HET COLLEGE BESCHERMING PERSOONSGEGEVENS ZIET ER OP GROND
VAN DE WET BESCHERMING PERSOONSGEGEVENS ALS ONAFHANKELIJKE INSTANTIE
OP TOE DAT PERSOONSGEGEVENS ZORGVULDIG WORDEN GEBRUIKT EN BEVEILIGD
EN DAT DE PRIVACY VAN BURGERS OOK IN DE TOEKOMST GEWAARBORGD BLIJFT.

HET CBP ONDERHOUDT ACTIEF CONTACT MET ALLERLEI ORGANISATIES IN DE SAMENLEVING.
HET CBP STIMULEERT DE EIGEN VERANTWOORDELIJKHEID VAN BURGERS EN ORGANISATIES
EN ONDERSTEUNT ZELFREGULERING BINNEN DE WETTELIJKE KADERS.
ZO NODIG TREEDT HET CBP HANDHAVEND OP.

ten geleide

DNA, HET ULTIEME PERSOONSGEGEVEN, IS VERWERKT IN HET LOGO VAN HET CBP

Op 1 september 2001 is de Wet bescherming persoonsgegevens (WBP) in werking getreden en is de Wet persoonsregistraties (WPR) ingetrokken. De Registratiekamer is toen als toezichthouder opgevolgd door het College bescherming persoonsgegevens (CBP). Dit jaarverslag over 2001 staat dan ook in het teken van deze overgang.

Het CBP doet verslag van de activiteiten en bevindingen van de Registratiekamer in het laatste jaar van haar bestaan, en geeft aan wat het in de eerste maanden van zijn bestaan heeft ondernomen. Omdat de WBP en de WPR op dezelfde beginselen berusten, is er inhoudelijk sprake van een grote continuïteit. Het CBP kan zodoende voortbouwen op de bevindingen van de Registratiekamer. De samenstelling van het CBP sloot in het afgelopen jaar aan op die van de Registratiekamer. Het CBP kan daarom verantwoording afleggen over de activiteiten en bevindingen van zijn voorganger.

De invoering van de WBP heeft ook geleid tot nieuwe elementen, zowel in de rechten en plichten van belanghebbenden en gegevensverwerkende organisaties, als in de taken en bevoegdheden van de toezichthouder. De activiteiten van de Registratiekamer en het CBP in het afgelopen jaar hebben daarom mede in het teken gestaan van de nodige voorlichting en de vereiste aanpassingen in organisatie en werkwijzen. De maatschappelijke verankering van de toezichthouder is nog verder versterkt door de installatie van een Raad van Advies.

De gelegenheid is gebruikt om de inhoud en de vormgeving van het jaarverslag aan te passen. Gestreefd is naar een grotere beknoptheid en een betere toegankelijkheid, die onvermijdelijk ook gepaard gaan met grotere selectiviteit. Over tal van onderwerpen is op de website van het CBP (www.cbpweb.nl) nadere informatie beschikbaar, zo nodig met verwijzing naar andere bronnen.

Privacy is vooral een zaak van en voor mensen, in de verschillende rollen die zij dagelijks spelen. Door de grote inzet van zijn medewerkers is het CBP in staat daarbij zijn rol als toezichthouder te vervullen. Ook de betrokkenheid van vele anderen in de samenleving is weldadig en onontbeerlijk. Bijzondere vermelding verdienen hierbij de functionarissen voor de gegevensbescherming, voor wie dit verslag onder de WBP mede is bestemd.

mr. P.J. Hustinx
Voorzitter
College bescherming persoonsgegevens

HET COLLEGE VERGADERT

samenstelling

college en raad van advies

college 2001

mr. P.J. Hustinx
loorzitter van het college

mr. dr. U. van de Pol
lid van het college

drs. J.J. Borking
lid van het college

raad van advies 2001

R. Bandell
burgemeester van Dordrecht

prof. dr. T. Bemelmans
hoogleraar informatica Technische Universiteit Eindhoven

mr. G. Corstens
raadsheer Hoge Raad

prof. mr. E. Dommering
hoogleraar informatierecht Universiteit van Amsterdam

mw. mr. A. van Es
oud-lid van de Tweede Kamer

prof. mr. H. Franken
hoogleraar informaticarecht Rijksuniversiteit Leiden

prof. mr. J. Gevers
hoogleraar gezondheidsrecht Universiteit van Amsterdam

mw. mr. L. Gonçalves-Ho Kang You
collegelid OPTA, voorzitter Amnesty International

prof. mr. P. van der Heijden
hoogleraar arbeidsrecht Universiteit van Amsterdam

drs. A. Kool
oud-lid Verzekeringskamer

drs. P. van Ommeren
oud-lid Raad van Bestuur ABN-AMRO

drs. C. Rog
voorzitter commissie privacy VNO-NCW

D. Westendorp
oud-directeur Consumentenbond

2001 in vogelvlucht

De digitale revolutie beïnvloedt meer dan wat ook de manier waarop de samenleving met informatie en dus ook met persoonsgegevens omgaat. Burgers en consumenten kijken gretig uit naar de voordelen van digitale dienstverlening. Zij houden echter ook hun aarzelingen over de veiligheid en vertrouwelijkheid van de online diensten en relaties. Marktpartijen en overheden - in de vastberaden wens om commerciële of politieke doelstellingen te verwezenlijken - zien privacywaarborgen nog te vaak als obstakels. Tegelijkertijd onderschatten zij de speelruimte die gecreëerd wordt door 'privacy' van begin af mee te nemen in het ontwerp van informatiesystemen en -processen.

