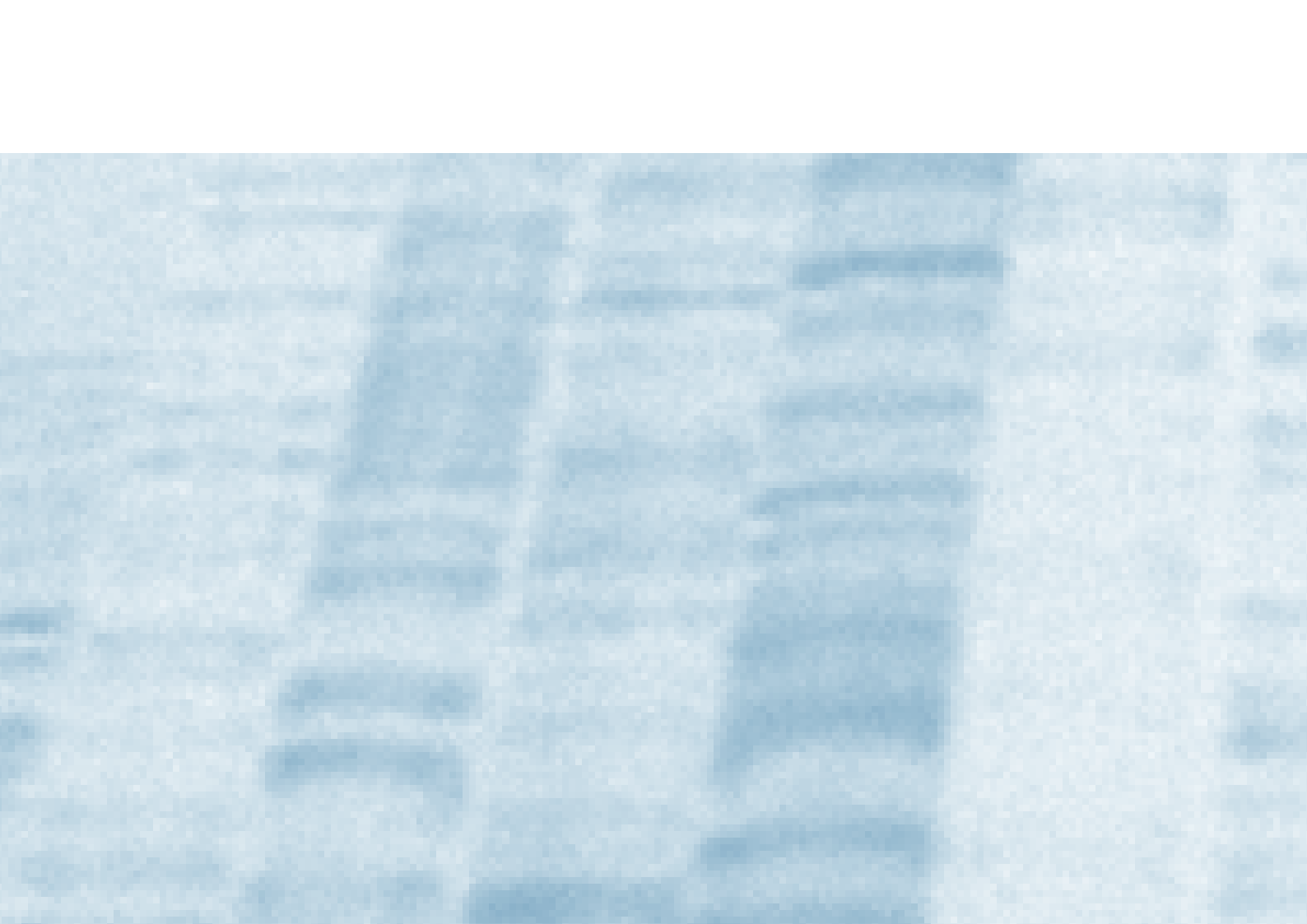




jaarverslag 2006



Iedereen heeft recht op een zorgvuldige omgang met zijn of haar persoonsgegevens.

Het College bescherming persoonsgegevens bevordert de naleving van de wettelijke regels die zien op de bescherming van persoonsgegevens, zo nodig met behulp van sancties.

Daarbij heeft het CBP oog voor de maatschappelijke context van de aan hem voorgelegde problemen of klachten. Bij het uitvoeren en verantwoorden van zijn werkzaamheden streeft het naar een open dialoog met de samenleving en naar samenwerking met andere maatschappelijke organisaties.

Bij alle maatregelen...

Inleiding door Jacob Kohnstamm, voorzitter CBP.

pagina 2

Samenstelling College en Raad van Advies

Door de benoeming van Madeleine McLaggan-van Roon is het College sinds 1 september 2006 weer voltallig.

pagina 6

2006 in vogelvlucht

Globaal overzicht van de terreinen waarop het CBP in 2006 actief is geweest, een kort overzicht van het onderzoek in 2006 en de lijst met doelen voor 2007.

pagina 8

Activiteiten van het CBP

Een bloemlezing van het werk van de toezichthouder, sectoroverstijgend, in internationale context en op verschillende maatschappelijke en beleidsterreinen.

pagina 25

Organisatie

De snelle maatschappelijke ontwikkelingen die van invloed zijn op privacy en de verwerking van persoonsgegevens stellen eisen aan de beleidskeuzes en de organisatie van het CBP.

pagina 60

Bijlagen

Overzichten van wetgevingsadviezen, onderzoeksrapporten, gedragscodes, modelreglementen, documenten van de Europese Artikel 29-werkgroep en publicaties van het CBP.

pagina 72

Summary

- Preface by Jacob Kohnstamm, chairman of the Dutch DPA
- Summary of activities and results in 2006 and objectives for 2007

page 82

> **Waar zitten mensen mee?**

Jaarlijks krijgt het CBP zo'n 7800 brieven, e-mails of telefoontjes binnen. Het grootste deel daarvan is afkomstig van 'gewone mensen die niets te vrezen hebben', maar die boos zijn, zich zorgen maken of schade ondervinden door al dan niet opzettelijk onverantwoorde of onzorgvuldige verwerking van hun persoonsgegevens. Voorbeelden van hun vragen zijn in dit jaarverslag uitgestrooid.



Bij alle maatregelen...

'Bij alle maatregelen verantwoordt de overheid de gevolgen voor de privacy van de burgers'. Deze voor de bescherming van de persoonlijke levenssfeer veelbelovende beleidslijn besloten CDA, PvdA en CU in het coalitieakkoord als opdracht aan het toen nog te vormen kabinet mee te geven.

De meest uiteenlopende activiteiten kunnen gevolgen hebben voor de privacy van gewone burgers en de noodzaak zich in de private en publieke sector rekenschap te geven van deze gevolgen neemt ontegenzegglijk toe. Allerlei vormen van technische innovatie scheppen in combinatie met internet en bestaande ICT schier oneindige mogelijkheden voor informatievergaring en communicatie van deze informatie. De voordelen daarvan springen direct in het oog. We omarmen allen de nieuwe mogelijkheden tot ontplooiing van mensen, tot betere en effectievere private en publieke dienstverlening, tot verantwoorde vormen van productie. Verfijnde logistieke systemen, via persoonsnummers gekoppelde elektronische overheidsdossiers voor gemakkelijke dienstverlening aan de burger, publieke en financiële dienstverlening via internet, de OV-chipkaart, online handel in vliegtickets, software, films, muziek en andere goederen, mobiele communicatie van spraak, beeld en tekst, multiplayer online role playing games, weblogs en chat-programma's, krachtige zoekmachines en continue nieuwsvoorziening: we beleven een revolutie even grenzeloos als uitdagend.

Al dat moois heeft ook een keerzijde. Al deze toepassingen van ICT maken grote hoeveelheden persoonsgegevens in principe beschikbaar voor analyse, profilering, opsporing en controle. Zonodig wordt wellicht het bewaren ervan wettelijk verplicht gesteld om dat mogelijk te maken, zoals bij de 'verkeersgegevens' van alle telecommunicatie van bijna een half miljard EU-burgers. Deze grenzeloze mogelijkheden kunnen mensen en de samenhang in de samenleving lelijk opbreken. Want wie bepaalt en handhaaft in een wereld waar de technologie alle grenzen slecht, de normen en waarden die iedere samenleving nodig heeft om leefbaar te blijven, om 'de boel een beetje bij elkaar te houden'? Welke maatschappelijke consequenties heeft het feit dat een bedrijf, overheid of individu iemands handel en wandel van minuut tot minuut in kaart zal kunnen brengen? Hoe veilig en vertrouwd zullen mensen zich in zo'n samenleving nog voelen?

Het leidt geen twijfel dat de mogelijkheden om gegevens over de persoonlijke levenssfeer en het gedrag van individuen voor een ieder inzichtelijk en bruikbaar te maken aan banden moet worden gelegd. Wanneer iemand op een zwarte lijst op internet wordt geplaatst, heeft het bijvoorbeeld tot gevolg dat die persoon – mogelijk volstrekt ten onrechte – voor onbepaalde tijd aan een mondiale schandpaal te kijk wordt gezet. Wanneer een argeloos jong mens een opname met een webcam via internet verzonden heeft, is het de vraag of deze persoon jaren later op een volstrekt onverwacht moment daarmee geconfronteerd mag worden in een sollicitatieprocedure. Zo kan ook de koppeling van via internet verzonden zoekopdrachten aan allerlei andere databestanden – waaronder opnames met videocamera's – tot verdenkingen of profilering leiden die kant noch wal raken. Het 'hergebruik' van een beperkt aantal over een persoon verzamelde en gekoppelde gegevens kan tot kostbare en rampzalige vormen van identiteitsfraude en -diefstal leiden. Mensen die onnadenkend en totaal onverantwoord zeiden toch niets te verbergen te hebben, zullen van een koude kermis thuiskomen omdat steeds achteraf zal blijken dat zij nergens en nimmer meer onbespied of ongeregistreerd door het leven zijn gegaan.

Techniek, zeker als de optimale inzet daarvan wordt gekoppeld aan efficiencydoelstellingen, is 'waardenloos'. De wetgever heeft er met de Wet bescherming persoonsgegevens en een aantal andere wetten en wettelijke bepalingen voor gezorgd dat het verzamelen en verwerken van gegevens door private en publieke organisaties wel degelijk langs bepaalde normen en waarden dient te worden gelegd: verzamel gegevens niet dan nadat is vastgesteld dat dat noodzakelijk is; gebruik die verzamelde gegevens in beginsel niet voor een ander doel dan waarvoor ze oorspronkelijk verzameld werden; behandel verzamelde persoonsgegevens ook overigens zorgvuldig en met respect.

In het krachtenveld van de geschetste technisch-maatschappelijke ontwikkelingen is de handhaving van het normenstelsel zoals neergelegd in de Wet bescherming persoonsgegevens er al met al niet gemakkelijker op geworden - zeker niet voor een terughoudend gefinancierde toezichthouder. Voor het CBP is het zaak om scherpe en evenwichtige keuzen te maken bij de beantwoording van de vraag hoe en op welke terreinen wij de bescherming van persoonsgegevens in het bijzonder tot gelding moeten brengen.

Het voornemen van de coalitie om bij alle maatregelen de gevolgen voor de privacy van de burgers te verantwoorden, levert daartoe in ieder geval een welkome bijdrage.

J. Kohnstamm

voorzitter



A blue-tinted photograph of four people walking across a street. From left to right: a woman in a patterned skirt and jacket, a man in a suit, a woman in a dark suit, and a woman in a dark suit with white trim. They are walking towards the camera. In the background, there are trees and a white van.

Samenstelling

college en raad van advies

College 2006



mr. J. Kohnstamm
Voorzitter



mw. mr. dr. J. Beuving
Collegelid, plv. voorzitter



mw. mr. M.W. McLaggan-van Roon
Collegelid (per 1 september 2006)

Raad van Advies 2006

mw. prof. mr. I.P. Asscher-Vonk

Hoogleraar sociaal recht Radboud Universiteit Nijmegen, lid SER

R. Bandell

Burgemeester van Dordrecht

mr. G. Corstens

Raadsheer in de Hoge Raad (tot 2 februari 2006)

prof. mr E. Dommering

Hoogleraar informatierecht Universiteit van Amsterdam

mw. drs. A. van Es

Oud-lid van de Tweede Kamer

prof. dr. E.J. Fischer

Bijzonder hoogleraar bedrijfsgeschiedenis Universiteit van Amsterdam

prof. mr. H. Franken (voorzitter)

Hoogleraar informaticarecht Universiteit Leiden

prof. mr. J.K.M. Gevers

Hoogleraar gezondheidsrecht Universiteit van Amsterdam

mw. drs. K. de Jonge

Directeur Consumentenbond

drs. R. van Ommeren

Oud-lid Raad van Bestuur ABN-AMRO

drs. C. Rog

Voorzitter commissie privacy VNO-NCW

drs. L.J.E. Smits

Directeur Het Expertise Centrum

Directie



mw. ing. C.E. Romanesko

Directeur

Buitengewoon lid College 2006

mr. dr. U. van de Pol

Ombudsman Amsterdam



2006 in vogelvlucht

Privacybescherming roept uiteenlopende reacties op. Een zeer gangbare is: 'Ik vind dat niet zo nodig. Ik heb niets te vrezen, want niets te verbergen en veiligheid is belangrijker dan mijn privacy'. Een andere: 'Het maakt mij niet veel uit. Ze weten toch al alles van je'. En een derde: 'Het is heel belangrijk dat dat gebeurt, want je wilt toch niet voortdurend bespied door het leven gaan'. Het CBP blijft zich inzetten voor het vinden van een goede balans tussen veiligheids-, controle- en utiliteitsbelangen en het zoveel mogelijk garanderen van de bescherming van de persoonlijke levenssfeer die door die belangen onder druk kan komen te staan.

Het recht op integriteit van de persoonlijke levenssfeer waar een zorgvuldige omgang met persoonsgegevens onlosmakelijk mee verbonden is, wordt in toenemende mate als minder vanzelfsprekend beschouwd. Waar dit grondrecht geschoffeld dreigt te raken onder veiligheids- en opsporingsbelangen of verdampt in de grenzeloze mogelijkheden die het internet en andere technologische ontwikkelingen bieden, heeft de toezichthouder een taak als alerte 'privacy-waakhond'. Controle op de naleving van de Wbp is zijn taak bij uitstek. Maar effectief toezicht en zonodig handhaving van de regels voor de omgang met persoonsgegevens is niet voldoende. Door voorlichting, advisering en overleg met maatschappelijke partijen treedt het CBP proactief op om burgers, overheden, bedrijven en instellingen te doordringen van de noodzaak om zorgvuldig met persoonsgegevens om te gaan. Omwille van vergroting van het vertrouwen dat gewone mensen die niets te verbergen hebben moeten kunnen stellen in instanties die met hun gegevens omgaan. En omwille van verbetering van de kwaliteit van wetgeving en dienstverlening. Dit hoofdstuk geeft een globaal overzicht van het werk van de toezichthouder in het afgelopen jaar.

Veiligheid en controle

Van twee kanten wordt de bescherming van de persoonlijke levenssfeer belaagd. Aan de ene kant breiden overheden uit veiligheidspolitieke overwegingen op nationaal, regionaal en internationaal niveau hun bevoegdheden om proactief grote hoeveelheden data over steeds grotere groepen burgers te verzamelen drastisch uit.

Aan de andere kant worden door steeds verfijndere technieken en koppeling van databestanden de mogelijkheden om de handel en wandel van een ieder te volgen en te registreren steeds groter.

De internationale conferentie van toezichthouders waaraan het CBP jaarlijks deelneemt, waar schuwt in november 2006 dat het wat de bescherming van gegevens betreft de vraag is of de traditionele methoden van toezicht met het oog op de nieuwe technieken nog wel voldoen. Gezamenlijke actie om tegengas te geven aan overmatige vormen van controle is geboden, aldus de toezichthouders.

Passagiersgegevens

Uiterlijk in augustus 2007 moet een nieuwe overeenkomst in werking treden tussen de Verenigde Staten en de Europese Unie over de verstrekking van passagiersgegevens door luchtvaartmaatschappijen aan de VS. De Artikel 29-werkgroep van Europese toezichthouders op de gegevensbescherming, waar het CBP deel van uitmaakt, is bezorgd over de thans geldende tijdelijke afspraken die de opmaat vormen voor het te sluiten verdrag, omdat zij een bredere verspreiding van de informatie onder de Amerikaanse autoriteiten voor ook weer nieuwe doeleinden mogelijk lijken te maken. De voorzitter van het CBP onderstreept tijdens een bijeenkomst in december 2006 te Brussel dat duidelijk moet worden gemaakt dat de te nemen veiligheidsmaatregelen noodzakelijk en proportioneel zijn en wijst op het belang van transparantie en verantwoording.

Justitie- en politiesamenwerking

De daadkracht van de regeringen van de EU-lidstaten als het gaat om het invoeren van veiligheidsmaatregelen waarbij grensoverschrijdende gegevensuitwisseling centraal staat, steekt schril af tegen het aannemen van het Europees Kaderbesluit bescherming persoonsgegevens ten behoeve van politie- en justitiesamenwerking. Volgens de Europese toezichthouders is de enige werkbare optie voor een ruimere uitwisseling van persoonsgegevens een geharmoniseerde hoge beschermingsstandaard in de derde pijler. Dit geldt ook voor overdracht van gegevens aan derde landen en aan internationale instellingen. Een beperkte benadering zal volgens de

toezichthouders in de praktijk niet werkbaar blijken en bovendien afbreuk doen aan vertrouwen in de samenwerking tussen politie en justitie op Europees niveau.

Opsporing terroristische misdrijven

In Nederland is in het kader van de terrorismebestrijding de laatste jaren sprake van een cumulatieve van bevoegdheden van de politie en van justitiële autoriteiten. Het CBP heeft de afgelopen jaren de minister van Justitie en de Tweede Kamer geadviseerd over het wetsvoorstel tot verruiming van de opsporing en vervolging van terroristische misdrijven. De kritiek van het CBP richt zich vooral op het ontbreken van een deugdelijke motivering van de noodzaak van de voorgestelde maatregelen, waaronder een ruimer verkennend onderzoek naar bepaalde groepen in de samenleving. Omdat aan de punten van kritiek op veel punten geen gevolg is gegeven, heeft het CBP in 2006 op verzoek van de voorzitter van de Eerste Kamer de vaste commissie van Justitie van de Senaat nader geadviseerd over de maatregelen die volgens hem nodig zijn om een beter evenwicht te bereiken tussen toezicht op de verwerking van persoonsgegevens en de groeiende macht van de strafvorderlijke autoriteiten.

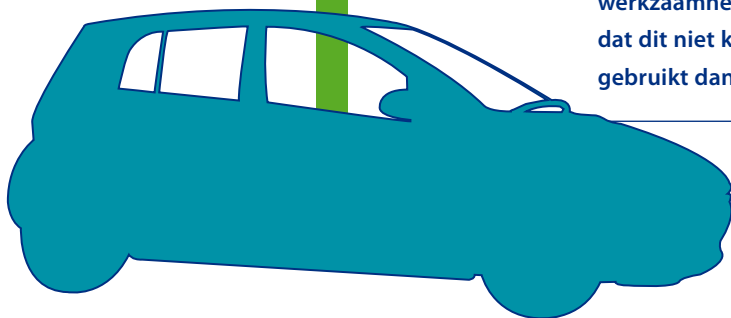
Themaverwerkingen

De vervagende grens tussen opsporings- en vervolgingsbevoegdheden heeft onmiskenbaar implicaties voor de bescherming van persoonsgegevens. Een van de grote vernieuwingen die de nieuwe Wet politiegegevens zal meebrengen is het invoeren van de zogeheten themaverwerking. Door een themaverwerking worden stelselmatig proactief persoonsgegevens verwerkt van 'onverdachte' burgers – mensen jegens wie op grond van feiten en omstandigheden geen redelijk vermoeden van schuld bestaat. In tegenstelling tot de huidige Wet politieregisters zal de nieuwe wet geen apart regime meer kennen voor gegevens over deze 'een beetje verdachte' personen. Het CBP waarschuwt dat zonder extra bescherming, bijvoorbeeld door middel van codering, van deze persoonsgegevens, het gevaar onaanvaardbaar groot is dat burgers ten onrechte worden onderworpen aan politieoptreden. In 2006 heeft het CBP met de vaste commissie van Justitie van de Eerste Kamer gesproken over de noodzaak van permanente bewaking van de juistheid en kwaliteit van politiegegevens.



> Camera voor enquête

Een automobilist vraagt zich bij het lezen van een bericht op teletekst af of Rijkswaterstaat niet te ver gaat met het registreren van weggebruikers op de A2. Hij leest dat camera's worden gebruikt om weggebruikers te vragen mee te werken aan een enquête over wegwerkzaamheden aan die snelweg. "Mijn gevoel zegt me dat dit niet klopt. Die camera's worden voor iets anders gebruikt dan waarvoor ze zijn geplaatst".



De virtuele slotgracht

De Raad van Hoofdcommissarissen lanceerde in 2005 het idee dat de politie zich in het kader van de criminaliteitsbestrijding zou gaan richten op de infrastructuur waarlangs mensen, geld, goederen en informatie zich verplaatsen. Dat zou onder meer gebeuren door het volgen daarvan met behulp van camera's, gericht op de toegangswegen van steden. Het CBP heeft aan de minister van BZK zijn zorgen over deze visie geuit.

Het CBP onderscheidt bij de voorgestelde werkwijze drie graden van acceptatie. Het met behulp van kentekenherkenning signaleren van verdachten en het registreren van hun gegevens is aanvaardbaar. Het registreren van bekenden van de politie – veelplegers – zonder dat dezen op dat moment verdacht worden van een strafbaar feit, is niet zonder meer aanvaardbaar. Per geval zou moeten worden bezien of deze gegevensopslag in strijd is met de wet. Het registreren van iederéén die zich op die route begeeft gaat volgens het CBP te ver, zeker als deze registraties naderhand worden geanalyseerd.

Nieuwe methoden zoals deze, waarbij de bescherming van persoonsgegevens in het gedrang kan komen, zouden volgens het CBP alleen overwogen moeten worden als de politie kan aantonen dat de bestaande bevoegdheden ontoereikend zijn om meer veiligheid te garanderen. Het CBP overlegt in het eerste kwartaal van 2007 met de Raad van Hoofdcommissarissen over de ervaringen met het systeem tot nu toe.

Grootschalige gegevensverwerkingen

Geholpen door de technologische ontwikkelingen is het voor zowel overheden als voor dienstverlenende en handelssectoren mogelijk om op grote schaal gegevens te verwerken, waaronder persoonsgegevens. Dat kan handig zijn en lucratief, maar kan als het fout gaat individuele personen schade berokkenen. Het is zaak al in het ontwerpstadium – zowel technisch als voor regelgeving – te trachten deze fouten te voorkomen.

- > **Europees onderzoek zorgverzekeraars**
De Europese gegevensbeschermingstoezichthouders hebben gecoördineerd onderzoek gedaan naar de verwerking van persoonsgegevens door de particuliere zorgverzekeringssector. De uitkomsten van het onderzoek zullen in 2007 worden gepubliceerd.
- > **Informatiebeveiliging ziekenhuizen**
In november 2006 hebben het CBP en de Inspectie voor de Gezondheidszorg een samenwerkingsprotocol ondertekend. Het doel is te komen tot een effectiever toezicht op het gebruik van persoonsgegevens in de zorgsector, waaronder in het Elektronisch Patiëntendossier. In 2006 zijn pilots uitgevoerd voor een breder gezamenlijk onderzoek in 2007 naar de informatiebeveiliging in ziekenhuizen.
- > **Elektronisch kinddossier**
Het elektronisch kinddossier beoogt vanaf (voor) de geboorte de ontwikkeling van een kind en de kenmerken uit zijn omgeving vast te leggen. De ingebruikneming van het EKD in de jeugdgezondheidszorg is uitgesteld tot 1 januari 2008 en zal naar verwachting pas in 2009 wettelijk verplicht worden gesteld. Het CBP heeft in 2006 nogmaals aangedrongen op beantwoording van de belangrijkste privacyvragen die bij het EKD spelen. Ook in 2007 zal het de ontwikkelingen intensief blijven volgen, vooral waar een mogelijk gebruik van de gegevens buiten de gezondheidszorg wordt overwogen, bijvoorbeeld in een nog in te voeren landelijke verwijzingsindex risicjongeren.
- > **Interventieteams voor fraudebestrijding**
In interventieteams werken verschillende overheidsorganisaties samen aan de bestrijding van fraude in de sociale zekerheid. Het kan daarbij nodig zijn op grond van eigen waarneming gegevens over personen te verzamelen en vast te leggen, zonder dat dezen daarvan op de hoogte zijn. De Wbp verplicht organisaties ertoe, betrokkenen te informeren over deze zogenoemde heimelijke waarnemingen, ook als er geen belastend materiaal is of wordt gevonden. De werkwijze bij heimelijke waarneming door de interventieteams is vastgelegd in de procesbeschrijving *Heimelijke waarneming door de interventieteams*. Een herziene versie van deze procesbeschrijving is in 2006 door het CBP goedgekeurd. Het in 2006 voorbereide onderzoek naar de werkwijze bij een aantal interventieteamprojecten is onlangs gestart.
- > **Fraudebestrijding in de sociale zekerheid**
Om misbruik van gemeenschapsgeld aan de poort zoveel mogelijk tegen te houden, willen gemeenten reeds in een vroeg stadium van het contact met een aanvrager van een uitkering zoveel mogelijk van diens gegevens verifiëren bij andere gegevensbronnen. Daarnaast willen gemeenten ter bestrijding van fraude met uitkeringen steeds meer gegevensbestanden ontsluiten en koppelen. In 2006 heeft het CBP de notitie *Fraudebestrijding door bestandskoppeling* uitgebracht. Daarin geeft het aan waarop gelet moet worden bij het vinden van een evenwicht tussen fraudebestrijding en respect voor de persoonlijke levenssfeer.
- > **Binding Corporate Rules**
Binding Corporate Rules zijn interne gedragscodes van multinationals op basis waarvan zij een vergunning kunnen krijgen voor de doorgifte van persoonsgegevens naar concernonderdelen die in derde landen zijn gevestigd. In 2006 zijn de eerste gecoördineerde Europese vergunningprocedures van start gegaan en zijn de eerste BCR's via deze procedures in meerdere landen goedgekeurd.
- > **De plicht om burgers te informeren**
Transparantie over de verwerking van persoonsgegevens is een van de pijlers van de Wbp. Eind 2005 is in opdracht van het CBP door TNS NIPO in drie sectoren, te weten huisartsen, onderwijsinstellingen en woningbouwcorporaties, een onderzoek uitgevoerd naar de naleving van de informatieplicht op grond van de Wbp. Tevens is onderzoek gedaan naar de naleving van de informatieplicht zoals burgers die ervaren. De onderzoeksrapporten zijn in mei 2006 gepubliceerd. De aanbevelingen van het onderzoek moeten leiden tot een betere bekendheid met en betere naleving van de informatieplicht.
- > **Internetpublicaties en privacy**
Gebruikers van het internet zien zich geconfronteerd met vragen over hun privacy en over het gebruik van hun persoonsgegevens. Het CBP werkt verder aan het afbakenen van de mogelijkheden voor effectief toezicht op internet. Een eerste versie van een discussiestuk over dit onderwerp is tijdens een intern symposium besproken. Publicatie van richtsnoeren wordt in 2007 verwacht.

> **RFID**

In oktober 2006 is een extern discussiestuk van het CBP over de maatschappelijke implicaties van het gebruik van Radio Frequency Identification gepubliceerd. RFID is een technologie waarmee allerhande voorwerpen, maar ook mensen en dieren, kunnen worden voorzien van – ook op afstand – uitleesbare chips met informatie. Welke informatie op de chip wordt opgeslagen en wat er vervolgens met die informatie gebeurt, raakt ook en in toenemende mate de bescherming van persoonsgegevens. Het rapport is inmiddels ook in een Engelstalige versie beschikbaar en vormt de basis voor verdere gedachtevorming en overleg over dit onderwerp.

> **Biometrie in reisdocumenten**

Het CBP heeft in 2006 een expertmeeting georganiseerd over het gebruik van biometrie in reisdocumenten. Aan de orde kwamen nut, noodzaak en mogelijke nadelen van grootschalige gecentraliseerde opslag van biometrische gegevens. De deelnemers aan de bijeenkomst wijzen de overheid op de risico's van 'function creep', identiteitsfraude en onvoldoende beveiliging.

> **Burgerservicenummer**

De invoering van het burgerservicenummer (BSN) is andermaal uitgesteld. Het CBP heeft in 2006 de beide Kamers van de volksvertegenwoordiging regelmatig op de hoogte gesteld van zijn standpunten over enkele heikle kwesties die aan de invoering verbonden blijven. Ook over de invoering van het BSN in de zorg, waarbij zorgvuldig gebruik van de juiste persoonsgegevens soms letterlijk van levensbelang is, heeft het CBP geadviseerd.

> **Veiligheid en privacy**

Het op verzoek van het CBP en de ministers van Justitie en BZK door prof. mr. H.R.B.M. Kummeling en prof. mr. dr. E.R. Muller uitgevoerde onderzoek naar het vinden van een goede balans tussen veiligheid en privacy zal in 2007 leiden tot publicatie en een congres.

Het paspoort

In de lidstaten van de Europese Unie worden paspoorten voorzien van biometrische gegevens. In verband daarmee komt er in Nederland een centrale opslag van reisdocumenten, waarin ook de biometrische gegevens van de aanvrager zullen worden opgenomen. Waarom is zo'n centrale opslag nodig? Zijn de argumenten die de overheid daarvoor aanvoert steekhoudend? Deze en andere vragen over nut, noodzaak en eventuele nadelen van deze grootschalige gegevensopslag zijn besproken tijdens een door het CBP georganiseerde expertbijeenkomst in februari 2006. De discussie levert een dubbel beeld op: het centraal bijeenbrengen van biometrische gegevens kan zowel identiteiten beschermen door de aanwezigheid van een centraal ijkpunt, als afbreuk doen aan die bescherming door risico's op het punt van beveiliging en mogelijk gebruik van biometrische gegevens voor een ander doel.

Het burgerservicenummer

De invoering van het burgerservicenummer (BSN) is een wederkerend onderwerp in het CBP-jaarverslag. Sinds zijn eerste advies over het wetsvoorstel uit 2004 is het CBP bezig minister en parlement te overtuigen van de noodzaak in essentiële onderdelen van de wet waarborgen in te bouwen voor de zorgvuldige omgang met de persoonsgegevens van de burger. Wanneer immers in de keteninformatie in backoffices iets fout gaat met het gebruik van het BSN en de daaraan gekoppelde persoonsgegevens, zijn door de olievlekwerking van de verspreiding van deze gegevens de gevolgen voor de burger vaak niet te overzien. De wet biedt daarvoor ontoereikende reparatiemogelijkheden. Dit is niet bevorderlijk voor het vertrouwen dat de burger moet kunnen stellen in de omgang met zijn persoonsgegevens door de overheid.

> *Persoonsverwisseling*

Wanneer een klant inlogt op een website krijgt hij tot zijn verbazing niet zijn eigen persoonsgegevens maar die van een ander voorgeschoteld: inlognaam, geboortedatum, naam, adres en woonplaats, e-mail-adres, sofi- en bankrekeningnummer en jaarinkomen. De klant vreest dat iemand anders nu zijn gegevens te zien krijgt en neemt daarom contact op met de web-host. Die checkt de gegevens van de klant en kan hem enigszins geruststellen: zijn gegevens zijn niet voor anderen inzichtelijk. Door een fout in het systeem krijgt hij echter wel de data van een ander op het scherm. "Onacceptabel", vindt de klant.



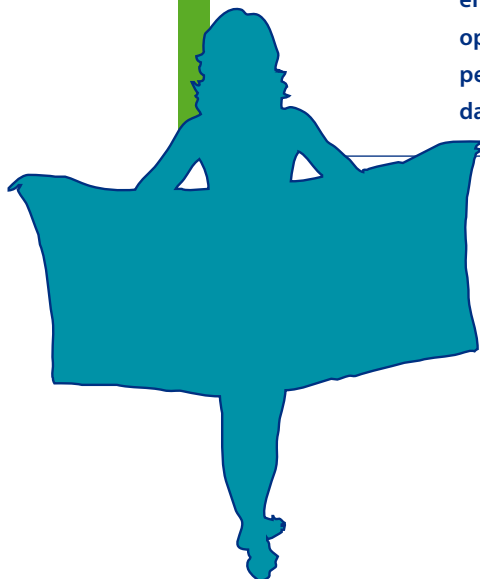
De invoering van het BSN, gepland voor 2006, is uitgesteld. Vanaf 2008, zo is de bedoeling, zal het in de zorgsector het huidige sofinummer vervangen. Dit 'BSN-z' zal worden gebruikt in de communicatie over patiënten tussen zorgaanbieders, ziektekostenverzekeraars en indicatie-organen. Het is essentieel dat daarbij een meer dan zorgvuldige registratie van persoonsgegevens plaatsvindt. Veel huisartsen waren vooruitlopend op het BSN-z al begonnen met het registreren van de sofinummers van hun patiënten. Vanwege de fouten in door de patiënten zelf opgegeven nummers heeft de Landelijke Huisartsen Vereniging op verzoek van het CBP alle verwijzingen naar het opvragen van het sofinummer uit haar informatiemateriaal geschrapt.

De andere pijler van het BSN-stelsel in de zorg is de identificatieplicht. Het CBP, doorgaans geen voorstander van identificatieplicht, vindt deze in de zorg juist wel van groot belang, gezien de gezondheidsrisico's die onjuiste identificatie voor patiënten kan meebrengen. Huisartsen vinden het belastend aan hun patiënten een identiteitsbewijs te vragen. De Tweede Kamer heeft hiervoor begrip en heeft een motie aangenomen die in het Besluit gebruik BSN in de zorg de identificatieplicht versoepelt tot een verificatieplicht. Het CBP heeft de minister aangeraden hieraan geen gevolg te geven, of op zijn minst aanvullende maatregelen te nemen om ervoor te zorgen dat na eenmalige identificatie van een patiënt diens gegevens zodanig controleerbaar zijn dat persoonsverwisseling wordt uitgesloten.

Het BSN zal worden gebruikt om het Elektronisch Patiëntendossier mogelijk te maken. Het CBP is bij de ontwikkeling daarvan actief betrokken. Daarbij gaat het vooral om het goed regelen van verantwoordelijkheid, toegang, beveiliging en toezicht met betrekking tot het dossier.`

> **Cameratoezicht in douche**

De directie van een 24-uursbedrijf wil in de douche- en kleedruimtes van de terminalmedewerkers camera's ophangen om zo toezicht te kunnen houden op het personeel. Een van de medewerkers vraagt zich af of dat wel mag.



De OV-chipkaart

Begin 2006 publiceert het CBP het visiedocument *Privacy en de OV-chipkaart*. De bezwaren van het CBP tegen het gebruik door vervoerders van reisgegevens van op naam gestelde kaarten voor serviceverlening en direct marketingdoeleinden leiden ertoe dat de Tweede Kamer er bij de minister op aandringt de privacyproblemen op te lossen. Naar aanleiding van deze opdracht heeft het ministerie getracht in overleg met de NS en het CBP een aantal knelpunten in kaart te brengen en op te lossen. In 2007 zal het CBP bij een vervoerder die de OV-chipkaart gedeeltelijk heeft ingevoerd, onderzoeken of en hoe de maatregelen om persoonsgegevens te beschermen worden uitgevoerd.

Het CBP zal in 2007 meer nadruk leggen op handhaving door middel van controlerend onderzoek en minder op advisering van individuele partijen. De verschuiving naar meer controle is nodig om het bewustzijn van het belang van privacyregels te vergroten en de naleving ervan te verbeteren. Voorgenomen onderzoeken zullen niet altijd tevoren worden bekendgemaakt en zijn ook niet alle hieronder vermeld.

Het komend jaar worden vooral de volgende resultaten nagestreefd:

> **Publicaties op internet**

Persoonsgegevens kunnen via publicatie op internet gemakkelijker en breder dan ooit in de openbaarheid komen. Ook blijven deze gegevens nog jaren gemakkelijk voor een ieder toegankelijk. In 2007 zal het CBP richtsnoeren publiceren voor de eisen die de Wbp stelt aan dergelijke publicaties en enkele onderzoeken uitvoeren.

> **OV-chipkaart**

Per 1 januari 2009 – zo zijn de plannen – zal de OV-chipkaart in heel Nederland worden ingevoerd. De minister van Verkeer en Waterstaat heeft toegezegd alles in het werk te stellen om het OV-chipkaart-systeem te laten voldoen aan de Wet bescherming persoonsgegevens en bemiddelt in de discussie tussen de vervoerders en het CBP. De OV-chipkaart wordt geleidelijk ingevoerd. Het CBP zal daarom onderzoek doen op een van de in 2007 in te voeren systemen.

> **Invoering Elektronisch Patiëntendossier**

Het Elektronisch Patiëntendossier (EPD) komt steeds dichterbij. Voor de privacy van de patiënt zijn de toegang tot de gegevens, de beveiliging van de gegevens en het systeem en het correct informeren van de patiënt belangrijke aspecten. Het CBP zal daarom onderzoek doen in een regio waar met (delen van) het EPD wordt proefgedraaid.

> **Naleving GBA**

De Gemeentelijke basisadministratie (GBA) is voor de meeste burgers niet transparant, terwijl vele organisaties systematisch wijzigingen in de persoonsgegevens verstrekt krijgen uit de GBA. Uit onderzoek in 2005 naar deze verstrekking aan derden uit de GBA bleek onder andere dat een groot deel van de afnemers niet anders omgaat met gegevens met een geheimhoudingsindicatie dan met gegevens zonder geheimhoudingsindicatie. In 2007 zal het CBP een controlerend onderzoek uitvoeren. Tevens zal handhavend worden opgetreden tegen gemeenten die niet voldoen aan de verplichting audits uit te voeren op de GBA.

> **Fraudebestrijding bij de sociale zekerheid**

Bij de fraudebestrijding in de sociale zekerheid is de tendens op dit moment het uitvoeren van grootschalige controle. Dit gebeurt bijvoorbeeld door het koppelen van zoveel mogelijk bestanden met gegevens van grote aantallen burgers. Bij het onderkennen van de noodzaak tot fraudebestrijding is het uitgangspunt van het CBP dat niet iedere uitkeringsgerechtigde bij voorbaat moet worden bestempeld als potentieel fraudeur en dat burgers die worden gecontroleerd daarover ook moeten worden geïnformeerd. Het CBP zal in 2007 onderzoek verrichten naar enkele koppelingen.

> **Digitale leerlingdossiers**

De digitalisering van leerlingdossiers maakt uitwisseling van gegevens binnen de onderwijssector en met andere sectoren steeds eenvoudiger. Daarnaast bevatten leerlingdossiers steeds meer gegevens. Het is belangrijk dat ouders hierover goed geïnformeerd zijn en dat scholen zich bewust zijn van de regels rondom het verwerken en/of verstrekken van persoonsgegevens. In 2007 zal de onderwijssector met nadruk worden gewezen op deze regels.

> **Arbodienst en ICT**

In 2007 zal een controlerend onderzoek onder arbodiensten worden uitgevoerd. Samenwerkingsverbanden tussen arbodiensten en verzekeraars worden meestal ook digitaal ondersteund (gezamenlijke databank, intensieve gegevensuitwisselingen). Onderzocht zal worden of deze relatief nieuwe technologische ontwikkelingen voldoen aan de wettelijke regels voor de verwerking van persoonsgegevens.

> **Privacyregels bij de politie**

De functionarissen voor de gegevensbescherming (FG's) zijn binnen de politie de toezichthouder op de zorgvuldige omgang met persoonsgegevens. Met vragen, klachten of verzoeken om kennisname van hun gegevens kunnen burgers terecht bij de privacy-functionarissen (PF's) van de korpsen. In 2007 zal het CBP in het belang van eenduidige en uniforme verwerking van gegevens bij de politie extra aandacht besteden aan de relatie met beide functionarissen.

