**



Model 4: **als model 3, maar nu is er ook nog een authentieke registratie die gegevens levert aan (en krijgt teruggekoppeld van) zowel de backoffices als de front-offices van de andere instanties.**



Model 5: **als model 3, maar er is nu een *virtueel* frontoffice, waarmee de burger communiceert met behulp van zijn WWW-browser (geen-loketgedachte).**

Summary

This report is a revised version of a document published by the CBP in December 2001. It is aimed primarily at government employees involved in policymaking in the area of electronic governement. The goals of the report are twofold:

- **to indicate a direction for the development of an information infrastructure by means of design principles that further the protection of personal data;**
- **to illustrate the broad margins the privacy rules leave by means of an analysis of two current topics in the area of e-government.**

Summary

Infrastructure

Within e-government a development towards the establishment of an information infrastructure is taking shape. For this infrastructure to function properly it is essential that citizens have trust in it. The protection of personal data therefore deserves attention on the infrastructural level. The crux is to find a balance between privacy and other interests within legal boundaries. Building in privacy afterwards turns out to be really difficult, and therefore it should be taken into account from the very beginning. *Privacy by design* is the motto.

Identity

An identity infrastructure for the government is developing, which will form the basis for its information infrastructure. Besides identities, pseudo-identities are indispensable tools for protecting privacy in information systems. As a consequence pseudonimity is an essential design principle for a government identity infrastructure.

Unique identifiers play an important role in identity management. Systems of identifiers without an underlying common problem turn out to be hard to manage. Therefore from an information science point of view there is much to be said for a differentiated approach in which several sectoral and chain numbers co-exist. Such an approach can at the same time be considered a contribution to the infrastructural guaranteeing of privacy.

Control

Trust is an essential condition for a properly functioning information infrastructure. Recently it has been argued repeatedly that a good way of embedding this trust is by allowing citizens as much control of their own personal data as possible. Citizens can shape their information relationship with the government in different ways. The more they trust the government, the less they will feel the need to keep an eye on it.

The government must ensure *optimal* transparency. That way the citizen is provided not just with a *view of*, but also with *insight into* his personal data. Only when citizens have insight into how their personal data are processed, the time is ripe for also allowing them control of those data. Even then, however, they will neither be willing to nor able to keep track in detail of everything the government does with their personal data. Therefore informational self-determination has its limits. Intentionally in the Data protection act[40] a system of checks and balances was chosen in which consenting and objecting play only a correcting role. More important is that the government also works in a clear and trust-inspiring manner without direct instructions from its citizens. Finality as a design principle for its information infrastructure can be an important contribution to achieving this.

Privacy by design

Characteristic of an infrastructure is that it involves generic basic provisions of a relatively permanent character. In order to truly embed data protection mea-

[40] Wet bescherming persoonsgegevens (WBP).

sures in such an infrastructure they must have the same characteristic. Only when privacy is built in in a robust way it can be guaranteed in the long term. This illustrates the importance of design principles for information infrastructures that ensure that protection of personal data are incorporated as an organic part.

Trust is an essential condition for a properly functioning information infrastructure. Therefore design principles that support the protection of personal data are in themselves insufficient. Mechanisms must also be embedded in the infrastructure that promote citizens' trust in its privacy-friendly mode of operation.

Summary

Analyses

Pro-active services
Pro-active provision of services involves the government actively approaching a citizen with a specific service offer or carrying out measures automatically without the citizen intervening.

Personal data must be collected for specified, explicit and legitimate purposes. Further use not directly related to these purposes requires a basis in law. This will normally be that the processing is necessary to comply with a legal obligation or for the performance of a task carried out in the public interest. A condition then is that it not be possible to achieve this in a less intrusive way. Further use must also be compatible with the purpose for which the data have been collected; relevant factors include how closely the original and the new purposes are related, the nature of the data and the likely expectations of the citizen. Finally, a specific legal secrecy provision may stand in the way.

The rules of the Data protection act in connection with sectoral legislation in themselves are no impediment to providing pro-active services, but they do have a role in determining how this can be carried out. Pro-active services will only be effective when the data used are sufficiently up to date and suitable for matching. If this is not the case the cost of data matching for both government and citizen may be considerable. Finally it must be considered if the intended positive effects may not also have drawbacks for citizens.