Privacy is een succesfactor. Of het nu gaat om het elektronische overheidsloket, controle op e-mailgebruik van werknemers, opsporingsbevoegdheden voor de politie, uitwisseling van medische gegevens voor de reïntegratie van werknemers, de doorgifte van klantgegevens naar landen buiten Europa of de verkoop van adresgegevens voor direct marketing: een rechtmatige, integere omgang met persoonsgegevens is een voorwaarde voor commercieel en bestuurlijk succes. Zonder waarborgen voor de privacy zal het nodige vertrouwen bij burger en consument ontbreken.

Het College bescherming persoonsgegevens (CBP) heeft in 2001 vanuit deze gedachte de studie *Klant te koop, privacyregels voor adressenhandel* aangeboden op de jaarlijkse Direct Marketing-dagen aan de voorzitter van de brancheorganisatie, de DMSA. Het CBP wilde hiermee een einde maken aan de onzekerheid in de branche en duidelijkheid scheppen over de mogelijkheden voor adressenhandel binnen het kader van de wet.

Ook de commerciële belangen bij een soepel én rechtmatig gegevensverkeer met landen buiten de Europese Unie zijn gebaat bij duidelijkheid over de privacyvoorwaarden die gesteld worden aan de doorgifte van persoonsgegevens. Het CBP heeft daarom in 2001 het *Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act* gepubliceerd waarin deze problematiek stapsgewijs wordt uiteengezet. Voor de verantwoordelijke bedrijven en instellingen is hiermee in principe ook de rol van het CBP in het vergunningtraject transparant geworden.

Privacy en informatie- en communicatietechnologie

Het CBP investeerde ook in 2001 in onderzoek naar de bedreigingen en kansen die informatie- en communicatietechnologie scheppen voor de bescherming van de persoonlijke levenssfeer. De Registratiekamer publiceerde *Beveiliging van persoonsgegevens*, dat een kader biedt voor de implementatie van de Wet bescherming persoonsgegevens bij informatiesystemen. In 2001 werden ook de in samenwerking met overheid en bedrijfsleven ontwikkelde privacyauditinstrumenten voor de beoordeling en controle van informatiesystemen breed gepresenteerd.

Daarbij wees het CBP nadrukkelijk op de kansen van privacy bevorderende technologie. Deze technologie voorkomt de onnodige verwerking van persoonsgegevens in informatiesystemen, een vorm van *privacy by design*. Ronduit futuristisch is op dit gebied het Europese PISA-project waaraan het CBP in 2001 deelnam. De ambitie van het project Privacy Incorporated Software Agents is het ontwikkelen van ontwerpspecificaties voor autonome software agents die de 'eigenaren' in staat zullen stellen allerlei elektronische transacties te (laten) verrichten met behoud van zeggenschap over hun persoonsgegevens.

In de nabije toekomst kan Nederland een grootschalige invoering verwachten van zogenaamde *trusted third parties* (TTP's), zowel publiek als privaat. TTP's zullen een sleutelrol spelen door het uitgeven van digitale identiteitscertificaten. De Registratiekamer bracht daarom in 2001 het rapport *Sleutels van vertrouwen* uit, de eerste uitwerking van de implicaties van de Europese privacyrichtlijn en de Nederlandse Wet bescherming persoonsgegevens voor de TTP-sector.

Elektronische overheid

De mate van zorgvuldigheid waarmee overheid en instellingen persoonsgegevens uitwisselen, heeft de Registratiekamer soms grote zorgen gebaard. Vooral waar instellingen in samenwerkingsverbanden persoonsgegevens uitwisselen, is niet altijd duidelijk wie voor welke verwerking van persoonsgegevens verantwoordelijk is of zelfs maar kan zijn. In dergelijke situaties kan efficiënter gegevensverkeer ten nadele van het individu uitpakken of ronduit in strijd zijn met de wet. Deze samenwerking en uitwisseling van gegevens tussen overheidsinstellingen zal in de nabije toekomst uitgroeien tot een vaste informatie-infrastructuur. Het CBP heeft daarom in 2001 de privacyaspecten van de overheidsplannen op het gebied van de 'elektronische overheid' onderzocht. In 2002 zal het CBP zijn visie op elektronische overheid en privacy publiceren.

Politieregisters

De registratie van burgers bij politie en justitie en de wijze waarop informatie over hen wordt vergaard, kan ingrijpende gevolgen hebben voor hun privacy. Het CBP en de Registratiekamer hebben hiervoor een bijzondere belangstelling. Vooral de registers van de Criminele Inlichtingeneenheden (CIE) vormen een grote bedreiging voor de privacy.

Verkoop van gegevens na faillissement

Bestanden met persoonsgegevens zijn geld waard. Na een faillissement wordt daarom vaak overwogen het bestand te verkopen. Dit gebeurt zowel met klantenbestanden als met kandidatenbestanden of personeelsbestanden. In 2001 speelde het geval van een bureau voor werving en selectie dat na faillissement zijn kandidatenbestand uit privacyoverwegingen grotendeels vernietigd had.

De curator stelde dat het klantenbestand een financiële waarde had en had daarom om overgave van de administratie gevraagd. De curator deed vervolgens aangifte bij de politie van het vermoedelijk plegen van bedrieglijke bankbreuk. De vraag was nu of het kandidatenbestand aan een derde verstrekt/verkocht had mogen worden. Er was geen wettelijk voorschrift om dit te doen en het zou ook niet gebeurd zijn met de toestemming van de geregistreerden. De curator zou het kandidatenbestand dus alleen aan een ander bureau hebben mogen verkopen als de verkoop zou zijn voortgevloeid uit het doel van de registratie.
Een werving- en selectiebureau heeft als doel het bemiddelen voor de kandidaten bij het vinden van geschikt werk. Dat is dus ook het doel voor het registreren van de

Resultaten 2001

IN HET VORIGE JAARVERSLAG IS AANGEKONDIGD DAT IN 2001 ZOU WORDEN GEMIKT OP DE VOLGENDE RESULTATEN:

• Voorlichtingscampagne

Rond de invoering van de Wet bescherming persoonsgegevens is in samenwerking met de ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties een voorlichtingscampagne gehouden. De Registratiekamer verzorgde de voorlichting aan koepel- en brancheorganisaties. Daarbij kon op de specifieke behoefte van elke branche worden ingespeeld.