> **Controlesamenleving**

Informatiesystemen die het ook mogelijk maken individuen nauwkeurig te volgen en te controleren en systemen die specifiek als controle-instrument bedoeld zijn (o.a. camera's gekoppeld aan herkenningssystemen, chips in smartcards, GPS, registratie van telecommunicatiegegevens) spelen een steeds grotere rol in de samenleving. Als een controlesamenleving onafwendbaar blijkt, zullen we ons op zijn minst bewust moeten zijn van de risico's van de massale inzet van informatietechnologie. Het CBP zal in 2007 aandacht vragen voor deze ontwikkelingen.

> **Samenwerking met andere toezichthouders**

In 2007 zal intensiever worden gezocht naar samenwerking met andere toezichthouders. Het CBP zal een samenwerkingsconvenant sluiten met de Nederlandse Zorgautoriteit. Het in 2006 voorbereide gezamenlijke onderzoek van de Inspectie Gezondheidszorg en het CBP naar de informatiebeveiliging van ziekenhuizen zal in 2007 worden uitgevoerd, evenals het gezamenlijke onderzoek met de Inspectie Werk en Inkomen naar de verwerking van persoonsgegevens in bedrijfsverzamelgebouwen met gemeenschappelijke voorzieningen voor publieke en private partijen (CWI, sociale dienst, UWV, reïntegratiebedrijf).

> **Jurisprudentiebundel Wbp**

In 2007 zal een bundel verschijnen met oordelen van het CBP op basis van de Wbp. Deze bundel is een vervolg op de bundel *Persoonsgegevens beschermd* uit 1999 die gewijd is aan uitspraken op basis van de Wet persoonsregistraties (WPR). Ook uitspraken van geschillencommissies en de rechter die een grote betekenis kunnen hebben voor de rechtspraak worden opgenomen. Het samenstellen van de bundel is een samenwerkingsproject met adviesbureau Duthler. In de redactie nemen twee onafhankelijke rechtsgeleerden plaats, prof. mr. D.W.F. Verkade en prof. mr. H.Ph.J.A.M. Hennekens.

Het digitaal klantdossier

Efficiëntere bedrijfsvoering, effectievere bestrijding van fraude en verbetering van de dienstverlening aan de burger zijn de doelstellingen van het digitaal klantdossier zoals voorgesteld in de Wet eenmalige gegevensvraag werk en inkomen. Het wetsvoorstel voorziet in het eenmalig verzamelen van alle gegevens van een klant die afkomstig zijn van organisaties als de sociale dienst, het CWI, de UWV, de Sociale Verzekeringsbank, de Rijksdienst voor het Wegverkeer en de Informatie Beheer Groep. Het digitaal klantdossier dat uit deze gegevens wordt samengesteld moet voorkomen dat de overheid burgers vaker dan één keer vraagt naar gegevens waarover zij al beschikt. Het CBP benadrukt in zijn advies aan de staatssecretaris van Sociale Zaken en Werkgelegenheid het belang van goede informatieverstrekking aan de burger, die zijn inzage- en correctierecht moet kunnen uitoefenen, en op de noodzaak van transparantie. Anders dreigt het digitaal klantdossier vooral een systeem te worden over in plaats van voor de burger.

Tien Gouden Regels

Mag de sociale dienst mijn bankafschriften bekijken en daar kopieën van maken? Mag zij mijn huisarts bellen om te vragen of ik langs ben geweest? Mag de sociale dienst afgaan op tips van mijn buurman over mij? Dit soort vragen over verwerking van persoonsgegevens door de sociale dienst komt regelmatig binnen bij het CBP. Met behulp van enkele medewerkers van verschillende sociale diensten heeft het CBP in 2006 voor de sociale diensten een brochure gemaakt met richtlijnen voor de beantwoording ervan. De Tien Gouden Regels beogen vooral een praktische handreiking te bieden aan de medewerkers die de intake en begeleiding van cliënten voor hun rekening nemen.

RFID

Radio Frequency Identification is een technologie waarmee voorwerpen kunnen worden voorzien van een minuscule chip die gegevens bevat die onmerkbaar kunnen worden uitgelezen. Toepassing van deze technologie kan – vooral op logistiek terrein – grote voordelen meebrengen, maar kan ook leiden tot maatschappelijke zorg. De eigenschappen van RFID lenen zich voor ongebreideld gebruik van gegevens in velerlei sectoren. De zorg ontstaat als mensen door massale toepassing van de techniek, door overheden zowel als door private partijen, de controle verliezen over de gegevens die over hen worden verzameld en vervolgens in backoffices verwerkt en opgeslagen.

RFID stelt de naleving en toepassing van de regels voor de verwerking van persoonsgegevens voor bijzondere problemen. Om de maatschappelijke discussie over het gebruik van RFID te stimuleren heeft het CBP in 2006 een studie uitgebracht onder de titel *RFID. Veelbelovend of onverantwoord?*

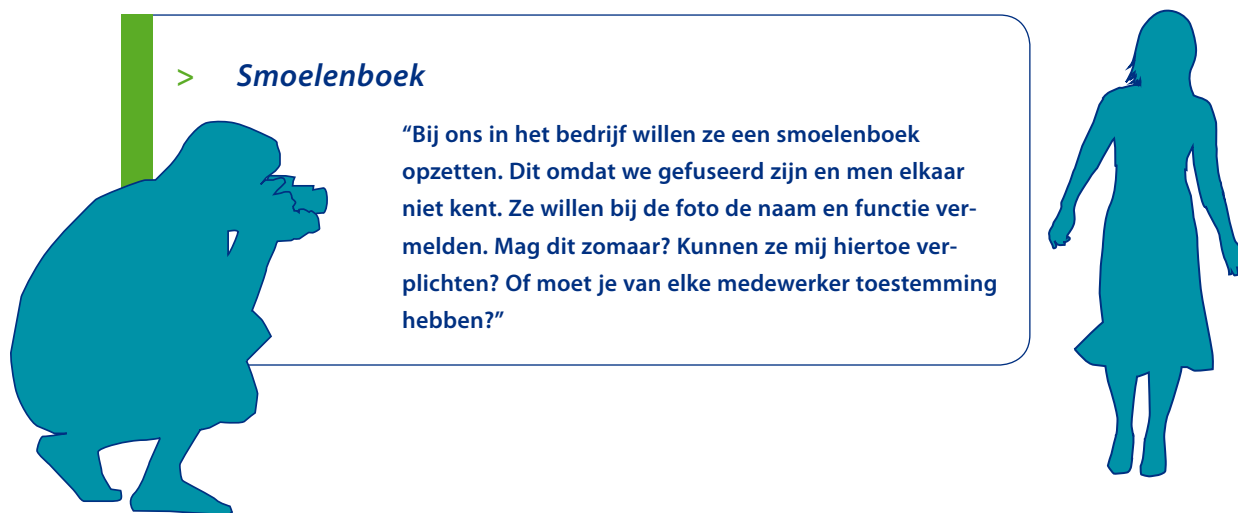
Fraudebestrijding en koppeling van bestanden

Net zo min als elke bewoner van een achterstandswijk een potentieel terrorist is, is elke uitkeringsgerechtigde een mogelijk fraudeur. Het bestrijden van misstanden in een concern door het openstellen van kliklijnen of het invoeren van zwarte lijsten is een gerechtvaardigd belang, evenals het door heimelijke waarneming boven water krijgen van mogelijke uitkeringsfraude. Maar voor dergelijke gegevensverwerkingen geldt dat de nagestreefde belangen opwegen tegen de aantasting van de persoonlijke levenssfeer van degene over wie wordt geklikt of van wie wordt vermoed dat hij frauduleus handelt.

Kliklijnen en zwarte lijsten

De Amerikaanse Sarbanes-Oxley wetgeving verplicht in de Verenigde Staten gevestigde bedrijven een concernbrede interne kliklijn te openen, met als doel bevordering van integere bedrijfsvoering. Voor bedrijven in Nederland, ook voor dochterondernemingen van een multinational, levert deze verplichting echter geen wettelijke grondslag op voor het instellen van zo'n bedrijfsklokkenluidersregeling. Daarvoor is vereist dat het bedrijf zich houdt aan de regels die de Wbp stelt voor het doorgeven van persoonsgegevens naar landen buiten de EU. Omdat de concernbrede kliklijn in de meeste gevallen is opengesteld om het moederbedrijf in de VS te informeren, mogen persoonsgegevens uitsluitend worden doorgegeven ingeval van misstanden waarvan duidelijk is dat afhandeling van de melding niet naar behoren op lager niveau kan plaatsvinden. De Artikel 29-werkgroep heeft richtsnoeren opgesteld over de verenigbaarheid van klokkenluidersregelingen die onder de Sarbanes-Oxley wetgeving tot stand zijn gekomen enerzijds en de EU gegevensbeschermingsregels anderzijds. Dit om rechtszekerheid te bieden aan bedrijven die zowel aan de Europese gegevensbeschermingsregels als aan de Sarbanes-Oxley wetgeving onderworpen zijn. In lijn met die richtsnoeren is voor een doorgifte van persoonsgegevens via de kliklijn een vergunning vereist van de minister van Justitie, tenzij de gegevens in het derde land adequaat worden beschermd.

Een andere methode om misdragingen van personeel – variërend van een greepje uit de kas tot ernstiger vergrijpen – tegen te gaan is het aanleggen van zwarte lijsten. Voor de sector detailhandel, die ernstige hinder van misdragingen ondervindt, is een waarschuwingsregister in het leven geroepen waarin de gegevens zijn opgenomen van overtreders, tegen wie aangifte is gedaan en die daarvoor zijn ontslagen. Bij het werven van personeel kunnen werkgevers de lijst raadplegen om te zien of de sollicitant er op voorkomt. In 2007 zal het CBP uitsluitsel geven over een onderzoek dat het heeft gedaan naar de werking in de praktijk van zo'n zwarte lijst.



Er is een grens aan koppeling van bestanden

Bij de bestrijding van woonfraude door personen met een bijstandsuitkering kan een gemeente gegevens opvragen over hun gas-, water- en elektriciteitsgebruik. Een gemeente wilde daarnaast gegevens van de vuilverwerkingsadministratie koppelen aan de administratie van de sociale dienst, om een indicatie te krijgen van de bewoning van een pand. Dit vindt het CBP te ver gaan. De gemeente heeft niet aan kunnen tonen dat naast de al beschikbare gegevens en de huisbezoeken deze extra gegevens nodig zijn. Bovendien is deze bestandskoppeling in strijd met het doelbindingsbeginsel. Burgers zijn verplicht huisvuil aan te leveren en het vuilverwerkingsbedrijf beschikt over hun gegevens met het oog op facturering. De gegevens mogen niet voor een ander doel worden gebruikt.

Overzicht van in 2006 verrichte onderzoeken

> Europol

Het CBP heeft ook in 2006 deelgenomen aan de jaarlijkse audit van de Europol-systemen door het Gemeenschappelijk Controleorgaan van Europol. Uit deze controles blijkt telkens weer het grote belang van een goede kwaliteit van de door de lidstaten aangeleverde gegevens. Naast de kwaliteit van de gegevens is onderzocht of het Informatiesysteem functioneert in overeenstemming met de Europolovereenkomst. Bij de audit van 2006 is tevens onderzocht in hoeverre invulling is gegeven aan de in 2004 en 2005 gegeven aanbevelingen ter verbetering van de bedrijfsvoering bij Europol. Bij de inspectie is gebleken dat Europol de meeste van de verbeterpunten uit eerdere controleonderzoeken heeft geïmplementeerd.

> Eurodac

Eurodac is een EU-breed systeem voor het vergelijken van vingerafdrukken van vreemdelingen. De database is gebaseerd op een hit/no hitsysteem: lidstaten nemen vingerafdrukken af van asielzoekers en in het land aangetroffen illegalen en vergelijken deze met de in het systeem aanwezige gegevens om zo te kunnen vaststellen welke lidstaat krachtens de Overeenkomst van Dublin verantwoordelijk is voor de behandeling van een asielerzoek. Het CBP, toezichthouder op onder meer de nationale verwerking van persoonsgegevens ten behoeve van Eurodac, heeft op verzoek van de Europese Toezichthouder op de Gegevensbescherming in 2006 onderzoek uitgevoerd als onderdeel van gecoördineerde controle in de verschillende lidstaten. Een samenvattend rapport over de bevindingen in Europees verband volgt naar verwachting in 2007.

> Sociale recherche

Door heimelijke waarnemingen controleert de sociale recherche of mensen met een bijstandsuitkering frauderen. In 2003 heeft het CBP de procesbeschrijving voor deze waarnemingen goedgekeurd. Een belangrijk onderdeel daarvan is dat de gecontroleerde burgers hiervan op de hoogte worden gesteld. Uit controleonderzoek dat in 2006 is uitgevoerd, blijkt dat de naleving van de informatieplicht voor verbetering vatbaar is.

> Vernietiging van getapte gesprekken met geheimhouders

In de periode juni 2005 – december 2006 is onderzoek gedaan naar de naleving van de regels voor de vernietiging van opgenomen telefoongesprekken met geheimhouders – artsen, advocaten, notarissen en geestelijk raadslieden.

De resultaten van dit onderzoek hebben het CBP aanleiding gegeven om het onderzoek te vervolgen. Daarom zal het CBP in de eerste helft van 2007 nogmaals een controle uitvoeren naar de naleving van de vernietigingsplicht met betrekking tot opgenomen telecommunicatie met geheimhouders. De resultaten van dit onderzoek worden naar verwachting in 2007 gepubliceerd.

> Bijzondere opsporingsdiensten

Als onderdeel van het systematisch toezicht op de verwerking van

persoonsgegevens door Criminele Inlichtingen Eenheden (CIE-en) heeft het CBP in 2006 onderzoeken bij de CIE-en van twee Bijzondere Opsporingsdiensten afgerond. Uit de onderzoeken is gebleken dat de inhoud van de registers voor zover onderzocht op nagenoeg alle punten voldeed aan de door de wet- en regelgeving daaraan te stellen eisen. Met betrekking tot organisatorische en technische aspecten heeft het CBP, evenals bij de eerder in 2003/2004 uitgevoerde onderzoeken bij CIE-en, enkele punten die verbetering behoeven onder de aandacht van de verantwoordelijke ministers gebracht.

> Particuliere recherche

In 2006 zijn de resultaten gepubliceerd van in 2005 verricht onderzoek naar de naleving van een aantal normen uit de Wbp door particuliere recherchebureaus. Het ging vooral om de naleving van de informatieplicht. Het blijkt dat in een groot aantal gevallen de bureaus niet weten of zij daaraan hebben voldaan, omdat zij het aan hun opdrachtgever overlaten om de onderzochte persoon in te lichten en niet controleren of de opdrachtgever dat ook daadwerkelijk heeft gedaan. Bijna geen enkel bureau heeft hierover een werkinstructie of procedure opgesteld. Het CBP vindt het noodzakelijk dat bureaus de naleving van de informatieplicht schriftelijk met de opdrachtgever regelen.

> Zwarte lijsten detailhandel

Personeelsleden tegen wie aangifte is gedaan wegens diefstal of fraude en die zijn ontslagen, kunnen op een zwarte lijst worden geplaatst. Werkgevers kunnen die lijst raadplegen om sollicitanten te screenen. In 2006 heeft het CBP onderzoek gedaan naar de werking van dit zogeheten waarschuwingsregister in de detailhandel om te controleren of het systeem functioneert in overeenstemming met de Wbp en het Protocol voor het waarschuwingsregister. De resultaten worden in 2007 gepubliceerd.

> Financiële dienstverleners

Een zorgvuldige verwerking van persoonsgegevens in de financiële sector acht het CBP van groot belang. In 2006 is onderzoek gedaan naar de naleving van de Privacygedragscode Financiële Instellingen. Het doel van het onderzoek was om zicht te krijgen op de naleving van de eisen die in de Wbp en in de gedragscode zijn neergelegd. De resultaten van het onderzoek worden in 2007 verwacht.

> Zorgverzekeraars

De Europese nationale toezichthouders hebben in de context van hun werkzaamheden in de EU-Artikel 29-werkgroep besloten tot gecoördineerd onderzoek naar de verwerking van persoonsgegevens in de zorgverzekeringssector. Het onderzoek moet Europabreed de stand van zaken weergeven van de naleving van de privacywetgeving in de sector. Het onderzoek is tussen april en oktober 2006 uitgevoerd. Publicatie van de uitkomsten wordt medio 2007 verwacht.

Het internet

Er is sprake van een internetparadox. Aan de ene kant zijn mensen bereid de intiemste gegevens en verrichtingen op het internet prijs te geven. Aan de andere kant kunnen mensen veel schade en verdriet ondervinden door bekendmaking van hun gegevens op het net.

Publicaties op het internet

In 2005 is het CBP een project gestart om de privacyproblemen te inventariseren die burgers in de alledaagse praktijk ondervinden door publicaties op het internet. Van meet af aan bleek de complexiteit van de vraag naar wat wel en wat niet geoorloofd zou moeten zijn bij de verwerking van persoonsgegevens op websites zeer groot te zijn. Voor 2006 heeft het CBP zich tot doel gesteld een voorlopige beleidslijn te ontwikkelen die kan dienen als aanzet tot verdere discussie over dit onderwerp. Deze beleidslijn is neergelegd in een verkennend rapport dat is gepresenteerd tijdens een symposium ter gelegenheid van het afscheid van J.W. Broekema als lid van het College. In het voorjaar van 2007 zal het CBP richtsnoeren publiceren voor de omgang met persoonsgegevens bij publicaties op internet.

Het gebruik van gepersonaliseerde diensten op internet, zoals G-mail, levert de aanbieders van deze diensten steeds grotere 'datapakhuisen' met persoonsgegevens op, zoals zoekopdrachten, de inhoud van e-mail of de inhoud van de hele harde schijf van de computer. De verstrekking aan derden van deze gegevens kan internetgebruikers aardig in de problemen brengen.

Google Europe erkent tijdens een door het CBP en de Consumentenbond georganiseerde debatmiddag op 7 december 2006 dat IP-adressen, de nummers waaronder computers kunnen worden geïdentificeerd, in veel gevallen persoonsgegevens zijn en dat daar de wettelijke bescherming van persoonsgegevens dus volledig op van toepassing is. Het CBP benadrukt dat het belangrijk is dat internetgebruikers voldoende informatie krijgen van de dienstaanbieders, dat het gebruik van hun gegevens in een andere context niet zo maar mag, dat iedereen zijn eigen gegevens moet kunnen inzien en zo nodig corrigeren en dat er een maximum termijn aan de gegevensopslag wordt gesteld.

> Stamboom op internet

Een vrouw komt op een genealogische website op het internet persoonsgegevens van haar en haar familie tegen. Het gaat om namen, adressen, geboortedata en -plaatsen en huwelijkspartners. "En daarvoor is nooit toestemming gevraagd, laat staan gegeven."

Een dringend verzoek aan de samensteller van de stamboom om deze gegevens van de site te halen, blijft onbeantwoord. De webhost belooft een en ander te laten uitzoeken, maar laat vervolgens ook niets meer van zich horen.



Openstelling archieven

Digitalisering en openstelling van bestaande archieven – we hebben het hier niet over de moderne digitale weblogs en dergelijke – voor een breed publiek worden van belang geacht en door de overheid gestimuleerd. Omdat in archieven (bijzondere) persoonsgegevens kunnen voorkomen is het van belang dat spelregels worden opgesteld voor de ontsluiting en digitalisering van bestaand archiefmateriaal waarin de vereisten van de Wbp worden uitgewerkt. Het CBP heeft hierover een advies gegeven voor de erfgoedsector. Onlinearchieven waarin persoonsgegevens voorkomen moeten worden gemeld bij het CBP ofwel bij de Functionaris voor de gegevensbescherming indien de erfgoedinstelling een dergelijke toezichthouder heeft benoemd.

Het openstellen van archieven via internet verdient speciale aandacht. Het bijzondere aan een onbelemmerde verstrekking via internet is dat persoonsgegevens ter beschikking worden gesteld aan een ieder, wereldwijd en onbeperkt in tijd. De verantwoordelijke weet niet aan wie hij persoonsgegevens levert. Het is de vraag of hij op deze wijze zorgvuldig handelt. Hij kan zich in elk geval niet verschuilen achter een wettelijke plicht, want er bestaat geen wettelijke plicht om persoonsgegevens via internet openbaar te maken.



> *Anoniem stamcafé*

De anonieme schrijvers van het internetweblog 'stamcafé' vinden het leuk om af en toe ook in real life samen een biertje te drinken. Daarbij wordt uitdrukkelijk afgesproken dat hun persoonsgegevens niet online mogen worden gezet. Een zakenman, lid van het schrijversgilde, merkt dat niet iedereen zich aan die afspraak houdt. Hij ontdekt dat iemand door geregeld zijn website te bezoeken naar zijn persoonsgegevens, zoals zijn mobiele telefoonnummer, vist. De zakenman ziet zich zelfs genoodzaakt zijn site tijdelijk van het internet te halen. "Ik kan het me niet permitteren dat mijn klanten, naar wie ik op mijn website direct doorlink, worden lastiggevallen door gekken".

Onderwijs en studie

Gegevens over ouders en leerlingen

In maart 2006 stuurde het CBP een wetgevingsadvies naar de minister van Onderwijs, Cultuur en Wetenschap over de nieuwe gewichtenregeling ten behoeve van de bekostiging van de basisscholen door het ministerie. In de nieuwe bekostigingssystematiek voor het wegwerken van onderwijsachterstanden wordt het extra geld in hoofdzaak verdeeld op basis van het opleidingsniveau van de ouders. Het CBP adviseerde de minister om in de Nota van toelichting bij het wetsvoorstel meer expliciet aandacht te schenken aan de belangen die met de verwerking van de gegevens van ouders in het geding zijn.



> **Verkeerd bezorgde post**

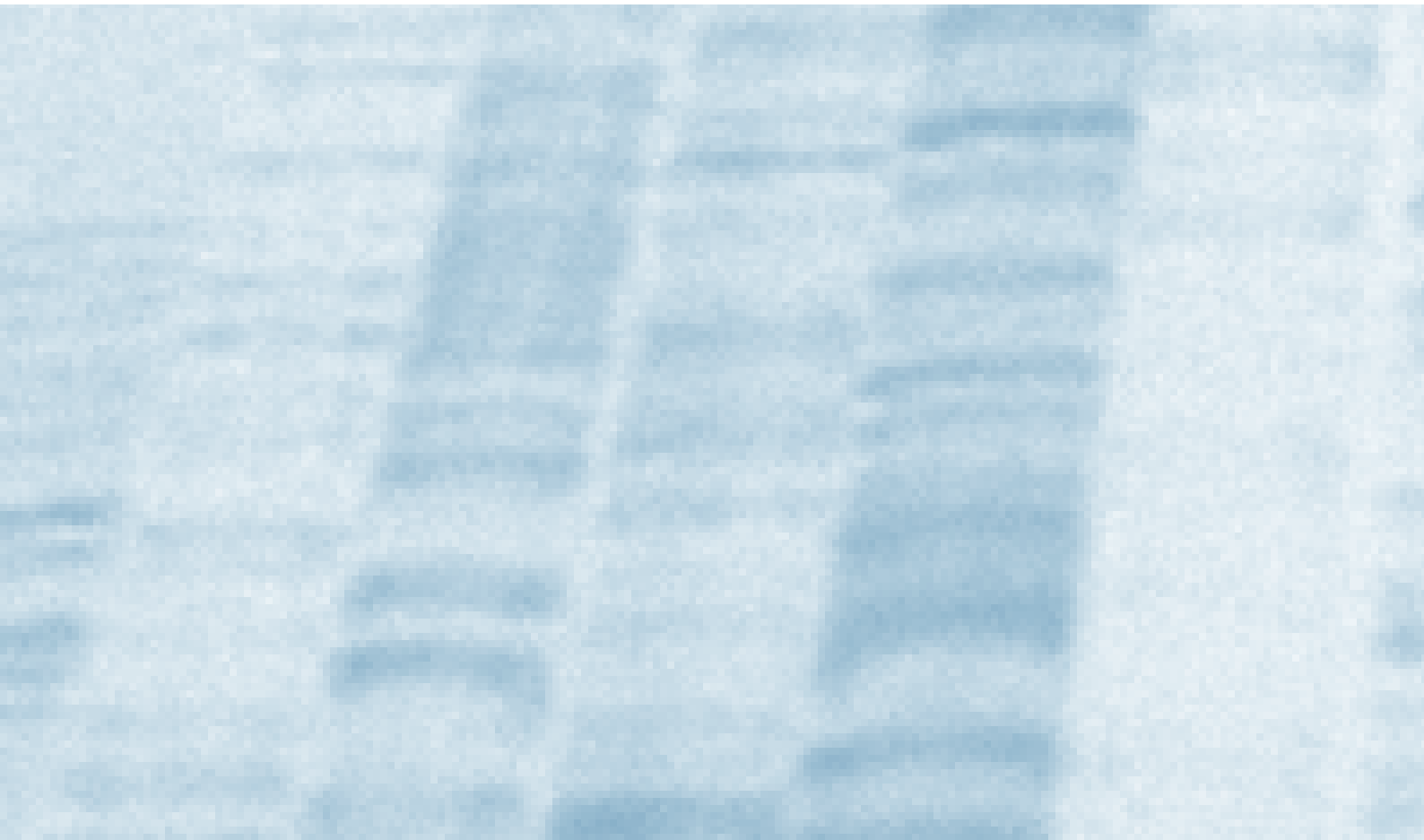
Een re-integratiebureau stuurt de voortgangsrapportage van een van zijn cliënten niet naar de bestemde gemeente maar naar een andere cliënt. Die doet schriftelijk zijn beklag bij het bureau, aangezien hij geconfronteerd is met de – gevoelige – persoonsgegevens van een ander. Op zijn klacht verneemt hij, afgezien van een ontvangstbevestiging van zijn brief, niets meer. “Het lijkt wel of ze dit niet belangrijk vinden”, reageert hij, “terwijl het in mijn ogen toch gaat om een ernstige schending van de privacy.”

In juli 2006 werd het CBP benaderd door ouders die uit de brochure van de school van hun kind begrepen dat zij verplicht waren gegevens over hun opleidingsniveau te verstrekken. Deze verplichting bestaat evenwel niet. Het CBP heeft de minister in een spontaan advies van 20 juli 2006 voorgesteld via de Cfi-website van het ministerie, maar ook via andere beschikbare kanalen, schooldirecties en -besturen op de hoogte te stellen van het feit dat van een plicht van de ouders geen sprake is. De minister heeft het CBP laten weten de suggesties over te nemen. De tekst van de ouderverklaring is vernieuwd zodat duidelijk blijkt dat ouders niet verplicht zijn deze in te vullen. In een volgende druk zal ook de tekst van de voorlichtingsbrochure worden aangepast.

Gegevensuitwisseling voor beroep of studie

Het wetsvoorstel dat de regering wil indienen om de EG-richtlijn voor de erkenning van beroepskwalificaties in Nederlands recht om te zetten moet in de huidige vorm niet worden ingediend, meent het CBP. Dat het voor de erkenningsprocedure nodig is om persoonsgegevens uit te wisselen staat buiten kijf, maar het voorstel is zo vaag dat het voor de burger volstrekt onduidelijk is om welke gegevens het daarbij zal gaan.

Studeren in het buitenland wordt steeds populairder. Het zal daarbij mogelijk worden naar veel meer landen studiefinanciering mee te nemen dan nu het geval is. Voor het controleren van aanspraken op studiefinanciering is uitwisseling van gegevens met autoriteiten van andere landen nodig. Het CBP wijst de staatssecretaris van OCW op de noodzaak voorzichtig te zijn met doorgifte van bepaalde gegevens aan landen buiten de EU, wanneer die informatie voor de student onbedoelde negatieve gevolgen kan hebben, zoals gegevens over diens samenlevingsvorm.



Sectoroverstijgend

pagina 26

Samenwerking, verbreding van het draagvlak en krachtiger communicatie worden ingezet om te bevorderen dat de wettelijke regels die persoonsgegevens beschermen beter en bewuster worden nageleefd.

Internationaal

pagina 31

Het is vijf voor twaalf, wat de bescherming van de persoonlijke levenssfeer en van persoonsgegevens betreft, waarschuwt de internationale conferentie van dataprotectie-toezichthouders. Onzichtbare en ongecontroleerde toezichtsvormen nemen hand over hand toe.

Openbaar bestuur

pagina 36

De invoering van het burgerservicenummer is ook in 2006 voor het CBP een zorgenkind gebleven. Ook op andere terreinen wijst het CBP op het belang van risicobeperking bij het gebruiken van persoonsinformatie voor het behoud van het vertrouwen van de burger in het bestuur.

Politie en justitie

pagina 39

Onder de paraplu van de terrorismebestrijding nemen op strafvorderlijk terrein de bevoegdheden om steeds meer gegevens over steeds meer burgers te verzamelen nog steeds toe. Het CBP hamert op de noodzaak van behoorlijk toezicht op de uitoefening van deze bevoegdheden.

Arbeid en sociale zekerheid

pagina 44

Bedrijven brengen kliklijnen en zwarte lijsten in stelling tegen disfunctionerende leidinggevendenden of frauderende werknemers. Sociale diensten controleren hun cliënten intensief. De inzet van deze middelen moet steeds worden afgewogen tegen de belangen van het gescreende individu.

Gezondheidszorg

pagina 47

Het CBP is nauw betrokken bij het overleg over het gegevensverkeer in deze gevoelige sector. De kwaliteit van de gezondheidszorg staat of valt met de juistheid van patiëntgegevens. Het CBP is kritisch over de versoepeling van de identificatieplicht in de zorg.

Handel en diensten

page 51

De OV-chipkaart werpt zijn schaduw vooruit. Het CBP is op diverse fronten actief om een zo zorgvuldig mogelijke invoering ervan te bepleiten en te controleren. Veel aandacht is er ook voor de verwerking van persoonsgegevens in de financiële sector.

Telecom en Internet

pagina 54

Wat mag wel en niet met het verwerken van persoonsgegevens op het internet? En wat mag gescreend worden bij publicaties op het net? Daarover ontstaat gaandeweg meer duidelijkheid.

Technologie

pagina 57

Biometrie en RFID bieden de mogelijkheid voor grootschalige opslag van persoonsgegevens. Het CBP neemt deel aan de maatschappelijke discussie over de inzet van deze technologieën en propageert het van meet af aan waarborgen van privacy met technische middelen.



Sectoroverstijgend

Om de naleving van de bescherming van persoonsgegevens te bevorderen, maakt het CBP gebruik van een veelheid aan middelen. Daartoe behoren het hoog houden van de toegankelijkheid van het CBP voor de burger met problemen, het effectief communiceren, het deelnemen aan het maatschappelijk debat, het samenwerken met maatschappelijke bondgenoten, het verbreden van het draagvlak en certificering.

De eerste lijn: www.mijnprivacy.nl

De wetgever heeft het CBP een loketfunctie gegeven voor de behandeling van klachten van burgers. Voor het draagvlak voor de bescherming van persoonsgegevens en voor de rol van het CBP is de toegankelijkheid van het CBP voor mensen met klachten, problemen en vragen van wezenlijk belang. Niet alleen voor de personen die hun klachten behandeld zien, hun problemen opgelost en hun vragen beantwoord. Ook voor het CBP is het contact met wat er in het gewone daagse leven speelt en mis kan gaan bij de omgang met persoonsgegevens essentieel. Het afgelopen jaar zijn 7794 e-mails, brieven en telefoontjes bij het CBP binnengekomen. Het grootste deel daarvan is afkomstig van individuele burgers – ‘gewone’ mensen ‘die niets hebben te vrezen’, maar die zich zorgen maken over hoe hun persoonsgegevens worden gebruikt of die door verkeerde verwerking daarvan in de knel komen.

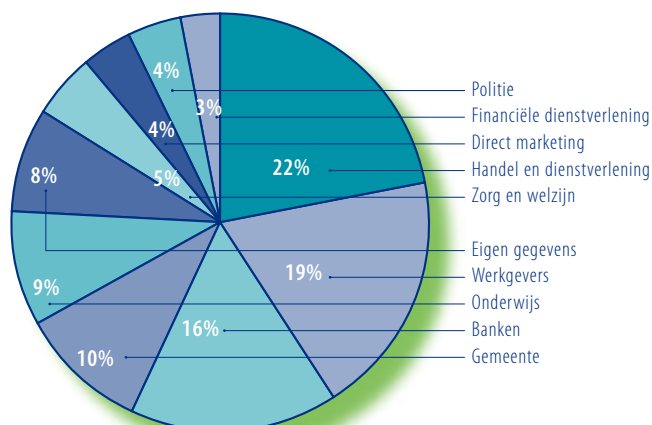
Om burgers gemakkelijker in staat te stellen zelf hun problemen met het gebruik van hun persoonsgegevens aan te pakken, is in 2006 de publiekswebsite www.mijnprivacy.nl ontwikkeld. De website geeft antwoord op de meestvoorkomende vragen. De site is de lucht ingegaan op 28 januari 2007, de eerste keer dat de door de Raad van Europa ingestelde Data Protectie Dag is gevierd. De datum verwijst naar de ondertekening op 28 januari 1981 van het Europese gegevensbeschermingsverdrag. Het doel van deze dag is de Europese burgers beter te informeren over hun rechten als het gaat om het gebruik van hun persoonsgegevens door overheden, bedrijven en andere organisaties.

Krachtiger communicatie

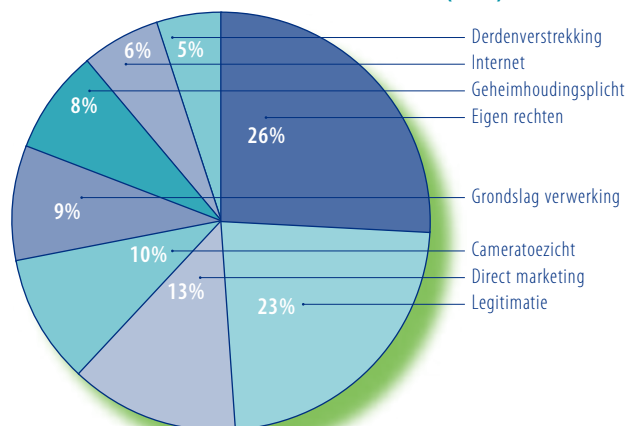
Het belang van goede voorlichting en krachtige communicatie daarover als essentiële voorwaarden om gegevensbescherming effectiever te maken, wordt gedeeld door alle nationale toezicht-houders. Burgers moeten weten welke rechten zij hebben en wat deze voor hen betekenen. Vooral de jeugd, opgevoed met nieuwe technologie, moet bewuster worden gemaakt van de gevaren van toenemende surveillancetechnieken. Communicatie kan daarnaast dienen als krachtige hefboom voor effectuering van privacyrechten.

Dit is een van de aanbevelingen die zijn opgesteld door de Internationale Conferentie van datatoezichthouders op 2 en 3 november 2006 te Londen. De toezichthouders overlegden aan de hand van een op initiatief van de Britse toezichthouder opgesteld rapport onder de titel *A Surveillance Society*. Het rapport biedt onder meer een inzicht in het dagelijks leven in de controlesamenleving over tien jaar, wanneer technische middelen bij wijze van routine en op grote schaal worden gehanteerd om onze activiteiten te volgen en te registreren, met gevolgen die veel verder gaan dan aantasting van het privéleven. De toezichthouders hebben afgesproken om in onderlinge samenwerking te bezien of de traditionele methoden van toezicht gezien de nieuwe technieken nog voldoende effectief zijn en hoe zij zouden moeten worden aangepast. De nadruk ligt daarbij op verhoging van het bewustzijn, meer resultaatgericht werken en een communicatie-ver behandeling van zaken. Het CBP heeft zijn steun toegezegd aan het initiatief, waarin het veel van zijn de afgelopen jaren ontwikkeld gedachtegoed terugvindt.

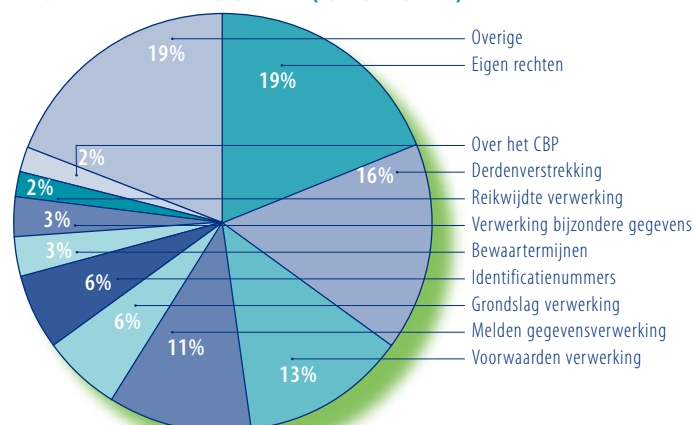
TELEFONISCHE VRAGEN VAN BURGERS OVER WELKE SECTOR (TOP 10)



TELEFONISCHE VRAGEN VAN BURGERS NAAR ONDERWERP (TOP 8)



VRAGEN VIA E-MAIL NAAR ONDERWERP (TOP 10 EN OVERIG)



Het maatschappelijk debat: de precare balans tussen veiligheid en privacy

De opkomst van de surveillance society die hierboven aan de orde is gesteld, komt dicht bij huis het duidelijkst tot uiting in de uitbreiding van controle- en opsporingsbevoegdheden als reactie op de angst voor de reële dreiging van terrorisme. In Nederland is omwille van de veiligheid, maar waarschijnlijk ook omwille van de veiligheidsbeleving, meer geïnvesteerd in uitbreiding van de bevoegdheden van politie en justitie en daarnaast in wetgeving om het verzamelen en bewaren van grote hoeveelheden gegevens van onverdachte burgers mogelijk te maken, dan in maatregelen die sociale cohesie kunnen bevorderen. Door deel te nemen aan het maatschappelijk en politiek debat wil het CBP bijdragen aan het vinden van een evenwicht tussen de noodzakelijk geachte controle van overheidswege enerzijds en het recht van de burger om van controle gevrijwaard te zijn anderzijds. Drie activiteiten uit 2006 worden hier aangestipt.

Veiligheid en de Wet bescherming persoonsgegevens

In de 'Johan de Wittlezing' die hij op 4 oktober 2006 te Dordrecht houdt, gaat CBP-voorzitter Jacob Kohnstamm in op de zijns inziens negatieve gevolgen van de proliferatie van maatregelen die de persoonlijke levenssfeer van de burger raken. "De rechtsstaat vormt een essentiële voorwaarde voor de duurzaamheid van het vertrouwen van burgers in elkaar en in de samenleving. Die rechtsstaat moet de burgers niet alleen een grote mate van veiligheid bieden maar moet ook de kaders aangeven waarbinnen de vrijheid geldt die nodig is om zich ten volle te kunnen ontplooiën, individueel en in alle relevante en legale vormen van samenwerking, in de zogenaamde civil society. Het vinden van de juiste maatvoering tussen die twee essentiële elementen van de rechtsstaat vergt een knap staaltje van evenwichtskunst". Kohnstamm geeft in zijn lezing enkele concrete spelregels aan die kunnen bijdragen tot dit evenwicht. Hiertoe behoren het aantonen van de noodzaak van nieuwe politieke of justitiële bevoegdheden en het vermijden van een niet ongevaarlijke vermenging van inlichtingen- en politiewerk.

De andere helft van de dubbellesing is gehouden door de toen net demissionaire minister van Justitie Donner.