Frontoffice/backoffice
More and more the government carries out its tasks divided into two phases, viz. an intake and first part of the service in a frontoffice and the completion thereof, if necessary, by a backoffice. The frontoffice often collects a set of basic data needed for the service the citizen wants the government to provide him. The backoffice assesses whether the citizen is eligible for the requested service. In this way, the government is able to provide a single (sometimes virtual) counter for different services.

The responsibilities of the government agencies involved must be clarified and demarcated as clearly as possible. This should also make it clear to which legal obligations and conditions they are bound when organizing their cooperation. In addition it prevents citizens from being sent from pillar to post when exercising their rights and serves to prevent the responsibility for certain parts of the process from going missing in practice.

In practice problems arise sometimes as a result of the consequences of privacy legislation being recognized in too late a stage, whence they are hard to fit in and felt to be restraining. This is easy to prevent by taking these consequences into account from the early stages. If at that time balanced decisions are taken

that are also worked out carefully in organisational terms, privacy legislation stands in the way of few legitimate purposes.

The Data protection act, then, poses limits to but mostly directs cooperation within government. Exactly where those limits are depends on the government agencies involved, the public interests served and the field in which cooperation takes place.

Literatuur

Adviescommissie Modernisering GBA (2001). **GBA in de toekomst: Gemeentelijke basisadministratie persoonsgegevens als spil voor toekomstige identiteitsinfrastructuur**. Den Haag. Beschikbaar op http://www.gba.nl.

Algemene Rekenkamer (1998). **Elektronische uitwisseling werknemersgegevens in de sociale zekerheid**. Den Haag.

Victor Bekkers (2001). **'De mythen van de elektronische overheid. Over retoriek en realiteit'**. Bestuurswetenschappen 2001, nr. 4, blz. 277–295.

Frank Biesboer (1998). **Wie bepaalt uw identiteit? Opstel over de Burgerservicekaart en informationele zelfbeschikking**. Den Haag: Rathenau Instituut. Werkdocument W 67. ISBN 90 346 3627 5.

Commissie ICT en overheid (2001). Burger en overheid in de informatiesamenleving: De noodzaak van institutionele innovatie. Den Haag. Beschikbaar op http://www.minbzk.nl.

Commissie Toekomst overheidscommunicatie (2001). **In dienst van de democratie**. Den Haag.

Ian Goldberg (2000). **A Pseudonymous Communications Infrastructure for the Internet**. PhD Thesis. Berkeley, CA: University of California at Berkeley.

Jan Grijpink (2001). **Nummerstelsels en nummerstrategie: Bijdrage aan het maatschappelijk debat over de wenselijkheid van een openbaar verplicht algemeen persoonsnummer in Nederland**. Den Haag: Ministerie van Justitie.

Jan Grijpink (1999). **Keteninformatisering met toepassing op de justitiële bedrijfsketen: Een informatie-infrastructurele aanpak voor communicatie tussen zelfstandige organisaties**. Den Haag: Sdu Uitgevers. 2e druk.

Jeroen van den Hoven (2000). **Wadlopen bij opkomend tij: Denken over ethiek en informatiemaatschappij**. Inaugurele rede Erasmus Universiteit Rotterdam.

Peter Hustinx (2001). **Privacy, data protection and informational self-determination**. Paper presented at the Spring Conference of European Data Protection Commissioners, Athene, 10-11 mei 2001.

Bert-Jaap Koops (2001). **'Een nieuwe GBA, digitale kluisjes en identificatiedrang'**. Nederlands Juristenblad 2001, afl. 32, blz. 1555-1561.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2001). **Voortgangsrapportage Stroomlijning Basisgegevens**. Brief van de minister voor grote steden- en integratiebeleid aan de Tweede Kamer. Kamerstukken II, 2001-2002, 26387, nr. 11.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2000). **Contract met de toekomst**. Kamerstukken II, 1999-2000, 26387, nr. 8.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (1998). **Actieprogramma elektronische overheid**. Kamerstukken II, 1998–1999, 26387, nr. 1.

Ministerie van Binnenlandse Zaken (1995). **Terug naar de toekomst: Over het gebruik van informatie en informatie- en communicatietechnologie in de openbare sector**. Beleidsnota Informatiebeleid Openbare Sector 3. Kamerstukken II, 1994-1995, 20644, nr. 23.

Ministerie van Binnenlandse Zaken (1991). **BIOS II: De computer gestuurd**. Beleidsnota Informatiebeleid Openbare Sector 2. Kamerstukken II, 1990-1991, 20644, nr. 15.