• Internetsite & informatiemateriaal

De internetsite van het CBP (www.cbpweb.nl) is opnieuw ingericht en toegankelijker gemaakt. Verdere verbeteringen zijn in 2002 te verwachten. Het informatiemateriaal is integraal herzien en uitgebreid. Alle publicaties zijn op de website gratis beschikbaar.

• Zelfregulering

Er is een brochure uitgebracht over de mogelijkheid om een 'functionaris voor de gegevensbescherming' aan te stellen (artikel 62 e.v. WBP). Aanmeldingen voor de eerste tientallen functionarissen zijn ontvangen en verwerkt. Een toetsingskader is ontwikkeld voor organisaties die overwegen om een gedragscode te gaan opstellen (artikel 25 WBP). Een brochure daarover is in productie.

• Beveiliging & PET

Het rapport *Beveiliging van persoonsgegevens* geeft aan hoe invulling kan worden gegeven aan de verplichting om persoonsgegevens op een passende wijze te beveiligen (artikel 13 WBP). In een aparte brochure is ingegaan op de inzet van "Privacy-Enhancing Technologies' (PET). Een symposium over dit onderwerp is in voorbereiding genomen.

• Auditaanpak

Samen met koepelorganisaties en marktpartijen is een methode ontwikkeld om de kwaliteit van gegevensbescherming binnen organisaties systematisch te beoordelen. De producten van dit project *(Quickscan, WBP Zelfevaluatie en Raamwerk Privacy Audit)* zijn op de CBP-website voor ieder toegankelijk en worden in de praktijk toegepast. In een vervolgproject worden de mogelijkheden van certificering onderzocht.

• Meldingen

Tijdig vóór de invoering van de nieuwe wet is een WBP-meldingsprogramma ontwikkeld waarmee een WBP-melding kan worden opgesteld en ingezonden op een diskette. Het programma voorziet in een handreiking om te bepalen of er sprake is van een vrijstelling. De handreiking is raadpleegbaar op de CBP-website. Voor de melding zijn ook nieuwe formulieren met toelichting ontwikkeld.

persoonsgegevens van de kandidaten. Het doel van de registratie moet dus in de omstandigheden van het faillissement met zich meebrengen dat de gegevens worden doorverkocht.
Aannemelijk was echter wel dat de behoefte tot bemiddeling bij de ingeschrevenen ook na de faillietverklaring van het bureau nog bestond. Hoewel het doel van de registratie niet de verstrekking aan een nieuw bureau was, kan een dergelijke verstrekking daarom wel voortvloeien uit het oorspronkelijke doel. Dit betekent dat de verkoop van het kandidatenbestand aan een nieuw bureau rechtmatig had kunnen zijn.
Voor de beoordeling van de rechtmatigheid van de verkoop speelt echter ook een grote rol of de privacybelangen van de geregistreerden voldoende in acht zouden zijn genomen. Een voorwaarde is dat de kandidaten goed geïnformeerd zouden worden over de op handen zijnde verkoop en de mogelijkheid zouden krijgen hier bezwaar tegen te maken. Ook de aard van de gegevens en mogelijke gevolgen voor de betrokkenen kan er nog toe doen ●

• Handhaving

De werkprocessen voor het opleggen van bestuurlijke boete of last onder dwangsom, dan wel het toepassen van bestuursdwang, zijn in concept ontwikkeld en worden inmiddels ingevoerd. De uitgangspunten en beleidsregels voor het gebruik van deze bevoegdheden zullen in de loop van 2002 worden gepubliceerd.

• Werkprocessen

De werkwijzen en procedures voor de uitoefening van de overige taken en bevoegdheden zijn ontwikkeld en worden in fasen ingevoerd. De uitgangspunten en beleidsregels voor deze taken en bevoegdheden zullen in de loop van 2002 worden gepubliceerd.

• Derde landen

Een beleidsnota over gegevensverkeer met derde landen (artikel 76-77 WBP) staat op de CBP-website. Een brochure en informatieblad over hetzelfde onderwerp zijn daar ook beschikbaar. Gedrukte versies in het Nederlands en het Engels zijn in voorbereiding.

• Bestuur en organisatie

Een bestuursreglement is ontwikkeld en inmiddels goedgekeurd door de Minister van Justitie. Ook is een organisatie- en formatieplan vastgesteld, dat de basis vormt voor de invoering van competentiemanagement.

Het toezicht op en de kwaliteit van de registratie bleek in 2001 echter nog steeds beneden de maat. Wel constateerde het CBP zo langzamerhand een serieuze bereidheid bij politie en justitie om hier verbetering in te brengen. Inmiddels is in 2002 een circulaire van de minister van Binnenlandse Zaken en Koninkrijksrelaties in werking getreden waarin toezicht door middel van (externe) audits wordt voorgeschreven.

Opsporingsbevoegdheden

Bedrijven en instellingen kregen allerlei verzoeken en vorderingen van politie en justitie om inzage en afgifte van persoonsgegevens (van bijvoorbeeld klanten) uit computerbestanden. Deze vorderingen waren echter veelal onrechtmatig. Bedrijven kwamen hierdoor in een lastige positie. Naar aanleiding van de klachten heeft de Registratiekamer de minister van Justitie schriftelijk om een standpunt in deze kwestie verzocht. Inmiddels heeft de minister zich uitgesproken tegen een dergelijke wijze van informatie-inwinning.