Veiligheid en privacy van burgers

De boodschap van de hierboven genoemde voordracht herhaalt de CBP-voorzitter tijdens een debat 'Nederland controlestaat?' in De Balie in Amsterdam op 17 november. "Een beetje privacy inleveren omwille van grotere veiligheid valt onder omstandigheden zeker te billijken. Maar dan moeten nut en noodzaak van nieuwe bevoegdheden in de strijd tegen terrorisme wel aangetoond worden. Want inadequaat optreden van daarbij betrokken overheidsorganen mag geen reden zijn om aan grondrechten van burgers te tornen". Tot nu toe zijn nut en noodzaak niet aangetoond, aldus Kohnstamm. Dat is gebleken uit de evaluatie van de aanslagen van 11 september 2001 en de moord op Theo van Gogh. Politie, justitie en veiligheidsdiensten beschikten vooraf wel degelijk over relevante informatie over de daders, maar gebrek aan samenwerking en/of onjuiste analyse van die informatie stond verijdeling van de aanslagen in de weg.

Veiligheidsbelangen en privacy-noden

De spanning tussen veiligheid en privacy in het publieke en politieke debat is naar het CBP vermoedt niet zozeer te wijten aan de positionering van veiligheid en privacy als tegenpolen. Meer voor de hand ligt het te veronderstellen dat emotioneel of cultureel bepaalde drijfveren verhinderen dat crime fighters en privacyfundamentalisten zich in elkaars standpunten willen inleven. Met medewerking van en medefinanciering door de ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties heeft het CBP in 2005 prof. mr. H.B.R.M. Kummeling en prof. dr. mr. E.R. Muller opdracht gegeven een onderzoek te doen naar de verhouding tussen veiligheid en privacy. In 2006 is het grootste deel van het uitvoerend werk gedaan. Dat bestond uit uitgebreid multidisciplinair literatuuronderzoek en het voeren van groepsgesprekken met vertegenwoordigers van uiteenlopende groepen die in het dagelijks leven geconfronteerd worden met de afwegingen tussen veiligheidsbelangen en privacyvereisten. In 2007 zullen de resultaten van het onderzoek in enige vorm hun beslag krijgen. Het CBP zal op basis daarvan een congres organiseren.

Verbreding draagvlak: het Nationaal Mensenrechteninstituut

Op 24 oktober 2006 is door de Tweede Kamer een motie aangenomen over de oprichting van een Nationaal Instituut voor de Rechten van de Mens. Dat betekent dat er na een langdurig voortraject parlementaire steun is voor het NIRM. In de motie wordt de regering opgeroepen zo spoedig mogelijk alle beleidsmatige en juridische voorbereidingen te treffen om te komen tot de oprichting van het instituut.

Het 'oprichtingsconsortium' waarin naast het CBP de Nationale ombudsman, de Commissie gelijke behandeling en het Studie en Informatiecentrum Mensenrechten deelnemen, is bezig met de afronding van een rapport over het takenpakket en de inrichting van het NIRM. Dit zal naar verwachting begin 2007 gereed zijn.

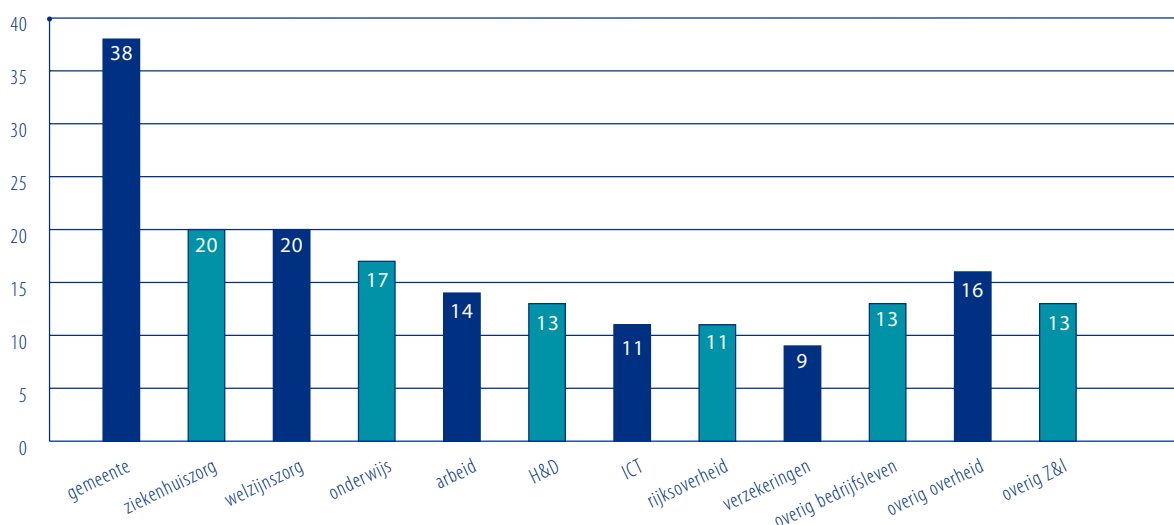
In een brief van 5 december 2006 schrijft de demissionair minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Kamer zich voor te stellen dat gezien de meerjarige financiële consequenties die aan het instellen van een mensenrechteninstituut verbonden zijn, de politieke besluitvorming daarover in het volgend kabinet plaats zal vinden. Het CBP blijft alert op de ontwikkelingen.

Samenwerking met andere toezichthouders

Functionarissen voor de gegevensbescherming

Integratie van het toezicht op de naleving van de Wbp in de reguliere bedrijfsvoering levert een effectieve bijdrage aan de bescherming van de persoonlijke levenssfeer van klanten, personeelsleden en burgers. Het CBP is daarom een sterke voorstander van het aanstellen van interne toezichthouders bij bedrijven, instellingen en brancheorganisaties in zowel de publieke als de private sector. Waar een 'eigen' functionaris is aangesteld, kan het CBP op afstand blijven. De FG's zijn verenigd in het in 2003 opgerichte Nederlands Genootschap van Functionarissen voor de Gegevensbescherming. Het College overlegt een keer per jaar met het Genootschap. Het uitwisselen van visies op en ervaringen met toezicht draagt bij aan een effectieve en eigentijdse invulling van de Wbp.

FG'S PER SECTOR (TOTAAL 195)



Protocol met IGZ ondertekend

De inspecteur-generaal van de Inspectie voor de gezondheidszorg (IGZ), G. van der Wal en de voorzitter van het CBP, J. Kohnstamm, hebben in november 2006 een samenwerkingsprotocol ondertekend, waarin de samenwerking tussen beide toezichthouders met overlappende bevoegdheden op het terrein van de gezondheidszorg structureel vorm krijgt. De samenwerking tussen het CBP en de IGZ moet leiden tot een effectiever toezicht op de nieuwe ontwikkelingen ten aanzien van het gebruik van persoonsgegevens in de zorgsector, zoals het Elektronisch Patiëntendossier, en tot grotere transparantie voor de sector.

Zowel de IGZ als het CBP houden toezicht op het gebruik van persoonsgegevens in de zorgsector. In het samenwerkingsprotocol, dat een geldigheidsduur heeft van drie jaar, is vastgelegd dat bij samenloop van bevoegdheden de IGZ zich primair zal richten op het toezicht op de kwaliteit van zorgverlening en het CBP op de toepassing en naleving van de Wbp. In 2007 zal een gezamenlijk onderzoek worden uitgevoerd naar de informatiebeveiliging in ziekenhuizen.

Verwerking bijzondere persoonsgegevens door toezichthouders

In het kader van hun onderzoeken verzamelen de gemeentelijke, provinciale en nationale ombudsmannen en rekenkamers, accountants e.d. bijzondere persoonsgegevens. Dat is vaak onvermijdelijk. De vereiste wettelijke grondslag voor een dergelijke verwerking ontbreekt echter. Het CBP heeft de minister van Justitie daar in 2005 reeds op gewezen. Omdat het een verwerking is van structurele aard ligt het voor de hand dat er een wettelijke grondslag gecreëerd wordt. Ontheffing als bedoeld in artikel 23 Wbp door het CBP zou oneigenlijk zijn. Onder de strikte voorwaarde dat de voor de totstandkoming van de desbetreffende wettelijke regeling verantwoordelijk bewindspersoon aangeeft dat wetgeving op korte termijn zal worden geïnitieerd, is het CBP wel bereid om over te gaan tot een inhoudelijke beoordeling van een verzoek om voor een beperkte periode de gevraagde ontheffing te verlenen.

In november 2006 heeft het CBP de minister van Justitie nogmaals geattendeerd op het gebrek en hem de suggestie aan de hand gedaan om dit urgente probleem mee te laten liften met het hieronder te bespreken voorstel voor administratieve lastenverlichting.

Minder administratieve lasten door wijziging van de Wbp

De reeds lang lopende voorstellen van het CBP tot verlichting van administratieve lasten zonder dat aan het beschermingsniveau van de Wbp wordt getornd, zijn in november 2006 ten langen leste met enige urgentie door het ministerie van Justitie opgepakt.

In december 2004 heeft het CBP de minister van Justitie tien voorstellen gedaan voor administratieve lastenverlichting samenhangend met de Wbp. Deze voorstellen hadden de steun van VNO-NCW. Pas in juni 2006 heeft de minister de Tweede Kamer hierover een brief gezonden. Daarin zijn slechts enkele van de voorstellen van het CBP overgenomen. De minister heeft daarbij de toezegging gedaan om na het najaar alsnog wijzigingsvoorstellen te doen ter verlichting van de administratieve lasten. Het uitblijven van actie tot op dat moment en de inhoud van de brief gaven het CBP de indruk dat het uitvoeren van zijn voorstellen geen hoge prioriteit had. In september 2006 heeft het CBP er daarom samen met VNO-NCW bij de minister op aangedrongen, deze voorstellen alsnog met voorrang op te pakken. Bij uitblijven van een reactie heeft het in november 2006, nu samen met VNO-NCW en ACTAL, dit verzoek herhaald.

In beide brieven ligt de nadruk op een drietal voorstellen:

- een vrijstelling van de vergunningplicht voor de doorgifte van persoonsgegevens naar landen buiten de Europese Unie bij gebruik van ongewijzigde EU-modelcontracten;
- het uitbreiden en verduidelijken van het Vrijstellingenbesluit Wbp;
- het nader wettelijk invullen van de open uitzondering op het verbod op de verwerking van strafrechtelijke gegevens, met het oog op het terugdringen van de hoeveelheid voorafgaande onderzoeken door het CBP.

Ditmaal heeft Justitie wel voortvarend gereageerd. Naar verwachting zal op korte termijn een voorstel tot wijziging van de Wbp worden ingediend bij de Tweede Kamer, waarin de voorstellen van het CBP zijn verwerkt.

Openbaarheid van toezicht

Het actief openbaar maken van informatie van toezichthouders is sterk in beweging. Niettemin was tot voor kort nog maar weinig onderzoek gedaan naar dit specifieke onderwerp. Wel was duidelijk dat er op dit gebied grote verschillen bestaan tussen de verschillende toezichthouders en dat de informatie die actief openbaar wordt gemaakt, vaak intensief door het publiek wordt geraadpleegd. In december 2006 heeft Advies Overheid.nl een rapport uitgebracht waarin een inventarisatie is gemaakt van de openbaarheid van informatie van vijftientig van de meer dan honderd toezichthouders in Nederland, waaronder het CBP. Wat de informatie over de inrichting van het toezicht betreft, constateren de onderzoekers dat het CBP deze verstrekt, zonder onderbouwing of operationele details, zoals de meeste toezichthouders. Deze informatie scoort wel positief wat betreft de directe beschikbaarheid ervan op de website.

Resultaten van onderzoeken worden openbaar gemaakt. Wat betreft de openbaarmaking van de naam van de onderzochte organisatie hanteert het CBP een glijdende schaal. Bij overheden is het CBP minder terughoudend dan bij bedrijven.

Certificering

Bedrijven en organisaties die een Privacycertificaat hebben ontvangen, kunnen met dit certificaat zowel intern als aan de buitenwereld inzichtelijk maken dat zij aan de Wbp willen voldoen en dat zij hun administratieve bedrijfsprocessen hebben ingericht conform de eisen die de Wbp aan gegevensverwerkingen stelt. Voor de burger betekent dit dat hij er in beginsel van uit kan gaan dat gecertificeerde organisaties zorgvuldig met zijn persoonsgegevens omgaan.

In oktober 2006 heeft het CBP het project Audit Aanpak afgerond met de goedkeuring van een door de marktpartijen ontwikkelde richtlijn Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens. Doel van deze richtlijn is grondslagen vast te stellen en aanwijzingen te geven voor de uitvoering van deze opdrachten. Daarnaast wordt door middel van deze richtlijn ook de mogelijkheid geboden voor externe beoordeling en certificering.

Organisaties kunnen zo de kwaliteit van de bescherming van persoonsgegevens in het proces van verwerkingen (laten) toetsen en een complianceonderzoek uitvoeren.

Het certificaat kan het vertrouwen van de consument in het bedrijf vergroten en de kwaliteit van de bedrijfsvoering positief beïnvloeden.

In het nu afgeronde project 'Audit Aanpak' hebben het CBP en zijn voorganger de Registratiekamer in samenwerking met marktpartijen (accountantsorganisaties, adviesbureaus en beroepsorganisaties) een viertal zelfreguleringsproducten ontwikkeld: de Quickscan, de Wbp-zelfevaluatie, het Raamwerk Privacy Audit en de Handreiking bij het raamwerk Privacy Audit.

> Wachtwoord voor iedereen toegankelijk

Een werkgever wil dat zijn werknemers hun persoonlijke wachtwoord om in te loggen op de computer prijsgeven. Zo heeft iedereen op het werk toegang tot andermans persoonlijke e-mails en documenten. De reden is dat de werkgever vindt dat ook bij ziekte of vakantie van een werknemer diens gegevens toegankelijk moeten zijn. "Hoewel ik niets te verbergen heb, vind ik niet dat dit van ons gevraagd mag worden", klaagt een werknemer.





Internationaal

Burgers en bedrijven worden steeds mobieler, niet alleen fysiek, maar ook door gebruik te maken van het internet. Verwerking van gegevens gaat steeds vaker over grenzen heen. Privacybescherming is niet meer denkbaar zonder rekening te houden met internationale ontwikkelingen. Ook vanwege de toenemende focus in internationaal en Europees verband op de bestrijding van terrorisme en grensoverschrijdende criminaliteit is het essentieel dat het CBP en collega-toezichthouders de vinger aan de pols houden bij de uitwerking van plannen voor de uitwisseling van gegevens.

Passagiersgegevens

Op 30 mei 2006 heeft het Hof van Justitie EG de door Europa getroffen maatregelen die de verstrekking van passagiersgegevens aan de Amerikaanse autoriteiten mogelijk moesten maken, nietig verklaard. De Amerikaanse autoriteiten willen met het oog op onder meer het bestrijden van terrorisme en andere zware criminaliteit dat luchtvaartmaatschappijen informatie verstrekken over passagiers die naar de Verenigde Staten vliegen. Na de uitspraak van het Hof is tussen de EU en de VS een tijdelijk verdrag overeengekomen. De Artikel 29-werkgroep van de Europese databeschermingstoezichthouders heeft zich kritisch uitgelaten over dat tijdelijke verdrag, dat de opmaat zal vormen voor onderhandelingen over een nieuwe en langduriger overeenkomst over de verstrekking van passagiersgegevens die uiterlijk in augustus 2007 in werking moet treden. Het tijdelijke verdrag lijkt een ruimere interpretatie van de eerder overeengekomen afspraken ter bescherming van persoonsgegevens mogelijk te maken, zoals een bredere verspreiding van de informatie onder de Amerikaanse autoriteiten voor nieuwe doeleinden. De werkgroep heeft ook het belang van de zogenaamde 'joint review' onderstreept, de jaarlijkse evaluatie van de toepassing van de afspraken door EU en VS tezamen. Deze zou ook in 2007 doorgang moeten vinden.

Het belang van voldoende transparantie werd beklemtoond door de voorzitter van het CBP in een met KLM, Air France en de Franse toezichthouder georganiseerde bijeenkomst met beleidsmakers in Brussel in december 2006. Indien op grond van informatie over effectiviteit en efficiency niet aannemelijk kan worden gemaakt dat de te nemen veiligheidsmaatregelen noodzakelijk en proportioneel zijn, kunnen geen goede afwegingen worden gemaakt tussen veiligheid, de bescherming van grondrechten en de economische belangen van luchtvaartmaatschappijen, aldus Kohnstamm. In de onderhandelingen met de VS zal Europa met één stem moeten spreken en aandringen op de noodzakelijke transparantie en verantwoording. Deze kritische blik ten aanzien van nut en noodzaak van nieuwe maatregelen en deze eensgezindheid zal ook essentieel zijn in het licht van de Europese plannen voor het gebruik van passagiersgegevens, die in 2007 zullen worden uitgewerkt.

De Swift-zaak: verstrekking bankgegevens

In juni 2006 ontvingen verscheidene nationale toezichthouders een alarmerende brief van een niet-gouvernementele organisatie over de verstrekking van bankgegevens aan de Amerikaanse overheid. Swift, een in België gevestigde en wereldwijd opererende financiële dienstverlener, faciliteert voor banken wereldwijd de internationale geldoverboeking. De Amerikaanse overheid had Swift sinds 2001 verplicht om in het kader van terrorismebestrijding informatie over deze overboeking van in Europa gevestigde banken aan de United States Treasury te overleggen. Dit gegevenstransport is in strijd met de Europese Richtlijn. De Europese toezichthouders hebben besloten deze kwestie gezamenlijk te benaderen. Hierbij heeft de Belgische toezichthouder, onder wiens toezicht Swift valt, het voortouw genomen en is in nauw onderling overleg een opinie uitgebracht door de Artikel 29-werkgroep.

De werkgroep heeft geconcludeerd dat de informatie aan de Amerikaanse autoriteiten is verstrekt op een wijze die niet in overeenstemming is met de Europese regels voor gegevensbescherming. Naar aanleiding van deze analyse wordt overleg gevoerd met Swift over de acties die het moet ondernemen om rechtmatigheid te garanderen. Ook op nationaal niveau ondernemen de toezichthouders activiteiten. Zo heeft het CBP contact gezocht met De Nederlandsche Bank, de Nederlandse Vereniging van Banken en de minister van Financiën. Het CBP heeft banken gewezen op hun verantwoordelijkheid om, als gebruikers van het Swift-systeem, te garanderen dat gegevens van hun klanten in overeenstemming met de wet worden verwerkt. Swift, nationale partijen en de Europese Commissie onderzoeken alle de mogelijkheden om rechtmatigheid op de kortst mogelijke termijn te garanderen. De eerste resultaten hiervan worden in 2007 verwacht.

Vergroting bewustzijn

De problemen rond de verstrekking van passagiersgegevens en van bankgegevens tonen aan hoe in het alledaagse leven van burgers het belang van gegevensverwerkingen toeneemt. Deze verwerkingen gaan steeds vaker over grenzen heen, wat mede mogelijk is gemaakt door de voortschrijdende technologie, waaronder het gebruik van internet. Niet alleen de burgers zelf worden via internet en fysiek mobiel. Ook bedrijven organiseren zich in toenemende mate mondiaal. Multinationals 'outsourcen' hun activiteiten - inclusief de daarbij behorende persoonsgegevens - naar landen buiten de EU zoals India en China en in het buitenland gevestigde bedrijven zijn actief op de Nederlandse markt. Door globalisering internationaliseert ook de (georganiseerde) criminaliteit, wat noodzaakt tot samenwerking op het terrein van politie en justitie binnen en buiten de EU. Ook zet deze ontwikkeling overheden van landen buiten de EU er in toenemende mate toe aan om steeds meer verplichtingen op te leggen die rechtstreeks gevolgen hebben voor bedrijven en burgers die zich bevinden binnen de grenzen van de EU en de bescherming van de Europese wetgeving.

Burgers zijn zich niet altijd bewust van de mogelijke gevolgen hiervan voor hun privacy. Daarom hebben de Raad van Europa en de Europese Unie in 2006 besloten om vanaf 2007 een jaarlijkse Europese dataproductiedag te organiseren op 28 januari, de verjaardag van het Verdrag van Straatsburg van 1981, het 'moeder-verdrag' voor gegevensbescherming. Dit initiatief om het bewustzijn van burgers over privacy te vergroten is ontwikkeld door het Raadgevend Comité van het Verdrag van Straatsburg, waarin het CBP zitting heeft.

De eerste dataproductiedag is gehouden op 28 januari 2007. Ongeveer dertig Europese landen hebben activiteiten georganiseerd. Het CBP heeft op die dag zijn nieuwe burgerwebsite, www.mijnprivacy.nl, gelanceerd.

Surveillance society

De intensivering van gegevensverwerking kan bedrijfseconomische en organisatorische voordelen meebrengen, maar bergt ook risico's in zich. Deze zijn in november 2006 uiteengezet door de Britse gastheer van de 28e Internationale Conferentie van

dataprotectietoezichthouders. In het rapport over de 'surveillance society' dat in opdracht van de Britse toezichthouder is opgesteld, wordt aangegeven hoe door technische ontwikkelingen er steeds meer en breder inzetbare controlemogelijkheden komen, die alle activiteiten van burgers kunnen volgen en registreren. Onzichtbare, ongecontroleerde of overmatige vormen van controle kunnen gevolgen hebben die veel verder gaan dan aantasting van het privé leven.

"Surveillance is two-sided, and its benefits must be acknowledged. Yet at the same time risks and dangers are always present in large-scale systems and of course power does corrupt or at least skews the vision of those who wield it".

(*Surveillance Studies Network, A Report on the Surveillance Society, September 2006, p. 2*)

De toezichthouders hebben afgesproken om in onderlinge samenwerking te bezien of de traditionele methoden van toezicht met het oog op de nieuwe technieken nog wel voldoen en hoe deze eventueel moeten worden aangepast.

Strategie onder de loep

De toenemende controletechnieken maken ook een herbezinning nodig op de werkwijze van de toezichthouders zelf. Om beter op trends en technologische ontwikkelingen te kunnen anticiperen hebben zij tijdens de Internationale Conferentie besloten om hun eigen efficiency en effectiviteit grondig onder de loep te nemen en hun technische kennis te versterken. Om deze ideeën kracht bij te zetten werd de verklaring 'Gegevensbescherming communiceren en effectiever maken' aangenomen. In de verklaring wordt gewezen op de noodzaak van gegevensbescherming in de samenleving, wordt uitvoerig ingegaan op de bedreigingen van de burgerrechten en de bescherming van persoonsgegevens die zich overal ter wereld voordoen en op de vele hoofdbreken die dit de toezichthoudende instanties kost. Uit de verklaring worden bovendien diverse voorstellen gedistilleerd voor gecoördineerde acties en initiatieven evenals voor de ontwikkeling van een nieuwe, gemeenschappelijke communicatiestrategie, die in 2007 verder zullen worden ontwikkeld.

Samenwerking bij handhaving

In een internationaliserende omgeving vergroot ook het gezamenlijk optrekken bij onderzoek en handhaving de effectiviteit van de toezichthouders. Daarom hebben de nationale toezichthouders

in het kader van de Artikel 29-werkgroep van de Europese Unie in 2006 een gecoördineerde handhavingssactie ondernomen. In alle landen is een gezamenlijk ontwikkeld onderzoek gedaan naar de naleving van de privacyregels bij de zorgverzekeraars. Hierover meer in het hoofdstuk Gezondheidszorg. De medewerking van de sector aan het onderzoek was zeer bevredigend. In 2007 zal de Artikel 29-werkgroep uit dit eerste gezamenlijke onderzoek conclusies trekken, zowel over de naleving bij de zorgverzekeraars, als over het middel handhaving in Europa. Ook zullen mogelijke volgende gezamenlijke onderzoeken en handhavingssacties worden besproken.

Europese aanpak van doorgifte van persoonsgegevens door multinationals

De afgelopen jaren heeft de Artikel 29-werkgroep een gezamenlijk beleid ontwikkeld voor de behandeling van Binding Corporate Rules (BCR's), interne gedragscodes van multinationals op grond waarvan zij van de nationale toezichthouders een vergunning kunnen krijgen voor de doorgifte van gegevens naar onderdelen van het concern gevestigd in derde landen. Op basis van dit beleid zijn in 2006 de eerste gecoördineerde Europese vergunningenprocedures van start gegaan en is de eerste BCR via deze procedure in meerdere landen goedgekeurd. Het CBP hecht zeer groot belang aan vertrouwen en samenwerking tussen toezichthouders op dit terrein en aan een zo efficiënt mogelijke inzet van schaarse middelen. Op een door de Artikel 29-werkgroep en de Europese Commissie georganiseerde conferentie over de internationale doorgifte van persoonsgegevens in oktober 2006, heeft het CBP daarom aangekondigd dat het, indien juridisch mogelijk, van plan is om de in het kader van de gecoördineerde vergunningenprocedure door andere toezichthouders voorgelegde BCR's zonder nadere inhoudelijke beoordeling goed te keuren.

Justitie- en politiesamenwerking

De daadkracht van EU-regeringen als het gaat om het invoeren van veiligheidsmaatregelen waarbij grensoverschrijdende gegevensuitwisseling centraal staat, staat in scherp contrast tot het aannemen van het Kaderbesluit bescherming persoonsgegevens ten behoeve van politie- en justitiesamenwerking. Volgens de Europese privacytoezichthouders is de enige werkbare optie een geharmoniseerde hoge beschermingsstandaard in de zogenaamde derde pijler. Dat is een logisch gevolg van de EU-afspraken over de ruimte van vrijheid, veiligheid en rechtvaardigheid. Een beperkte benadering zal in de praktijk niet werkbaar blijken en zal niet lei-

Het CBP neemt op reguliere basis deel aan de volgende internationale gremia:

- de Artikel 29-werkgroep van alle EU-dataprotectietoezichthouders
- toezichthoudende organen binnen de derde pijler van de EU, nl. de Gemeenschappelijke Controleautoriteit Schengen-informatiesysteem, de Gemeenschappelijke Controleautoriteit Douane-informatiesysteem, het Gemeenschappelijk Controleorgaan Europol en het Gemeenschappelijk Controleorgaan Eurojust
- het Raadgevend Comité van het Verdrag van Straatsburg; in 2006 had het CBP zitting in het Bureau van het Comité
- de jaarlijkse Internationale Conferentie van dataprotectietoezichthouders
- de jaarlijkse lenteconferentie van Europese dataprotectietoezichthouders
- de aan de lenteconferentie verbonden halfjaarlijkse Case Handling Workshop voor de uitwisseling van best practices tussen DPA's
- de aan de lenteconferentie verbonden Working Party on Police van alle Europese dataprotectietoezichthouders

den tot vertrouwen in Europese politie- en justitiesamenwerking. Ruimere uitwisseling van informatie en beschikbaarstelling van gegevens in het kader van opsporing aan justitie en politie in andere lidstaten kan alleen als er een toereikend en geharmoniseerd systeem beschikbaar is voor de bescherming van persoonsgegevens. Dit moet bovendien niet alleen gelden voor de uitwisseling tussen lidstaten onderling, maar ook voor de overdracht van gegevens aan derde landen en internationale instellingen. Aangezien de Europese toezichthouders zich ernstig zorgen maken over het verloop van de onderhandelingen over het Kaderbesluit hebben ze op 2 november 2006 en marge van de Internationale Conferentie van Data Protection Commissioners te Londen een verklaring uitgegeven waarin zij nogmaals wijzen op de absolute noodzaak van een hoog beschermingsniveau voor persoonsgegevens die worden uitgewisseld. De toezichthouders hebben daarbij een dringend beroep gedaan op de lidstaten om de fundamentele rechten en vrijheden van de burgers in de Unie te respecteren en te versterken.

Europees visuminformatiesysteem

Nadat het CBP in 2005 had bijgedragen aan een opinie van de Artikel 29-werkgroep over de Europese VIS-verordening, die de uitwisseling van visumgegevens tussen de EU-lidstaten mogelijk maakt, heeft het CBP in 2006 op nationaal niveau hierover geadviseerd. Geen enkel Europees systeem is qua omvang en capaciteit met het VIS vergelijkbaar. Er zullen persoonsgegevens, waaronder biometrische gegevens, van miljoenen mensen in een centrale gegevensbank worden opgeslagen en uitgewisseld. Het voorstel maakt ruime toegang tot het VIS mogelijk voor brede doeleinden. Het CBP begrijpt de noodzaak om misbruik van visa aan te pakken, evenals het fenomeen van malafide sponsors, waaronder mensensmokkelaars. Het is echter onduidelijk of en hoe de huidige voorstellen daaraan daadwerkelijk een bijdrage gaan leveren. Het CBP heeft bovendien zorgen geuit over het gebrek aan garanties voor gegevensbescherming in de huidige voorstellen, over het feit dat gegevens uit VIS voor wetshandavingsdoeleinden gebruikt kunnen worden en over de hoeveelheid informatie die over sponsors van visa-aanvragers wordt opgeslagen, wat kan leiden tot de registratie van persoonsgegevens van vele veelal bonafide Europese burgers.

Schengen Informatiesysteem II

Het CBP is vertegenwoordigd in diverse toezichthoudende organen binnen de derde pijler van de EU, waaronder de Gemeenschappelijke Controleautoriteit Schengen-informatiesysteem (GCA Schengen). De belangrijkste ontwikkeling in 2006 bleef het proces om het huidige Schengen Informatiesysteem (SIS) te vervangen door een nieuw systeem (SIS II). Daardoor moet het mogelijk worden voor de nieuwe EU-lidstaten om mee te doen aan het systeem, dat is opgericht om de controle aan de buitengrenzen van de EU te versterken zodat grenscontroles tussen de deelnemende landen opgeheven konden worden. In vervolg op het eerdere advies van oktober 2005, adviseerde de GCA Schengen wederom over het door de Europese Commissie voorgestelde juridische kader voor het nieuwe informatiesysteem. De GCA Schengen is daarnaast een onderzoek gestart naar het gebruik van signaleringen op grond van artikel 99 van de

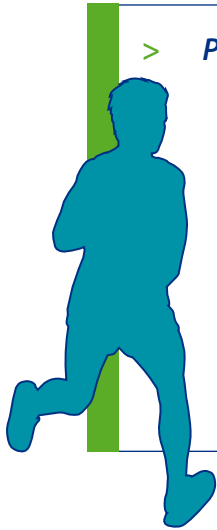
Schengen Uitvoeringsovereenkomst in alle EU-lidstaten. Artikel 99 ziet op onopvallende controle en gerichte controle ter vervolging van strafbare feiten, ter voorkoming van gevaar voor de openbare veiligheid of ter voorkoming van bedreiging van de veiligheid van de Staat. Het gezamenlijke onderzoek zal begin 2007 zijn afgerond.

Verdrag van Prüm

Het Verdrag inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie van 27 mei 2005 (hierna: het verdrag van Prüm) regelt onder andere een vereenvoudigde informatie-uitwisseling tussen opsporings- en politiele autoriteiten. Naast Nederland hebben ook Duitsland, Frankrijk, Luxemburg, België, Spanje, Oostenrijk en Italië het verdrag van Prüm ondertekend. Italië, Portugal, Slovenië, Finland, Zweden en Roemenië hebben formeel aangekondigd te willen toetreden. Met dit verdrag wordt het onder meer mogelijk om voor identificatie en opsporing een individueel DNA-profiel rechtstreeks te vergelijken met DNA-profielen uit de geautomatiseerde databanken van de overige aangesloten lidstaten. Het geeft daardoor de mogelijkheid om direct te weten te komen of een onbekend spoor dat in de ene lidstaat is aangetroffen een link heeft met een onderzoek in een van de aangesloten landen. Dit wordt ook mogelijk gemaakt voor vingerafdrukken en voertuigregisters. Daarnaast is afgesproken dat ter voorkoming van terroristische aanslagen persoonsgegevens tussen de lidstaten kunnen worden uitgewisseld.

Het CBP heeft op 27 juli 2006 samen met de toezichthouders uit de landen die het verdrag van Prüm hebben ondertekend, de tekst van het verdrag beoordeeld en de opstellers van het implementatieverdrag geadviseerd. De toezichthouders oordelen dat, aangezien het systeem van Prüm uitgaat van bevraging van indexgegevens binnen een hit/no hit-systeem, waarbij identificerende data niet mogen worden meegenomen in een hit (daarvoor is een rechtshulpverzoek nodig), het verdrag van Prüm in principe voldoende waarborgen biedt. De toezichthouders benadrukken evenwel dat voor de goede werking van het systeem een overkoepelend, geharmoniseerd en hoog niveau van gegevensbescherming nodig is. Daarin zou het bovengenoemde Kaderbesluit bescherming persoonsgegevens ten behoeve van politie- en justitiesamenwerking moeten voorzien.

Vooruitkijkend: Duitsland zal tijdens zijn voorzitterschap van de EU in de eerste helft van 2007, namens alle ondertekenaars van het verdrag van Prüm, aan de lidstaten die het verdrag nog niet hebben ondertekend, de vraag voorleggen of zij instemmen met het één op één omzetten van het Prüm verdrag in EU-regelgeving. Omzetting in EU-regelgeving zou de doelstelling van het Haags Programma om vanaf 1 januari 2008 de informatie-uitwisseling in de Unie te baseren op het zogenaamde beschikbaarheidsbeginsel dichterbij brengen. Waar Prüm zich nog beperkt tot DNA en vingerafdrukken, zal een verdergaande samenwerking ook andere databanken betreffen waarbij de bevragingen zien op reeds geïdentificeerde individuen. Het CBP zal uiteraard ook deze ontwikkelingen volgen en erop toezien dat bij eventuele omzetting in EU-regelgeving er geen afbreuk wordt gedaan aan bestaande waarborgen en individuele rechten.



> *Privéleven topsporter*

Een lid van de Nederlandse topsportselectie moet elke dag bijhouden waar hij op welk moment is en hoe hij daar is te bereiken. De bond zegt dat dit mede nodig is ten behoeve van out of competition dopingcontroles. Die moeten op elk willekeurig moment kunnen plaatsvinden. De topsporter vindt echter dat het niemand wat aangaat wat hij buiten zijn wedstrijd- en trainingsuren in zijn privéleven doet. "Is deze werkwijze van de bond geoorloofd?" wil hij graag weten.

Toekomst van Europol

Europol verwerkt een grote hoeveelheid gevoelige persoonsgegevens over criminele activiteiten met het doel de samenwerking van de politie bij de bestrijding van terrorisme, illegale drugshandel en andere ernstige vormen van internationale georganiseerde criminaliteit te verbeteren. Het waarborgen van gegevensbescherming is een belangrijk element en vormt de hoeksteen van het wettelijk stelsel voor de verwerking van persoonsgegevens door Europol.

Op 17 oktober 2006 organiseerde het Gemeenschappelijk Controleorgaan van Europol (GCO), waarvan het CBP lid is, een conferentie waarbij gegevensbescherming binnen Europol centraal stond. Het GCO meent dat op het terrein van politie-samenwerking doeltreffend kan worden opgetreden zonder afbreuk te doen aan individuele rechten. Bovendien meent het GCO dat het in Europols eigen belang is persoonsgegevens te beschermen, aangezien dit ook waarde toevoegt aan de kwaliteit van haar gegevens.

Volgende op de discussie hoe de effectiviteit van Europol te verbeteren, presenteerde de Europese Commissie op 20 december 2006 een voorstel voor een nieuw Europol Besluit. Met dit voorstel worden de taken en bevoegdheden van Europol uitgebreid, krijgt Europol een andere juridische status en krijgt Europol bovendien meer mogelijkheden om informatie op te slaan en te bewerken, bijvoorbeeld over terroristische groepen of over kinderpornografie. Het CBP blijft binnen het GCO van Europol de ontwikkelingen met betrekking tot dit voorstel nauwlettend in de gaten houden om erop toe te zien dat een hoog niveau van gegevensbescherming ook in de toekomst bij Europol zal worden gewaarborgd.

Het CBP heeft in 2006 deelgenomen aan de jaarlijkse audit van de Europol-systemen door het GCO. Onderzocht is onder andere het gebruik van analysebestanden en in hoeverre Europol gevolg heeft gegeven aan aanbevelingen van het GCO van voorafgaande jaren.



Openbaar bestuur

Het wetsvoorstel tot invoering van het burgerservicenummer heeft het afgelopen jaar met vertraging de Eerste Kamer bereikt. Enkele zwaarwegende punten van kritiek van het CBP worden door verschillende fracties in beide kamers gedeeld, maar het kabinet is daaraan niet tegemoetgekomen. Ook op een veelheid aan andere, zeer uiteenlopende, terreinen, van de aanpak van hennepkwekerijen tot de export van studiefinanciering, is het CBP alert op ontwikkelingen die mogelijk schadelijk zijn voor het vertrouwen van burgers in de wijze waarop centrale of lagere overheden met hun persoonsinformatie omgaan.

Burgerservicenummer

Het burgerservicenummer (BSN) had op 1 januari 2006 ingevoerd moeten zijn als opvolger van het sofinummer. Deze datum is niet gehaald en 1 januari 2007 evenmin. De behandeling in de Tweede Kamer van de Wet algemene bepalingen burgerservicenummer vergde meer tijd dan was verwacht en voor de behandeling in de Senaat geldt hetzelfde.

Het CBP heeft in het voorjaar van 2006 de verschillende fracties in de Tweede Kamer nogmaals benaderd om zijn standpunt over het wetsvoorstel kenbaar te maken en aan te geven dat het wetsvoorstel op essentiële onderdelen geen waarborgen biedt voor een zorgvuldige omgang met de persoonsgegevens van de burger. Wanneer in de keteninformatie in backoffices iets fout gaat met het gebruik van het BSN en de daaraan gekoppelde persoonsgegevens, zijn de gevolgen voor de burger niet te overzien. Het CBP heeft daarom nogmaals gewezen op de noodzaak voor een wettelijke verankering van een vangnet waar de burger terecht kan bij klachten over, of fouten of fraude met zijn of haar BSN. Deze input heeft geleid tot verschillende amendementen. Bij de uiteindelijke stemming in de Tweede Kamer hebben deze het echter niet gehaald.

Ook aan de vaste commissie in de Eerste Kamer heeft het CBP zijn zorgen over het wetsvoorstel geuit. Het CBP heeft gesproken over essentiële onderdelen uit zijn advies dat de minister en de Tweede Kamer niet hebben gevolgd. In het voorlopig verslag (21 november 2006) hebben alle fracties van de Eerste Kamer gezamenlijk de nodige kanttekeningen geplaatst bij het wetsvoorstel. In de memorie van antwoord van 19 december 2006 heeft de minister de vragen beantwoord. De antwoorden van de minister zijn voor het CBP niet bevredigend. Het CBP heeft de Eerste Kamer hierover geïnformeerd. Voor de vaste commissie is dat aanleiding geweest om begin 2007 opnieuw vragen te stellen aan de minister.

Zie voor de ontwikkelingen rond de invoering van het burgerservicenummer in de zorg p. 48 e.v.

Verwijsindex Antilliaanse risicjongeren

De minister voor Vreemdelingenzaken en Integratie heeft mede namens de burgemeesters van 21 zogenoemde Antillianengemeenten het CBP verzocht ontheffing te verlenen voor het verwerken van persoonsgegevens op basis van etniciteit in de 'Verwijsindex Antillianen' (VIA) en in de daarmee samenhangende gemeentelijke casusoverleggen. De VIA is – vooruitlopend op een algemene verwijsindex risicjongeren of andere wetgeving – een pilot voor intergemeentelijke informatie-uitwisseling ten behoeve van een persoonsgerichte benadering van specifieke doelgroepen. Het CBP is van oordeel dat door de minister de noodzaak van de gegevensverwerking in de VIA en in de gemeentelijke casusoverleggen is aangetoond en dat zij heeft zorg gedragen voor passende waarborgen voor de bescherming van de persoonlijke levenssfeer. Voor de inrichting en uitwerking van de VIA en de casusoverleggen zijn modellen opgesteld. De ontheffing is onder vijf voorwaarden en voor de duur van twee jaar verleend. Twee organisaties hebben bezwaar gemaakt tegen de ontheffing.