Ministerie van Binnenlandse Zaken (1988). **Beleidsnotitie Informatievoorziening Openbare Sector**. Kamerstukken II, 1987–1988, 20644, nr. 2.

Bruce Schneier (1999). **Secrets and Lies: Digital Security in a Networked World.** New York: John Wiley & Sons.

Koen Versmissen (2001). **Sleutels van vertrouwen: TTP's, digitale certificaten en privacy**. Den Haag: Registratiekamer, 2001. Achtergrondstudies en Verkenningen 22. Beschikbaar op http://www.cbpweb.nl.

Jan de Zeeuw (1999). **Informatieverstrekking door de fiscus: Ontheffing van de geheimhoudingsplicht in het licht van privacywetgeving**. Den Haag: Registratiekamer, 1999. Achtergrondstudies en Verkenningen 16. Beschikbaar op http://www.cbpweb.nl.

Jan de Zeeuw (1998), **Informatiegaring door de fiscus: Privacybescherming bij derdenonderzoeken**. Den Haag: Registratiekamer 1998. Achtergrondstudies en Verkenningen 8. Beschikbaar op http://www.cbpweb.nl.

Lijst van afkortingen

ABW	Algemene bijstandswet
BIOS	Beleidsnotitie Informatievoorziening Openbare Sector
BPR	Basisregistratie Persoonsgegevens en Reisdocumenten
BZK	(Ministerie van) Binnenlandse Zaken en Koninkrijksrelaties
CBP	College bescherming persoonsgegevens
EU	Europese Unie
EVRM	Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
GBA	Gemeentelijke basisadministratie persoonsgegevens
ICT	Informatie- en communicatietechnologie
NAW	Naam, adres, woonplaats
OSV	Organisatiewet sociale verzekeringen
PET	Privacy-enhancing technologies
PKI	Public-key infrastructure
SUWI	Structuur Uitvoering Werk en Inkomen
UWV	Uitvoeringsinstelling werknemersverzekeringen
VROM	(Ministerie van) Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
WBP	Wet bescherming persoonsgegevens
WPR	Wet persoonsregistraties

Verantwoording

Deze studie is een bewerking van een notitie van het CBP uit december 2001[41]. Deze verantwoording licht de relatie met de notitie van december 2001 toe.

Evenals de notitie richt deze studie zich met name op diegenen bij de overheid die betrokken zijn bij de beleidsvorming op het gebied van elektronische overheid.

De studie valt uiteen in twee delen.

Infrastructurele aspecten vormen de invalshoek van de eerste vier hoofdstukken.

- In hoofdstuk 1 constateren we dat er een informatie-infrastructuur voor de overheid aan het ontstaan is. We behandelen in abstracte zin de rol die de bescherming van persoonsgegevens speelt bij de totstandkoming daarvan. In de volgende twee hoofdstukken gaan we vanuit de privacyoptiek op zoek naar ontwerpprincipes voor de informatie-infrastructuur van de overheid. We doen dat aan de hand van twee thema's.
  - Hoofdstuk 2, een bewerking van paragraaf 5.2 van de notitie, gaat over identiteitsmanagement.
  - Hoofdstuk 3, een bewerking van paragraaf 5.3 van de notitie, gaat over regie over de eigen persoonsgegevens.
- In hoofdstuk 4 bundelen we de opgedane inzichten tot een visie op van persoonsgegevens in de informatie-infrastructuur van de overheid.

Concrete ontwikkelingen vormen de invalshoek van de laatste drie hoofdstukken.

- In hoofdstuk 5, een bewerking van hoofdstuk 3 van de notitie, zetten we kort de hoofdpunten van de privacywetgeving op een rijtje.
- In de volgende twee hoofdstukken diepen we de privacyaspecten uit van twee belangrijke trends op het gebied van elektronische overheid.
  - Hoofdstuk 6, vrijwel identiek aan paragraaf 4.1 van de notitie, gaat over pro-actieve dienstverlening.
  - Hoofdstuk 7, vrijwel identiek aan paragraaf 4.2 van de notitie, gaat over de verdeling van overheidsdienstverlening over een frontoffice en een back-office.zs

[41] J.A.G. Versmissen en A.C.M. de Heij (2001). *Elektronische overheid en privacy*. Den Haag: College bescherming persoonsgegevens. Het CBP bedankt alle personen en organisaties die het bij zijn beeldvorming hebben ondersteund door te reageren op deze notitie.