De Commissie Strafvorderlijke gegevensverga-ring (Commissie Mevis) heeft in 2001 de kwestie van de politiebevoegdheden onderzocht. Zij stelde voor politie en justitie vergaande bevoegdheden te geven tot het vorderen van inlichtingen bij bedrijven en overheidsinstellingen. Het CBP daarentegen achtte een duidelijke wettelijke regeling nodig die alle belanghebbenden meer rechtszekerheid biedt. Een bedrijf of overheidsinstelling is geen verlengstuk van justitie of politie voor de opsporing.

De opsporingsinstanties zullen zorgvuldiger met informatie om moeten gaan. Volgens de voorstellen zal voortaan van grote groepen onverdachte personen informatie beschikbaar komen: een uitbreiding van bevoegdheden terwijl de huidige spelregels in de praktijk al niet voldoende bleken te worden nageleefd.

Vertrouwelijke communicatie

In het Wetsvoorstel vorderen gegevens telecommunicatie werd aan de gegevens over het telecommunicatieverkeer zelf categorisch de bijzondere bescherming van het grondrecht op vertrouwelijke communicatie onthouden. Het CBP meende en meent dat grote terughoudendheid geboden is bij het verplichten van de telecommunicatiesector tot het bewaren van gegevens in het algemeen. Het kabinetsvoorstel voor een nieuw artikel 13 Grondwet op basis van het eindrapport van de Commissie Grondrechten in het digitale tijdperk,

schoot echter in hoge mate te kort. Het grondrecht dient niet beperkt te worden tot de inhoud van het berichtenverkeer, maar moet zich ook uitstrekken tot de gegevens over het telecommunicatieverkeer zelf, de verkeersgegevens.

Controle van de werknemer

De werknemer ziet zijn werkplek meer en meer geautomatiseerd. Dat betekent ook dat hij wordt omringd door systemen die geschikt zijn als personeelsvolgsysteem: het digitale toegangspasje, de beveiligingscamera, GSM, RSI-programma's en andere software. De controle op het gebruik van e-mail en internet stond in 2001 maatschappelijk volop in de belangstelling. Het CBP heeft daarbij steeds duidelijk gemaakt dat de regelingen voor de controle op het werk maatwerk dienden te zijn en in bedrijven zelf tot stand dienden te komen. Het CBP heeft daarvoor ook hulpmiddelen aangeboden, die in 2002 opnieuw zullen worden uitgebracht; verder stelt het CBP zich hier op in tweede lijn.

De zieke werknemer

Het CBP heeft in 2001 de regelgeving rond de sociale zekerheid en met name de reïntegratie van de zieke werknemer met argusogen gevolgd. Sinds 1 januari 2002 hebben de eerste wijzigingen van de uitvoeringsstructuur hun beslag gekregen door de inwerkingtreding van de Wet SUWI (Structuur Uitvoering Werk en Inkomen). Het CBP adviseerde te zorgen voor grote transparantie en helderheid van de gegevensstromen. Het moet voor alle betrokken personen, instellingen en bedrijven duidelijk zijn welke informatie, tussen welke partijen voor welke doeleinden mag worden uitgewisseld. Dit kan worden bereikt door duidelijke regelgeving waarin met name de doelen van verstrekking afdoende gespecificeerd worden.

Het proces van reïntegratie bij arbeidsongeschiktheid wordt steeds vaker uitbesteed aan particuliere bedrijven. In verscheidene wetgevingsadviezen heeft het CBP de noodzaak benadrukt van specifieke regelgeving – bij voorkeur vastgelegd in wetgeving - voor de gegevensuitwisseling bij reïntegratie. De te reïntegreren werknemer verkeert in een kwetsbare positie en het gaat om medische gegevens. De evidente spanning tussen privacybelang en de belangen gemoeid met reïntegratie vragen om een oplossing voor de uitvoeringspraktijk. Hierin is nog niet voorzien.

Zorgtoewijzing

Toepassing van informatie- en communicatietechnologie is ook in de gezondheidszorg een trend naast de toename van regionale en landelijke elektronische registraties en van marktwerking. Wachtlijsten en zorgtoewijzing beheersten verder de discussie in de wereld van de gezondheidszorg. De gegevensverzameling en -verstrekking die daarbij een rol spelen, zijn buitengewoon privacygevoelig. In veel situaties bleek ook het medisch beroepsgeheim in het geding. De privacyrechten van patiënten dienen evenwel structureel beschermd te blijven. Het gezondheidsbelang van de patiënt laat deze anders geen ruimte om ook zijn privacybelang te laten gelden in een complexe, snel digitaliserende sector, die op zoek is naar efficiëntie en waar ook grote financiële belangen mee gemoeid zijn.

Doelen 2002

IN 2002 ZULLEN MET NAME DE VOLGENDE RESULTATEN WORDEN NAGESTREEFD:

- **Elektronische overheid**

De inzet van ICT kan de overheid toegankelijker, effectiever en klantgerichter maken, en de administratieve lasten voor bedrijven en instellingen terugdringen. Het CBP zal een visie publiceren op de privacyaspecten van deze ontwikkeling die kan bijdragen aan het vinden van kansrijke oplossingen en mogelijkheden tot verbetering.

- **Informatietechnologie in de zorg**

Ook in de gezondheidszorg zijn veranderingen gaande die ingrijpende gevolgen kunnen hebben voor de bescherming van de persoonlijke levenssfeer. Het CBP zal bijdragen aan een evenwichtige ontwikkeling op dit gebied door een publikatie over ICT in de zorg.

- **Onderzoek en statistiek**

Toenemende belangstelling voor resultaten en effecten leidt tot een grotere behoefte aan wetenschappelijk onderzoek en statistiek. Het CBP zal een kaderdocument uitbrengen waarin de wettelijke regels voor het gebruik van persoonsgegevens op dit gebied zullen worden verhelderd.