Bijdragen aan politieke partijen

Politieke partijen beschikken over een aantal inkomstenbronnen, zoals overheidssubsidies en ledencontributies. Ook zijn er bedrijven en personen die aan partijen bijdragen in geld of in natura verstrekken. Donateurs geven financiële steun vanwege sympathie voor de politieke opvattingen die de partij uitdraagt. Een ander oogmerk bij steunverlening kan zijn het uitoefenen van invloed op de standpuntbepaling van de politieke partij.

Oneigenlijke beïnvloeding van democratische processen is ongewenst. Om te voorkomen dat door de financiële ondersteuning alleen al de schijn van belangenverstrengeling ontstaat, schrijft de (ontwerp) Wet financiering politieke partijen voor dat politieke partijen inzicht verschaffen in de bijdragen die zij naast de overheidssubsidie ontvangen.

Omdat de politieke partijen in het oog moeten houden hoe hoog de bijdrage is die zij van een gever in een jaar ontvangen, dienen zij te beschikken over identificerende gegevens van elke niet-anonieme gever, ongeacht het bedrag per keer. Bijdragen vanaf € 2000 per jaar vallen in de 'gevaarzone'. Anonimiteit van de gever is daarbij niet gewenst.

Het CBP heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties geadviseerd over de ontwerp-wet. Het CBP is van oordeel dat de verwerking van bijdrage, naam, adres en woonplaats van een gever, zijnde een natuurlijke persoon, zoals die voortvloeit uit de (ontwerp)wet geen verwerking van bijzondere persoonsgegevens is, omdat uit een bijdrage niet rechtstreeks de politieke gezindheid van betrokkene kan worden afgeleid.

Aanpak hennepkwekerijen

Op 14 december 2006 is het landelijke voorbeeldconvenant aanpak hennepkwekerijen gepresenteerd door de minister van BZK (op te vragen via www.hetccv.nl). Het CBP heeft over concepten van dit convenant geadviseerd en enkele suggesties tot aanpassing gedaan. Het CBP is van oordeel dat het voorbeeldconvenant de basis kan bieden voor een samenwerking tussen politie, openbaar ministerie, gemeenten, uitkeringsinstanties en relevante private partijen (zoals woningbouwverenigingen en energiebedrijven) voor de integrale aanpak van hennepkwekerijen, en daarmee een bijdrage kan leveren aan het verminderen van de maatschappelijke problemen rond hennepcultuur. Het daarbij rekening houden met het belang van een zorgvuldige omgang met persoonsgegevens kan een wezenlijke bijdrage leveren aan de kwaliteit van de taakuitvoering.

Door de integrale aanpak zullen bij de samenwerking persoonsgegevens worden uitgewisseld die nodig zijn om acties te kunnen ondernemen tegen illegale hennepkwekerijen.

Het nut en de noodzaak van de samenwerking en uitwisseling van gegevens staan niet ter discussie. Het CBP wijst er in zijn adviezen op dat de beoogde aanpak ook gebaat is bij een zorgvuldige omgang met de persoonsgegevens waarover men rechtmatig beschikt.

Een zorgvuldige gegevensverwerking stelt de betrokken instanties in staat om het vertrouwen van de burgers in de daadkracht en integriteit van de (lokale) overheid te verwerven en te behouden.

EG-beroepskwalificaties

Het wetsvoorstel dat de regering wil indienen om de EG-richtlijn voor de erkenning van beroepskwalificaties om te zetten in Nederlands recht zou in de huidige vorm niet moeten worden ingediend. Dat het voor de erkenningsprocedure nodig is om (bijzondere) persoonsgegevens te verzamelen en uit te wisselen, staat buiten kijf. Maar het conceptvoorstel is zo vaag dat het voor de burger volstrekt onduidelijk is om welke persoonsgegevens het daarbij zal gaan.

Het CBP is van oordeel dat de concept Algemene wet erkenning EG-beroepskwalificaties schromelijk tekortschiet in de noodzakelijke onderbouwing en rechtvaardiging van de verwerking van (bijzondere) persoonsgegevens. Deze gebreken hebben tot gevolg dat niet duidelijk wordt welk juridisch kader van toepassing is op de gegevensverwerking.

Het is de taak van de formele wetgever om een zodanig heldere wet uit te vaardigen dat de betrokkene (in de zin van de Wbp) kan weten waar hij aan toe is en in hoeverre de wetgever rekening houdt met zijn grondrecht op bescherming van de persoonlijke levenssfeer.

Export studiefinanciering

Studeren over de grenzen wordt steeds meer populair. Daaraan gepaard gaat een wetsvoorstel om de meeneembaarheid van studiefinanciering uit te breiden naar alle vijfenveertig landen die deelnemen aan het realiseren van één Europese hogeronderwijsruimte. Om dubbele aanspraken te voorkomen en te controleren of studenten voldoen aan de eisen om studiefinanciering in den vreemde te ontvangen, moeten er met de autoriteiten van andere landen persoonsgegevens worden uitgewisseld. Het CBP heeft in een ambtelijk vooroverleg over het wetsvoorstel tot wijziging

van de Wet studiefinanciering dat deze uitbreiding mogelijk moet maken, gewezen op de vereisten die de Wbp stelt aan doorgifte van persoonsgegevens aan landen buiten de EU die geen passend beschermingsniveau bieden. Het aan die landen verstrekken van bepaalde gegevens, zoals over de samenlevingsvorm van betrokken student, zou wel eens voor die student zeer ongewenste en onbedoelde gevolgen kunnen hebben. Het CBP heeft de staatssecretaris van OCW verzocht hiermee rekening te houden en in de memorie van toelichting bij het wetsvoorstel aan te geven onder welke voorwaarden en omstandigheden gegevensuitwisseling kan plaatsvinden.

Selectief woningtoewijzingsbeleid

De gemeente 's-Hertogenbosch, het Regionaal politiekorps Noord-Brabant (district 's-Hertogenbosch) en twee woningcorporaties maken sinds februari 2005 gebruik van een selectief woningtoewijzingsbeleid voor huurwoningen in de Graafsewijk (Bartjes-Zuid). Op basis van informatie uit politieregisters wordt getoetst of kandidaat-huurders voor deze woningen op grond van hun eerdere gedrag een groot risico vormen voor de leefbaarheid van dit gebied. Het doel is om het intimidatieklimaat in de Graafsewijk te verminderen.

Het CBP heeft de deelnemende partijen aangeraden de procedure van de Verklaring omtrent Gedrag, zoals geregeld in de Wet justitiële en strafvorderlijke gegevens, voor dit beleid te volgen. De deelnemende partijen hebben aangegeven hiervan af te willen zien. Het CBP is begin 2006 een onderzoek gestart naar dit selectief woningtoewijzingsbeleid: hoe werkt het in de praktijk en gebeurt het conform de wettelijke voorschriften? Dit onderzoek wordt begin 2007 afgerond.



> Video-opname leerling

Een jongetje van acht jaar, leerling op een school voor speciaal onderwijs, krijgt een speciale fysiotherapie-behandeling. Zijn ouders komen erachter dat tijdens die behandeling video-opnamen zijn gemaakt van hun kind. De school wil die video gebruiken tijdens een ouderavond. De ouders hebben laten weten daar niets voor te voelen. De moeder vraagt zich af of de school zomaar video-opnamen mag maken van een leerling, zonder toestemming van de ouders. "Wat kunnen we doen om te voorkomen dat dit in de toekomst nog eens gebeurt?"



Politie en justitie

Op strafvorderlijk terrein eigent de overheid zich in steeds ruimere mate de bevoegdheid toe om in het kader van bestrijding van georganiseerde criminaliteit en terrorisme over steeds meer gegevens te kunnen beschikken van 'onverdachte' burgers. Verkennende onderzoeken en themaverwerkingen bergen het gevaar in zich dat burgers ten onrechte worden onderworpen aan politieoptreden. Net zo min als iedere uitkeringsgerechtigde een potentieel fraudeur is, is elke bewoner van een achterstandswijk een mogelijk terrorist. Het CBP pleit herhaaldelijk voor zorgvuldigheid en het opnemen in wetgeving van meer waarborgen voor burgers om aantasting van hun fundamenteel recht op bescherming van hun persoonlijke levenssfeer tegen te kunnen gaan.

Opsporing terroristische misdrijven

In het licht van het bestrijden van terrorisme is de laatste jaren sprake van een cumulatie van bevoegdheden van de politie en justitiële autoriteiten. In 2004 adviseerde het CBP de minister van Justitie over het wetsvoorstel verruiming opsporing en vervolging terroristische misdrijven. Omdat aan de kritiek van het CBP op veel punten geen gevolg is gegeven, heeft het CBP deze in 2005 onder de aandacht gebracht van de vaste commissie voor Justitie van de Tweede Kamer. De kritiek richtte zich vooral op het ontbreken van een deugdelijke motivering van de noodzaak van de voorgestelde maatregelen, waaronder een ruimer verkennend onderzoek naar bepaalde groepen in de samenleving, afgezet tegen andere, vergelijkbare maatregelen. Ook houdt volgens het CBP de ontwikkeling van controlemechanismen onvoldoende gelijke tred met de groeiende macht van de, in het bijzonder strafvorderlijke, autoriteiten.

In 2006 heeft het CBP de vaste commissie voor Justitie van de Eerste Kamer op verzoek van de voorzitter van de Kamer nader geadviseerd over zijn eigen rol als toezichthouder en over de maatregelen die naar zijn oordeel nodig zouden zijn om de checks and balances op het terrein van de strafrechtelijke terrorismebestrijding op peil te houden.

Na de toezegging van de minister van Justitie om op de kritiek van het CBP in te gaan voor de behandeling van het verwante wetsvoorstel politiegegevens, is het wetsvoorstel op 14 november 2006 door de Eerste Kamer aanvaard. Het is op 1 februari 2007 in werking getreden.

Wet politiegegevens

Bij de hiervoor behandelde wet tot verruiming van de opsporingsbevoegdheden bij de bestrijding van terroristische misdrijven is een van de belangwekkendste onderdelen de mogelijkheid tot het voeren van een verkennend onderzoek.

In het wetsvoorstel dat moet leiden tot een integrale herziening van de Wet op de politieregisters, die wordt omgedoopt tot Wet op de politiegegevens, is een van de grote vernieuwingen het invoeren van zogeheten themaverwerkingen. Een themaverwerking brengt een stelselmatige proactieve verwerking mee van persoonsgegevens van 'onverdachte' burgers. Het CBP heeft als toezichthouder op de Wet politieregisters in 2004 de minister van Justitie uitgebreid geadviseerd over de voorgenomen vernieuwingen. In 2006 heeft het CBP met de vaste commissie voor Justitie van de Eerste Kamer gesproken over enkele onderdelen uit zijn advies dat de minister en de Tweede Kamer niet hebben gevolgd.

De hoofdpunten van kritiek zijn in het kort de volgende. De nieuwe wet kent geen apart regime meer voor gegevens over 'onverdachte' personen – mensen jegens wie op grond van feiten en omstandigheden geen redelijk vermoeden van schuld bestaat ('een beetje verdacht'). Zonder de extra bescherming in de vorm van aparte waarborgen is het gevaar onaanvaardbaar groot dat burgers ten onrechte worden onderworpen aan politieoptreden. Het CBP heeft daarom gewezen op de noodzaak van permanente bewaking van de juistheid en kwaliteit van politiegegevens door middel van coderingen. In de derde plaats heeft het CBP kritiek op de beperkte reikwijdte van de wet. Verkeerde verwerking van

gegevens door bijzondere opsporingsambtenaren kan voor een burger net zulke nadelige gevolgen hebben als verwerking door de politie. De Wet politiegegevens zou dus ook van toepassing moeten zijn op bijzondere opsporingsambtenaren.

Besluit politiegegevens

Het Besluit politiegegevens geeft nadere regels ter uitwerking van de Wet politiegegevens. In 2006 heeft het CBP de minister van Justitie erover geadviseerd. In zijn advies gaat het CBP in op de toepasbaarheid van themaverwerkingen, de afscherming van informanten, codering van politiegegevens, het verstrekken van politiegegevens aan derden en het buitenland en de verplicht voorgeschreven audits waardoor de politie zijn eigen gegevens-huishouding moet laten controleren door een onafhankelijke deskundige.

Uitwisseling politiegegevens Antillen

Snelle en zorgvuldige uitwisseling van politiegegevens tussen de Nederlandse Antillen en Nederland is belangrijk voor de bestrijding van koninkrijksbrede criminaliteit. Om deze uitwisseling mogelijk te maken is in 2004 het Protocol gegevensuitwisseling tussen de Nederlandse Antillen en Nederland van kracht geworden. Het CBP houdt krachtens het Protocol toezicht op de werking van het systeem. De resultaten van een onderzoek van het CBP naar de wijze waarop de uitwisseling van gegevens verloopt en naar de naleving van het Protocol zijn in april 2006 gepubliceerd. Het onderzoek wijst uit dat de regels die door het Protocol en het bijbehorend reglement worden voorgeschreven, onvoldoende waarborgen dat het systeem op een zorgvuldige wijze wordt gebruikt.

Dit is vooral te wijten aan een onvoldoende fysieke en logische toegangsbeveiliging tot het systeem en aan een gebrekkige organisatie, waardoor het gestelde doel, zorgvuldige gegevensuitwisseling, niet kan worden gerealiseerd. Ondanks de goede intentie van de medewerkers schiet het privacybewustzijn tekort. Gedurende de tijd dat het systeem in gebruik is geweest heeft er geen controle op de werking ervan plaatsgevonden. De lokale overheid heeft daardoor geen zicht op de huidige werkwijze en kan haar verantwoordelijkheid niet waarmaken. Het CBP heeft aanbevolen om indien het gebruik van het systeem wordt voortgezet, de gesignaleerde tekortkomingen op te lossen en heeft daarvoor suggesties gedaan.

Virtuele slotgracht

In juni 2005 lanceerde de Raad van Hoofdcommissarissen het idee dat de politie zich in het kader van criminaliteitsbestrijding zou gaan richten op de infrastructuur waarlangs mensen, goederen en informatie zich verplaatsen (de zogeheten 'nodale oriëntatie'). Dit zou onder meer gebeuren door het volgen van die infrastructuur met behulp van camera's, gericht op de toegangswegen tot steden. De gevolgen van deze 'virtuele slotgracht' voor de bescherming van persoonsgegevens waren niet helder.

Het CBP heeft in 2006 in een brief aan de minister van BZK zijn zorgen over deze visie kenbaar gemaakt. Het College betwijfelt of de voorgestelde maatregelen nuttig en nodig zijn om het doel, het



> Geen verklaring omtrent gedrag

Een jongen van vijftien jaar trapt onder invloed van alcohol een winkelruit in. Als straf moet hij twaalf uur werken bij een supermarkt. De filiaalchef vindt dat hij zijn taakstraf niet naar behoren heeft uitgevoerd. De officier van justitie doet er daarom twintig uur bij. Omdat de jongen een stage gaat lopen bij een bank – niet te verwarren met de taakstraf – vragen zijn ouders voor hem een verklaring omtrent het gedrag aan. Die krijgt de jongen niet vanwege het incident met de ingetrapte winkelruit. “Kan dit zonder dat wij ooit van die aantekening bij Justitie op de hoogte zijn gesteld?” vragen de ouders.

uit de anonimiteit halen van kwaadwillenden, te bereiken.

Naar aanleiding van gesprekken met de Raad van Hoofdcommissarissen concludeert het CBP dat de voorgestelde mogelijkheden om mensen te volgen in een glijdende schaal zijn in te delen:

- 1 Het inzetten van de techniek van kentekenherkenning om sneller verdachten te kunnen aanhouden is aanvaardbaar.
- 2 Het registreren van de gegevens van bekenden van de politie – de draaideurcriminelen – die op dat moment niet worden gezocht, is twijfelachtig. Mensen die hun straf hebben uitgezeten moeten niet eeuwig een beetje verdacht blijven.
- 3 Het registreren van de gegevens van iederéén die zich op een bepaalde route begeeft, gaat te ver, zeker als deze registraties naderhand worden geanalyseerd. Van niet verdachte personen mogen geen gegevens worden opgeslagen.

Het CBP is van mening dat nieuwe methoden op basis van nieuwe bevoegdheden, waarbij de bescherming van persoonsgegevens in het gedrang kan komen, alleen overwogen zouden moeten worden als de politie kan aantonen dat de huidige bevoegdheden ontoereikend zijn en dat het voor het vergroten van de veiligheid nodig is dat nieuwe bevoegdheden in het leven worden geroepen.

Het CBP heeft in 2006 een werkbezoek afgelegd bij een politie-regio waar de virtuele slotgracht al is aangelegd. Mede naar aanleiding daarvan zal in het eerste kwartaal van 2007 opnieuw met de Raad van Hoofdcommissarissen worden overlegd over de werking van het systeem.

Aanwijzing Voorlichting, opsporing en vervolging

Op 7 juni 2006 heeft het CBP de concept Aanwijzing Voorlichting, Opsporing en Vervolging (de Aanwijzing) van het Openbaar Ministerie ter advisering voorgelegd gekregen. Op 14 december 2006 heeft het OM een themadag gewijd aan dit onderwerp. Het CBP was daarbij aanwezig. De Aanwijzing is met ingang van 1 januari 2007 in werking getreden.

Het CBP acht de nieuwe aanwijzing grotendeels een verbetering. Over een belangrijk punt verschillen het CBP en het OM echter van mening. De Aanwijzing bepaalt dat wanneer verdachten of hun advocaat informatie over hun strafzaak openbaar maken het OM ervan uit gaat dat zij in redelijkheid geen bezwaar meer kunnen maken tegen de schending van hun privacy in die zaak.

Het CBP stelt zich op het standpunt dat als burgers of advocaten zich in de ogen van het OM misdragen door feiten – al dan niet op misleidende wijze – uit een strafdossier aan de openbaarheid prijs te geven, dat nog geen reden is om dat zelf ook te gaan doen. Het OM beschikt over bijzondere machtsmiddelen. Per geval zal de afweging moeten worden gemaakt of verstrekking van persoonsgegevens in redelijke verhouding staat tot het belang van de betrokkene en diens recht op bescherming van de persoonlijke levenssfeer. Voorkomen moet worden dat de verstrekte informatie direct of indirect kan leiden tot op individuele personen te herleiden informatie. De in individuele dossiers verzamelde gegevens zijn niet bedoeld om het OM te wapenen tegen onheuse aanvallen in media.

Het OM is bij de uitoefening van zijn taak gehouden het grondrecht op bescherming van de persoonlijke levenssfeer te respecteren. Als een verdachte zelf de publiciteit zoekt, wil dat niet zeggen dat hij daarmee zijn recht op grondrechtelijke bescherming verspeelt. Deze afweging is eerder in 2006 aan de orde geweest in het onderzoek dat het CBP heeft gedaan naar de verstrekking van persoonsgegevens van Taïda Pasic aan de Telegraaf door minister Verdonk van Vreemdelingenzaken en Integratie. Het CBP concludeerde toen onder meer dat deze handelwijze van de minister een inbreuk maakte op de bescherming van de persoonlijke levenssfeer van Pasic die niet in verhouding stond tot het door de bewindsvrouw aangevoerde belang van informatieverstrekking. De verstrekking van – deels ook nog onjuiste en kwalificerende – persoonsgegevens was onverenigbaar met het doel waarvoor de gegevens waren verkregen, namelijk het nemen van een beslissing over de door Pasic gevraagde verblijfsvergunning.

OM-afdoening

In de tweede helft van 2006 is de Wet justitiële en strafvorderlijke gegevens (Wjsg) gewijzigd als gevolg van de nieuwe Wet OM-afdoening. Het CBP houdt toezicht op gegevensverwerkingen die plaatsvinden in het kader van de Wjsg. Het CBP is per abuis niet geconsulteerd over deze wijziging en heeft het ministerie van Justitie, tijdens het wetgevingsoverleg in december 2006, hierop gewezen. Besloten is dat de op te stellen AMvB wel aan het CBP wordt voorgelegd. Dat is inmiddels begin 2007 gebeurd.

Registreren van verhoren

Het OM wenst in de concept-Aanwijzing audiovisueel en auditief registreren van verhoren een regeling op te nemen over de verstrekking van de vastgelegde verhoren uit politieregisters aan hulpverlenende instanties en verstrekking van deze gegevens aan niet nader gespecificeerde ontvangers in het kader van opleiding van politiefunctionarissen. Het concept is aan het CBP ter advisering voorgelegd.

Het CBP constateert een aantal knelpunten. In de eerste plaats worden de ontvangers van de gegevens in beide gevallen niet genoemd in de Wet of het besluit. Dat betekent in beginsel dat een dergelijke verstrekking juridisch gezien niet mag plaatsvinden.

In de tweede plaats spelen verschillende verantwoordelijkheden en gezagsrelaties een rol. De korpsbeheerder draagt verantwoordelijkheid voor de inhoud en het gebruik van de politieregisters. Hij is dus ook verantwoordelijk voor de verstrekking. Wanneer dergelijke gegevens verstrekt worden ter handhaving van de openbare orde of in het kader van hulpverlening, is niet het OM maar de burgemeester het bevoegde gezag over de politie. Alleen wanneer de verhoren worden verstrekt in het kader van de strafrechtelijke handhaving van de rechtsorde heeft het OM het gezag over de politie en kan het in het licht daarvan aanwijzingen geven en regels opstellen.

Het CBP vraagt zich, gelet op de bovengenoemde gezagsproblematiek, af of het om enkel een OM-aanwijzing gaat. Op zijn minst genomen moet het geheel sluitend worden gemaakt met de burgemeester en de korpsbeheerder. Daarnaast heeft het CBP in overweging gegeven dat een afweging van alle in het geding zijnde belangen steeds noodzakelijk is. Ook moet bedacht worden dat op de ontvanger van de gegevens in ieder geval een geheimhoudingsverplichting ingevolge de Wet politieregisters rust.

Het OM heeft aangegeven contact op te nemen met de andere betrokken organisaties voordat hieraan wordt verder gewerkt.

Uitbreiding antecedentenonderzoek politie

Op 21 november 2006 is het wetsvoorstel Politiewet 200. aan de Tweede Kamer aangeboden. Het wetsvoorstel bevat een nieuw artikel dat het mogelijk maakt de screening door de politie te verruimen.

Als gevolg van de gekozen versnelde procedure is het CBP in strijd met de wet niet in de gelegenheid gesteld zijn wettelijke advies taak uit te voeren voordat het wetsvoorstel aan de Tweede Kamer is voorgelegd. Het CBP legt de verantwoordelijkheid voor die

procedure en de consequenties daarvan geheel bij het ministerie, maar heeft alsnog inhoudelijk gereageerd op het toegevoegde nieuwe artikel. Het CBP erkent nadrukkelijk het belang van integriteit van de politie en is verheugd te kunnen constateren dat de verruimde screening door de politie bij wet wordt geformaliseerd. Daarbij plaatst het twee kanttekeningen. De noodzaak tot uitbreiding van de screening moet worden onderbouwd en de reikwijdte en verschillende onderzoeksmogelijkheden zouden wettelijk moeten worden verankerd.

In de toelichting op het huidige voorstel wordt slechts opgemerkt dat 'recent onderzoek van het Nederlands Politie Instituut naar integriteitsschendingen binnen de politie die behoefte onderstreept'. Enige onderbouwing van die behoefte in de vorm van bijvoorbeeld een inzicht in de uitkomst van het onderzoek wordt niet gegeven en de noodzaak van uitbreiding komt geheel niet aan de orde. Daarmee is de noodzaak in het wetsvoorstel niet aangetoond.

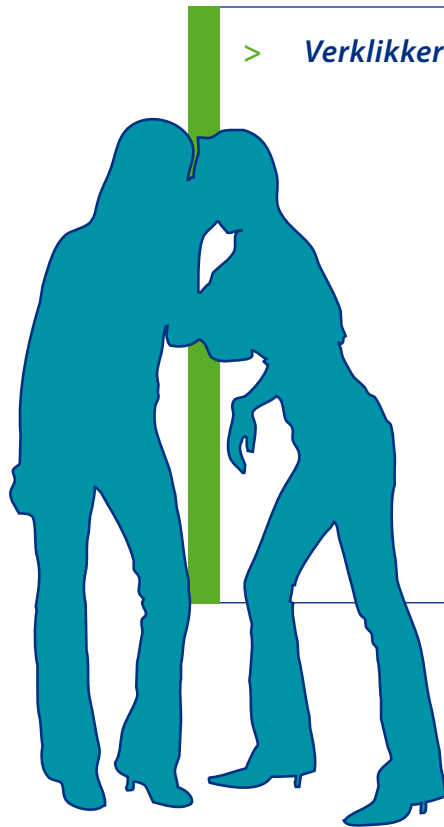
Het voorgestelde artikel 54, eerste lid, onder b, Politiewet is ruim geformuleerd en schept naar het oordeel van het CBP te veel onduidelijkheid. Zo blijkt uit de wet niet wie er in het kader van een betrouwbaarheidsonderzoek 'nagetrokken' kunnen worden door de politie, wat het onderzoek inhoudt en wie aan een betrouwbaarheidsonderzoek onderworpen zouden kunnen worden. Daarnaast is niet benoemd of er verschillende soorten betrouwbaarheidsonderzoeken worden ingevoerd, zoals het CBP eerder heeft geadviseerd. Bovendien zou uit de wettekst zelfs kunnen worden afgeleid dat het betrouwbaarheidsonderzoek op sommige punten gelijk te stellen is met het A-veiligheidsonderzoek, uitgevoerd door de AIVD, of zelfs nog verdergaande inbreuken op de persoonlijke levenssfeer dan het A-veiligheidsonderzoek toestaat. Het feit dat de wet deze ruimte laat, is mede gelet op het voortraject niet alleen onbegrijpelijk maar ook zeer onwenselijk.

Het CBP heeft de minister verzocht de Tweede Kamer te informeren over het advies en hem op de hoogte te houden van de stand van zaken.

De minister heeft het CBP inmiddels begin maart laten weten dat de Tweede Kamer de behandeling van het wetsvoorstel opschort tot naar het zich laat aanzien 2009 en dat nu wordt gezien of het onderwerp op een andere wijze aan de orde kan komen. De bewindsman geeft aan dat hij daarbij de opmerkingen van het CBP zal laten meewegen.

Gebruik vingerafdrukken vreemdelingen

De minister van Justitie stelt dat de politie behoefte heeft aan uitgebreidere mogelijkheden om vingerafdrukken van vreemdelingen te gebruiken voor opsporingsdoeleinden. Nu mogen vingerafdrukken van vreemdelingen alleen voor opsporingsdoeleinden gebruikt worden als er sprake is van een redelijk vermoeden dat de dader een vreemdeling is, het een ernstig delict betreft waardoor de maatschappelijke rechtsorde ernstig geschokt is en het onderzoek is doodgelopen en/of er onvoldoende zicht is op een snel resultaat waar dat wel gewenst is. De minister stelt dat dit in de praktijk als te knellend wordt ervaren en wil de passage 'een ernstig misdrijf dat de maatschappelijke rechtsorde ernstig geschokt heeft' uitbreiden tot 'een misdrijf waarvoor voorlopige hechtenis is toegelaten'. Het CBP adviseert de minister van Justitie in april 2006 informatie aan te dragen die aantoont waarom verruiming van de geldende wet- en regelgeving op dit vlak noodzakelijk is.



> *Verklikker bedreigd*

Een dertienjarige jongen wordt met enkele kameraden door de politie opgepakt wegens graffitivandalisme. De door hen afgelegde verklaringen leiden vervolgens tot de aanhouding van elf drugsverdachten. Die raken op de hoogte van de identiteit van hun 'verklidders' omdat de belastende verklaringen in hun strafdossiers zijn gevoegd. De dertienjarige jongen is een bekende van de drugsverdachten en wordt later bedreigd. Zijn moeder klaagt vergeefs bij de politie over het bekend worden van de identiteit van haar zoon bij de drugsverdachten. De politie zegt niets te kunnen doen. Aangifte wegens bedreiging ziet ze niet zitten. "Dan worden we weer aan de schandpaal genageld."



Arbeid en sociale zekerheid

Het bestrijden van misstanden in een bedrijf, het tegengaan van fraude door het eigen personeel en het boven water krijgen van fraude met sociale zekerheidsuitkeringen zijn gerechtvaardigde belangen. Om deze belangen veilig te stellen, kan het nodig zijn persoonsgegevens te verstrekken – via kliklijnen, zwarte lijsten of bestandskoppelingen.

Voor al deze vormen van gegevensverwerking geldt de eis dat de nagestreefde belangen afgewogen worden tegen de gevolgen voor de persoonlijke levenssfeer van degene over wie wordt geklikt of van wie wordt vermoed dat hij frauduleus handelt.

Kliklijnen in concerns

Organisaties kunnen een gerechtvaardigd belang hebben bij het instellen van een concernbrede kliklijn. Daarbij moet steeds een afweging worden gemaakt tussen het belang van de werkgever, de ernst van de misstanden en de consequenties voor de persoon over wie geklikt wordt.

De Amerikaanse Sarbanes-Oxley (SOX)-wetgeving verplicht in de Verenigde Staten gevestigde bedrijven een interne kliklijn te openen, met als doel bevordering van integere bedrijfsvoering. Voor bedrijven in Nederland, ook voor dochterondernemingen van een multinational, levert deze verplichting echter geen wettelijke grondslag op voor het instellen van een bedrijfsklokkenluidersregeling. Daarvoor is vereist dat het bedrijf de regels van de Wbp voor de doorgifte van persoonsgegevens naar landen buiten de Europese Unie in acht neemt. Dit heeft het CBP beslist naar aanleiding van een vergunningaanvraag van een bedrijf voor het instellen van een internationale kliklijn.

Onder normale omstandigheden zou iedere melding, van welke misstand dan ook, binnen een organisatie via de reeds bestaande kanalen moeten gebeuren (via leidinggevend, vertrouwenspersonen, de ondernemingsraad). Bij het melden van een misstand via een kliklijn moet het gaan om een substantiële misstand. Het uitgangspunt voor een interne kliklijn moet zijn dat de identiteit van de melder wordt vastgesteld. Anoniem klikken in organisaties moet niet worden aangemoedigd. De meldingen zelf dienen uit te gaan van feiten en niet van individuen. De in de melding genoemde personen moeten op de hoogte gebracht worden van het feit dat er een melding is binnengekomen waarin hun naam wordt genoemd. Dit moet gebeuren op het moment dat deze gegevens in het systeem vastgelegd worden. Alleen in zeer beperkte gevallen mag met het oog op het veiligstellen van bewijsmateriaal deze informatieplicht tijdelijk opgeschort worden.

Omdat de concernbrede kliklijn in de meeste gevallen is opgesteld om het moederbedrijf in de Verenigde Staten te informeren, mogen persoonsgegevens uitsluitend worden doorgegeven ingeval van misstanden waarvan duidelijk is dat afhandeling van de melding niet naar behoren op lager niveau kan plaatsvinden. De Artikel 29-werkgroep heeft richtsnoeren opgesteld over de verenigbaarheid van de klokkenluidersregeling die onder de SOX-wetgeving tot stand zijn gekomen enerzijds en de EU gegevensbeschermingsregels anderzijds. Dit om rechtszekerheid te bieden aan bedrijven die zowel aan de EU-gegevensbeschermingsregels als aan de SOX-wetgeving zijn onderworpen. In lijn met dat advies is voor een doorgifte van persoonsgegevens via de kliklijn een vergunning van de minister van Justitie vereist, tenzij er sprake is van een adequaat niveau van bescherming in het derde land.

Arbodiensten

De overdracht van werknemersdossiers van de ene arbodienst aan een andere arbodienst is zonder dat daar een wettelijke regeling aan ten grondslag ligt niet rechtmatig. Dat is de strekking van een uitspraak van het CBP van 18 april 2006. Voor een dergelijke overdracht moet de bedrijfsarts zijn medisch beroepsgeheim doorbreken. Dat kan alleen indien de werknemer in kwestie daarvoor toestemming verleent of indien op de arts een wettelijke plicht rust tot het verstrekken van het dossier. Van een wettelijke plicht

tot overdracht is in dit geval geen sprake. Daarnaast is het CBP van oordeel dat binnen een arbeidsrelatie, gezien de ongelijke machtsverhouding tussen partijen, toestemming voor de overdracht van het dossier niet geacht kan worden in vrijheid te zijn gegeven.

In de uitspraak, die op de website van het CBP is gepubliceerd, wordt aangegeven dat sprake is van een hiaat in de wetgeving. Tevens is erin aangekondigd dat het CBP het ministerie van Sociale Zaken en Werkgelegenheid hierover zal informeren en zal aandringen op een (werkbare) oplossing. Gezien de vele vragen die de uitspraak heeft opgeroepen, heeft het CBP echter besloten nader te onderzoeken of in deze zaak wellicht een andere oplossing tot de (juridische) mogelijkheden behoort.

Het digitaal klantdossier

De ontwikkeling van een digitaal klantdossier, zoals voorgesteld in de Wet eenmalige gegevensuitvraag werk en inkomen, is niet alleen bedoeld om de dienstverlening aan de burger te verbeteren, maar beoogt tevens efficiëntere bedrijfsvoering en effectievere bestrijding van fraude. Het CBP heeft de staatssecretaris van Sociale Zaken en Werkgelegenheid geadviseerd over de ontwerp-wet. Het wijst in zijn advies op het belang van goede informatieverstrekking aan de burger en op de noodzaak van transparantie. De burger moet zijn recht op inzage en correctie kunnen effectueren. Anders dreigt het digitaal klantdossier vooral een systeem te worden over de burger, zonder dat deze daar kennis van draagt en inspraak in heeft.

Het wetsvoorstel voorziet in het eenmalig verzamelen van alle gegevens van een klant die relevant zijn voor het terrein van werk en inkomen. De gegevens zijn afkomstig van organisaties binnen dit terrein, zoals de Sociale Dienst, het CWI en de UWV, maar ook van organisaties die buiten dit terrein opereren, zoals de Sociale Verzekeringsbank, de Rijksdienst voor het Wegverkeer en de Informatie Beheer Groep. Het digitaal klantdossier dat hieruit wordt samengesteld, moet voorkomen dat de overheid burgers vaker dan één keer vraagt naar gegevens waar zij al over beschikt.

Het CBP benadrukt in zijn advies dat de verdeling van verantwoordelijkheden tussen de actoren binnen de sector werk en inkomen helder moet zijn. Bovendien dient te zijn gewaarborgd dat medewerkers van deze instellingen alleen die gegevens verwerken die noodzakelijk zijn voor een goede taakuitoefening. Bepalend voor het succes van het digitaal klantdossier zal zijn de mate van juistheid en bruikbaarheid van de geregistreerde gegevens. Verder moet het de burger duidelijk zijn waar hij terecht kan voor inzage van zijn dossier en voor correctie op de gegevens daarin. Tenslotte wijst het CBP op de noodzaak van goede beveiliging van de opgeslagen gegevens van burgers.

De staatssecretaris van SZW heeft in februari 2007 het CBP een reactie op het advies gezonden, waarin hij positief reageert op de suggesties.

Informatieplicht na heimelijke waarnemingen

Heimelijke waarnemingen door de sociale recherche bij de controle op naleving van de Wet werk en inkomen vormen een ingrijpende inbreuk op de persoonlijke levenssfeer van de uit-

keringsgerechtigde burger. Door heimelijke waarnemingen wordt gecontroleerd of mensen met een bijstandsuitkering frauderen. Tijdens de waarnemingen worden persoonsgegevens verzameld zonder dat de uitkeringsontvanger zich daar op dat moment van bewust is. De gegevens worden gebruikt bij de herbeoordeling van het recht op een uitkering.

Begin 2003 heeft het CBP de procesbeschrijving 'Heimelijke waarnemingen door sociale diensten' goedgekeurd. In deze procesbeschrijving is de informatieplicht opgenomen. De informatieplicht houdt in dat burgers die onderwerp zijn geweest van heimelijke waarnemingen hier na afloop van het fraudeonderzoek over worden geïnformeerd. De burger heeft er recht op te horen waar hij het onderzoek van de sociale recherche aan 'te danken' heeft en wat de uitkomst is van dat onderzoek.

Conform zijn jaarplan voor 2006 heeft het CBP het afgelopen jaar de naleving van de informatieplicht na heimelijke waarnemingen door de sociale recherche steekproefsgewijs gecontroleerd. Uit het onderzoek is gebleken dat de naleving van de informatieplicht voor verbetering vatbaar is. Zo bleken slechts enkele gemeenten in het dossier vast te leggen dat aan de informatieplicht was voldaan wanneer er tijdens het onderzoek geen fraude aan het licht was gekomen. Een aantal gemeenten informeerden hun burgers helemaal niet over heimelijke waarnemingen bij onderzoeken waarbij geen fraude was aangetoond. Deze gemeenten hebben hun werkwijze inmiddels aangepast. Het onderzoeksrapport is naar alle gemeenten verzonden.

Koppeling van bestanden

Bij de bestrijding van woonfraude door personen met een bijstandsuitkering kan een gemeente gegevens opvragen over hun gas-, water- en elektriciteitsgebruik. Een gemeente wilde daarnaast gegevens van de vuilverwerkingsadministratie koppelen aan de administratie van de sociale dienst, om een indicatie te

krijgen van de bewoning van een pand. Volgens het CBP heeft de gemeente de noodzaak hiertoe niet kunnen aantonen. De gemeente beschikte al over voldoende gegevens om de bewoning van een pand te controleren en er zouden ook nog huisbezoeken worden afgelegd. Naar aanleiding van de voorlopige bevindingen van het onderzoek door het CBP heeft de gemeente laten weten af te zien van de voorgenomen koppeling van bestanden.

Behalve niet noodzakelijk was de koppeling van bestanden in strijd met het doelbindingsprincipe. De gegevens van het vuilverwerkingsbedrijf waren verkregen met het oog op facturering. De burgers zijn verplicht huisvuil aan te leveren en hebben deze gegevens niet vrijwillig verstrekt. De rekeningen kunnen niet worden gebruikt voor een ander doel, namelijk de opsporing van uitkeringsfraude, waarvan de burgers bovendien niet op de hoogte zijn. Daarom mogen de gegevens uit dit bestand niet gekoppeld worden aan die van de sociale dienst.

Tien Gouden Regels voor sociale diensten

Mag de sociale dienst mijn bankafschriften bekijken en daar kopieën van maken? Mag zij inlichtingen inwinnen bij mijn huisarts? Dit soort vragen over de verwerking van persoonsgegevens door de sociale dienst ontvangt het CBP regelmatig. Verder worden vragen gesteld over verstrekking van persoonsgegevens door de sociale dienst, hoe om te gaan met tips van anderen over mogelijke uitkeringsfraude, bestandskoppelingen, de informatieplicht en mogelijkheid van inzage in het dossier, proactieve dienstverlening, etc. Met hulp van enkele medewerkers van verschillende sociale diensten heeft het CBP in 2006 een brochure gemaakt met de tien meest gestelde vragen over de verwerking van persoonsgegevens en de antwoorden daarop. De brochure beoogt vooral een praktische handreiking te bieden aan de medewerkers die de intake en begeleiding van cliënten voor hun rekening nemen. Zij is aan alle sociale diensten aangeboden.



> **Yogales**

Een bijstandsgerechtigde verzorgt een paar uur per week yogalessen. De daarmee verworven inkomsten geeft hij altijd keurig op. Maar de sociale dienst wil nu ook persoonsgegevens van de mensen aan wie hij les geeft. "Van sommigen weet ik niet meer dan hun voor- naam", verzucht de yogaleraar. "En hoe zit het met de privacy van mijn klanten? Wat te doen met de mensen die hun persoonsgegevens niet willen prijsgeven?"