Achtergrondstudies en verkenningen

In de serie Achtergrondstudies en verkenningen zijn verschenen:

Eijk, M.M.M. van en Helden, W.J. van, **Klant te koop, Privacyregels voor adressenhandel**. A&V 24; College bescherming persoonsgegevens, Den Haag 2001.

Blarkom, G.W. van, **Beveiliging van persoonsgegevens**. A&V 23; Registratiekamer, Den Haag 2001.

Versmissen, J.A.G., **Sleutels van vertrouwen, TTP's, digitale certificaten en privacy**. A&V 22; Registratiekamer, Den Haag 2001.

Terstegge, J.H.J., **Goed werken in netwerken, regels voor controle op e-mail en internetgebruik van werknemers.** A&V 21 (1e druk; Registratiekamer, Den Haag 2000) 2e druk, herzien door drs. S. Lieon, College bescherming persoonsgegevens, Den Haag 2002.

Buitenhuis, R., Campen, N.G.M. van, Helden, W.J. van, Vries, H.H. de, **Bankverzekeraars en privacy, gegevensverwerking in financiële conglomeraten**. A&V 20; Registratiekamer, Den Haag 2000.

Helden, W.J. van, **Herkomst van de klant, privacyregels voor etnomarketing**. A&V 19; Registratiekamer, Den Haag 2000.

Wishaw, R.W.A. **De gewaardeerde klant, privacyregels voor credit scoring**. A&V 18; Registratiekamer, Den Haag 2000.

Artz, M. en Eijk, M.M.M. van, **Klant in het web. Privacywaarborgen voor internettoegang**. A&V 17; Registratiekamer, Den Haag 2000.

Zeeuw, J. de. **Informatieverstrekking. Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving**. A&V 16; Registratiekamer, Den Haag 2000.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M. **At face value. On biometrical identification and privacy**. A&V 15; Registratiekamer, Den Haag 1999.

Artz, M.J.T., Koning **Klant. Het gebruik van klantgegevens voor marketingdoeleinden**. A&V 14; Registratiekamer, Den Haag 1999.

Borking, J.J., e.a., **Intelligent software agents and privacy**. A&V 13; Registratiekamer, Den Haag 1999.

Hooghiemstra, T.F.M., **Privacy & Managed care**. A&V 12; Registratiekamer, Den Haag 1998.

Hes, R. en J. Borking, **Privacy-enhancing technologies: the path to anonimity**. A&V 11 revised edition; Registratiekamer, Den Haag 1998.

Almelo, L. van, e.a., **Gouden bergen van gegevens. Over datawarehousing, datamining en privacy**. A&V 10; Registratiekamer, Den Haag 1998.

Zandee, C., **Doelbewust volgen. Privacy-aspecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling**. A&V 9; Registratiekamer, Den Haag 1998.

Zeeuw, J. de, **Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken**. A&V 8; Registratiekamer, Den Haag 1998.

Hulsman, B.J.P. en P.C. Ippel, **Gegeven: de Genen. Morele en juridische aspecten van het gebruik van genetische gegevens**. A&V 7; Registratiekamer, Den Haag 1996.

Gardeniers, H.J.M., **Chipcards en privacy. Regels voor een nieuw kaartspel**. A&V 6; Registratiekamer, Den Haag 1995.

Rossum, H. van e.a., **Privacy-enhancing technologies: the path to anonymity, volume I and II**. A&V 5; Registratiekamer, Den Haag 1995.

Rommelse, A.F., **Zwarte lijsten. Belangen en effecten van waarschuwingssystemen**. A&V 4; Registratiekamer, Rijswijk 1995.

Rommelse, A.F., **Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer.** A&V 3; Registratiekamer, Rijswijk 1995.

Casteren, J.P.M. van, **Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden**. A&V 2; Registratiekamer, Rijswijk 1995 (niet meer beschikbaar).

Hulsman, B.J.P. en Ippel, P.C., **Personeelsinformatiesystemen - de Wet persoonsregistraties toegepast**. A&V 1; Registratiekamer, Rijswijk 1994 (niet meer beschikbaar).

Vrijwel alle publicaties van het CBP kunt u inzien en/of downloaden van de website www.cbpweb.nl. Voor het toezenden van gedrukte publicaties kunnen kosten in rekening worden gebracht.