Digitale beelden van de openbare omgeving

Een bedrijf maakt op allerlei plaatsen in Nederland digitale opnamen van de openbare ruimte. De digitale opnamen geven een 360°-beeld van een bepaalde locatie. Een bepaald gebouw op die locatie kan dus ook op afstand bekeken worden. Daarvoor koppelt het bedrijf de digitale beelden aan andere gegevens: gemeente, plaats, straat, huisnummer en kadastrale coördinaten. De beelden geven van het gebouw een buitenaanzicht, met algemene informatie over de aard van het object en het gebruik daarvan.

Klanten van het bedrijf zijn onder andere woningcorporaties, nutsbedrijven, en gemeentelijke en provinciale overheden. Het is de bedoeling uiteindelijk te komen tot een optische basisregistratie van Nederland, die periodiek zal worden geactualiseerd en de bron vormt voor uiteenlopende toepassingen. Een aantal gemeenten heeft inmiddels met steun van het bedrijf een eigen optische basisregistratie aangelegd. Een prachtig systeem dat echter ook gebruikt wordt voor toepassingen waarvan eigenaren of bewoners directe gevolgen kunnen ondervinden.
Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon, moeten als persoonsgegevens worden beschouwd. Ook gegevens over objecten zijn soms persoonsgegevens. Dit is het geval als deze gegevens invloed kunnen hebben op de manier waarop een bepaalde persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. De Registratiekamer wees in 2001 het bedrijf op de privacy-aspecten van de ondernemingsactiviteit.
De eigenaren en bewoners van de betrokken panden kunnen in de regel zonder onevenredige moeite worden geïdentificeerd. Toepassingen waarbij digitale beelden worden gebruikt voor de beoordeling van individuele objecten en waarbij de betrokken eigenaren of bewoners directe gevolgen van deze beoordeling ondervinden (zoals bij taxatie en belastingen), zullen dan ook leiden tot het 'verwerken van persoonsgegevens'. Zowel de klanten als het bedrijf zelf zullen voor verschillende punten als 'verantwoordelijke voor de verwerking' van persoonsgegevens moeten worden aangemerkt. Het maken en mede met het oog op dergelijke toepassingen beschikbaar houden van digitale rondkijkbeelden, zal kunnen worden beschouwd als het 'verzamelen' van persoonsgegevens. De digitale beelden dragen immers vanaf het begin de mogelijkheid van een dergelijk gebruik in zich, terwijl de activiteiten van het bedrijf er uitdrukkelijk mede op gericht zijn te bevorderen dat een dergelijk gebruik plaatsvindt. Digitale 'rondkijkbeelden' van openbare ruimten en andere geo-informatie vallen dus voor een deel onder de privacywetgeving ●

- **Werknemers**

De privacy van werknemers is aan de orde bij een nieuwe versie van het rapport over controle op het gebruik van e-mail en internet op het werk, en van de privacychecklist voor ondernemingsraden. Ook zal de basis worden gelegd voor een publicatie over de positie van zieke werknemers.

- **Handelsinformatie**

Uit onderzoek is gebleken dat behoefte bestaat aan duidelijkheid over de verwerking van persoonsgegevens door handelsinformatiebureaus. Het CBP zal bevorderen dat binnen deze branche duidelijke normen voor een rechtmatige verwerking van persoonsgegevens worden vastgelegd.

- **Gebruik van telecommunicatie**

Het CBP zal een verkennend onderzoek doen naar de verwerking van persoonsgegevens over het gebruik van telecommunicatie. In eerste instantie gaat het daarbij vooral om afwikkeling van kosten ('billing'). De resultaten zullen aan de orde worden gesteld in een workshop met deskundigen en vertegenwoordigers van de sector.

- **Bijzondere politieregisters**

Het beheer van de politieregisters met 'criminele inlichtingen' behoeft verbeteringen waarbij zowel de privacybescherming als de opsporing van strafbare feiten zijn gebaat. Naast een versterking van het structurele toezicht op deze registers streeft het CBP naar een stroomlijning van de behandeling van verzoeken om inzage.

- **Openbaar register van WBP-meldingen**

Op de CBP-website zal een openbaar register van ontvangen meldingen voor iedereen toegankelijk worden. Naast een verbeterde versie van het WBP-meldingenprogramma op diskette zal ook de mogelijkheid worden geboden van een rechtstreekse aanmelding via internet.

- **Voorafgaand onderzoek**

De ervaringen die worden opgedaan bij het voorafgaand onderzoek naar verwerkingen met bijzondere risico's (artikelen 31-32 WBP) zullen op de CBP-website bekend worden gemaakt. Voor categorieën van veel voorkomende verwerkingen zullen, in overleg met direct belanghebbenden, waar mogelijk standaarden worden ontwikkeld.

- **Handhavingsplan**

Het CBP zal de voorwaarden ontwikkelen voor een systematische controle op de naleving van de meldingsplicht. Deze zullen samen met verschillende andere activiteiten op het terrein van toezicht, onderzoek en interventie worden vastgelegd in een handhavingsplan.

Met het College bescherming persoonsgegevens is in 2001 een toezichthouder in het leven geroepen met nieuwe bevoegdheden op basis van een nieuwe wet. Daarom zal in dit hoofdstuk de nadruk vallen op de strategische visie en het meerjarenperspectief. De uitwerking van het beleid op het niveau van de taken en bevoegdheden zal in volgende jaarverslagen aan de orde komen.

Beleid van de toezichthouder

PUBLIEK IN DE HAL VAN ONS PARLEMENTSGEBOUW

Taken en bevoegdheden

Het CBP is op grond van artikel 51, eerste lid, van de WBP ingesteld om toezicht te houden op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Het kader voor de uitvoering van deze taak is in de WBP en daarmee samenhangende andere wetgeving vastgelegd.

De wetgever heeft hiermee uitvoering gegeven aan artikel 28 van Richtlijn 95/46/EG waarin het bestaan van een dergelijke toezichthoudende autoriteit uitdrukkelijk is voorzien, en waarin voorts is bepaald dat deze autoriteit zijn taak in volledige onafhankelijkheid dient te vervullen.