Gezondheidszorg

Op Europees niveau is onderzoek verricht naar de gegevensverwerking in de particuliere ziektekostenverzekeringssector. Daarnaast heeft het CBP zich op nationaal niveau de afgelopen jaren intensief beziggehouden met de gevolgen van de stelselwijziging in de zorg voor de verwerking van persoonsgegevens. Over de overheveling van de geestelijke gezondheidszorg naar de Zorgverzekeringswet is in 2006 veel rumoer ontstaan. Patiënten- en beroepsorganisaties zijn door het CBP nauw betrokken in het overleg over noodzakelijk gegevensverkeer in deze sector. In 2006 is voorts veel aandacht besteed aan de invoering van het burgerservicenummer in de zorgsector die naar verwachting in 2008 haar beslag zal krijgen. De kwaliteit van de gezondheidszorg staat of valt met de juistheid van patiëntgegevens. Het CBP heeft zich kritisch uitgelaten over versoepeling van de identificatieplicht in de zorg en nogmaals gewezen op de noodzaak van goede voorlichting over het burgerservicenummer.

> Medisch geheim?

Een voormalig patiënt van een centrum voor psychotherapie klaagt zich over de loslippigheid van medewerkers van het centrum. Zo bevestigt een balie-medewerker – zonder toestemming van de patiënt – aan diens schoonmoeder dat hij in het centrum is opgenomen. Ook ontdekt hij dat medepatiënten soms eerder op de hoogte zijn van de vordering in zijn behandeling dan hijzelf. “Twee behandelaars vertelden dat het beleid is dat cliënten geen recht hebben op privacy”.



Europees onderzoek zorgverzekeraars 2006

De verwerking van gevoelige persoonsgegevens vormt een essentieel onderdeel van de activiteiten van de particuliere ziektekostenverzekeringssector. Het is voor alle burgers en ook voor de verzekeringssector zelf van groot belang dat deze verwerking in overeenstemming met de wet en correct geschiedt. De nationale gegevensbeschermingsautoriteiten van de EU-lidstaten hebben in de context van hun activiteiten in de Artikel 29-werkgroep besloten tot een gecoördineerde actie om de gegevensverwerking te controleren. Het onderzoek, dat bestond uit analyse van schriftelijke antwoorden op vragen over dezelfde soort verwerkingen, is in alle lidstaten uitgevoerd tussen april en oktober 2006.

De respons wordt op zowel nationaal als EU-niveau geëvalueerd. Van alle nationale rapporten zal met inachtneming van nationale regels aangaande vertrouwelijkheid een samenvatting worden gepubliceerd als onderdeel van een rapport van de Artikel 29-werkgroep. Het rapport, dat naar verwachting medio 2007 gereed zal zijn, zal de stand van zaken weergeven van de naleving van privacywetgeving in de sector. Aan de hand van de bevindingen kan de werkgroep besluiten om nadere aanbevelingen en praktische richtlijnen uit te vaardigen voor de sector in zijn algemeenheid en aangeven op welke terreinen er in de toekomst nog actie ondernomen moet worden.

Burgerservicenummer in de zorg

Het burgerservicenummer (BSN) zal vanaf 2008 in de zorgsector het huidige sofinummer vervangen. Het Wetsvoorstel gebruik burgerservicenummer in de zorg bepaalt dat zorgaanbieders, ziektekostenverzekeraars en indicatieorganen het BSN zullen moeten gebruiken in hun onderlinge communicatie over hun patiënten/cliënten. Het BSN zal in de toekomst in het bijzonder worden gebruikt om het Elektronisch Medicatiedossier en het landelijk Elektronisch Patiëntendossier mogelijk te maken.

Het oorspronkelijke wetsvoorstel dat aan de Tweede Kamer is voorgelegd schoot naar het oordeel van het CBP op een aantal onderdelen tekort. In 2005 en 2006 heeft het CBP de Tweede Kamer hierover geïnformeerd. Naar aanleiding van dat commentaar heeft de Tweede Kamer de minister van VWS vragen gesteld. In antwoord daarop heeft de minister onder meer toegezegd dat

er een ministeriële regeling zal komen die duidelijk aan zal geven aan welke beveiligingseisen de zorgsector moet voldoen bij het verwerken van het BSN.

Ook heeft de minister verduidelijkt wie het toezicht op het gebruik van het BSN in de zorg voor hun rekening moeten nemen:

- de Nederlandse Zorgautoriteit zal toezicht houden op het gebruik van het BSN door ziektekostenverzekeraars;
- de Inspectie voor de Gezondheidszorg zal toezicht houden op het gebruik van het BSN door zorgaanbieders en
- het CBP zal zich vooral richten op het algemene toezicht op het gebruik van het BSN op grond van de Wet bescherming persoonsgegevens.

In de protocollen tussen het CBP en de Inspectie voor de Gezondheidszorg enerzijds en tussen het CBP en de Zorgautoriteit anderzijds wordt de verdeling van het toezicht nader uitgewerkt. In de correspondentie met het parlement, maar ook in wetenschappelijke artikelen, heeft het CBP daarnaast aandacht gevraagd voor goede voorlichting met betrekking tot de invoering van het BSN in de zorg.

Onduidelijkheid bij invoering van het BSN in de zorg

Dat goede voorlichting van groot belang is, blijkt uit de onduidelijkheid die in de zorgsector bestaat over de invoering van het BSN. Begin 2006 heeft het CBP veel klachten binnengekregen van patiënten van wie de huisarts het sofinummer had opgevraagd. Aangezien het BSN wat het nummer betreft gelijk is aan het sofinummer, wilden veel huisartsen hun administratie alvast op orde brengen door de sofinummers van hun patiënten te registreren. Dit was hen aangeraden door de Landelijke Huisartsen Vereniging (LHV), die wilde anticiperen op de administratieve verplichtingen die de huisartsen te wachten zouden staan. Hun registraties vulden zich hierdoor met door patiënten zelf opgegeven sofinummers. Ook veel andere zorgaanbieders zullen naar verwachting al sofinummers van hun patiënten hebben geregistreerd. Een nieuwsbrief van de Nederlandse Vereniging van Ziekenhuizen meldde in 2005 bijvoorbeeld onterecht dat zorgaanbieders vanaf de invoering van de Zorgverzekeringswet verplicht zouden worden het sofinummer te registreren. Niet alleen is het verwerken

van het sofinummer bij de uitvoering van de Zorgverzekeringswet onrechtmatig, ook kunnen er schrijffouten optreden of valse nummers worden opgegeven. De Belastingdienst heeft de administratie met sofinummers verschillende keren gecorrigeerd op fouten en dubbele nummers. Het is niet voor niets dat de verificatieplicht - de verplichting om het BSN op te vragen bij een landelijke voorziening (Sectorale Berichtenvoorziening in de zorg, sbv-z) - één van de pijlers van het BSN-stelsel in de zorg is. De LHV heeft inmiddels, op verzoek van het CBP, alle verwijzingen naar het opvragen van het sofinummer uit haar informatiemateriaal geschrapt.

Identificatieplicht in de zorg

De andere pijler van het BSN-stelsel in de zorg is de identificatieplicht. Op grond van het wetsvoorstel gebruik BSN in de zorg wordt de bestaande identificatieplicht in de zorg uitgebreid naar alle zorgaanbieders. Dit geldt in ieder geval bij het eerste bezoek van de patiënt na invoering van de wet en daarnaast wanneer dat nodig is om er als zorgaanbieder zeker van te zijn de juiste persoon tegenover zich te hebben. In het Besluit gebruik BSN in de zorg wordt vervolgens nader invulling gegeven aan de identificatieplicht.

Het CBP heeft in 2006 de minister van VWS tweemaal geadviseerd over concepten van het voorstel Besluit gebruik BSN in de zorg. In zijn adviezen heeft het CBP onder meer aandacht besteed aan de beveiliging van (de gegevens bij) de Sectorale Berichtenvoorziening in de zorg (sbv-z), de middelen die toegang verschaffen tot de sbv-z en het waarborgen van effectief toezicht. De kritiek van het CBP richt zich echter vooral op de regeling van de identificatieplicht in het concept Besluit. Het CBP, doorgaans geen voorstander van identificatieplicht, vindt deze in de zorg juist wel van groot belang, gezien de gezondheidsrisico's die onjuiste identificatie voor patiënten kan meebrengen.

In het conceptvoorstel wordt onder meer een uitzondering gemaakt op de identificatieplicht voor mensen die hun identiteitsbewijs vergeten, weigeren mee te werken aan identificatie of een verlopen/vervalst/niet in omloop zijnd identiteitsbewijs tonen. Dit zijn bij uitstek de gevallen waarin sprake kan zijn van identiteitsfraude. Naar aanleiding van een door de Tweede Kamer aangenomen motie heeft de minister bovendien in het Besluit de hele identificatieplicht uit het wetsvoorstel gebruik BSN in de zorg versoepeld. Deze is in het conceptvoorstel verworden tot een vergewisplicht: de verplichting zich van de juiste identiteit van de cliënt te vergewissen. Deze versoepeling van de identificatieplicht vergroot de kans op een onjuiste identificatie van patiënten. Gezien de gevolgen die een onjuiste identificatie oplevert voor de juistheid van de patiëntengegevens en daarmee de kwaliteit van de gezondheidszorg, heeft het CBP de minister geadviseerd af te zien van deze versoepeling van de identificatieplicht. Het CBP is van oordeel dat identificatie bij ieder bezoek van een patiënt aan een zorginstelling verplicht zou moeten worden gesteld, dan wel tenminste éénmalig na invoering van het wetsvoorstel, in combinatie met verplichte aanvullende maatregelen op dit terrein. Ook heeft het CBP in dit kader nogmaals aangedrongen op het belang van goede voorlichting over het BSN.

Het Elektronisch Patiëntendossier

Het burgerservicenummer zal worden gebruikt om het Elektronisch Patiëntendossier (EPD) mogelijk te maken. Bij de ontwikkeling van dit EPD is het CBP actief betrokken. Daarbij heeft het aandacht gevraagd voor de volgende punten:

- de verantwoordelijkheid voor het Landelijk Schakelpunt (LSP),
- de toegang tot het Elektronisch Patiëntendossier,
- de mate waarin en de wijze waarop toestemming een rol speelt bij de toegang tot de EPD's,
- beveiliging en
- het toezicht (vanuit de invalshoek bescherming persoonsgegevens).

Het CBP wil dat zoveel mogelijk vooraf wordt gecontroleerd of de zorgverlener die bij het LSP toegang vraagt tot een EPD een behandelrelatie met de betrokken patiënt heeft. Gelet op de landelijke schaal waarop deze inzage in gegevenssets voor alle betreffende zorgverleners met een UZI-pas mogelijk is en omdat pas achteraf gecontroleerd kan worden of deze inzage rechtmatig is geweest, meent het CBP dat de kans op misbruik groot is. Logging van de transacties van de behandelaar en controle achteraf vormen onvoldoende waarborg tegen misbruik.

Het CBP heeft ook het Nationaal ICT Instituut in de Zorg (NICTIZ) geadviseerd over de modelrichtlijn en het modelvoorlichtingsmateriaal van het elektronisch spoeddossier, over het Elektronisch Medicatiedossier en het Waarneemdossier Huisartsen.

Met het ministerie van VWS is gesproken over de waarborgen die in wetgeving kunnen worden vastgelegd rond het opzetten en gebruiken van een landelijk EPD.

In 2006 heeft het CBP klachten ontvangen over de regionaal opgezette invoering van het Elektronisch Patiëntendossier. Patiënten uitten hun zorgen over opname van hun gegevens in het elektronisch dossier en over de toegang tot dat dossier, zonder dat zij daarover tevoren zijn geïnformeerd en de mogelijkheid hebben gehad zich daartegen te verzetten. De vragen van patiënten zullen door het CBP worden meegenomen in een onderzoek dat het CBP in 2007 in een regio zal uitvoeren.

Geestelijke gezondheidszorg

Per 2008 zal een groot deel van de geestelijke gezondheidszorg (GGZ) worden vergoed via de Zorgverzekeringswet (Zvw). Nu valt de GGZ nog onder de Algemene wet bijzondere ziektekosten (Awbz). De bedoeling is om de 'op genezing gerichte' geestelijke gezondheidszorg onder de Zvw te brengen.

De overheveling van de GGZ heeft geleid tot onrust onder zowel patiënten als zorgverleners in verband met de verstrekking van gevoelige persoonsinformatie aan de verzekeraars. Aantasting van de essentiële vertrouwensrelatie tussen arts en patiënt wordt gevreesd. Het CBP heeft zowel patiënten- als beroepsverenigingen nauw betrokken bij het overleg over het noodzakelijke medische gegevensverkeer in de sector en de grenzen die daaraan in verband met de medische geheimhouding worden gesteld.

Door de overheveling van de geneeskundige GGZ naar de zorgverzekeringswet worden ook DBC's in de GGZ ingevoerd en worden aan declaraties aan de zorgverzekeraar nieuwe eisen gesteld.

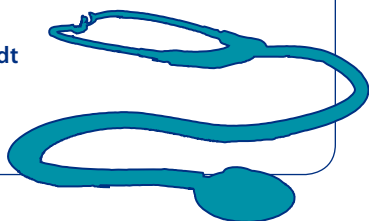
Om beter inzichtelijk te maken welke prestatie is geleverd, stelt het ministerie van Volksgezondheid, Welzijn en Sport een declaratiesysteem voor waarbij gebruik wordt gemaakt van veertien diagnosehoofdgroepen. Dit geldt uitsluitend voor de lang ambulante zorg, waarbij een relatie kan worden aangetoond tussen de diagnose – bijvoorbeeld angststoornissen of dementie – en de prijs van de behandeling. Bij de kort ambulante trajecten en de klinische trajecten zal geen diagnose-informatie op de declaratie van de verzekerde worden vermeld. Informatie over zorgtypen die verband houden met een rechterlijke uitspraak, zoals ter beschikking stelling, zal evenmin op de declaratie worden opgenomen. Persoonsgegevens van cliënten en patiënten in de GGZ zijn bijzondere persoonsgegevens waarvoor de Wbp een strenger regime kent. Gegevens betreffende een GGZ-behandeling worden veelal als extra gevoelig ervaren. Het CBP merkt in zijn commentaar op de door VWS voorgestelde declaratiestructuur op dat de noodzaak van het vermelden van diagnose-informatie maar net opweegt tegen de substantiële aantasting van de persoonlijke levenssfeer van de patiënt die daar een gevolg van is. Eventuele uitbreiding in de toekomst van vermelding van diagnose-informatie zal door het CBP dan ook uiterst gereserveerd tegemoet worden gezien.

DIS/ Risicoverevening

Het CBP heeft met de minister van VWS in 2005 afspraken gemaakt over de inzet van Privacy Enhancing Technologies (PET) bij het gebruik van gegevens in het DBC-informatiesysteem (DIS) en ten behoeve van de risicoverevening in het kader van de nieuwe Zorgverzekeringswet. Door het gebruik van pseudo-identiteiten (een unieke, anonieme codering van een bepaald persoonsgegeven) kan het gebruik van persoonsgegevens worden vermeden. Het CBP heeft in 2006 toegezien op de verdere uitwerking van de pseudonimisering. De aandacht is daarbij vooral gericht op de inrichting van de in te schakelen Trusted Third Party en de privacy-audits waaraan het DIS periodiek zal worden onderworpen.

> Medische gegevens kwijt

Na zijn verhuizing vraagt een patiënt aan zijn oude huisarts om zijn medisch dossier door te sturen naar de nieuwe dokter. Ondanks beloftes komt het daar niet van. Navraag leert dat de oude huisarts noch over een papieren, noch over een digitaal dossier van zijn ex-patiënt beschikt. Vierendertig jaar aan medische gegevens weg. “Geen prettige gedachte, dat zo slordig wordt omgesprongen met je persoonsgegevens”, vindt de benadeelde patiënt.



De definitieve implementatie wordt in 2007 verwacht. Tot die tijd worden de gegevens anoniem aangeleverd.

Het CBP heeft in 2006 geadviseerd over de aanpak binnen de risicoverevening. Het definitieve systeemontwerp wordt in 2007 verwacht.

Addendum Zorgverzekeraars

Op 27 april 2006 heeft het CBP het Addendum Zorgverzekeraars (hierna: Addendum) van een goedkeurende verklaring voorzien. Het Addendum, opgesteld door Zorgverzekeraars Nederland (ZN), bevat gedragsregels voor de omgang met persoonsgegevens door ziektekostenverzekeraars. Het is een aanvulling op de reeds bestaande Gedragscode Verwerking Persoonsgegevens Financiële Instellingen. Het Addendum bevat onder meer regels met betrekking tot de omgang met declaratiegegevens en het uitvoeren van materiële controle op de declaraties. Aan de goedkeuringsverklaring is intensief overleg voorafgegaan van het CBP met ZN, het ministerie van VWS, de artsenfederatie KNMG en de Nederlandse Patiënten Consumenten Federatie (NPCF), die eind 2005 reeds overeenstemming bereikten over de inhoud van het Addendum. In 2006 heeft een viertal organisaties c.q. personen bezwaar aangetekend tegen het goedkeuringsbesluit van het CBP. De verwachting is dat de bestuursrechter in de eerste helft van 2007 uitspraak doet in deze procedures.

Wet marktordening in de gezondheidszorg

Op 1 oktober 2006 is de Wet marktordening in de gezondheidszorg (Wmg) in werking getreden. Met deze wet is de Nederlandse Zorgautoriteit (NZa) ingesteld als opvolger van het voormalig College toezicht zorgverzekeringen en het voormalig College tarieven gezondheidszorg. De NZa heeft er ook nieuwe taken bij gekregen, waaronder het toezicht op de marktwerking in de gezondheidszorg. De NZa houdt onder meer toezicht op de verwerking van persoonsgegevens door zorgverzekeraars, in overeenstemming met de Zorgverzekeringswet en onder meer het hierboven al aangestipte Addendum Zorgverzekeraars.

Tijdens de parlementaire behandeling van het wetsvoorstel Wmg is het CBP met het ministerie van VWS overeengekomen dat de sanctiemogelijkheden voor de NZa moesten worden verruimd en dat de naleving van het Addendum Zorgverzekeraars wettelijk verplicht moet worden gesteld. Naar aanleiding van dit overleg is in de Derde nota van wijziging bij de Wmg opgenomen dat de NZa een last onder dwangsom of bestuurlijke boete kan opleggen aan zorgverzekeraars die onrechtmatig persoonsgegevens verwerken. Tevens is de naleving van het Addendum door zorgverzekeraars daadwerkelijk wettelijk verplicht gesteld.

Gezien de overlap in het toezicht op de verwerking van persoonsgegevens tussen het CBP en de NZa, is in de Wmg bepaald dat de NZa afspraken moet maken met het CBP. In 2006 is het CBP dan ook in overleg getreden met de Zorgautoriteit (in oprichting), met als doel een protocol te sluiten over de verdeling van toezicht en samenwerking op dit terrein. De verwachting is dat dit protocol in 2007 kan worden ondertekend.



Handel en diensten

Bij de verwachte invoering van de OV-chipkaart houdt het CBP de vinger aan de pols bij de ontwikkeling van normen die maatgevend moeten zijn bij de gegevensbescherming in de gehele openbaar vervoersector. De regels voor zwarte lijsten zijn voldoende helder. Het afgelopen jaar is onderzoek gedaan naar het hanteren van zwarte lijsten in de detailhandel. De hausse aan zwarte lijsten, waaronder dubieuze initiatieven vooral op het internet, zal blijvende aandacht vergen.

OV-Chipkaart

Begin 2006 heeft het CBP – ter afsluiting van het advies- en informatietraject aan vervoerders en andere partijen – het visie-document *Privacy en de OV-chipkaart* gepubliceerd.

De bezwaren van het CBP richten zich kort gezegd tegen het gebruik door vervoerders van reisgegevens bij op naam gestelde OV-chipkaarten voor serviceverlening en voor marketingdoeleinden. Het CBP is van mening dat NS de noodzaak voor het verwerken van persoonsgegevens moet aantonen. De standpunten van NS en het CBP over vooral het gebruik van gedetailleerde reisgegevens voor marketingdoeleinden liggen nog altijd ver uiteen. Op initiatief van het ministerie van Verkeer en Waterstaat is medio 2006 opnieuw, overigens zonder veel tastbare resultaten, overlegd tussen NS en CBP over de privacyissues.

Op uitnodiging van de vaste commissie voor Verkeer en Waterstaat van de Tweede Kamer heeft het CBP in juni 2006 tijdens een openbare hoorzitting zijn zorgen over bepaalde ontwikkelingen rond de OV-chipkaart toegelicht. Een en ander heeft er toe geleid dat de Tweede Kamer er bij de minister op heeft aangedrongen dat alles in het werk moet worden gesteld om de privacyproblemen op te lossen.

Naar aanleiding van deze opdracht aan de minister heeft het ministerie getracht een aantal knelpunten in overleg met NS en CBP in kaart te brengen en op te lossen. Bij brief van 1 november 2006 heeft de minister de Tweede Kamer nader geïnformeerd over de resultaten.

De minister schrijft dat het de komende tijd aan de NS en de openbaar vervoersector is om de privacymaatregelen verder uit te werken, te implementeren en deze tijdig kenbaar te maken aan het CBP die als toezichthouder de maatregelen zal beoordelen. Zij acht het raadzaam dat de hele vervoersector zoveel mogelijk op dezelfde wijze met persoonsgegevens omgaat, hierover afspraken maakt en deze vastlegt, bijvoorbeeld in een code. De reiziger weet dan waar hij aan toe is, ongeacht bij welke aanbieder hij zijn chipkaart aanschafte en gebruikt.

Inmiddels heeft het CBP besloten in 2007 onderzoek te doen bij een van de vervoerders die de OV-chipkaart gedeeltelijk heeft ingevoerd, om te bezien of en hoe de maatregelen ter bescherming van persoonsgegevens worden geïmplementeerd. Naar het oordeel van het CBP moet de opslag van gegevens zodanig worden ingericht dat onnodige koppeling van gegevens wordt tegengegaan. Ook de OV-bedrijven hebben de noodzaak daartoe inmiddels ingezien. Het CBP zal controleren of en in welke gevallen de gegevens worden gekoppeld voor direct marketingdoeleinden. De vervoerders denken daarbij aan het doen van speciale reisaanbiedingen, bijvoorbeeld aan 60-plussers.

RDW verstrekt geen kentekengegevens meer voor reclamedoeleinden

Het CBP heeft de afgelopen jaren relatief veel klachten binnengekregen over het feit dat gegevens uit het Kentekenregister zoals naam-, adres- en woonplaatsgegevens, door de Rijksdienst voor het wegverkeer (RDW) aan vertegenwoordigers van de automobielbranche werden gegeven ten behoeve van direct marketing. In het conceptwetsvoorstel tot wijziging van de

Wegenverkeerswet waarover het CBP in juni 2006 heeft geadviseerd, is vastgelegd dat vanwege het toegenomen belang van privacybescherming aan dit gebruik per 1 maart 2007 een einde komt. De automobielbranche mag wel delen van gegevens uit het kentekenregister gebruiken voor statistische doeleinden. Het CBP plaatst in zijn wetgevingsadvies hierbij de kanttekening, dat de RDW de nodige voorzieningen moet treffen om te verzekeren dat de verdere verwerking van gegevens inderdaad alleen voor dit specifieke doel gebeurt. Er moet voor worden gewaakt dat niet via deze 'achterdeur' de gegevens alsnog voor commerciële doeleinden worden gebruikt. De RDW zou met de branche afspraken hierover in een overeenkomst moeten vastleggen en de naleving van de afspraken periodiek moeten controleren.

Identificatie bij banken

In het kader van het bestrijden van het witwassen van geld en van potentiële financiering van terroristische activiteiten verplicht de Wet identificatie bij dienstverlening (Wid) banken om de identiteit van hun cliënten vast te stellen. Het afgelopen jaar heeft het CBP veel vragen en klachten van burgers gekregen over de wijze waarop banken deze plicht uitvoeren. Het ging daarbij vooral om het maken en bewaren van kopieën of scans van de identiteitsbewijzen. De bevoegdheid hiertoe is niet in de Wid genoemd.

Het ministerie van Financiën en De Nederlandsche Bank (DNB) hebben inmiddels begin 2007 op verzoek van de Nederlandse Vereniging van Banken (NVB) het CBP een schriftelijke verduidelijking gestuurd over de wijze waarop zij te werk zijn gegaan met deze verwerking van persoonsgegevens. De banken moeten aan DNB kunnen aantonen dat zij aan de identificatieverplichting van de Wid hebben voldaan. Het tonen van kopieën of scans van identiteitsbewijzen is daartoe, zeker met grote aantallen cliënten, de voor banken minst belastende methode. Deze wordt door veel banken toegepast en door DNB aanvaard. Gelet op het belang van de banken bij een werkbare uitvoering van hun wettelijke verplichtingen, de aard van de betrokken gegevens en de waarborgen waarmee de verwerking is bekleed (de Wbp en de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen) is het CBP van oordeel dat bij de afweging van deze belangen de banken redelijkerwijs tot het oordeel hebben kunnen komen dat daarbij voldoende rekening is gehouden met de bescherming van de persoonsgegevens van hun cliënten. Het CBP heeft besloten het onderzoek naar de werkwijze van banken af te sluiten.

Waarschuwingssysteem fraude in de detailhandel

Bedrijven, organisaties en instellingen kunnen gebaat zijn bij het gebruik van zwarte lijsten. Personeelsleden die in een waarschuwingssysteem zijn opgenomen omdat tegen hen aangifte is gedaan en die zijn ontslagen wegens frauduleuze handelingen kunnen bij een sollicitatie bij een ander bedrijf in de branche daarop worden gescreend.

Het waarschuwingssysteem kan een bijdrage leveren aan de aanpak van frauderend personeel, dat volgens de sector een groot probleem vormt. Een zwarte lijst blijft echter een gevoelig instrument met een grote impact op de persoonlijke levenssfeer



> **Duur verlies**

Verlies van zijn portemonnee komt een man duur te staan. Hoewel hij die een paar dagen later – zonder geld erin – op zijn deurmat terugvindt, blijkt een paar maanden nadien dat twee keer een bedrag van zijn rekening is afgeschreven vanwege een nooit door hem aangevraagd mobiel telefoonabonnement. Ook van een andere provider krijgt hij zomaar een torenhoge rekening voorgeschoteld. Het blijkt dat de vindsters van zijn portemonnee misbruik hebben gemaakt van zijn persoonsgegevens. Daarvan kan hij de providers uiteindelijk overtuigen. Maar hij kan echter niet voorkomen dat hij op een zwarte lijst is geplaatst. “Ik kan nergens meer een telefoonabonnement afsluiten. Ik moet boeten voor iets waar ik niets aan kan doen.”

van de betrokken personeelsleden. Het gebruik ervan dient dus met grote zorgvuldigheid te geschieden.

Het CBP heeft in 2006 onderzoek gedaan naar de werking in de praktijk van het waarschuwingssysteem in de detailhandel. Aan de hand van het onderzoek kan worden beoordeeld of de Wbp en het Protocol Waarschuwingregister Detailhandel worden nageleefd. Centrale vraag daarbij is hoe het belang van de organisatie zich verhoudt tot de consequenties van plaatsing op de lijst voor een individu. Het vergrijp of het wangedrag moet ernstig genoeg zijn om die plaatsing te rechtvaardigen. De resultaten van het onderzoek worden naar verwachting in de eerste helft van 2007 bekend.

Particuliere recherche

In 2005 heeft het CBP onderzoek gedaan naar de naleving van een aantal normen uit de Wbp door particuliere recherchebureaus. Het onderzoek bestond uit een enquête onder dertig bureaus naar de naleving van de informatieplicht en een breder onderzoek bij enkele bureaus naar de nakoming van verplichtingen als het gebruik van externe informatiebronnen, de rechtvaardiging voor heimelijk onderzoek en de bewaartermijnen.

De resultaten van het onderzoek zijn in 2006 in twee rapporten gepubliceerd. Wat de naleving van de informatieplicht betreft blijkt dat in een groot aantal gevallen de onderzochte particuliere recherchebureaus niet weten of aan de informatieplicht is voldaan omdat zij zelf niet de onderzochte betrokkene hebben ingelicht maar dat aan de opdrachtgever hebben overgelaten. Bijna geen enkel bureau heeft een specifieke procedure of werkinstructie opgesteld hierover. In de privacygedragscode die is opgesteld door de Vereniging van Particuliere Beveiligingsbureaus die sinds 1 juni 2004 verplicht is gesteld, is niets geregeld over het ‘uitbesteden’ van de informatieplicht. Of door de opdrachtgever wel aan de informatieplicht is voldaan, wordt doorgaans niet door het bureau gecontroleerd. Het CBP vindt het noodzakelijk dat

bureaus de naleving van de informatieplicht schriftelijk met de opdrachtgever regelen.

Het onderzoek bij de drie bureaus heeft een aantal aandachtspunten opgeleverd. Een duidelijke constatering is dat de Wbp wordt overtreden indien een recherchebureau opdracht geeft aan een handelsinformatiebureau om persoonsgegevens te verzamelen terwijl het weet dat deze gegevens niet op rechtmatige wijze verkregen kunnen worden.

Voorkoming afsluiting energievoorzieningen

Als mensen niet reageren op herhaalde verzoeken om hun energierekening te betalen en daardoor in de wintermaanden dreigen te worden afgesloten van gas en elektriciteit, zouden energieleveranciers de persoonsgegevens van deze afnemers zonder hun toestemming moeten kunnen doorgeven aan de gemeente of de sociale dienst. Dat moet het mogelijk maken de afnemer te benaderen met de vraag of hij deel wil nemen aan schuldhulpverlening.

Op snel en doeltreffend ingrijpen door energiebeheerders en netbedrijven bij het aanpakken van betalingsachterstanden is aangedrongen door de Tweede Kamer bij de behandeling van de voorgestelde wijziging van de elektriciteits- en gaswetgeving. Het CBP heeft de minister van Economische Zaken geadviseerd over een concept voor een ministeriële regeling afsluitingen. Het is van oordeel dat de inbreuk op de persoonlijke levenssfeer van de afnemer gerechtvaardigd kan zijn als daarmee wordt voorkomen dat mensen tussen 1 oktober en 1 april van gas en elektriciteit worden afgesloten, met alle gezondheidsrisico's van dien. Wel vindt het CBP dat duidelijk moet zijn welke inspanningen de energieleverancier zich moet getroosten om de afnemer de rekening te laten betalen voordat hij overgaat tot het doorgeven van de persoonsgegevens. Persoonlijk contact is belangrijk: een deel van het probleem is immers dat de afnemer op schriftelijke betalingsverzoeken niet reageert.



Telecom en internet

In de alledaagse praktijk op het internet ondervinden burgers de nodige privacyproblemen. Het CBP is bezig met het ontwikkelen van een beleidslijn over wat op websites wel en niet mag met betrekking tot de verwerking van persoonsgegevens. Wat betreft de status van IP-adressen is tijdens een discussie-middag in december 2006 meer helderheid ontstaan. De Artikel 29-werkgroep heeft een advies uitgebracht over de vertrouwelijkheid van communicatie en het screenen van berichten.

Je leven op internet: datapakhuizen en privacy

IP-adressen zijn in veel gevallen persoonsgegevens, zo erkent ook inmiddels Google Europe bij monde van zijn Privacy Counsel Peter Fleischer. De wettelijke bescherming van persoonsgegevens is dus volledig van toepassing. Tot voor kort stelde Google zich op het standpunt dat de IP-adressen die het verwerkt en langdurig bewaart, bijvoorbeeld door zoekvragen op internet, maar ook door het gebruik van andere diensten als G-mail, Orkut en Google Earth, geen persoonsgegevens waren.

Dit is een belangrijke uitkomst van een discussiemiddag in De Balie te Amsterdam op 7 december 2006, georganiseerd door het CBP en de Consumentenbond.

Het onderwerp van de bijeenkomst was welke privacyrisico's het gebruik van gepersonaliseerde diensten op internet meebrengt. Het debat was toegespitst op grote en innovatieve internet-dienstverleners die door het verlenen van meerdere persoonlijke diensten gedetailleerd inzicht krijgen in het gedrag van hun klanten, ter gelegenheid van het debat 'personal service providers' (PSP's) gedoopt.

Google en andere PSP's zoals Microsoft, Yahoo en in Nederland de Ilse Media Groep zijn bij uitstek innovatief in het verlenen van steeds persoonlijker diensten, waarbij steeds meer persoonsgegevens worden verwerkt. Door de toenemende bundeling van diensten bij enkele grote aanbieders ontstaan grote datapakhuizen met persoonsgegevens, waaronder bijvoorbeeld gevoelige gegevens als zoekopdrachten door de tijd heen, de inhoud van e-mail of de inhoud van de hele harde schijf van een computer.

Ondanks zijn herhaalde verzekering dat Google zo transparant mogelijk wilde zijn, bleef Fleischer echter tijdens het debat het antwoord schuldig op vragen over de specifieke algemene voorwaarden per dienst of over bewaartermijnen.

Collegelid Madeleine McLaggan-van Roon gaf aan dat het CBP en de Consumentenbond drie zorgen delen. De eerste zorg is het gebrek aan duidelijkheid en van algemene voorwaarden en privacyverklaringen. De tweede betreft onvoldoende gegevensbescherming door miskenning van de definitie van persoonsgegevens. De derde ziet op onverwacht gebruik van gegevens, bijvoorbeeld door de overheid.

Tegenover deze zorgen stelde zij vier waarborgen die de Wet bescherming persoonsgegevens en de Europese privacy richtlijn bieden.

- Informatieplicht

In de eerste plaats moeten dienstverleners voldoen aan hun informatieplicht. De algemene voorwaarden zijn vaak vaag en onduidelijk. Hoewel veel dienstverleners proberen om hun algemene voorwaarden in begrijpelijke taal op te stellen, is het voor consumenten niet duidelijk wat voor gegevens de dienstverleners precies verzamelen, hoe ze die verwerken in verschillende diensten en of ze gegevens eventueel verstrekken aan derde partijen. Transparantie is ook vereist bij de inzet van technische middelen.

- Doelbinding

Dienstverleners zouden de doeleinden van de verwerking veel nauwkeuriger moeten vaststellen en naleven. Gegevens mogen niet zomaar worden gebruikt voor een ander doel dan waarvoor ze zijn verzameld, ook niet bij een andere dienst van dezelfde aanbieder. 'Function creep', onverwacht gebruik van gegevens in een andere context, moet worden voorkomen.

- Rechten van betrokkenen

De Wet bescherming persoonsgegevens geeft iedereen het recht op inzage, correctie en/of verwijdering van zijn of haar persoonsgegevens. Betrokkenen moeten op elk gewenst tijdstip de gelegenheid hebben hun profielen voor controle in te zien. Bovendien moeten ze het recht hebben de opgeslagen gegevens te corrigeren en te laten verwijderen.

- Bewaartermijn

Tot slot dient een maximum gesteld te worden aan de bewaartermijn van gegevens.

> Persoonsgegevens op het internet

De heer X krijgt ongevraagd en ongewild een e-mail-adres op zijn naam aangeboden door een telecommunicatiebedrijf. Hij beklaagt zich over het verwerken van zijn persoonsgegevens door het bedrijf. Dat verzamelt en bewaart ook de telefoongegevens van al zijn klanten. X zegt al zijn gegevens van de afgelopen drie jaar te hebben teruggevonden op het internet: kosten, starttijd en duur van de gesprekken. Wissen van de gegevens is volgens hem niet mogelijk. Ook een (test)telefoontje aan Meld misdaad anoniem blijkt te zijn geregistreerd. "Hoezo anoniem?" reageert de klant verbolgen.

De vertrouwelijkheid van communicatie en het screenen van berichten

De Artikel 29-werkgroep, het EU-samenwerkingsverband van toezichthouders op de bescherming van persoonsgegevens, heeft in 2006 een advies uitgebracht over de mate waarin aanbieders van communicatiediensten kennis kunnen nemen van de inhoud van berichten. Het CBP heeft actief bijgedragen aan de totstandkoming van het advies.

De steeds grotere verscheidenheid aan online communicatiediensten, zoals gratis e-maildiensten, en het toenemende gebruik ervan, leiden tot vragen over de mate waarin aanbieders van communicatiediensten (geautomatiseerd) kennis mogen nemen van de inhoud van de met die diensten uitgewisselde berichten. Voor dit screenen bestaan diverse redenen. Het kan gaan over het willen tegenhouden van spam en het weren van virussen, maar ook over het automatisch genereren van gepersonaliseerde advertenties, samengesteld aan de hand van trefwoorden in de berichten. Hoe verhouden dergelijke screenactiviteiten zich tot de aanspraak op vertrouwelijke communicatie? Dat het daarbij niet gaat om een theoretische discussie wordt duidelijk als men zich realiseert dat netwerken en netwerkdiensten als gevolg van computervirussen en door het toenemende volume aan spamberichten zouden kunnen ophouden te functioneren.

De regelgeving voor de bescherming van persoonsgegevens bij telecommunicatiediensten biedt ruimte voor het onderzoeken van berichten, maar was op het punt van de betekenis van de randvoorwaarden uit de betreffende bepalingen nog niet voldoende uitgewerkt. De vraag naar die betekenis wordt gelet op de genoemde ontwikkelingen op het gebied van online communicatiediensten steeds belangrijker.

In het advies van de Artikel 29-werkgroep (WP118) wordt uiteengezet welke aanspraken op de vertrouwelijkheid personen kunnen maken bij het gebruik van online communicatiediensten. Daarna komt aan de orde hoe screeningsactiviteiten zich tot deze aanspraken verhouden, waarbij onderscheid wordt gemaakt tussen screening ten behoeve van het weren van virussen, ter bestrijding van spam en screening waarmee wordt beoogd een vooraf bepaalde inhoud op te sporen. Het advies wijst op de informatieverplichtingen die dienstverleners hebben en wil aanbieders van de betreffende diensten er toe aanzetten om te

streven naar het inbouwen van privacywaarborgen in systemen en infrastructuren.

Verstreking telecommunicatiegegevens aan politie en justitie

Als iemand met zijn auto het water is ingereden en voor hulp met zijn mobieltje het alarmnummer belt, is het goed denkbaar dat hij niet precies kan doorgeven waar hij zich bevindt. In zo'n geval kan de politie de telecommunicatieaanbieder vragen het mobieltje uit te peilen. Er is hier, anders dan bij het verstrekken van gegevens aan politie of justitie voor de opsporing van strafbare feiten, geen sprake van een wettelijke verplichting. Om de telecommunicatieaanbieders in deze gevallen een handvat te bieden bij de afweging wel of niet persoonsgegevens te verstrekken, heeft het CBP voorlichtingsmateriaal opgesteld. In april 2007 zal dit verschijnen in de vorm van een informatieblad.

Bij het opsporen van strafbare feiten doen politie en justitie regelmatig een beroep op aanbieders van telefoondiensten en internettoegang om hen gegevens te verstrekken. In de afgelopen jaren zijn als gevolg van nieuwe wetgeving de bevoegdheden om gegevens te vorderen verruimd en zijn de telecommunicatieaanbieders verplicht de gevorderde gegevens te verstrekken. Daarmee is beoogd een einde te maken aan de praktijk waarin door politie en justitie op telecommunicatieaanbieders een beroep werd gedaan om vrijwillig gegevens te verstrekken. Niettemin is er in een beperkt aantal gevallen, zoals in het voorbeeld van de te water geraakte automobilist, waar het gaat om leven of dood, of in gevallen van mogelijke ontvoering, nog ruimte voor vrijwillige gegevensverstrekking. Bedrijven die vaste en mobiele telefonie dan wel internettoegang aanbieden aan het publiek kunnen in het informatieblad lezen in welke gevallen op hen hiertoe een beroep kan worden gedaan.

In zijn voorlichting over de Wbp probeert het CBP zoveel mogelijk aan te sluiten bij de voorlichting van het Agentschap Telecommunicatie van het ministerie van EZ en het Handboek voor de opsporingspraktijk van het Openbaar Ministerie. Aangrenzende onderwerpen zoals het bestuursrechtelijk vorderen van telecominformatie (onder meer door OPTA), het tappen van geheimhouders en het toezicht op de notificatieplicht zijn in de zaaksbehandeling door het CBP opgepakt.