Het CBP vervult voorts een aantal andere taken die hem bij wet of ingevolge verdrag zijn opgedragen. Een deel daarvan vloeit ook rechtstreeks voort uit de richtlijn. Op grond van artikel 51, tweede lid, van de 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. Ook is het CBP op grond van artikel 25 WBP belast met de toetsing van gedragscodes die uitvoering geven aan de wetgeving op dit gebied.

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 of over de uitoefening van het recht op verzet. Voorts kan het CBP op grond van artikel 60 WBP, al dan niet 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.

Tot de internationale taken van het CBP behoort de deelname aan de Werkgroep van toezichthouders als bedoeld in artikel 29 van Richtlijn 95/46/EG en het lidmaatschap van de Gemeenschappelijke Controle Autoriteiten voor Schengen en Europol.

Daarnaast heeft de WBP nieuwe taken aan het CBP opgedragen, met name in de sfeer van toezicht en handhaving. In een aantal gevallen is het CBP bijvoorbeeld belast met een voorafgaand onderzoek naar de rechtmatigheid van verwerkingen of het nemen van besluiten over de verwerking van bijzondere gegevens (artikelen 23 en 31 WBP). Ook kan het CBP bestuurlijke boeten opleggen en besluiten tot het opleggen van dwangsommen en het toepassen van bestuursdwang (artikel 65 e.v. WBP). Met het oog daarop zijn de waarborgen voor een juiste taakvervulling in de wet aangescherpt.

Zo is voorzien in de mogelijkheid van bezwaar en beroep op de bestuursrechter tegen besluiten van het CBP en van een klacht bij de Nationale ombudsman. Ook de Wet openbaarheid van bestuur is van toepassing. Tenslotte is het CBP ingevolge artikel 56, derde lid, van de WBP verplicht tot vaststelling van een bestuursreglement dat onder meer regels dient te bevatten over werkwijzen en procedures met het oog op een goede en zorgvuldige uitoefening van de verschillende taken. Het CBP is als bestuursorgaan uiteraard ook gebonden aan de algemene beginselen van behoorlijk bestuur.

Bij deze taken gaat het soms om verplichtingen, maar in de regel om bevoegdheden over de uitoefening waarvan het CBP, met inachtneming van de wet en het oordeel van de rechter, zelf kan beslissen. Andere taken, zoals het geven van voorlichting en het doen van onderzoek naar nieuwe ontwikkelingen, vloeien voort uit de algemene toezichthoudende taak. Mede gelet op zijn onafhankelijkheid heeft het CBP dus een betrekkelijk grote ruimte om binnen de kaders van de wet zelf invulling te geven aan zijn taak en daarbij de nodige prioriteiten te stellen en accenten te leggen.

Medische dossiers op internet

Het idee om medische dossiers toegankelijk te maken via het internet wordt door verschillende partijen onderzocht en getest.

Het internetbedrijf Medlook biedt patiënten de mogelijkheid zelf hun dossier via de website van Medlook on line te brengen, overal en altijd te raadplegen. Ook kunnen zij hun gegevens on line laten controleren en bevestigen door hun hulpverleners. Het bedrijf beheert de wachtwoorden van de patiënten en zorgverleners. Op verzoek van de Landelijke Huisartsenvereniging heeft de Registratiekamer onderzocht of Medlook hierbij in overeenstemming handelt met de Wet bescherming persoonsgegevens.
De wet schrijft een adequate beveiliging van persoonsgegevens voor. De verwerking van medische gegevens via internet brengt echter risico's met zich mee. Hiervoor zijn in de eerste plaats Medlook, maar ook de patiënt zelf en de hosting-aanbieder verantwoordelijk. De toegang tot een dossier is beveiligd met een loginnaam en een wachtwoord. Dat vormt een zwakke schakel in de beveiliging. De beveiliging klemt des te meer omdat de opgeslagen patiëntengegevens gecombineerd met het gebruik ervan door anderen het direct dan wel indirect mogelijk maken om de patiënt te identificeren. Bij de huidige stand van de techniek en gezien de beveiligingsmaatregelen die Medlook heeft gekozen, kan in redelijkheid echter niet meer van het bedrijf worden gevergd.Wel was het zo dat de voorlichting aan de patiënt onvoldoende was. Ten onrechte maakte Medlook op zijn algemene site geen melding van de risico's die aan internetgebruik zijn verbonden.
De wet vraagt ook om waarborgen voor de kwaliteit van de gegevens. Hoewel Medlook maatregelen heeft genomen om vast te stellen welke gegevens door de patiënt in het dossier zijn gezet en welke door artsen en apothekers zijn geaccordeerd, kunnen de volledigheid en juistheid van de gegevens in een dossier niet worden gegarandeerd. Volgens de Registratiekamer moet zorgverleners daarom worden afgeraden uitsluitend op basis van gegevens in het dossier ingrijpende beslissingen ten aanzien van de patiënt te nemen ●

Positionering

Als toezichthouder in het publieke domein speelt het CBP verschillende rollen: van voorlichter, adviseur, onderzoeker en beoordelaar tot sanctieoplegger. Steeds dient daarbij de positie van het CBP als onafhankelijk toezichthouder verzekerd te zijn, waarbij een juiste afbakening van de verschillende rollen en een functiescheiding voor de handhavingstaken noodzakelijk zijn. De uitbreiding van de bevoegdheden van het CBP ten opzichte van die van de Registratiekamer noopt tot een heldere en transparante visie op deze herpositionering.

Tegen deze achtergrond heeft het CBP zich beraden over de strategische keuzen voor de komende jaren. Daarbij was een centrale vraag op welke wijze het meest effectief invulling zou kunnen worden gegeven aan zijn verschillende taken ten dienste van de bescherming van de persoonlijke levenssfeer. Dit heeft geleid tot de volgende keuzen en aandachtspunten.