> **Verbinding verbroken**

Piet laat een klein bedrag storneren van een preselectbelbedrijf dat werkt met automatische incasso. Hij krijgt later alsnog de rekening gepresenteerd: hij kan zich bij geen enkel pre-selectbelbedrijf meer aanmelden. Zonder dat hij dat weet, is Piet besmet verklaard. Pogingen om de registratie ongedaan te maken, stranden op gebrek aan contactgegevens. E-mails worden niet beantwoord. "Op deze manier krijg ik geen enkele kans op inzage of correctie van mijn gegevens".



Technologie

Radio Frequency Identification (RFID) en biometrie zijn technologieën met grote maatschappelijke gevolgen. Doordat zij de mogelijkheid bieden van grootschalige opslag van persoonsgegevens hebben beide ook aanzienlijke invloed op privacy en privacybeleving. Toepassing van deze technologieën kan voordelen meebrengen, maar kan ook leiden tot maatschappelijke zorg. Het CBP blijft wijzen op de noodzaak om doordacht af te wegen of, waarom en hoe deze nieuwe technologieën zouden moeten worden ingezet. En, indien hiertoe wordt besloten, op de noodzaak om daarbij van meet af aan privacy ook met technische middelen te waarborgen.

> Vingerafdruk voor klantenkorting



Een rijwielhandelaar wil voor zijn vaste klanten een nieuw kortingensysteem invoeren. Daarvoor wil hij van zijn klanten niet alleen naam, adres, woonplaats, geslacht, geboortedatum en e-mailadres, maar ook de vingerafdruk. Dan hoeven zij bij het afrekenen bij de kassa geen pasje meer bij zich te hebben. "Gemak dient de mens", denkt de fietsenmaker. Maar mag dit?

De kans op goede bescherming van persoonsgegevens is het grootst door deze al in de ontwikkelingsfase van informatiesystemen als uitgangspunt te nemen. Het CBP benadrukt het belang van 'Privacy by Design', vooral voor belangrijke ICT-projecten. Een goede omgang met persoonsgegevens vergroot het vertrouwen van burgers, klanten en consumenten in bedrijven en instellingen.

Biometrie

In de Europese Unie is besloten dat paspoorten moeten worden voorzien van biometrische gegevens. In verband daarmee ontwikkelt de Nederlandse overheid plannen om te komen tot een centrale opslag van biometrische en andere gegevens van burgers. Waarom is zo'n centrale opslag nodig? Zijn de argumenten die de overheid daartoe hanteert valide?

Dit zijn twee van de vragen die tijdens een door het CBP georganiseerde expertbijeenkomst op 20 februari 2006 aan de orde kwamen. Op de agenda van die bijeenkomst stonden nut, noodzaak en eventueel nadeel van grootschalige gecentraliseerde opslag van biometrische gegevens centraal, gezien vanuit een maatschappelijke invalshoek.

Aan de bijeenkomst namen naast CBP-ers vertegenwoordigers deel van diverse maatschappelijke geledingen: wetenschappers, beleidsmakers, producenten van biometrische apparatuur en representanten van sectoren waarin biometrie met succes wordt toegepast.

De discussie spitste zich toe op de volgende vragen:

- Zijn de door de overheid gegeven argumenten om tot een Centrale Reisdocumentatie Administratie te willen komen valide?
- Waarom is centrale opslag van (biometrische) gegevens nodig?
- Wat zijn de effecten van grootschalig biometriegebruik?
- Waarom wil de overheid op voorhand allerlei gegevens vergaren?

- In welke mate zijn biometrische successen in bijvoorbeeld strafrecht- of vreemdelingenketens maatgevend om op nationale schaal te kunnen worden ingezet?
- Moeten gegevens die centraal worden verzameld alle onder controle van de overheid staan?

Tijdens het debat werd ook ingegaan op de intrinsieke zwaktes van biometrie.

Ook werd er aandacht besteed aan internationale ontwikkelingen rond het gebruik van biometrie in bijvoorbeeld visumsystemen.

Het CBP acht de argumenten die het kabinet hanteert om te komen tot centrale opslag onvoldoende. Ook los daarvan is het geen steekhoudende argumenten tegengekomen die de noodzaak van centrale opslag onderbouwen. Het is volgens het CBP twijfelachtig of biometrische technieken bij grootschalig gebruik de voordelen kunnen brengen die men ervan verwacht. Het CBP ziet risico's voor de betrokkenen, niet alleen voor wat betreft beveiliging maar ook voor gebruik van gegevens in een niet bedoelde context. Het gevaar van function creep is niet denkbeeldig. Wat betreft de beveiliging geldt dat door het bijeenbrengen van biometrische gegevens waaraan waarde is toegekend, een aantrekkelijk doelwit ontstaat voor het verkrijgen en daarna misbruiken van gegevens. Slachtoffers hebben daartegen nauwelijks verweer. Dit steekt temeer omdat gecompromitteerde biometrische gegevens niet gemakkelijk door andere te vervangen zijn.

Daartegenover staat de visie dat het voor de controle op identiteiten (en de bescherming ervan) noodzakelijk is om over een centraal ijkpunt te beschikken. Identiteitsfraude is een reëel probleem aan het worden. Iemand die gebruik zou willen maken van andermans identiteit moet betrapt kunnen worden, ter bescherming van die ander. Andere argumenten voor een centraal geregisseerd gebruik van biometrische gegevens zijn het voorkomen van dubbele uitgaven van reisdocumenten en de door terroristische aanslagen aangewakkerde behoefte aan een steeds

strakkere controle.

De discussie tijdens de expertmeeting levert een dubbel beeld op. Het centraal bijeenbrengen van biometrische gegevens kan zowel identiteiten beschermen als afbreuk doen aan die bescherming.

Als resultaat van de bespreking kunnen enige voorzichtige conclusies worden geformuleerd die duidelijk maken dat de door de overheid voorgestelde centrale opslag een mix van doelstellingen kent en dat het nog maar de vraag is of het voorstel de beste oplossing is voor het halen van die doelstellingen. Omdat het nog te vroeg lijkt om uitspraken te doen over de effectiviteit van het grootschalig toepassen van biometrie lijkt het onverstandig om nu al grootse initiatieven in die richting te ontplooien. Een stap-voor-stap benadering, waarin geleerd kan worden van ervaringen en waarin ruimte is voor het herstellen van technologische zwakten, is een zinvol alternatief. De daarbij aan te brengen beveiliging moet dan onderdeel zijn van een groter beveiligingsprogramma. Inmiddels is in december 2006 het voorstel tot wijziging van de Paspoortwet voor advies aan het CBP aangeboden. Zoals verwacht blijkt ook uit het wetsvoorstel het streven om te komen tot een centrale reisdocumentenadministratie, waarin ook de biometrische gegevens van de aanvrager van een reisdocument worden opgenomen.

RFID

Radio Frequency Identification (RFID) is een technologie waarmee voorwerpen kunnen worden voorzien van een nauwelijks waarneembare chip die gegevens bevat die onmerkbaar kunnen worden uitgelezen. Toepassing van deze technologie kan voordelen meebrengen, maar kan ook leiden tot maatschappelijke zorg. Zorg die vooral ontstaat in scenario's waarin mensen als gevolg van massale toepassing van de technologie de controle verliezen over de gegevens die over hen verwerkt worden. De eigenschappen van RFID lenen zich voor ongebreideld gebruik van gegevens in velerlei sectoren.

Door de explosieve groei van RFID-toepassingen in de laatste jaren is de technologie volop in de aandacht van privacytoezichthouders komen te staan. RFID stelt naleving en toepassing van de regels voor de verwerking van persoonsgegevens voor bijzondere problemen. De Artikel 29-werkgroep van de Europese Unie onderzoekt of het bestaande normenkader tegen deze ontwikkelingen bestand is. Het CBP draagt als lid van de werkgroep daaraan actief bij. Daarnaast heeft het CBP in 2006 zelf een studie over RFID gepubliceerd: *RFID. Veelbelovend of onverantwoord?* Bijdrage aan

de maatschappelijke discussie over RFID (nummer 29 in de reeks Achtergrondstudies en Verkenningen). Daarin wordt in de eerste plaats een overzicht gegeven van de oorzaken van privacyeffecten die samenhangen met gebruik van de technologie. In de tweede plaats doet het rapport suggesties voor activiteiten die partijen die bij het gebruik van RFID betrokken zijn, kunnen ontplooien om te bereiken dat de maatschappelijke voordelen van RFID-gebruik behaald kunnen worden met zo min mogelijk nadelen.

Met het uitbrengen van de studie wil het CBP het debat over de voor- en nadelen van de technologie verder stimuleren.

De nadelen van RFID-gebruik ontstaan doordat via de RFID-gegevens personen beoordeeld kunnen worden, vaak buiten hun medeweten. De belangrijkste waarborg om hier risico's te voorkomen of te verzachten moet worden gezocht in Privacy by Design: bij het ontwerpen van applicaties en van infrastructuur dient van meet af aan rekening te worden gehouden met privacyrisico's.

Voor zover RFID-toepassingen persoonsgegevens betreffen, is het bestaande juridisch kader van toepassing. Er zijn echter ook schemergebieden waarvoor kan blijken dat nadere normering nodig is.

Het te vroeg inzetten van nieuwe beperkende middelen kan verstikkend werken voor innovaties, het te laat inzetten daarvan tot onomkeerbare maatschappelijke nadelen. Gezien de snelheid waarmee RFID zich ontwikkelt, lijkt het voor het ontwikkelen van evenwichtige standpunten over de inzet van de techniek op dit moment verstandig vooral de nadruk te leggen op de mogelijkheden die Privacy by Design kan bieden voor het inbouwen van garanties voor verantwoorde toepassing.

Het rapport geeft voor betrokkenen – burgers, consumenten –, toepassers, onder wie de overheid, en systeemontwikkelaars aan welke aandachtspunten specifiek voor deze doelgroepen van belang zijn.

> Artikel ruilen

Een artikel omruilen in de winkel, met kassabonnetje, lijkt niet vanzelfsprekend meer, meldt mevrouw P. Sommige winkeliers willen behalve het bonnetje ook een aantal persoonsgegevens van de ontevreden klant hebben, zoals naam, adres, telefoonnummer en soms zelfs...het identiteitsbewijs. "Mag dit?" vraagt zij zich af.



Organisatie

Technologische ontwikkelingen en veiligheidsmaatregelen veranderen in hoog tempo de samenleving en hebben aanzienlijke gevolgen voor de privacy en voor de verwerking van persoonsgegevens. Het CBP is alert op de eisen die deze ontwikkelingen stellen aan zijn beleidskeuzes en organisatie.

Het College is sinds september 2006 weer op volle sterkte. De personeelscapaciteit is het afgelopen jaar licht toegenomen. Desondanks blijft het omwille van het leveren van kwalitatief hoogwaardige adviezen, uitspraken, onderzoeken en acties en het effectief communiceren daarvan, nodig accenten te verleggen. Het CBP blijft, vanuit de nieuwe locatie waarin het sinds het voorjaar van 2006 huist, welbewust een organisatie in verandering.

De maatschappelijke ontwikkelingen die direct van invloed zijn op of raken aan het werk van het CBP nemen snel toe. In 2005 is veel aandacht besteed aan het beter kunnen inspelen op deze externe ontwikkelingen en de toename van de werklast van de organisatie. Dat heeft geleid tot een organisatiestructuur met als uitgangspunt inhoudelijk management met integrale verantwoordelijkheid. In 2006 is deze opzet uitgewerkt en vastgelegd in een formatieplan. De wijzigingen in functies en rollen zijn vervolgens doorgevoerd.

De strategische managementdoelstelling gaat daarbij uit van sturing in een overgang van:

- Voornamelijk vraaggestuurd werken naar proactief en resultaatgericht werken;
- Ad-hocbehandeling van dossiers naar projectmatig werken;
- Intern/zaakgericht opereren naar strategisch denken gericht op extern resultaat.

In dit veranderingsproces zal in de komende periode nog een flinke slag moeten worden gemaakt om er voor te zorgen dat er ultimo 2007 een organisatie staat die de gestelde managementdoelstelling op een adequate wijze kan omzetten in concrete resultaten die door de samenleving worden begrepen en gerespecteerd.

Deze verandering in denkwijze vraagt van medewerkers in hoge mate een externe oriëntatie gericht op de volgende competenties:

- Gevoel hebben voor de juiste timing van handelen door het CBP;
- Open staan voor de maatschappelijke vraag achter de aan de wet gerelateerde vraag en
- Open staan voor contact met maatschappelijke partijen als bondgenoten.

Personeel en formatie

Ondernemingsraad

Na een periode waarin het CBP het zonder ondernemingsraad (OR) heeft moeten stellen, is in mei 2006 een nieuwe OR gekozen, bestaande uit vijf leden.

De OR heeft zich in eerste instantie ingewerkt, de taken verdeeld en zich laten bijscholen over onder meer het advies- en instemmingsrecht. Vervolgens heeft de OR gewerkt aan profilering binnen de organisatie, ten opzichte van zowel de achterban als de bestuurder.

In zijn beginperiode heeft de OR zich voornamelijk gericht op de afhandeling van de vele advies- en instemmingsverzoeken die het jaar daarvoor waren blijven liggen of onvoldoende aan bod waren gekomen. Signalen uit de organisatie en een groot verandertraject dat voor de organisatie op stapel staat, hebben voor een belangrijk deel de agenda aan het eind van het verslagjaar bepaald.

De OR kijkt terug op een soms tumultueus verlopen verslagjaar, waarin hij zijn weg heeft moeten zoeken. Daarbij constateert de OR dat juist op die momenten waarin eenheid tussen bestuurder en OR in optreden noodzakelijk was, die eenheid is bereikt. Vanuit deze ervaring verwacht de OR op constructieve wijze een bijdrage te kunnen leveren aan de verdere ontwikkeling van het CBP.

Formatie

Uitgangspunt voor de formatie in 2006 was: 70 fte. Er zijn 18 nieuwe medewerkers in dienst genomen.

Werken bij het CBP is enerzijds aantrekkelijk voor goed opgeleide mensen die op het onderwerp privacy hun kennis verder willen ontwikkelen. Voor de persoonlijke ontwikkeling is een vervolgstap extern een logische. Met een zeker personeelsverloop moet dan ook steeds rekening worden gehouden.

Anderzijds blijkt het niet eenvoudig te zijn om personeel met specifieke expertise en ervaring op de verschillende beleidsterreinen te werven. Investeren in werving en selectie en de begeleiding bij het inwerken van nieuwe medewerkers blijft noodzakelijk.

Gelukkig heeft de minister van Justitie in 2006 de financiële middelen beschikbaar gesteld die reeds in 2002 waren toegezegd om de beoogde formatie van 75 fte per 2007 te kunnen realiseren.

FORMATIE 2004-2006

	2004		2005		2006	
	m	v	m	v	m	v
In dienst	2	3	0	8	5	13
Uit dienst	2	1	5	5	1	6
Bezetting einde jaar m / v	26	45	21	48	26	54
Bezetting einde jaar totaal	71		69		80	
Full time	21	23	16	25	21	41
In tijdelijke dienst	8		7		18	
In vaste dienst	63		62		62	
Gemiddelde bezetting (fte's)	63,3		59,6		67,6	
Bezetting einde jaar totaal (fte's)	64,9		62,5		72,6	
Vacatures per einde jaar	0		9		3	
Overzicht medewerkers buiten formatie						
Uitzendkrachten (fte's)	0,12		0		0,17	
Stagiaires (fte's)	1,8		1,5		3,3	
Interim (fte's)	0		0,34		0	

Ziekteverzuim

Het ziekteverzuim is in 2006 verder afgenomen. In het sociaal-medisch team wordt periodiek afgestemd met de bedrijfsarts en de personeelsfunctionaris en zonodig gezocht naar passende oplossingen. Evenals vorig jaar blijft de beleving van de werkdruk een aandachtspunt.

OVERZICHT ZIEKTEVERZUIM, ZWANGERSCHAPS- EN OUDERSCHAPSVERLOF EN OVERIGE PERSONELE INFORMATIE 2004-2006

	2004	2005	2006
Totaal ziekte excl. zwangerschap	6,5%	5,82%	3,58%
Waarvan langdurig verzuim	0	2,55%	0,41%
Ouderschapsverlof	4	6	9
Verlof zwangerschap/bevalling	3	2	5
Seniorenregeling	3	2	1
Opleiding (EUR x 1.000)	145	105	142
Opleiding in % t.o.v. p-budget	4%	2,65%	3%

Het CBP prijst zich gelukkig met een relatief groot contingent jonge medewerkers. Dat brengt mee dat ook relatief veel zwangerschaps- en ouderschapsverlof wordt genoten. Vooral op kleine afdelingen drukt de afwezigheid van een collega gedurende enkele maanden zwaar. In deze gevallen moet in tijdelijke vervanging kunnen worden voorzien. Het ministerie van Justitie stelt evenwel de door verzekeraars hiertoe uitgekeerde gelden niet ter beschikking.

Mandaatregeling

De Regeling mandaat beheer directeur CBP en de Regeling volmacht en machtiging beheer afdelingshoofden, coördinatoren en controller CBP is vastgesteld en bekendgemaakt in de Staatscourant nr. 72, 11 april 2006. Met de Regeling mandaat beheer directeur CBP draagt de voorzitter van het CBP de dagelijkse leiding voor beheerszaken over aan de directeur van het secretariaat. In de Regeling volmacht en machtiging beheer afdelingshoofden, coördinatoren en controller CBP geeft de directeur volmacht en machtiging voor bepaalde beheerstaken aan de afdelingshoofden, coördinatoren en de controller.

Het Besluit mandaat en machtiging voorzitter en andere leden CBP en het Besluit mandaat en machtiging secretariaat CBP is vastgesteld en bekendgemaakt in de Staatscourant nr. 83, 28 april 2006. De Besluiten geven individuele collegeleden en medewerkers van het CBP de bevoegdheid om bepaalde besluiten zelfstandig te nemen. Op de website van het CBP wordt eveneens een regeling gepubliceerd waarin de taakverdeling en onderlinge vervanging van de collegeleden is vastgelegd.

Integriteit

Vanuit zijn rol als toezichthouder dient het CBP ook toegang te hebben tot informatie bij verantwoordelijken dat als 'staatsgeheim' is aangemerkt. In beperkte mate zal deze informatie ook bij het CBP moeten kunnen worden opgeslagen. Voor het archiveren van dergelijke dossiers heeft het CBP specifieke maatregelen getroffen. Er is voorzien in een afgesloten ruimte en in kluiskasten. De notitie Beleid veiligheidsonderzoeken van december 2005 (voor beperkte kring beschikbaar), besteedt hier speciale aandacht aan. Enkele functionarissen zijn op basis van hun functie onderworpen aan een veiligheidsonderzoek (A-screening).

Productie

Voorlichting (via de website, via e-mail, op schrift en telefonisch) is een kerntaak van het CBP. Als gevolg van de groei van het aantal verzoeken om voorlichting in 2005, de toenemende complexiteit van de voorgelegde kwesties en een oplopende zakenlast was het medio 2006 niet meer mogelijk om de verzoeken om voorlichting binnen een redelijke termijn af te handelen. Het College heeft het derhalve noodzakelijk geacht om op 7 augustus 2006 een tijdelijke stop – tot 1 oktober 2006 – op de behandeling van uitgebreidere verzoeken om voorlichting in te stellen.

Deze in een persbericht van 7 augustus 2006 toegelichte stop betrof de voorlichtingsvragen die van het CBP een behoorlijke tijdsinvestering vragen. Telefonische piket- en algemene voorlichtingsvragen (schriftelijk en via e-mail) die met een standaard informatieblad kunnen worden afgehandeld, zijn wel behandeld.

Het in 2004 ingerichte e-mailpiket, waarmee het CBP een mogelijkheid heeft geboden om (eenvoudige) voorlichtingsvragen via de e-mail voor te leggen aan het CBP, blijkt in toenemende mate ook voor de meer ingewikkelde kwesties te worden gebruikt. Evenmin is bij het in het leven roepen van deze vorm van dienstverlening voorzien dat men via e-mail veel eerder geneigd is om na beantwoording een vervolgvraag te stellen. Tijdige beantwoording, 80% binnen 5 werkdagen, bleek door de omvang en de complexere vraagstelling niet meer haalbaar. Door de tijdelijke stop en het strikt toepassen van de selectiecriteria (op grond van de gepubliceerde beleidsregels) op het in behandeling nemen van dergelijke verzoeken, is de zaakvoorraad niet verder toegenomen. Nadere maatregelen om de zaakvoorraad beheersbaar te houden, zullen echter noodzakelijk blijven.

PRODUCTIE 2004-2006

	2004	2005	2006	Prognose
Wetgevingsadvies	34	51	40	35
Gedragscodes	9	0	3	3
Reglement WPR (tot 1 sept. 2001) en Wpolr	23	8	3	10
Wbp-meldingen vanaf 01-09-2001	5.242	4.865	4.130	5.000
Voorafgaand onderzoek	174	97	93	100
Voorlichtingsverzoeken, verzoeken om advies + presentaties	821	637	635	430
Internationale zaken	66	62	61	50
Ontheffing bijzondere gegevens	3	2	1	2
Gegevensverkeer doorgifte derde landen	21	30	38	25
Bemiddeling en klachten	409	355	394	400
Ambsthalve onderzoek	56	25	42	70
Nacontrole bij verantwoordelijke		8	41	
Boete	35	9	3	25
Dwangsom	3	2	0	5
Bestuursdwang	1	0	2	1
Beroep	2	14	2	8
Bezwaar	19	6	2	10
Wet openbaarheid bestuur	11	5	4	5
Incasso		9	0	
Toegezonden uitspraken		10	7	
Algemene voorlichting (telefonisch spreekuur)	3.426	3.253	3.280	3.500
Algemene voorlichting (via e-mail)	1.957	3.039	2.959	3.000
Afgehandelde klachten over het CBP	6	16	12	9
Werkvoorraad per einde van het jaar	343	387	454	

Toelichting op de productie

Wbp-meldingen

Het aantal meldingen bij het CBP voor registratie in het Openbaar register begint naar de verwachte hoogte te groeien. Inmiddels maakt 65% van de melders gebruik van het meldingsprogramma via internet. Het aantal mutaties op bestaande meldingen maakt ca. 15 % van de binnenkomende meldingen uit.

MELDINGEN WBP, FUNCTIONARISSEN GEGEVENSBESCHERMING/GBA MELDINGEN 2004-2006

	2004	2005	2006
Meldingen Wbp in Openbaar register	25.565	27.999	30.078
Functionarissen voor de gegevensbescherming	170	183	195
Aanpassingen gemeentelijke basisadministratie	481	483	454

Scheiding voorlichting en advies

Door het toenemend gebruik van e-mail, ook voor complexe verzoeken om advies, is het onderscheid zoals deze in de jaarrapportages tot nu toe was opgebouwd (voorlichtingsvragen en algemene voorlichting via e-mail) niet reëel gebleken. Algemene voorlichtingsvragen kenmerken zich door een snelle behandeltijd met een beperkte tijdsinvestering. Verzoeken om advies zijn complexe meervoudige vragen, vaak onderbouwd met bijgevoegde bijlagen, waarvoor overleg met de verzoeker noodzakelijk is om de vraag goed te kunnen beantwoorden. Het gaat hier met name om vragen van organisaties, bedrijven, branches en overheden die om diverse redenen gebruik willen maken van bestanden met persoonsgegevens en daarvoor op voorhand van het CBP willen weten hoe de Wbp in de specifieke casus moet worden geïnterpreteerd. Het CBP heeft de procedure omtrent de intake van zaken die het CBP via de e-mail bereiken, aangepast door de e-mailverzoeken net als de schriftelijke verzoeken in twee stromen te behandelen: de algemene voorlichtingsvragen en de verzoeken om advies. Voor algemene voorlichtingsvragen geldt de prestatie-indicator dat 80% binnen 5 werkdagen af te handelen dient te zijn.

Ambtshalve onderzoek en preventieve controle

Ambtshalve onderzoek vindt plaats op basis van:

- de gekozen beleidsterreinen/ sectoren of branches die zijn opgenomen in het beleidsplan;
- een ernstige klacht of een signaal uit de samenleving en
- een onderzoek van de branche in een eerder jaar, waarbij verbeterpunten zijn afgesproken met de branche en/of de verantwoordelijke.

Deze laatste groep van onderzoeken wordt thans vastgelegd als 'nacontrole bij verantwoordelijke'. Er zijn in 2006 in totaal 83 onderzoeken uitgevoerd.

Bezwaar en beroep

Door een serieuze behandeling van heroverwegingsverzoeken blijft het aantal bezwaren achter bij de prognose.

Telefonisch spreekuur

De openingstijden voor het telefonisch spreekuur zijn beperkt tot 12 uur per week.

Werkvoorraad

Het CBP beoordeelt regelmatig de mogelijkheden voor verbetering van de efficiency. Door de stijgende werkvoorraad, met name door de verzoeken om voorlichting/advies via e-mail, is het CBP tot de conclusie gekomen dat er een duidelijker onderscheid moet worden gemaakt tussen algemene voorlichting en verzoeken om advies. Algemene voorlichting en vragen van burgers moeten enerzijds tot gestandaardiseerde informatie leiden die geplaatst kan worden op de website en/of een informatieblad en anderzijds tot een snel en adequaat antwoord, waarbij de verzoeker waar mogelijk wordt verwezen naar helpdesks van een specifiek beleidsterrein. Voor het in behandeling nemen van verzoeken om advies dient het CBP strikt de selectiecriteria toe te passen zoals bekend gemaakt via de beleidsregels (zie Uitgangspunten en beleidsregels werkwijze CBP in de Staatscourant nr. 190, van 4 oktober 2004 en op de website van het CBP). Dit betekent dat het CBP individuele verzoeken niet altijd in behandeling kan nemen. Het CBP motiveert zijn afwijzing zo veel als mogelijk met een doorverwijzing naar een andere instantie.

Communicatie

De zichtbaarheid van de toezichthouder lijkt groter te zijn geworden, gezien de gestage stijging van het aantal bezoekers van de website en de grotere aandacht die het CBP in de media krijgt.

CBPweb.nl

De website van het CBP neemt een prominente plaats in bij voorlichting van zowel de betrokkene (degene van wie persoonsgegevens worden gebruikt) als de verantwoordelijke (degene die persoonsgegevens van anderen verwerkt). De website statistieken laten een toenemend gebruik van het aangeboden informatiemateriaal zien.

OVERZICHT WEBSITEBEZOEK 2004-2006

	2004	2005	2006
Gemiddeld aantal bezoekers per maand	44.931	65.744	86.831
Aantal abonnees elektronische nieuwsbrief CBP	4.069	4.617	5.214
Aantal downloads A&V-studies	52.446	59.863	49.814
Aantal downloads auditinstrumenten	15.453	19.207	13.451
Aantal downloads Wbp-meldingsprogramma	6.233	5.602	6.632

* Onder de naam 'Contouren voor Compliance' zijn vier zelfreguleringsproducten beschikbaar met behulp waarvan verantwoordelijken de naleving van de Wbp in de eigen organisatie kunnen evalueren en verbeteren: Quickscan, Wbp-Zelfevaluatie, het Raamwerk Privacy Audit (2001) en de handreiking bij het raamwerk Privacy Audit (2005).

mijnprivacy.nl

In 2006 is gewerkt aan de ontwikkeling van een nieuwe website die speciaal gericht is op het algemene publiek. De bestaande website zal zich meer op professionele gebruikers richten. Inmiddels is www.mijnprivacy.nl eind januari 2007 in gebruik genomen.

Perscontacten

Het CBP heeft dagelijks contact met landelijke media. Het aantal contacten bleef ongeveer gelijk.

OVERZICHT PERSCONTACTEN 2004-2006

Medium	2004	2005	2006
Persbureaus	43	63	41
Landelijke dagbladen	92	106	93
Landelijke radio en televisie	150	130	100
Regionale kranten	35	39	57
Regionale radio en televisie	23	13	40
Relevante vakbladen	73	33	42
Opiniebladen	9	8	8
Totaal	425	392	381

Klachten over het CBP

In de Algemene wet bestuursrecht is geregeld dat iedereen over de wijze waarop een bestuursorgaan zich tegenover hem of haar heeft gedragen, een klacht kan indienen bij dat orgaan. Het volgende overzicht geeft het aantal ingediende schriftelijke klachten weer met de wijze van afdoening. Geen van de klachten heeft geleid tot een vervolklacht bij de Nationale ombudsman.

OVERZICHT KLACHTEN OVER HET CBP 2004-2006

	2004	2005	2006
Klachten ongegrond verklaard	3	2	4
Klachten gegrond verklaard	10	0	2
Klachten gedeeltelijk gegrond verklaard	0	1	1
Minnelijke regeling/geen oordeel/ingetrokken/ andere wijze van afdoening/nog in behandeling	2	3	5
Nog in behandeling per einde van het jaar	2	3	3
Totaal aantal ontvangen klachten	17	7	12

Heroverwegingen

Verzoeken om heroverweging (en klachten over het CBP) worden vaak ingediend omdat de betrokkene het er niet mee eens is dat de eigen klacht geen prioriteit krijgt of dat het CBP deze niet van voldoende zwaarwegend belang acht om over te gaan tot een controlerend onderzoek.

OVERZICHT HEROVERWEGINGEN 2004-2006

	2004	2005	2006
Heroverwegingen ongegrond verklaard	18	14	13
Heroverwegingen gegrond verklaard	3	5	6
Heroverwegingen gedeeltelijk gegrond verklaard	3	5	1
Minnelijke regeling/geen oordeel/ingetrokken/ andere wijze van afdoening/nog in behandeling	1	3	2
Nog in behandeling per einde van het jaar	6	1	4
Totaal aantal ontvangen heroverwegingen	28	17	25

Financiën

Als gevolg van de vacatureruimte is het personele budget niet volledig benut. De personele kosten zijn lager uitgekomen dan voorzien. Voor 2006 was uitgegaan van een gemiddelde bezetting van 70 fte. Behaald is 67,6 fte.

BEGROTING (STAND PER JULI 2006, BEDRAGEN X 1000 EURO)

	2006	2007	2008	2009	2010
	5.905	5.919	5.922	5.928	5.927

BUDGETUITGAVEN (BEDRAGEN X 1000 EURO)

	2004	2005	2006
Personeel	3.604,8	3.875,8	4.046,7
Materieel	1.266,0	1.775,2	1.655,1
Boetes uit 2004 en rente t.l.v. CBP-budget 2005		92,2	
Totaal	4.870,8	5.742,2	5.701,8

Toelichting: in het budget voor materieel zijn de huurlasten niet opgenomen. Het ministerie van Justitie stelt de huisvesting beschikbaar. In 2006 is het CBP verhuisd van ruimte in het Paleis van Justitie naar het Bruggebouw Oost aan de Juliana van Stolberglaan.

INKOMSTEN UIT OPGELEGDE BOETES EN DWANGSOMMEN 2004-2006 (BEDRAGEN X 1000 EURO)

	2004	2005	2006
Inkomsten	155,0	16,8	12,6

Bezoldiging collegeleden

Bij Besluit rechtspositie leden College bescherming persoonsgegevens (Staatsblad 2001, 382) is de bezoldiging van de voorzitter van het College vastgesteld op het maximum van salarisschaal 18 van bijlage B van het Bezoldigingsbesluit Burgerlijke Rijksambtenaren 1984. Voor de overige leden geldt het maximum van schaal 17. De voorzitter is op grond van artikel 22 a van het Bezoldigingsbesluit Rijksambtenaren 1984 een toeslag toegekend en een representatievergoeding op grond van het Besluit vergoeding representatiekosten rijkspersoneel.

Uitgaven per beleidsterrein /sector

De keuzes voor inzet van de personele kosten zijn gemaakt op basis van het beleidsplan en de daarbij vastgestelde doelstellingen voor het jaar 2006. De tabel kosten per beleidsterrein/sector biedt inzicht in hoe het CBP zijn middelen heeft verdeeld over de verschillende aandachtsgebieden.

UITGAVEN PER BELEIDSTERREIN/SECTOR 2004-2006 (BEDRAGEN X 1000 EURO)

	2004	2005	2006
<i>Maatschappelijke sectoren</i>			
Overheid	1029	852	1158
Zorg en inkomen	621	838	984
Bedrijfsleven	751	914	889
<i>Beleidsterrein internationaal</i>			
Internationaal	117	122	161
<i>Onderzoek</i>			
Onderzoek	805	862	754
<i>Beheer en meldingen en openbaar register</i>			
Bestandsbeheer	323	322	199
<i>Communicatie</i>			
Communicatie	440	498	480
Frontoffice voor de sectoren	309	369	515
<i>Juridische Zaken</i>			
Sancties rechtsbescherming en institutionele zaken	432	456	512

Uitgaven internationale samenwerking

Het belangrijkste forum voor het CBP in de eerste pijler van de Europese Unie is de Werkgroep van nationale toezichthouders als bedoeld in artikel 29 van Richtlijn 95/46/EG, die optreedt als adviseur van de Europese Commissie en als forum voor afstemming van beleid tussen de betrokken toezichthouders. Het CBP is vertegenwoordigd in de volgende subgroepen:

- Justice, Freedom and Security (JLS) (veiligheid en terrorismebestrijding)
- Employment (voorbereiding aanbevelingen inzake privacy en arbeid)
- Contracts & Binding Corporate Rules (modelcontracten voor doorgiften naar derde landen)
- Enforcement Task Force (ETF) (harmonisatie handhaving en gezamenlijke handhavingsacties)
- Internet Task Force (ITF) (internet en privacy)
- PNR (doorgifte passagiersgegevens)
- Personal Data & RFID (toepassing begrip 'persoonsgegevens' bij nieuwe technologie).

Het CBP heeft zitting in het Raadgevend Comité van het Verdrag van Straatsburg. In 2006 heeft het CBP zitting gehad in het Bureau van het Comité.

Het CBP neemt op ambtelijk en collegeniveau deel aan de jaarlijkse conferentie van Europese toezichthouders op de bescherming van persoonsgegevens en de daaraan verbonden werkgroepen:

- Case Handling Workshops (voorheen Complaints Workshops); deze bijeenkomsten zijn speciaal bedoeld voor uitwisseling van best practices tussen de medewerkers van de verschillende Data Protection Authorities en vinden 2x per jaar plaats.
- Working Party on Police. Deze werkgroep is in 2006 3x bijeengekomen.

Het CBP neemt op ambtelijk en collegeniveau deel aan de jaarlijkse internationale conferentie van toezichthouders op de bescherming van persoonsgegevens.

Het CBP neemt op ambtelijk niveau deel aan de halfjaarlijkse International Working Group on Data Protection and Telecommunications.

CBP-collegeleden zijn vertegenwoordigd in, daarbij vanuit het CBP ambtelijk ondersteund, diverse toezichthoudende organen binnen de derde pijler van de EU. Ook worden gezamenlijk audits uitgevoerd. Het betreft de volgende organen:

- Gemeenschappelijke Controleautoriteit Schengen-informatiesysteem
- Gemeenschappelijke Controleautoriteit Douane-informatiesysteem
- Gemeenschappelijk Controleorgaan Europol
- Controleorgaan Eurojust

REISDAGEN INTERNATIONAAL OVERLEG EERSTE PIJLER

	2004	2005	2006
Internet Taskforce	6	10	9
Artikel 29-werkgroep (Richtlijn 95/46/EG)	48	42	45
Adviescommissie T-PD (artikel 18, dataverdrag van Straatsburg)	13	14	4
Berlijnwerkgroep	11	9	0
Europese Case Handling Workshop	12	14	12
Europese en mondiale conferentie van privacy-toezichthouders	49	46	48
Overige	36	34	24

REISDAGEN GEMEENSCHAPPELIJKE CONTROLEORGANEN DERDE PIJLER

	2004	2005	2006
GCA Schengen	14	13	11
GCO Europol	26	6	21
Beroepscomité	5	3	0
GCA Douane	5	1	6
GCO Eurojust	2	0	0
GCA Eurodac	11	0	4
GCO Interpol	0	0	0

> Wetgevingsadviezen

Op grond van artikel 51, tweede lid Wbp dient het CBP om advies te worden gevraagd over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of in belangrijke mate betrekking hebben op de verwerking van persoonsgegevens. Dit vloeit direct voort uit Richtlijn 95/46/EG en heeft ook betrekking op voorstellen die belangrijke gevolgen hebben voor de verwerking van persoonsgegevens. De uitvoering van deze adviestaak valt onder de bepalingen van de Kaderwet adviescolleges (Stb. 1996, 378). Dat neemt niet weg dat het CBP zich ook als toezichthouder kan wenden tot de regering, al dan niet onder toezending van een kopie aan een of beide Kamers van de Staten-Generaal. Ook maakt het CBP wel gebruik van de mogelijkheid om te reageren op bij de Tweede Kamer ingediende wetsvoorstellen. Ten slotte komt het regelmatig voor dat vaste commissies uit de Tweede of de Eerste Kamer het CBP uitnodigen om te reageren op aanhangige voorstellen.

> Gedragscodes

Op grond van artikel 25 Wbp is het CBP belast met de toetsing van gedragscodes die uitvoering geven aan de wettelijke bepalingen. In de Wbp is dit een belangrijk instrument om zelfregulering te stimuleren en de kwaliteit daarvan te waarborgen. De goedkeuring van een gedragscode is meestal de afsluiting van een intensief gezamenlijk traject, waarin bewustwording en normering in een sector hand in hand gaan. In 2002 heeft het CBP daartoe een handleiding ontwikkeld. De Wbp voorziet tevens in de mogelijkheid van bezwaar en beroep op de bestuursrechter.

> Reglementen

De Wbp voorziet niet meer in de verplichting om voor bepaalde verwerkingen van persoonsgegevens een reglement op te stellen. De opstelling van een reglement kan echter wel een goed middel zijn om de gegevensverwerking binnen organisaties te sturen of transparant te maken. Verzoeken om zulke reglementen te toetsen, neemt het CBP in principe slechts in behandeling als daarvoor een bijzondere reden bestaat. Ingevolge de Wet politieregisters zijn reglementen in bepaalde gevallen onderworpen aan een toetsing vooraf in het kader van een hoorprocedure. Tezamen met de portefeuillehouder privacy van de politie vanuit de Raad van Hoofddcommissarissen heeft het CBP een werkwijze ontwikkeld voor de harmonisatie van de inhoud van de reglementen en het stroomlijnen van de procedure voor goedkeuring. Door deze werkwijze kan het aantal procedures voor goedkeuring en het aantal meldingen van tijdelijke registers worden beperkt.

> Wbp-Melding

Ingevolge artikel 27 van de Wbp moeten geautomatiseerde verwerkingen van persoonsgegevens vooraf worden gemeld bij het CBP of een functionaris voor de gegevensbescherming, tenzij het Vrijstellingsbesluit voorziet in een vrijstelling. Voor het verrichten van de melding kan gebruik worden gemaakt van een daartoe bestemd formulier, van een elektronisch meldingsprogramma op diskette, of van een speciaal voor verzending via e-mail geschikt programma. Alle meldingen worden na verwerking opgenomen in een openbaar register en zijn via de website van het CBP raadpleegbaar. Ook het overzicht van functionarissen voor de gegevensbescherming is op de website raadpleegbaar.

> Voorafgaand onderzoek

Bepaalde categorieën van verwerkingen waaraan bijzondere risico's zijn verbonden, zijn krachtens artikel 31 van de Wbp onderworpen aan een voorafgaand onderzoek dat aan strakke termijnen is gebonden. De verantwoordelijke mag een dergelijke verwerking niet starten gedurende de looptijd van dit onderzoek. Het onderzoek resulteert meestal in een verklaring omtrent de rechtmatigheid van de verwerking, die vatbaar is voor rechtsbescherming op grond van de Algemene wet bestuursrecht.