Langs vier sporen in actie

Om haar taak als toezichthouder effectief te vervullen heeft de Registratiekamer er voor gekozen de bescherming van persoonsgegevens langs vier nauw met elkaar samenhangende sporen te bevorderen: bewustwording, normontwikkeling, technologie en handhaving.

- Door voorlichting en verschillende vormen van communicatie met uiteenlopende doelgroepen probeerde zij het privacybewustzijn te versterken en de normen onder de aandacht te brengen.
- In achtergrondstudies en verkenningen, maar ook in de adviezen die zij uitbracht, werden nieuwe normen voor gegevensbescherming ontwikkeld en de bestaande wettelijke normen verder geïnterpreteerd en uitgewerkt. In dit kader stimuleerde zij ook zelfregulering door branches en sectoren.
- Door onderzoek te doen naar ontwikkelingen en toepassingen van ICT probeerde zij de kritieke momenten in beeld te brengen en aan te geven hoe de normen van gegevensbescherming in de techniek een vertaling zouden kunnen vinden.
- Het sluitstuk was de doorwerking van de privacybescherming in de praktijk. Door privacyaudits en andere vormen van handhaving werd deze doorwerking bevorderd.

Het CBP onderschrijft de samenhangende en geïntegreerde benadering van bewustwording, normontwikkeling, technologie en handhaving in het kader van dit viersporenbeleid, en ziet daarin ook een solide basis voor de onderbouwing van de eerder bedoelde rollen. Het CBP streeft ernaar om de mogelijkheden van dit beleid uit te bouwen en door een stelselmatige aanpak te benutten.

De bedoelde sporen vormen niet alleen een logisch vervolg op elkaar, maar vormen ook een continu proces, waarin opgedane ervaringen bij de toepassing weer kunnen leiden tot verdere bewustwording en doorwerking van de privacybescherming in alle lagen van de betrokken organisaties. Waar dat nodig is zal het CBP gebruik maken van zijn aangescherpte handhavingsbevoegdheden.

Het CBP zal zich steeds bewust zijn van de consequenties van een bepaalde aanpak en rolopvatting. Een zorgvuldig en toetsbaar optreden, ingebed in beleidsregels, moet de taakvervulling van het CBP kenmerken. Een adequate mix van aandacht voor de verschillende sporen, verdeeld over de verschillende aandachtsgebieden, wordt jaarlijks vastgelegd in het plan van activiteiten dat onderdeel uitmaakt van het beleidsplan. Dit beleidsplan wordt door het CBP vastgesteld met inachtneming van de opmerkingen van de Raad van Advies.

Versterking van de tweedelijnspositie

De WBP gaat uit van de eigen verantwoordelijkheid van overheid en bedrijfsleven voor een adequate privacybescherming en geeft de maatstaven daarvoor aan in een stelsel van rechten en verplichtingen. Een ander uitgangspunt is dat de burger primair voor zijn eigen rechten moet opkomen.

Deze eigen verantwoordelijkheid aan beide kanten zal door het CBP worden gevoed door voorlichting, normontwikkeling en stimulering van 'privacyvriendelijke' technologie. Daarbij past het bevorderen van zelfregulering via gedragscodes en de aanstelling van functionarissen voor de gegevensbescherming, die in de WBP een prominente plaats hebben gekregen. Via het project Auditaanpak zijn de instrumenten ontwikkeld waarmee organisaties zelf een 'privacykwaliteitsbeleid' kunnen implementeren. Het gebruik van de bevoegdheden tot handhaving via bestuursdwang en dwangsommen komt in

Een rekening voor psychotherapie

Bij langdurig ziekteverzuim van werknemers wordt steeds vaker een reïntegratiebedrijf ingeschakeld. Reïntegratiebedrijven gebruiken dan ook medische gegevens van de werknemer en in het reïntegratieproces ontstaat ook weer informatie over de betrokkene die sterk privacygevoelig is. Zorgvuldigheid is dus geboden en hoe meer partijen betrokken zijn bij het proces, des te gemakkelijker kan het fout gaan.

Wim van Vloot – de naam is gefingeerd - meldde zich ziek met burn-outverschijnselen. De Arbo-dienst verwees hem naar een reïntegratiebedrijf en adviseerde behandeling door een psychotherapeut. In dergelijke gevallen verdeelt het reïntegratiebedrijf de kosten tussen (de zorgverzekeraar van) de werknemer en de werkgever. Voor de betaling van zijn deel kreeg de werkgever de rekening toegestuurd door de psychotherapeut. Tot Van Vloots onaangename verrassing informeerde zijn werkgever tijdens een ontmoeting naar de voortgang van de therapie.

Van Vloot voelde zich hierdoor ernstig aangetast in zijn privacy en wilde graag het oordeel van het CBP over deze gang van zaken. Wat had zijn werkgever te maken met zijn therapie? Het reïntegratiebedrijf meende dat de werkgever geïnformeerd mag worden zodat deze een goede financiële afweging zou kunnen maken. De werkgever zou doordat hij meebetaalde, toch te weten komen waar het geld aan werd besteed.

Het CBP vond de gang van zaken wat smoezelig. De werknemer was vooraf niet geïnformeerd over wat er met zijn persoonsgegevens zou gebeuren. Er waren ook oplossingen denkbaar waardoor de werkgever de rekening niet onder ogen hoefde te krijgen, bijvoorbeeld wanneer het reïntegratiebedrijf de rekening krijgt en vervolgens het bedrag declareert bij de werkgever. Het CBP adviseerde om de procedures voor de verstrekking van persoonsgegevens beter te regelen ●

deze benadering pas aan de orde indien andere middelen falen of ongeschikt blijken.