> Voorlichtingsverzoeken

Het CBP wordt vaak benaderd met verzoeken om voorlichting of advies over de interpretatie van de Wbp of een andere privacywet. De meest voorkomende verzoeken met een standaardkarakter worden behandeld door het frontoffice als deel van de publieksvoorlichting (telefonisch of via het e-mailpiket). Verzoeken om voorlichting kunnen ook aanleiding zijn voor verdergaande behandeling, diepgaande studie of een principiële standpunt. Hierbij valt te denken aan de ontwikkeling van privacykaders voor nieuwe ontwikkelingen of toetsingscriteria voor nieuwe producten en diensten. Dergelijke verzoeken worden door het CBP steeds beoordeeld op hun waarde in het kader van de toezichthoudende taak. Als zodanig vertegenwoordigen zij echter een aanzienlijke investering in maatschappelijke preventie van onrechtmatig gedrag. Omdat de beleidsvrijheid van het CBP in deze gevallen het grootst is, bestaat er alle ruimte om daarbij nadere invulling te geven aan het streven naar een tweedelijnspositie.

> **Internationale zaken**

Op grond van artikel 51, eerste lid Wbp houdt het CBP tevens toezicht op de verwerking van persoonsgegevens in Nederland, wanneer de verwerking plaatsvindt volgens het recht van een ander land van de Europese Unie. Ingevolge artikel 61, zesde lid Wbp is het CBP desgevraagd verplicht aan toezichthoudende autoriteiten van de andere lidstaten van de Europese Unie alle noodzakelijke medewerking te verlenen. Het Verdrag van Straatsburg bevat vergelijkbare verplichtingen met betrekking tot landen die daarbij partij zijn.

> **Bijzondere gegevens**

Artikel 16 Wbp bevat een verbod op de verwerking van bijzondere persoonsgegevens (zoals godsdienst, ras, politieke gezindheid, gezondheid en strafrechtelijk verleden), tenzij de wet voorziet in een uitdrukkelijke grondslag. Op grond van artikel 23, eerste lid, onder de Wbp, kan het CBP een ontheffing verlenen, indien dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer. Ook hier is bezwaar en beroep (bestuursrechter) mogelijk.

> **Doorgifte naar derde landen**

Op grond van artikel 77 lid 2 Wbp heeft het CBP de taak om de minister van Justitie te adviseren over het toekennen van een vergunning voor het doorgeven van persoonsgegevens naar een land buiten de EU dat geen waarborgen voor een passend beschermingsniveau biedt. Het gezamenlijk beleid van de minister en het CBP is eind vorig jaar bekend gemaakt. De verzoeken van bedrijven met internationale belangen om een vergunning beginnen nu goed op gang te komen. De behandeling van verzoeken door het CBP is erop gericht de minister van Justitie van een gedegen advies te voorzien zodat besluitvorming snel kan plaatsvinden.

Ook de samenwerking tussen de toezichthoudende autoriteiten wordt intensiever. Met zekere regelmaat bereiken het CBP dan ook verzoeken om bijstand van buitenlandse zusterinstellingen. Via een gemeenschappelijke, besloten website kunnen de eenvoudigste verzoeken snel worden afgewikkeld. In een aantal gevallen zijn nadere onderzoekshandelingen nodig.

> **Bemiddeling en klachtenbehandeling**

Het CBP is op grond van artikel 47 Wbp belast met de behandeling van verzoeken om bemiddeling bij geschillen over de uitoefening van het recht op inzage of correctie van persoonsgegevens en over de uitoefening van het recht op verzet. Deze procedure is mede bedoeld om de rechter te ontlasten. Belanghebbenden kunnen er ook voor kiezen om hun zaak voor te leggen aan de civiele of administratieve rechter, of gebruik maken van een geschillenregeling in een goedgekeurde gedragscode. Als het CBP de bemiddeling heeft beëindigd, kan de zaak alsnog aan de rechter worden voorgelegd.

De rechter kan besluiten om (opnieuw) het advies van het CBP in te winnen. Verder kan het CBP op grond van artikel 60 Wbp op verzoek van een belanghebbende een onderzoek instellen naar de naleving van het bepaalde bij of krachtens de wet. Daartoe beschikt het CBP over de nodige onderzoeksbevoegdheden op grond van de Wbp en de Algemene wet bestuursrecht. Bij het aannemen van dergelijke verzoeken voert het CBP een restrictief beleid. De mogelijkheid van toetsing door de Nationale Ombudsman stelt echter hoge eisen aan deze afweging.

> **Ambtshalve onderzoeken**

Artikel 60 Wbp geeft het CBP de bevoegdheid om uit eigen beweging een onderzoek in te stellen naar de naleving van de wet. In de beoogde grotere nadruk op toezicht en handhaving past dat het CBP in toenemende mate gebruik zal maken van deze bevoegdheid. Aanpak en diepgang van het ambtshalve onderzoek dienen per geval bepaald te worden. Het onderzoek kan dus een briefwisseling met verzoek om informatie behelzen of een onderzoek ter plaatse inhouden, al dan niet in de vorm van een audit, of een steekproef op meer plaatsen in een sector, met de mogelijkheid van openbare rapportage over de bevindingen. Het kan ook gaan om systematische onderzoeken binnen bepaalde sectoren of om gerichte onderzoeken (al dan niet met een privacyaudit) binnen bepaalde overheidsorganisaties, instellingen of bedrijven.

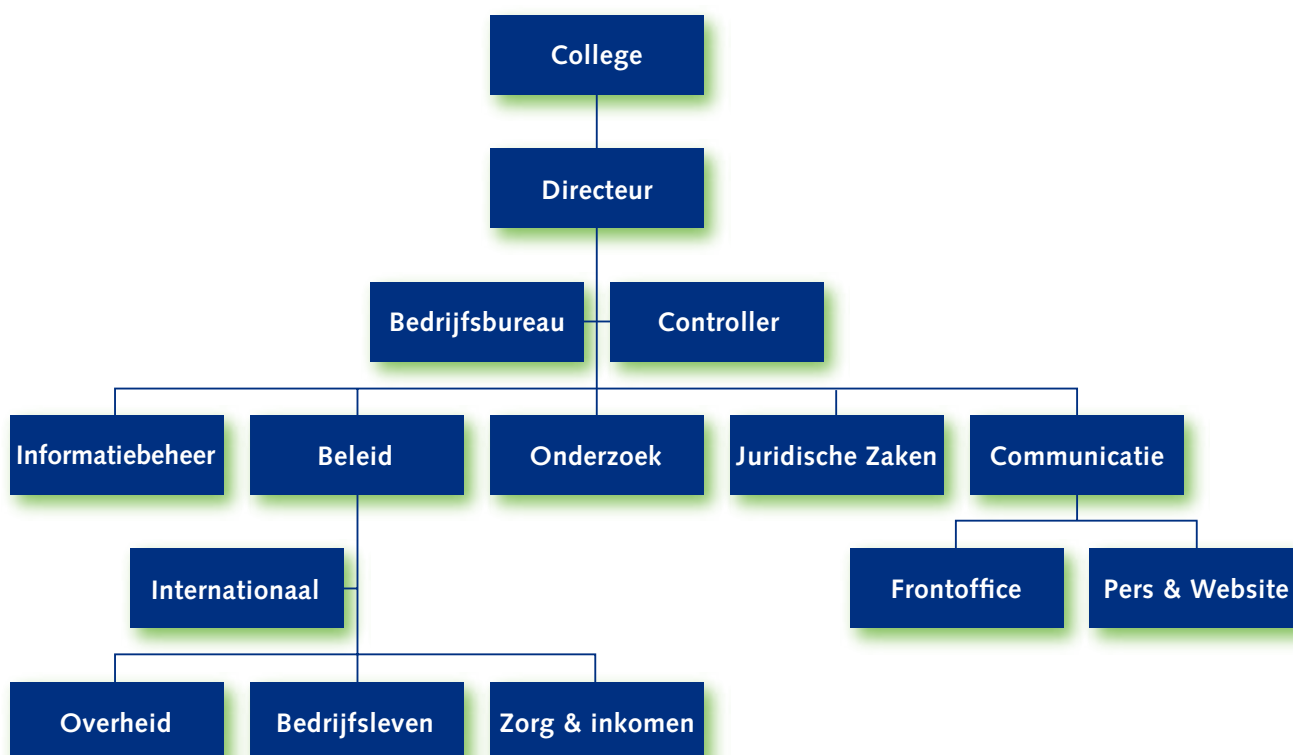
> **Boetes**

Bij overtreding van de meldingsplicht is het CBP bevoegd (artikel 66 Wbp) om een bestuurlijke boete op te leggen van 4.500 euro per verwerking, dan wel aangifte te doen bij het Openbaar Ministerie. Het CBP doet in eerste instantie door het uitvoeren van sectoranalyses op het meldingenbestand onderzoek naar de mate waarin een sector de meldingsverplichting naleeft. Hierop worden naar deze sector gerichte stappen ondernomen, voordat wordt overgegaan tot het beboeten van individuele verantwoordelijken. Echter, naar aanleiding van ter zake doende klachten, zal het CBP niet schromen individuele gevallen te beboeten of aan te geven bij het Openbaar Ministerie.

> **Dwangsom en bestuursdwang**

Bij andere overtredingen is het CBP bevoegd om gebruik te maken van de bevoegdheid tot het opleggen van een dwangsom of het toepassen van bestuursdwang. In al deze gevallen is bezwaar en beroep mogelijk.

Organigram 2006



Wetgevingsadviezen

Advies over de verwerking van persoonsgegevens bij de erkenning van beroepskwalificaties 21 december 2006, z2006-01435

Advies over wetsvoorstel eenmalige gegevensuitvraag werk en inkomen 13 december 2006, z2006-00896

Advies over Regeling Kentekenregister 23 november 2006, z2006-01286

Advies wetsvoorstel basisregistraties Inkomen en WOZ 20 november 2006, z2006-01448

Advies over het Besluit gebruik burgerservicenummer in de zorg 20 november 2006, z2006-01388 en z2006-01388

Advies over het wetsvoorstel tot verruiming van de mogelijkheden ter opsporing en vervolging van terroristische misdrijven 9 november 2006, z2006-01337

Advies over ontwerp Besluit politiegegevens 1 november 2006, z2006-00686

Adviesaanvraag ontwerpbesluit tot wijziging van het besluit SUWI 11 oktober 2006, z2006-01055

Advies over wijziging van het Besluit GBA 4 oktober 2006, z2006-01020

Advies over wetsvoorstel wijziging Leerlinggebonden financiering 21 september 2006, z2006-00945

Advies over wijzigingsvoorstel Besluit justitiële gegevens inzake de uitwisseling van gegevens uit strafregisters 8 augustus 2006, z2006-00738

Advies over wijziging Wet studiefinanciering 25 juli 2006, z2006-00794

Advies over verstrekking gegevens van ouders aan scholen (gewichtenregeling) 20 juli 2006, z2006-00154

Advies over wijziging Besluit gegevensverwerking CBS 12 juli 2006, z2006-00718/00744

Advies over wijziging Wegenverkeerswet 28 juni 2006, z2006-00533

Advies over wetsontwerp Basisregistratie adressen en gebouwen 28 juni 2006, z2006-00683

Advies wetsvoorstel financiering politieke partijen 22 juni 2006, z2006-00559

Advies Concept Aanwijzing Voorlichting, Opsporing en Vervolging 7 juni 2006, z2005-1404

Advies over het reguleren van toegang tot het kentekenregister 31 mei 2006, z2006-00560

Advies over gebruik vingerafdrukken van vreemdelingen voor opsporingsdoeleinden 31 mei 2006, z2006-00531

Advies over voorkoming afsluiting van energievoorzieningen 22 mei 2006, z2006-00548 j° 12 februari 2007, z2007-00042

Advies over wijziging Besluit verstrekking gegevens telecomcommunicatie 1 mei 2006, z2006-00403

Advies wijziging Wet bereikbaarheid en mobiliteit 30 maart 2006, z2006-00285

Advies aan de Tweede Kamer over invoering Burgerservicenummer in de zorg 20 januari 2006, z2005-0807

Advies over wijziging artikel 27 Bekostigingsbesluit WPO 14 maart 2006, z2006-00154

Advies over wetsvoorstel Marktordening in de gezondheidszorg 17 februari 2006, z2005-0760

Advies over wetsvoorstel Uitbreiding verbod ongevraagde elektronische communicatie 3 januari 2006, z2005-1389

Dit overzicht bevat de voornaamste wetgevingsadviezen van 2006. Vrijwel alle adviezen vanaf 1996 kunt u raadplegen op de website www.cbppweb.nl. Adviezen uit de periode 1991-1996 zijn ook opgenomen in de bundel *Persoonsgegevens beschermd, van WPR naar Wbp*. Den Haag, Sdu uitgevers, 1999.

Gedragscodes

Voor onderstaande gedragscodes is in 2006 een verklaring van overeenstemming verleend onder de Wbp.

Addendum Zorgverzekeraars

Geldig tot 2 mei 2011 (Staatscourant 2006, nr. 85).

Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek

Geldig tot 2 januari 2011 (Staatscourant 2006, nr. 1).

Alle gedragscodes zijn te vinden op www.cbpweb.nl

Modelreglementen vastgesteld voor politieregisters

Aandachtsvestigingen	(Stcrt. 2002, 243)
Arrestanten	(Stcrt. 2002, 243)
Arrestatiebevelen	(Stcrt. 2002, 243)
Bedrijfsprocessensysteem BPS	(Stcrt. 2002, 243)
Bedrijven informatiesysteem en waarschuwingadressen	(Stcrt. 2002, 243)
Bekeuringenafhandelingssysteem	(Stcrt. 2002, 243)
Beperkingen besturen motorrijtuigen	(Stcrt. 2002, 243)
Bureau financiële ondersteuning	(Stcrt. 2002, 243)
Cameratoezicht voor het tijdelijk register cameratoezicht	(Stcrt. 2006,140)
Fraudebestrijding	(Stcrt. 2002, 243)
Gegevensuitwisseling milieu- criminaliteit	(Stcrt. 2002, 243)
Gevonden en verloren goederen	(Stcrt. 2002, 243)
Graffitibestrijding	(Stcrt. 2002, 243)
Herkenningsdienstregister	(Stcrt. 2004, 124)
In beslag genomen goederen	(Stcrt. 2002, 243)
In bewaring genomen goederen	(Stcrt. 2002, 243)
Inbraakbestrijding	(Stcrt. 2002, 243)
Informantenregister	(Stcrt. 2002, 100)
Informantenregister openbare orde	(Stcrt. 2002, 238)
Internationale rechtshulp politie	(Stcrt. 2002, 243)
Jeugd- en zedenzaken	(Stcrt. 2002, 243)
Kabinetszaken	(Stcrt. 2002, 243)
Meldkamer	(Stcrt. 2002, 243)
Milieudelicten	(Stcrt. 2002, 243)
Multipol	(Stcrt. 2002, 243)
Openbare orde informatie	(Stcrt. 2002, 238)
Opkopers en helingbestrijding	(Stcrt. 2002, 243)
Overvallenbestrijding	(Stcrt. 2002, 243)
Permanent autoteam	(Stcrt. 2002, 243)
Processen-verbaal en rapporten	(Stcrt. 2002, 243)
Recidive	(Stcrt. 2002, 243)
Rijverboden	(Stcrt. 2002, 243)
Schietwapen incidentenregistratie- en informatiesysteem	(Stcrt. 2002, 243)
Signalen van mensenhandel	(Stcrt. 2002, 13)
Technische recherchezaken	(Stcrt. 2002, 243)
Tijdelijk Register	(Stcrt. 2002, 131)
Vakantiecontrolekaarten	(Stcrt. 2002, 243)
Vandalismebestrijding	(Stcrt. 2002, 243)
Verdovende middelen	(Stcrt. 2002, 243)
Voorlopig register	(Stcrt. 2000, 198)
Zware criminaliteit	(Stcrt. 2000, 198)

De politie werkt voor het uitoefenen van de politietaak (artikel 1 en artikel 2 Politiewet) met politieregisters. In artikel 12, eerste lid Wet politieregisters is de mogelijkheid gecreëerd om een modelreglement voor een register vast te stellen, onder andere ter bevordering van eenduidigheid en een efficiënte werkwijze. Degene die een modelreglement heeft vastgesteld, kan het CBP verzoeken te verklaren dat het model naar zijn oordeel in overeenstemming is met de Wet politieregisters. Beheerders van een register hoeven dan het CBP alleen te informeren over het bestaan van een register en van het model dat daarop van toepassing is. Mochten er afwijkingen van het model zijn, dan moet vermeld worden welke dat zijn. De modelreglementen zijn beschikbaar op de website van het CBP: www.cbpweb.nl.

Documenten van de Werkgroep inzake de bescherming van persoonsgegevens (artikel 29 van Richtlijn 95/46/EG)

22 november 2006 - **Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)** (WP 128)

27 september 2006 - **Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data** (WP 127)

26 september 2006 - **Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive** (WP 126)

26 september 2006 - **Working document on data protection and privacy implications in eCall initiative** (WP 125)

27 september 2006 - **Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement** (WP 124)

9 augustus 2006 - **Opinion 6/2006 on the Proposal for a Council Regulation on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations** (WP 123)

14 juni 2006 - **Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States** (WP 122)

14 juni 2006 - **Opinion 4/2006 on the Notice of proposed rule making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71)** (WP 121)

5 juni 2006 - **Work Programme 2006-2007** (WP 120)

25 maart 2006 - **Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC** (WP 119)

21 februari 2006 - **Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services** (WP 118)

1 februari 2006 - **Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime** (WP 117)

Deze documenten zijn te vinden op http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm

Onderzoeksrapporten

Rapporten kunt u doorgaans raadplegen op de website: www.cbpweb.nl (onder publicaties).

2006

- **Naleving van de informatieplicht door de sociale recherche**, november 2006
- **Particuliere recherche en bescherming van persoonsgegevens**, mei 2006.
- **Naleving van de informatieplicht door particuliere recherchebureaus**, mei 2006.
- **Zorgverzekeraars, gezondheidsgegevens en privacy**, mei 2006.
- **Bekendheid en beleving informatieplicht onder burgers. Kwantitatief onderzoek onder burgers**, mei 2006.
- **De naleving en beleving van de informatieplicht onder organisaties in Nederland. Onderzoek onder huisartsen, onderwijsinstellingen en woningcorporaties**, mei 2006.
- **Uitwisseling van politiegegevens tussen de Nederlandse Antillen en Nederland**, april 2006.

2005-2001

- **Reïntegratie van zieke werknemers en privacy: verkennend onderzoek bij drie reïntegratiebedrijven**, december 2005.
- **Reïntegratie van bijstandsgerechtigden en privacy: verkennend onderzoek bij drie reïntegratiebedrijven**, december 2005.
- **Landelijke zorgregistraties (verslag van oriënterend feitenonderzoek bij vijf grote landelijke registraties in de zorg)**, maart 2005.
- **Algemene bevindingen, naar aanleiding van de onderzoeken door het CBP naar de bijzondere politieregisters van criminele inlichtingen eenheden in 2003/2004**, september 2004.
- **Cameratoezicht in de openbare ruimte: Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten**, november 2003.
- **KPN informeert abonnees met geheim nummer onvoldoende over direct marketing. Onderzoek naar beleid omtrent 'geheime' nummers; bevindingen**, augustus 2003.
- **Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie**, juli 2003.
- **Onrechtmatig, onbehoorlijk en onzorgvuldig. De verwerking van persoonsgegevens door een handelsinformatiebureau voor rapportage van verhaalsinformatie**, april 2003.

- **Sociale diensten: bijstandsdossier en privacy**, februari 2002.
- **Privacy bij wetenschappelijk onderzoek en statistiek. Kader voor een gedragscode**, mei 2002.
- **Elektronische overheid en privacy**, december 2001.
- **Onrechtmatige handelswijze van een handelsinformatiebureau**, mei 2001.

Achtergrondstudies en verkenningen 1994 – 2006

In de serie Achtergrondstudies en verkenningen zijn verschenen:

drs. R.R.A. Beugelsdijk, **RFID, veelbelovend of onverantwoord? Een bijdrage aan de maatschappelijke discussie over RFID**. A&V 29, College bescherming persoonsgegevens, Den Haag, 2006

mr. A.H.C.M. Smeets, **Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde**. A&V 28, College bescherming persoonsgegevens, Den Haag, 2004

drs. S. Lieon, mr. M. Th. van Munster-Frederiks, **De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers**. A&V 27; College bescherming persoonsgegevens, Den Haag 2004

mr. drs. T.F.M. Hooghiemstra, **Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg**. A&V 26; College bescherming persoonsgegevens, Den Haag 2002

dr. J.A.G. Vermissen, mr. drs. A.C.M. de Heij, **Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid**. A&V 25; College bescherming persoonsgegevens, Den Haag 2002

mr. M.M.M. van Eijk, drs. W.J. van Helden, **Klant te koop. Privacyregels voor adressenhandel**. A&V 24; Registratiekamer, Den Haag 2001

G.W. van Blarckom RE en drs. J.J. Borking, **Beveiliging van persoonsgegevens**. A&V 23; Registratiekamer, Den Haag 2001

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

mr. drs. J.H.J. Terstegge, **Goed werken in netwerken. Regels voor controle op e-mail- en internetgebruik van werknemers**. A&V 21; tweede druk, herzien door drs. S. Lieon, College bescherming persoonsgegevens, Den Haag 2002

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

drs. W.J. van Helden, **Herkomst van de klant. Privacy-regels voor etnomarketing**. A&V 19, Registratiekamer, Den Haag 2000

mr. R.W.A. Wishaw MS, **De gewaardeerde klant. Privacy-regels voor credit scoring**. A&V 18; Registratiekamer, Den Haag 2000

mr. M.J.T. Artz en mr. M.M.M. van Eijk, **Klant in het web. Privacy waarborgen voor internettoegang**. A&V 17; Registratiekamer, Den Haag 2000

mr. J. de Zeeuw, **Informatieverstrekking door de fiscus, ontheffing van de geheimhoudingsplicht in het licht van privacywetgeving**. A&V 16; Registratiekamer, Den Haag 1999

dr. R. Hes, mr. drs. T.F.M. Hooghiemstra, drs. J.J. Borking, **At face value - on biometrical identification and privacy**. A&V 15; Registratiekamer, Den Haag 1999. With contributions from: P.J.A. Verhaar, T.G.A. van Rhee and H.A.M. Luijff (TNO Physics and Electronics Laboratory - The Hague).

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

drs. J.J. Borking, mr. B.M.A. van Eck en P. Siepel, **Intelligent Software Agents and Privacy**. A&V 13; Registratiekamer, Den Haag 1999

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

dr. R. Hes en drs. J.J. Borking, **Privacy Enhancing Technologies: the path to anonymity**. Revised edition. A&V 11; Registratiekamer, Den Haag 1998

drs. J.J. Borking, mr. M.J.T. Artz en mr. L. van Almelo, **Gouden bergen van gegevens. Over datawarehousing, datamining en privacy**. A&V 10; Registratiekamer, Den Haag 1998

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

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

mr. dr. P.C. Ippel, **Gegeven: de genen. Morele en juridische aspecten van het gebruik van genetische gegevens.** A&V 7; Registratiekamer, Den Haag 1996

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

ing. H. van Rossum, **Privacy-enhancing technologies: the path to anonymity, volume I and II.** A&V 5; Registratiekamer, Den Haag 1995. In 1998 verscheen een vernieuwde versie van deze studie, A&V 11.

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

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

drs. J.P.M. van Casteren, **Bevolkingsgegevens: wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden.** A&V 2; Registratiekamer, Rijswijk 1995

mr. B.J.P. Hulsman en mr. dr. P.C. Ippel, **Personeels-informatiesystemen - de Wet Persoonsregistraties toegepast.** A&V 1, Registratiekamer, Rijswijk 1994

Brochures

Tien Gouden Regels voor verwerking van persoonsgegevens door de sociale dienst, januari 2007

Functionaris voor de gegevensbescherming. Een handreiking herziene versie, januari 2007

Gedragcodes. Bescherming van persoonsgegevens door zelfregulering, oktober 2002

Third countries. Transfers of Personal Data to Countries outside the European Union, september 2002

Derde landen. De doorgifte van persoonsgegevens naar landen buiten de Europese Unie, september 2002

Privacy: checklist voor de ondernemingsraad, april 2002

Wet bescherming persoonsgegevens. Over de bescherming van uw persoonlijke gegevens, augustus 2001

Mag het een beetje minder zijn? Over Privacy Enhancing Technologie, april 2001

Doe het zelf met privacy. Een toelichting op de Audit Aanpak, 2001

Informatiebladen

Laatste geactualiseerde versies

Informatiebladen voor de betrokkene:

Als u gefilmd wordt met een videocamera, februari 2005
Als de politie gegevens over u vraagt, december 2006
Bemiddeling door het CBP inzake uw gegevens, december 2006
Bewaartermijnen van uw persoonsgegevens, december 2006
Camera's op de werkplek, december 2006
Correctie van uw persoonsgegevens, december 2006
De GBA en uw persoonsgegevens, december 2006
Doorgifte van uw gegevens naar derde landen, juni 2004
Functionaris voor de gegevensbescherming, juni 2004
Geadresseerde reclame, juni 2004
Gebruik van kentekengegevens en uw privacy, april 2005
Geheimhouding van uw medische gegevens, juni 2005
Inzage in uw persoonsgegevens, juli 2005
Nummeridentificatie bij telefoonverkeer, maart 2007
Omgang met uw medische gegevens, december 2006
Opnemen van uw telefoongesprekken op de werkplek, juni 2004
Rechten van de betrokkene, februari 2007
Sociale dienst en uw persoonsgegevens, maart 2004
Toetsen van uw kredietwaardigheid (creditscoring), december 2006
Uw gegevens bij de politie, oktober 2004
Uw gegevens op een zwarte lijst, juni 2004
Uw klacht en het CBP, december 2006
Uw personeelsdossier, juni 2004
Uw persoonsgegevens beveiligd, september 2003
Uw rechten als patiënt, juni 2005
Uw recht op informatie, februari 2007
Uw recht van verzet bij direct marketing, oktober 2004
Verstrekken van uw gegevens uit ledenadministratie, maart 2004
Verstrekken van uw personeelsgegevens, juni 2004
Verstrekken van uw persoonsgegevens, december 2006

Informatiebladen voor de verantwoordelijke:

Als de politie u vraagt persoonsgegevens te verstrekken, oktober 2004
Als u mensen filmt, februari 2005
Bemiddeling door het CBP inzake uw verwerkingen, december 2006
Bewaartermijnen van persoonsgegevens in uw bestanden, januari 2006
Bieden van correctie in persoonsgegevens, december 2006
Camera's op de werkplek, december 2006
De GBA en het gebruik daarvan, februari 2006
Doorgifte naar derde landen inzake uw gegevens-verwerkingen, juni 2004
Functionaris voor de gegevensbescherming, juni 2004
Geven van inzage in persoonsgegevens, juli 2005
Geheimhouding van medische gegevens, juni 2005
Informatie delen in samenwerkingsverbanden, december 2006
Informatieplicht, februari 2007
Klachtenbehandeling door het CBP, december 2006
Melden en vrijstellingen, maart 2004
Opnemen telefoongesprekken op de werkplek, juni 2004
Personeelsdossiers, juni 2004
Rechten van de betrokkene, februari 2007
Rechten van uw patiënt, december 2006
Recht van verzet bij direct marketing, oktober 2004
Uw omgang met medische gegevens, juni 2005
Verstrekken gegevens uit uw ledenadministratie, maart 2004
Verstrekken van personeelsgegevens aan derden, juni 2004
Verstrekken van persoonsgegevens, december 2004
Voorafgaand onderzoek, september 2001
Zwarte lijsten, juni 2004

Publicaties van het CBP kunt u inzien en/of downloaden van de website www.cbpweb.nl. Voor het toezenden van gedrukte publicaties kunnen administratie- en verzendkosten in rekening worden gebracht.

Publicaties in kranten, tijdschriften en vakbladen 2006

Je leven op internet, tekst van de presentatie van Madeleine McLaggan-Van Roon, Debat Je leven op internet: datapakhuizen en privacy, 7 december 2006

‘We komen in een controlesamenleving terecht’
Verslag van ‘Nederland controlestaat?’ Debat over veiligheid en privacy in De Balie, Amsterdam, 17 november 2006

Etniciteit, profilering en het gelijkheidsbeginsel Jannette Beuving, Jan-Willem Heuver en Willemijn van Helden. In Nederlands Juristenblad, nr. 34, 29 september 2006, p. 1954-1955

De staat van de privacybescherming van patiënten en cliënten 2005-2006 Sjaak Nouwt en Victoire Lucieer. In P&I, nr. 6 – december 2006, 314, p. 285-294

Binding Corporate Rules, tekst van de speech van Madeleine McLaggan-van Roon voor de conferentie over internationale doorgifte van persoonsgegevens, Brussel 23-24 oktober 2006

Veiligheid en de Wet bescherming persoonsgegevens Jacob Kohnstamm, Johan de Wittlezing, 4 oktober 2006

Gegevensuitwisseling door de politie binnen het Koninkrijk der Nederlanden Jeroen Obdam. In P&I, nr. 4 – augustus 2006, 185, p. 178-180

Invoering van het Burgerservicenummer in de zorg Victoire Lucieer. In JPG 2006/5 - juni 2006, p. 119-127

Interpretatie & harmonisatie: Het werkprogramma van de Artikel 29-werkgroep voor 2006 en 2007 Anne-Marije Fontein. In P&I, nr. 3 - juni 2006, 136, p. 127-128

Verlaten Patiëntendossiers Victoire Lucieer. In JPG 2006/2 - maart 2006, p. 34-37

Het beroepsgeheim in de zorginstelling: een reactie Jacqueline Krabben. In JPG 2006/1 - februari 2006 p. 3-7

Van Esch gaat te gemakzuchtig om met de WBP Anne Marie Terhorst. In Computerrecht 2006, aflevering 1, p. 42

Reactie op oratie van Mariëlle Bruning die als titel heeft ‘Over sommige kinderen moet je praten’, Anne Marie Terhorst. In Familie- en Jeugdrecht juni 2006, nummer 6, pagina 159



With any measures taken...

'With any measures taken, the Government is accountable for the consequences for citizens' privacy.' The political parties CDA, PvdA and CU decided to introduce this promising policy aimed at the protection of privacy as an assignment for the Cabinet, which had not yet been formed at that point.

A wide diversity of activities can have consequences for the privacy of ordinary citizens, and the necessity to take these into account, both in the private and public sector, is undeniably increasing. The creation of all kinds of technical innovations, in combination with the Internet and existing ICT applications create almost unlimited possibilities for the gathering of information, and for the communication of that information. The advantages of this situation are immediately apparent. We all are embracing new possibilities for personal development, for improved and more effective private and public services, and more responsible forms of production. Refined logistics systems, electronic government files that are connected by means of personal numbers for the benefit of a convenient service provision for citizens, public and financial services via the Internet, the Public Transport Smart Card, the ability to purchase air tickets, software, films, music and other goods online, mobile communication in speech, images, and text, multiplayer online role playing games, web logs and chat programmes, powerful search engines and continuous news provision: we are experiencing a revolution that is both limitless and challenging.

All these good things have disadvantages as well. In principle, such ICT applications make large amounts of personal data available for analysis, profiling, tracing, and controls. Where necessary, storage of the data may well be made into a legal obligation in order to enable this, such as in the case of traffic data of all the telecommunication of almost half a billion EU citizens. These unlimited possibilities can become very disadvantageous both to people and to the cohesion in society. In a world where technology transcends all boundaries, who determines and maintains the norms and values that every society needs to remain habitable, and to 'keep things together'? What social consequences are associated with the fact that a company, government or individual would be able to trace someone's daily life from one minute to the next? How safe can people still feel in such a society?

There is no doubt that the possibilities which allow everyone insight into and the use of details about the private life and the behaviour of individuals should be subjected to limitations. When someone is blacklisted on the Internet, the consequence could be that this person – often for no good reason at all – could be made infamous across the globe for an indeterminate period of time. When a guileless young person has sent a webcam recording over the Internet, it must be questioned whether it is permissible for that person to be confronted with it years later at a moment when it is least expected, such as during a job application procedure. The connection between all kinds of searches and all kinds of other data files – including video camera recordings – can lead to suspicions or profiling that bears no resemblance to reality. The 're-use' of a limited amount of collected or linked data about an individual can lead to expensive and disastrous forms of identity fraud and theft. People who, without thinking, and not taking reality into account, have remarked that they did not have anything to hide, will be confronted with the unwelcome side of reality when it turns out afterwards that they have not been able to do anything, anywhere, without being spied on or recorded.

Technology, especially when its maximum deployment is linked to efficiency targets, is 'without values'. Legislation has ensured, in the form of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act], and a number of other laws and legal regulations, that the gathering and processing of data by private and public organisations most certainly does need to comply with certain norms and values: namely that data should only be collected once it has been established that this is necessary; that in principle, the data should not be used for any purposes other than those for which they were originally collected; and that data should, in any case, be handled with due care and respect.

Within the operational arena of the socio-technical developments described above, maintaining the system of norms as laid down in the Wbp has not – all things considered – become any easier, especially for a supervisory body with such limited financing. For the Dutch Data Protection Authority, it is essential to make well-defined and balanced choices when addressing the issue as to how, and in what fields, personal data should particularly be protected. The coalition has expressed a commitment that, when formulating any measures in this area, the consequences of such measures for the privacy of citizens will be taken into account and justified. This will provide, in any case, a welcome contribution to this important endeavour.

J. Kohnstamm

chairman

2006 in a nutshell

The protection of privacy inspires a wide range of reactions. A very common one is 'I don't really think it's necessary. I've nothing to fear, because I've nothing to hide and security is more important than my privacy.' Or, for example 'It doesn't make any difference to me. They already know everything about you.' Or 'It's a really important thing, because you don't want to live your life being permanently spied on.'

The Dutch Data Protection Authority (Dutch DPA) continues in its efforts to strike a proper balance between the interests of security, control and utility, and to guarantee as far as possible the protection of the private life of individuals, which can come under pressure from those interests.

The right to integrity of one's private life, inseparably linked with careful use of personal data, is less and less something to be taken for granted. The Dutch DPA has a duty to act as a 'privacy watchdog' where there is any threat that this basic right might be overlooked in the interests of security and criminal investigations, or that it might evaporate in the limitless scope of the Internet and other technological developments. Its primary function is to keep a check on compliance with the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act]. But effective supervision and, where necessary, enforcement of the rules for dealing with personal data is not enough. By providing information and advice, and by consulting with social parties, the Dutch DPA adopts a proactive stance in order to persuade citizens, governments, companies and institutions of the necessity of handling personal data with care. This is in order to enhance the confidence that ordinary people, who have nothing to hide, should be able to have in institutions dealing with their data. It is also designed to improve the quality of legislation and service provision.

This chapter provides an overall summary of the work of the Dutch DPA during the past year.

Security and control

The protection of the private life of individuals is beset on two sides. On the one hand, for reasons of political security, governments are proactively and dramatically extending their powers at national, regional and international levels to collate large quantities of data concerning ever larger groups of citizens.

On the other hand, continually refined technology and the interlinking of data files provide ever more opportunities for tracking and recording the comings and goings of everyone.

The international conference of the data protection authorities, attended annually by the Dutch DPA, issued a warning in November 2006 that, as regards the protection of data, the question was whether the traditional supervisory methods were still adequate, in light of the new technologies. The supervisory agencies consider that joint action to counteract excessive forms of control is now necessary.

Passenger information

A new agreement will come into effect in August 2007 at the latest between the United States and the European Union concerning airlines providing passenger information to the USA. The 'Article 29 Working Party' of European data protection authorities, of which the Dutch DPA is a member, is concerned about the current temporary arrangements that form the basis for the proposed treaty, because they appear to facilitate an even wider dissemination of information among American authorities, for even more new purposes. The Chairman of the Dutch DPA emphasised during a meeting in December 2006 in Brussels that it had to be made clear that the security measures to be taken are necessary and proportionate, and also pointed out the importance of transparency and accountability.

Cooperation in the EU by Justice and the police

The decisiveness of EU member state governments in relation to the introduction of security measures based around cross-border exchange of information stands in stark contrast to the adoption of the European Framework Decision on personal data protection for collaboration between Justice and police. According to the European data protection authorities, the only



workable option for a more extensive exchange of personal data is a harmonised high standard of protection in the third pillar. The same applies in relation to transfer of information to countries outside the EU and to international institutions. The European data protection authorities consider that a limited approach will not be workable in practical terms, and will also have an adverse impact on confidence in the collaboration between police and Justice at European level.

Detection of terrorist offences

In the Dutch context of counterterrorism in recent years, there has been an accumulation of powers in the hands of the police and judicial authorities. The Dutch DPA has provided advice to the Minister of Justice and the Lower House of the Dutch parliament in recent years on legislative proposals to extend the scope of the detection and prosecution of terrorist offences. The Dutch DPA's criticisms are aimed primarily at the absence of clear justification of the need for the proposed measures, including more broadly targeted preliminary research into particular groups within society. Because many of these points of criticism were not followed up, the Dutch DPA provided more detailed advice last year to the Senate Standing Committee on Justice, at the request of the chairman of the Senate, regarding the measures he considered were necessary in order to achieve a better balance between supervision of the processing of personal data and the growing powers of the penal authorities.

Topic processing

The shifting boundary between investigative and prosecution powers has clear implications for the protection of personal data. One of the major innovations in the new Wet politiegegevens [Police Data Act] is introduction of "topic processing". Topic processing includes the systematic and proactive processing of personal data in relation to 'innocent' citizens - people against whom the facts and circumstances do not raise any reasonable suspicion of guilt. By contrast with the current Wet politieregisters [Police Registers Act], the new act will not have any separate regime for data relating to these 'slightly suspect' individuals. The Dutch DPA would warn that without extra protection for this personal data, for example by means of coding, there will be an unacceptably high risk of citizens being wrongly subjected to police action. In 2006, the Dutch DPA discussed with the Senate Standing Committee on Justice the need for permanent monitoring of the accuracy and quality of police data.

The virtual moat

In 2005, the Raad van Hoofdcommissarissen [Association of Chief Police Officers] put forward the notion that the police would start to focus on the infrastructure carrying people, money, goods and information, in the context of their offensive against crime. One of the ways this would happen would involve detection using cameras aimed at access routes into cities. The Dutch DPA expressed its concerns about this proposal to the Minister of Internal Affairs and Kingdom Relations, distinguishing between three degrees of acceptability in the proposed method of operation. Identifying suspects using registration plate recognition, and recording their details, would be acceptable. Recording details of repeat offenders - those known to the police - without them being suspected of a crime at that point would not be acceptable as a matter of course. There would have to be a check, on a case-by-case basis, as to whether the storage of this data was in breach of the law. Recording the details of everyone travelling on a particular route would be taking things too far, according to the Dutch DPA, certainly if these details were subsequently analysed.

These types of new methods, under which protection of personal data would be likely to suffer, should only, in the view of the Dutch DPA, be considered if the police can show that their existing powers are inadequate for guaranteeing further security. The Dutch DPA held

consultations with the Raad van Hoofddcommissarissen in the first quarter of 2007 concerning their experience with the system to date.

Large-scale data processing

Technical developments have now made it possible for governments, other service providers and trade sectors to process data, including personal data, on a large scale. This can be both useful and lucrative, but it can also be damaging to individuals if things go wrong. What needs to be done is to try and avoid such errors at the design stage, both as regards the technology and the legislation.

Passports

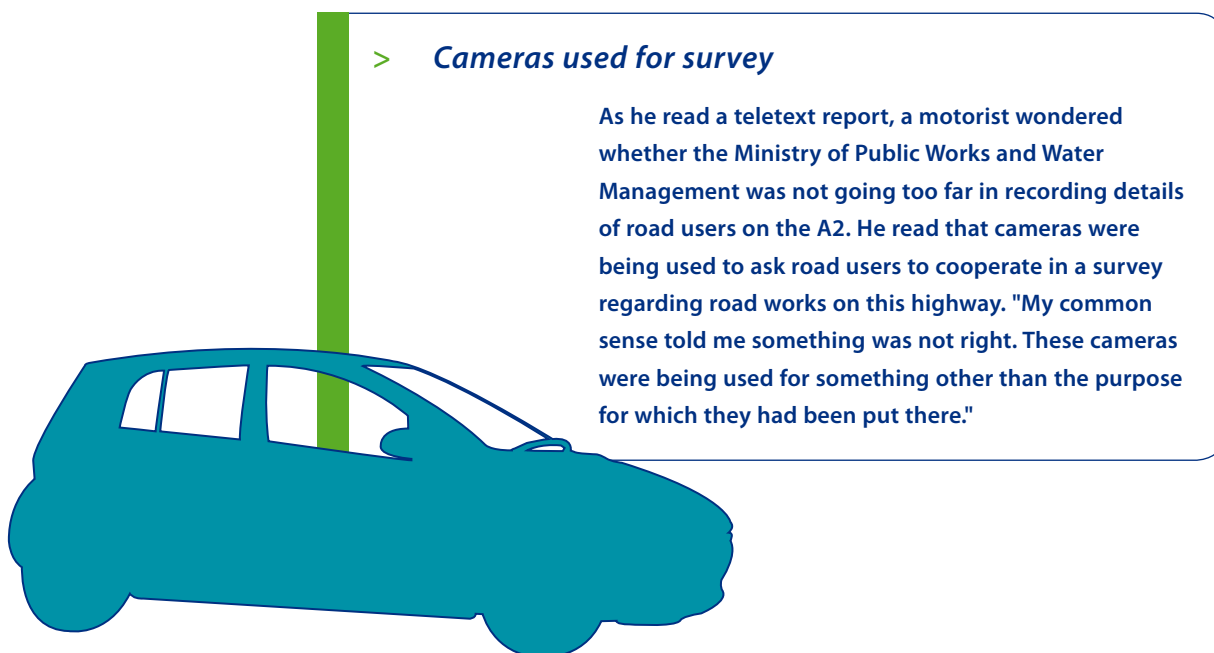
Passports are provided with biometric information in the member states of the European Union. In this context, the Netherlands will shortly have a central storage point for travel documents, which will also include biometric data for the applicants. Why is there a need for this type of central storage? Are the government's arguments for this convincing? These and other questions concerning usage, need and the potential disadvantages of this large-scale storage of data were discussed during an expert meeting organised by the Dutch DPA in February 2006. The results of the discussion were ambiguous: central collation of biometric data can on the one hand protect identities by having one central reference point, but on the other hand they can undermine that protection as a result of security risks and potential use of biometric data for other purposes.

The Citizens Service Number

The introduction of the burgerservicenummer (BSN) [Citizens Service Number] is once again a topic for discussion in the Dutch DPA annual report. Since 2004, when the first opinion on the Bill was presented, the Dutch DPA has been busy convincing the Minister and Parliament of the need to build in safeguards in some essential elements of the Act for a careful processing of citizens' personal data. After all, if something goes wrong with the information chain in back offices through the use of the BSN and its associated personal data, the oil slick effect of the dissemination of such information will often mean that the consequences for a citizen will be incalculable. The Act offers inadequate facilities for restitution in the circumstances. This is unlikely to promote the confidence that citizens should be able to have in the way in which the government deals with their personal data.

The introduction of the BSN, planned for 2006, has been postponed. The intention is that, from 2008 onwards, it will replace the present social insurance number in the healthcare sector. This 'BSN-z' will be used for patient-related communication between care providers, healthcare insurers and diagnostic bodies. It will be essential here to ensure that the recording of personal data is done with extreme care. Many general practitioners had already started to record their patients' social insurance numbers in preparation for the 'BSN-z'. Because of the errors in the numbers that the patients had provided, the Landelijke Huisartsen Vereniging [National General Practitioners' Association], at the request of the Dutch DPA, scrapped all references in its information material to the topic of asking for social insurance numbers.

The other pillar of the BSN system in health care is mandatory identification. The Dutch DPA, generally not a supporter of obligatory identification, nonetheless feels that it is very important in health care, bearing in mind the health risks that incorrect identification might involve for patients. General practitioners find it irksome to have to ask their patients for proof of identity.



The Lower House appreciates this and has adopted a motion that will relax the obligation of identification into a duty of verification in the Decree on the use of the BSN. The Dutch DPA advised the Minister not to follow this through, or at least to adopt additional measures in order to ensure that, once a patient's identification has been confirmed, this data would be available for audit in such a way that cases of mistaken identity are excluded.

The BSN will be used to facilitate the creation of the Elektronisch Patiëntendossier (EPD) [Electronic Patient File]. The Dutch DPA is actively involved in its development. The primary concerns here should be the proper regulation of accountability, access, security and supervision in relation to the file.

The public transport chip card

At the start of 2006, the Dutch DPA published the conceptual document Privacy en de OV-chipkaart [Privacy and the public transport chip card]. The Dutch DPA's objections against transport companies using travel data from named cards for service provision and direct marketing purposes resulted in the Lower House pressing the Minister to resolve the privacy problems. To deal with this issue, the Minister attempted, in consultation with the NS [the Dutch national railway system] and the Dutch DPA, to define and resolve a number of bottlenecks. During 2007, the Dutch DPA will carry out research with one of the public transport companies that has partially introduced the OV-chipkaart, to see whether and how the measures for protection of personal data are being implemented.

The digital customer file

More efficient commerce, more effective anti-fraud activities and an improvement of the provision of services to the citizen are the aims of the digital customer file as proposed in the Wet eenmalige gegevensuitvraag werk en inkomen [Act for a single data questionnaire for employment and income]. The Bill provides for a single collection of all data pertaining to a client, drawn from organisations such as social services, the CWI [Employment and Income Centre], the UWV [Employee Insurance Implementation Body], the Sociale Verzekeringsbank [National Insurance Bank], de Rijksdienst voor het Wegverkeer [National Road Transport Department] and the Informatie Beheer Groep [Information Management Group]. The digital customer file that will be prepared from this data is intended to avoid the government having to

Results for 2006

The previous annual report included an overview of the targets for 2006. Put briefly, this is how things now stand:

> European investigation into health care insurers

The European data protection authorities have carried out coordinated research into the processing of personal data by the private health care insurance sector. The results of the investigation will be published in 2007.

> Security of information at hospitals

The Dutch DPA and the Inspectie voor de Gezondheidszorg [Dutch Inspectorate for Healthcare] signed a collaborative protocol in November 2006. The purpose was to achieve effective supervision of the use of personal data in the healthcare sector including electronic patient files. Pilot studies were carried out during 2006 for a wider-ranging joint investigation in 2007 into security of information at hospitals.

> Electronic child file

The intention behind the electronic child file (the EKD) is to record a child's development from birth (or earlier) and also the child's environmental indicators. Bringing the EKD online for youth health care was postponed until 1 January 2008, and it is not expected to become compulsory by law until 2009. During 2006, the Dutch DPA again pressed for answers to the most important privacy issues involved in the EKD. It will continue its intensive tracking of developments in 2007, particularly where there is any consideration being given to possible use of the data outside the health care sector, for example in any national reference index of young people at risk that might be introduced.

> Intervention teams to combat fraud

Various government organisations collaborate within intervention teams on combating fraud in relation to social security. It can prove necessary in such situations, based on in-house observations, to collect and establish data in relation to individuals without them being aware that this is happening. The Wbp obliges organisations to inform the parties concerned about these 'secret observations', even if they do not discover any damaging material. The way that the intervention teams deal with secret observation is established in the procedural description *Heimelijke waarneming door de interventieteams* [Secret observation by intervention teams]. A revised version of this procedural description was approved by the Dutch DPA in 2006. An investigation into working methods, prepared in 2006, was recently commenced for a number of intervention teams.

> Combating fraud in social security

In order to stop abuse of public funds as far as possible, local authorities are keen to, as far as they can, verify information taken from benefit applicants against other sources of data at an early stage of their contact with the applicant. Local authorities also want to unlock and link up an increasing number of data files in their efforts to combat benefit fraud. In 2006, the Dutch DPA issued the notice entitled *Fraudebestrijding door bestandskoppeling* [Combating fraud by linking files]. This indicated the points requiring attention in order to strike a balance between combating fraud and respect for the private life of individuals.

> Binding Corporate Rules

Binding Corporate Rules are internal codes of conduct produced by multinationals, under which they can obtain a permit for passing on personal data to their associated group companies based in other countries. The first coordinated European permit procedures commenced in 2006, and the first BCR's were approved via these procedures in several countries.

> The duty to provide citizens with information

Transparency concerning the processing of personal data is one of the pillars of the Wbp. An investigation was carried out by the research bureau TNS NIPO on the instructions of the Dutch DPA at the end of 2005 in three sectors, namely general practitioners, educational institutions and housing associations, focusing on compliance with the duty to provide information under the Wbp. Research was also carried out into compliance with the duty to provide information as experienced by citizens. The research findings were published in May 2006. The recommendations from the research will result in better awareness of and better compliance with the duty to provide information.

> Internet publications and privacy

Internet users are faced with questions regarding their privacy and the use of their personal data. The Dutch DPA is continuing to work on establishing the facilities for effective supervision on the Internet. An initial version of a discussion document on this subject was debated during an internal symposium. It is expected that guidelines will be published in 2007.

> **RFID**

An external discussion document from the Dutch DPA concerning the social implications of the use of Radio Frequency Identification was published in October 2006. RFID is a technology which allows all sorts of items of property, as well as people and animals, to be equipped with information chips that can be read even at a distance. The sorts of information that can be stored on the chip, and what subsequently happens with that information, are increasingly impacting on the sphere of personal data protection. The report is now also available in an English-language version, and forms the basis for further brainstorming and consultation on this subject.

> **Biometrics in travel documents**

The Dutch DPA organised an expert meeting in 2006 on the use of biometrics in travel documents. The points that were discussed included usefulness, need and possible disadvantages of the large-scale centralised storage of biometric information. Those present at the meeting pointed out to the government the risks of 'function creep', identity fraud and inadequate security.

> **Citizens Service Number**

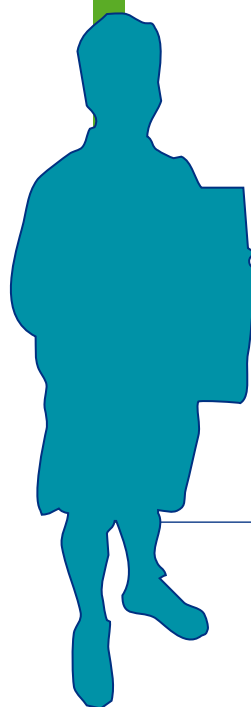
The introduction of the burgerservicenummer (BSN) [Citizens Service Number] has been postponed yet again. The Dutch DPA kept both houses of the Dutch Parliament regularly informed of its positions in relation to some thorny issues associated with this introduction. The Dutch DPA also provided advice on the introduction of the BSN in healthcare, where accurate personal data is sometimes of literally vital importance.

> **Security and privacy**

The research carried out by Prof. H.R.B.M. Kummeling and Prof. E.R. Muller, at the request of the Dutch DPA, the Minister of Justice and the Minister of Interior & Kingdom Relations, which was focussed on finding a proper balance between security and privacy, will result in publication and a congress during 2007.

> ***Wrongly delivered post***

Instead of sending it to the intended local authority, a reintegration bureau sent the progress report on one of its clients to another client. That other client submitted a written complaint to the bureau, having been faced with sensitive personal information relating to someone else. He heard no more about his complaint apart from an acknowledgement of his letter. "It seems as if they don't think this is important", was his response, "although it looks to me like a serious breach of privacy."



ask citizens more than once for information already in its possession. In the opinion it submitted to the Secretary of State for Social Affairs and Employment, the Dutch DPA emphasised the importance of adequate provision of information to the citizen, who must be able to exercise a right to inspect and correct information, as well as the need for transparency. Otherwise, the digital customer file is at risk of becoming primarily a system about instead of for the citizen.

Ten Golden Rules

Are the social services permitted to look at my bank statements and make copies of them? Can they phone up my GP to ask whether I've paid him a visit? Can they act on tips from my neighbours about me? The Dutch DPA regularly sees questions of this sort about the processing of personal data by the social services. With assistance from some employees in a range of social services, the Dutch DPA prepared a brochure in 2006 for the social services, containing answers to these questions. The Ten Golden Rules are designed primarily to provide a practical handbook to the employees who are responsible for intake and for assisting clients.

RFID

Radio Frequency Identification is a technology that can be used to implant objects with miniscule chips containing information that can be read remotely. The application of this technology can have great benefits, principally in the area of logistics, but can also be a matter of concern in society. The characteristics of RFID lend themselves to unlimited use of data in a wide range of sectors. The concern arises if, through mass application of this technology by governments and private individuals, people lose control over the data collected in relation to them and subsequently processed and stored in back offices.

RFID poses special problems for compliance with and application of the rules for processing personal data. In order to stimulate public debate on the use of RFID, the Dutch DPA issued a study in 2006 entitled *RFID. Veelbelovend of onverantwoord?* [RFID. Promising or irresponsible?]

> Mistaken identity

When a customer logs on to a website, he is surprised to find not his own details there but those of someone else: login name, date of birth, name and address, e-mail address, social insurance and bank account numbers and annual income. The customer fears that someone else can now see his information, and gets in touch with the web host. The web host checks the customer's information and can put his mind at ease to some extent: his information cannot be viewed by anyone else. An error in the system, however, has allowed him to see someone else's details on his screen. "Unacceptable", as far as the customer is concerned.



Anti-fraud measures and linking files

Not every inhabitant of one of the poorer areas is a potential terrorist, and not everyone entitled to benefit payments is a potential fraudster. Countering abuses in a business by opening up whistleblower lines or introducing black lists is a justified interest, as is the exposure of potential benefit fraud through secret surveillance. But the situation with this type of data processing is that the target interest must be weighed against the impact on the private lives of those on whom the whistle is blown or who are suspected of having acted fraudulently.

Whistleblower lines and black lists

The American Sarbanes-Oxley legislation obliges companies established in the United States to open up internal whistleblower lines throughout their subsidiary companies, with the aim of promoting commercial integrity. This obligation has no statutory basis in the Netherlands, however, even for multinational subsidiaries, that would allow them to set up this type of whistleblower scheme. The governing requirement here is that the company must observe the rules imposed by the Wbp for passing on personal data to countries outside the EU. Because the group-wide whistleblower line is usually set up to provide information to the parent company in the USA, personal data may only be passed on in the event of abuses where it is clear that the report cannot be dealt with properly at a lower level. The Article 29 Working Party has prepared guidelines on the compatibility of whistleblower schemes set up under the Sarbanes-Oxley legislation on the one hand and the EU data protection rules on the other hand. The aim of this is to offer some certainty to companies that are subject to the European data protection rules as well as the Sarbanes-Oxley legislation. Under the guidelines, a permit is required from the Minister of Justice to pass on personal data via the whistleblower line, unless the data is adequately protected in the relevant foreign country.

Another method of countering staff misconduct - ranging from pilfering the petty cash to more serious offences - is the introduction of black lists. For the retail trade sector, which suffers seriously from misconduct, a warning register has been created to store the details of perpetrators who have been charged, and who have therefore been dismissed. Employers can consult the list when recruiting staff to see whether the applicant is included on the list. In the course of 2007, the Dutch DPA will give its definite response to an investigation it has carried out into the practical operation of this type of blacklist.

There is a limit to linking of files

For combating housing fraud by individuals who are in receipt of benefit payments, local authorities can request information relating to their gas, water and electricity usage. One local authority also wanted to link information from waste treatment records with the social services records, to get some indication about the occupancy of a residence. The Dutch DPA considers this is going too far. The local authority was unable to demonstrate that this extra information was necessary, in addition to all of the information already available and the home visits. This type of file linking is also contrary to the finality principle. Citizens are obliged to hand over their household waste and the waste processing company has their information with a view to issuing invoices. The information may not be used for another purpose.

The Internet

The Internet poses a paradox. On the one hand, people are prepared to consign their most intimate information and transactions to the Internet. On the other hand, people can suffer a great deal of damage and grief as a result of their information becoming available on the net.

Objectives 2007

In 2007, the Dutch DPA will place greater emphasis on enforcement by means of investigative research and less emphasis on advising individual parties. The shift towards a greater degree of supervision is required in order to increase awareness of the importance of privacy rules and to improve compliance with them. The proposed investigations will not always be announced in advance, and not all of them are mentioned below.

These are some of the objectives we will be attempting to achieve in the coming year:

> **Publications on the Internet**

Personal information can now be published via the Internet more easily than ever, and on a wider scale. Such information also remains readily accessible to anyone for years on end. In 2007, the Dutch DPA will publish guidelines on the requirements imposed by the Wbp for this type of publication, and will also carry out some investigations.

> **The public transport chip card**

There are plans to introduce the OV-chipkaart [public transport chip card] throughout the whole of the Netherlands from 1 January 2009. The Minister of Transport, Public Works and Water Management has promised to do all that is necessary to ensure that the OV chip card system will comply with the Wbp, and is mediating in the debate between the transport companies and the Dutch DPA. The OV chip card will be introduced gradually. The Dutch DPA will accordingly carry out research on one of the systems to be introduced in 2007.

> **Introduction of electronic patient file**

The Elektronisch Patiëntendossier (EPD) [electronic patient file] is advancing steadily. Access to the data, data and system security and providing accurate information to the patient are important aspects for the patient's privacy. The Dutch DPA will therefore carry out research in one of the regions where the EPD (or elements of it) is being trialled.

> **Compliance of the Municipal Records Database**

The Gemeentelijke basisadministratie (GBA) [Municipal Records Database] is not transparent as far as most citizens are concerned, while many organisations systematically obtain details of amendments to personal data from the GBA. Research in 2005 into this provision of information to third parties from the GBA showed that those purchasing information did not use different methods

for dealing with information marked with a confidentiality indicator and information without any such indicator. The Dutch DPA will carry out investigative research in 2007. Enforcement action will also be taken against local authorities who fail to fulfil the obligation to carry out audits on the GBA.

> **Combating fraud in social security**

With fraud prevention in the area of social security, the tendency at this point is to carry out large-scale audits. One of the ways this is done is by linking as many files as possible with data concerning large numbers of citizens. While appreciating the need for fraud prevention, the Dutch DPA's principle is that not every individual entitled to benefits should be earmarked in advance as a potential fraudster, and that those citizens who are audited should also be informed of this process. The Dutch DPA will be carrying out investigative research into some of these linkages during 2007.

> **Computerised student files**

The computerisation of student files is steadily simplifying the exchange of data between the educational sector and other sectors. Student files also contain large amounts of information. It is important for parents to be properly informed about this and for schools to be aware of the rules covering the processing and/or provision of personal data. We shall be emphatically informing the educational sector about these rules during 2007.

> **Arbodienst [Occupational Health and Safety Service] and ICT**

Investigative research among occupational health and safety services will be carried out during 2007. Collaborative links between these services and insurers are usually also supported by computer (communal data banks, intensive exchange of information). The research will look into whether these relatively new technological developments meet the statutory rules for the processing of personal data.

> **Privacy rules and the police**

Within the police forces, the functionarissen voor de gegevensbescherming (FG's) [data protection officers] supervise the prudent use of personal data. Citizens can directly contact privacyfunctionarissen (PF's) [privacy officers] of the various forces with any questions, complaints or requests to find out about their information. In the interest of unambiguous and uniform processing of data by the police, the Dutch DPA will pay extra attention during 2007 to the relationship with both of these categories of officers.

> **Surveillance society**

An increasing part is being played in society by information systems that allow close following and checking of individuals, as well as systems intended specifically as instruments of supervision (including cameras linked to recognition systems, chips in smartcards, GPS, and the recording of telephone data). If a surveillance society seems unavoidable, then at the very least we have to be aware of the risks that the mass application of information technology poses. In 2007, the Dutch DPA will make sure that these developments are not lost sight of.

> **Collaboration with other supervisory authorities**

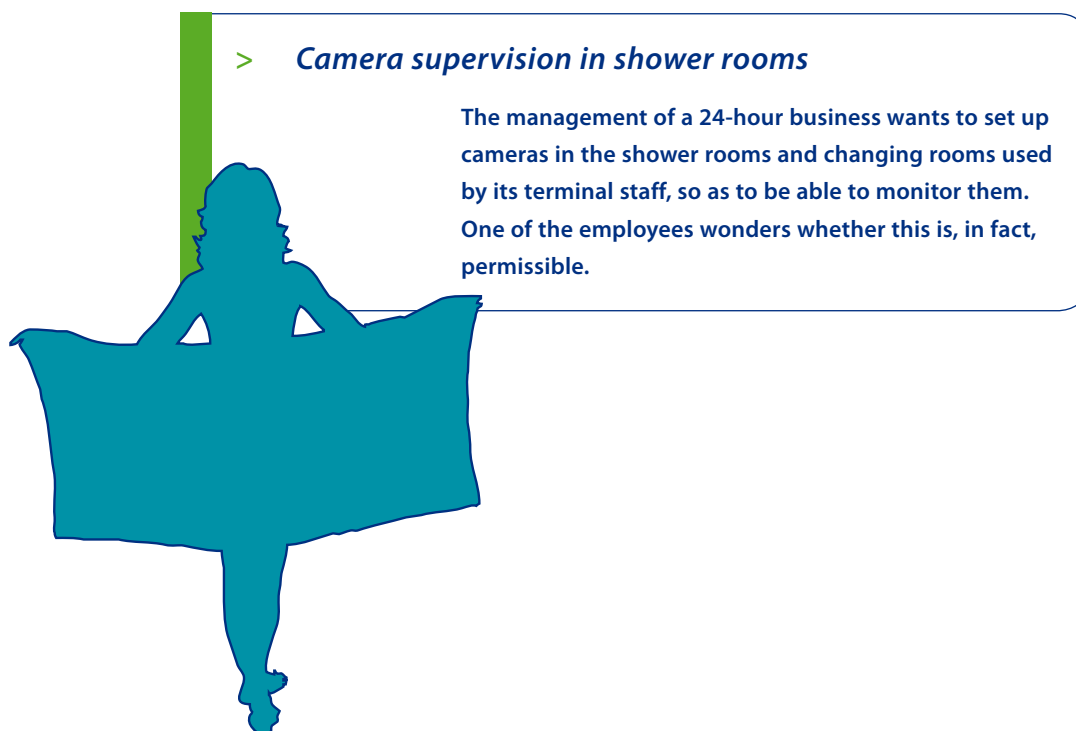
Closer collaboration will be sought with other supervisory agencies during 2007. The Dutch DPA will conclude a co-operative agreement with the Nederlandse Zorgautoriteit [Netherlands Healthcare Authority]. The joint investigation prepared in 2006 by the Inspectie Gezondheidszorg [Healthcare Inspectorate] and the Dutch DPA into the protection of information at hospitals, will be carried out during 2007 as well as an investigation, in collaboration with the Inspectie Werk en Inkomen [Inspection Work and Income], into the processing of personal data in buildings that house several businesses for public and private parties (CWI, Sociale Dienst [Social Services], UWV, reintegration agencies.).

> **Wbp case law**

A collection of opinions issued by the Dutch DPA, based on the Wbp, will be produced in 2007. This book is a sequel to the 1999 publication entitled *Persoonsgegevens beschermd* [Personal data protected], which was devoted to judgments based on the Wet persoonsregistraties (WPR) [the previous Data Protection Act]. It also includes pronouncements by dispute committees and the courts that are of major significance to the practice of the law. Collating the folder is a joint project with the Duthler advisory bureau. Two independent academic lawyers will act as editors, namely Prof. D.W.F. Verkade and Prof. H.Ph.J.A.M. Hennekens.

Publications on the Internet

The Dutch DPA commenced a project in 2005 to list the privacy problems experienced by citizens in their day-to-day lives from publications on the Internet. From the start, the issue of what should and should not be authorised as regards processing of personal data on websites was clearly very complex. The Dutch DPA set a target for itself in 2006 of developing a provisional policy that would serve as a prompt for further discussion on this topic. This policy suggestion was set out in a preliminary report presented during a symposium held to mark the occasion of J.W. Broekema leaving the Authority. The Dutch DPA will publish guidelines in 2007 for dealing with personal data in publications on Internet.



> *Camera supervision in shower rooms*

The management of a 24-hour business wants to set up cameras in the shower rooms and changing rooms used by its terminal staff, so as to be able to monitor them. One of the employees wonders whether this is, in fact, permissible.

The use of personalised services on the Internet, such as G-mail, leaves the providers of these services with ever larger 'data warehouses', containing personal information such as search instructions, the contents of e-mails or even the contents of the whole hard disk of a computer. Making this information available to third parties can cause serious problems to Internet users.

At a one-day debate on 7 December 2006, organised by the Dutch DPA and the Consumentenbond [Dutch Consumer Association], Google Europe acknowledged that IP addresses, the numbers used to identify computers, amount to personal data in many cases and are accordingly entirely subject to the statutory protection of personal data. The Dutch DPA emphasised the importance of Internet users receiving sufficient information from the service providers, that their information should not be used haphazardly in a different context, that everyone should be able to inspect and if necessary correct their own information, and that there should be a maximum time limit for storing information.

Opening up archives

Digitising and opening up existing archives - not including modern digital weblogs and suchlike - to a wider public is considered to be important, and is also promoted by the government. Because archives can contain specific personal data, it is important to set up rules of play for unlocking and digitising existing archive material, based on the requirements of the Wbp. The Dutch DPA has issued an opinion on this for the national heritage sector. Online archives containing personal data must be reported to the Dutch DPA or the data protection officer if the heritage institution has appointed this type of supervisor.

Opening up archives via the Internet merits special attention. The unusual thing about unlimited provision of information via the Internet is that personal information is made available to everyone throughout the world, without any time restriction. Those responsible do not know who will be receiving the personal information. It is doubtful whether they are acting with due care by doing this. In any case, they cannot hide behind any statutory duty, as there is no statutory obligation to publish personal information via the Internet.

Education and study

Information concerning parents and students

In March 2006, the Dutch DPA submitted its legislative opinion to the Minister of Education, Culture and Science in connection with the Ministry's new weighting scheme for elementary school budgets. Under the new budgeting system for dealing with educational disadvantages, the extra funds are allocated in principle on the basis of parental education levels. The Dutch DPA advised the Minister to use the explanatory memorandum for the Bill to devote specific attention to the interests involved in processing parental information.

In July 2006, the Dutch DPA was approached by parents who had taken their child's school brochure to mean that they were obliged to provide information on their own levels of education. There is no such obligation, however. In an independent advisory note of 20 July 2006, the Dutch DPA suggested to the Minister that he should publish information - via the Ministry's own Cfi website and also through other available channels such as school boards and directorates - to the effect that there was no such obligation incumbent on parents. The Minister informed the Dutch DPA that the suggestion would be taken on board. The text of the parental declaration has been amended to make it clear that parents are not obliged to complete these details. The text of the explanatory brochure will also be adjusted in a future edition.

Exchange of information for professions or study

The Dutch DPA considers that the Bill proposed by the government for translating the EU directive on recognising vocational qualifications into Dutch law should not be submitted in its present format. There is no doubt that the recognition procedure requires an exchange of personal information, but the Bill is so vague that it would be completely unclear to the citizen what information would be involved.

Studying abroad is becoming more and more popular. It is going to become possible to use student funding in many more countries than is presently the case. An exchange of information with the authorities in other countries is required to check on student finance arrangements. The Dutch DPA has indicated to the Secretary of State for Education, Culture and Science that there is a need to exercise caution when passing on particular information to countries outside the European Union, if such information might have unintended negative consequences for the student, such as information on cohabitation arrangements.

Summary of investigations carried out in 2006

Europol

In 2006, the Dutch DPA again took part in the annual audit of the Europol systems by the Joint Supervisory Body of Europol. These audits regularly show the great importance of the member states supplying high-quality information. In addition to the quality of information, the investigation also looked at whether the information system was operating in accordance with the Europol agreement. The audit in 2006 also investigated how far the recommendations for improving Europol's internal organisation, made in 2004 and 2005, had been implemented. The inspection showed that Europol had implemented most of the points for improvement disclosed by earlier audit investigations.

Eurodac

Eurodac is an EU-wide system for comparing fingerprints taken from foreign nationals. The database is based on a hit/no hit system: member states take fingerprints from asylum seekers and illegal immigrants found in their countries and then compare these with the data present in the system in order to establish which member state is responsible for dealing with the asylum application in accordance with the Dublin Convention. The Dutch DPA, one of whose tasks is to supervise national processing of personal data for Eurodac, carried out an investigation in 2006 at the request of the European Data Protection Authority as part of a co-ordinated audit in the various member states. An overall report on the findings, in the European context, is expected to appear during the course of 2007.

Sociale recherche [Social Security Fraud Department]

Through covert observation, the sociale recherche checks on whether individuals in receipt of benefit payments are acting fraudulently. The Dutch DPA approved the procedural description for these observations in 2003. An important element of this is that the citizens who are being checked should be made aware of the fact. Audit investigation during 2006 showed that there is room for improvement in meeting this duty of information.

Destruction of taped conversations with confidants

Investigation was carried out between June 2005 and December 2006 into compliance by the police with the rules for destruction of recorded telephone conversations with confidants such as doctors, lawyers, notaries and spiritual counsellors.

The results of this investigation prompted the Dutch DPA to follow up on the investigation. The Dutch DPA will accordingly carry out a further audit in the first half of 2007 into compliance with the duty of destruction in relation to recorded telecommunications with confidants. The results of this investigation are expected to be published in 2007.

Special Investigation Services

As part of its systematic supervision of the processing of personal data by Criminele Inlichtingen Eenheden (CIE's) [Criminal Investigation Units], the Dutch DPA completed its investigations at the CIE's of two Bijzondere Opsporingsdiensten [Special Investigation Services] in 2006. No data was found at the CIE's in question that ought not to have been processed by those CIE's. In relation to organisational and technical aspects, and just as with the earlier investigations at CIE's carried out in 2003/2004, the Dutch DPA brought some matters to the attention of the responsible Ministers that would benefit from improvement.

Private detective agencies

2006 saw the publication of the results of an investigation carried out in 2005 into compliance by private detective agencies with a number of standards under the Wbp. The main standard involved here was compliance with the obligation to provide information. It turned out that, in a large number of cases, the agencies did not know whether they had fulfilled this, having left it to their client to inform the individual under investigation and not having checked whether the client had actually done so. Virtually none of the agencies had prepared any working instructions or procedures regarding this process. The Dutch DPA considers it necessary for agencies to regulate compliance with the duty to provide information with their clients in writing.

Black lists in the retail trade

Members of staff who are charged with theft or fraud, and who are then dismissed, can have their names placed on a blacklist. Employers can consult the list in order to screen job applicants. The Dutch DPA carried out research during 2006 into the operation of this 'warning register' in the retail trade, in order to check whether the system was operating in accordance with the Wbp and the Protocol for the warning register. The results will be published in 2007.

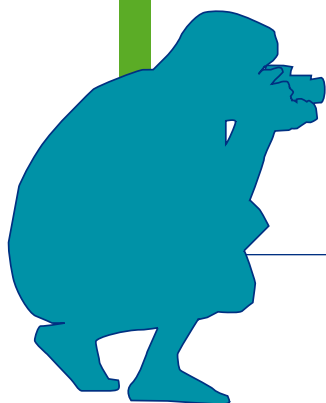
Financial service providers

The Dutch DPA considers careful processing of personal data to be of great importance in the financial sector. Compliance with the Privacygedragscode Financiële Instellingen [Privacy Code of Conduct for Financial Institutions] was investigated in 2006. The aim of the investigation was to gain some understanding of compliance with the requirements set out in the Wbp and the Code of Conduct. The results of the investigation are expected in 2007.

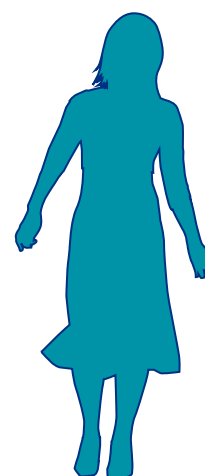
Healthcare insurers

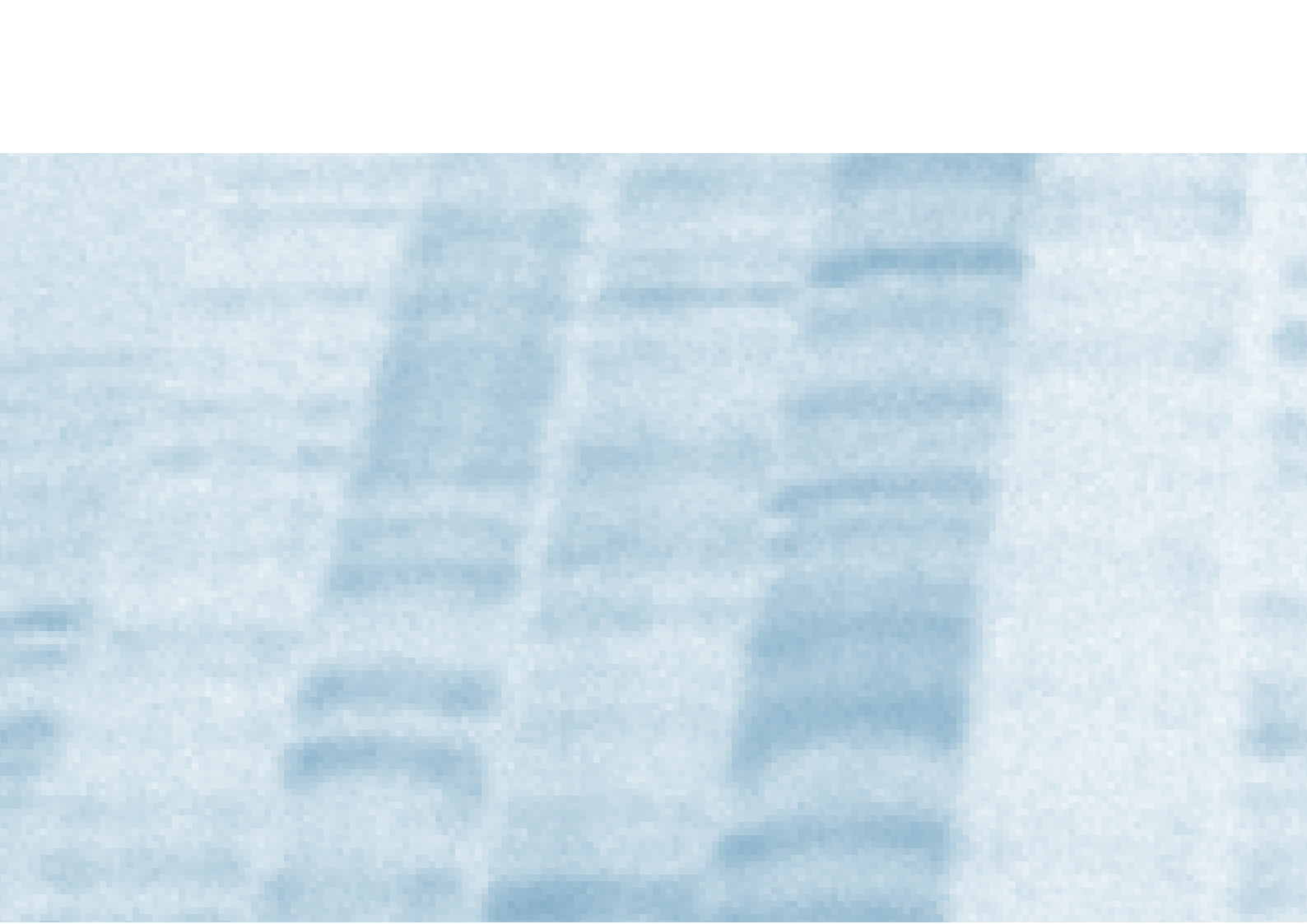
The European national supervisory authorities, in the context of their work in the EU Article 29 Working Party, resolved to carry out coordinated research into the processing of personal data in the health care insurance sector. The investigation is intended to reflect the state of affairs across Europe as regards compliance with privacy legislation in the sector. The research was carried out between April and October 2006. It is expected that results will be published in mid-2007.

> A 'rogues' gallery'



"They want to set up a 'rogues' gallery' at our company. This is because we recently had a merger and people don't know each other. They want to put our names and jobs beside the photographs. Can they just do this? Can they force me to do this? Or do you need permission from every employee?"





COLOFON

Jaarverslag 2006

© College bescherming persoonsgegevens, Den Haag, april 2007

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het College bescherming persoonsgegevens.

Dit jaarverslag is tot stand gekomen met medewerking van velen, in het bijzonder: S.M. Artz, J.H.M. Baart, F.E. van Beek, R.R.A. Beugelsdijk, E.T.H.M. Bool, V.H. Brouwer, P.G.C. Bunt, T.E. van Dijk, N. Doekharan, L. Dubbeld, M.M.M. van Eijk, A.C.J.M. Emmaneel, M.A.H. Fontein-Bijnsdorp, P.J.J. Frencken, A.C. Gräve, N.W. Groenhart, A. Haasnoot, W.J. van Helden, A.C.M. de Heij, J.W. Heuver, B.J.P. Hulsman, G.O. van de Klashorst, J. Kohnstamm, L. Kröner, P. Krul, V. Lucieer, S. Nas, J.J. Obdam, J.J. Pieterella, A. Regout, C.E. Romanesko, B. Schaafsma-Harteveld, B. Schippers, A.G.I. Terhorst, M.Twiss-van Geelen, R.J.A. Verhoeven, J.A.G. Versmissen, J. Vlug, M. Warmerdam, R.W.A. Wishaw.

Eindredactie: P.T.C. Hoefervan Dongen

Ontwerp: Proforma, ontwerpers en adviseurs (Miriam Monster, Claudy te Brake, Jonathan van Loon)

Fotografie College: Mark Kohn

Vertaling: Amstelveens Vertaalburo

Druk: Deltahage BV

Het College bescherming persoonsgegevens (CBP) houdt – onder de Wet bescherming persoonsgegevens (Wbp) – toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Bij het CBP moet het gebruik van persoonsgegevens worden gemeld, tenzij hiervoor een vrijstelling geldt.

Advies, bemiddeling, onderzoek en interventie

Het CBP adviseert de regering en organisaties over de bescherming van persoonsgegevens en onderwerpen die daarmee samenhangen. Het CBP toetst gedragscodes en bemiddelt in geschillen tussen burgers en gebruikers van persoonsgegevens. Op eigen initiatief of op verzoek van een belanghebbende kan het CBP onderzoeken of de manier waarop persoonsgegevens in een bepaalde situatie zijn gebruikt, in overeenstemming is met de wet en daaraan zonodig gevolgen verbinden. Voor in gebreke blijven bij de melding kan een boete worden opgelegd. Bij overtreding van de wet of daarop gebaseerde regelingen kan het CBP overgaan tot bestuursdwang of een dwangsom opleggen.

Over zijn werkzaamheden en bevindingen brengt het CBP jaarlijks een openbaar verslag uit. Het CBP is bij de uitvoering van zijn bevoegdheden gehouden aan de normen die worden gesteld in de Algemene wet bestuursrecht. Beslissingen van het CBP zijn vatbaar voor bezwaar en beroep. Het gedrag van het CBP kan onderzocht worden door de Nationale ombudsman.

Voor meer informatie kunt u kijken op de websites: www.cbppweb.nl of www.mijnprivacy.nl



COLLEGE BESCHERMING PERSOONSGEGEVENS

Juliana van Stolberglaan 4-10

2595 CL Den Haag

Postbus 93374

2509 AJ Den Haag

TELEFOON 070 888 85 00

FAX 070 888 85 01

E-MAIL info@cbpweb.nl

INTERNET www.cbpweb.nl