Het CBP streeft ernaar om bij de toepassing van het 'viersporenbeleid' waar mogelijk een tweedelijnspositie te betrekken. Wat geldt voor het beleid van de toezichthouder geldt immers tot zekere hoogte ook voor andere 'stakeholders' en uiteindelijk voor elke organisatie die tot de conclusie komt dat een adequate aanpak van de privacybescherming een kritische succesfactor vormt voor het realiseren van zijn doelstellingen. Ook in deze organisaties zullen voorlichting, bewustwording en normontwikkeling moeten leiden tot een verbeterde inrichting van systemen en daarop aansluitende processen en technieken die 'compliance' kunnen bevorderen.

Het CBP beoogt een ontwikkeling in gang te zetten en/of uit te bouwen waarbij degenen die verantwoordelijk zijn voor het verwerken van persoonsgegevens, de bescherming van de persoonlijke levenssfeer als een vanzelfsprekendheid ervaren en dit weten te vertalen in hun werkzaamheden. Dit streven beperkt zich niet tot het uitvoeringsniveau, maar richt zich ook op beleidsmakers en wetgever. Deze taakopvatting realiseert het CBP langs twee lijnen: door een adequate behandeling van de dagelijkse stroom zaken, en door het op de maatschappelijke agenda plaatsen van relevante onderwerpen.

Een en ander betekent dat het CBP gaandeweg vooral die activiteiten kan overlaten aan andere spelers waar de toezichthouder zelf niet in de eerste linie behoeft te opereren. Dat neemt niet weg dat het CBP wel vanuit een tweedelijnspositie andere 'stakeholders' kan ondersteunen en al dan niet met daarvoor in aanmerking komende partners, activiteiten kan ondernemen die ten goede komen aan de samenleving als geheel. Het CBP zal zich echter vooral richten op die onderdelen van zijn taak waarvoor specifieke ervaring of bevoegdheden noodzakelijk zijn.

Toenemende aandacht voor handhaving

Tegen deze achtergrond valt te verwachten dat zich tussen de genoemde sporen in de loop van de tijd een verschuiving zal voordoen in de richting van een toenemende aandacht van het CBP voor actief optreden in de sfeer van toezicht en handhaving. De hiervoor geschetste strategie betekent een geleidelijke accentverschuiving naar het spoor van de handhaving en een sterkere tweedelijnspositie voor het CBP, die samen leiden tot een 'olievlekwerking' of 'vliegwieleffect'. Doordat meer organisaties zich verantwoordelijk gaan voelen voor de privacybescherming, zal de totale aandacht daarvoor toenemen en kan de toezichthouder zich richten op die onderdelen van zijn taak die het meest op zijn weg liggen.

De notariszaak of het OM buiten z'n boekje

Strafrechtelijke gegevens kunnen van grote invloed zijn op de manier waarop mensen in de maatschappij behandeld of beoordeeld worden. Daarom rekent de Wet bescherming persoonsgegevens deze tot de bijzondere gegevens, gegevens die in principe niet gebruikt mogen worden buiten de sfeer waar ze thuis horen. Als strafrechtelijke gegevens toch verstrekt worden dan moet daar wel een heel goede reden voor zijn en moet het zeer zorgvuldig gebeuren. Het gebruik van de gegevensverzamelingen van politie en justitie is dan ook aan allerlei regels gebonden.

In 2001 verstrekte het Openbaar Ministerie (OM) gegevens over een notaris aan de Kamer van Toezicht over (kandidaat)notarissen (KvT). Dit gebeurde omdat het OM een tuchtrechtelijk onderzoek door deze Kamer van Toezicht wilde bevorderen. Het OM heeft de gegevens verstrekt uit het eigen registratiesysteem COMPAS. Het COMPAS-reglement – sinds september 2001 overigens vervangen door de Aanwijzing Wet bescherming persoonsgegevens – voorziet in dit soort gevallen. Iets preciezer gezegd, het voorziet in verstrekkingen aan derden voor buiten de strafrechtspleging gelegen doeleinden.

Op verzoek van de advocaat van de notaris heeft de Registratiekamer een onderzoek ingesteld naar de rechtmatigheid van deze concrete verstrekking. De eerste vraag die dan beantwoord moet worden is of het doorgeven van de gegevens wel klopt met het doel van het registratiesysteem. Dat is alleen het geval als het doorgeven van de gegevens nodig is voor een goede uitoefening van de taak van het OM en als de belangen van de geregistreerde daarbij voldoende in acht zijn genomen.

Uit de stukken bleek niet dat het OM met het privacybelang van de notaris rekening had gehouden. Alles was achter zijn rug om gebeurd, of om het nauwkeuriger te zeggen: uit niets bleek dat klager gehoord was over de voor-

Deze verschuiving zal naar verwachting – ook bij een selectief gebruik van bevoegdheden – gepaard gaan met een structurele taakverzwaring van het CBP door een toename van het aantal zaken en de complexiteit daarvan. Handhavingsonderzoeken leggen ook nu al een zwaar beslag op de beschikbare capaciteit. Bedrijven en organisaties zullen naar verwachting in veel gevallen gebruik maken van de verhoogde rechtsbescherming via bezwaar en beroep op de rechter.

Wil deze strategie slagen, dan moet een aantal voorwaarden zijn vervuld. Daartoe behoort een verdere professionalisering van organisatie en werkmethoden. Voor het realiseren van de beoogde strategie zal ook een kwantitatieve én kwalitatieve uitbreiding van de organisatie onontbeerlijk zijn. Ook zal een herstructurering van de organisatie op niet al te lange termijn aan de orde moeten komen. Dit onder meer om optimaal invulling te kunnen geven aan de handhavingstaken. Hiervoor is de aandacht gevraagd van de minister van Justitie. Daarnaast zal een geslaagde ontwikkeling in de richting van een 'tweedelijnspositie' er toe leiden, dat het CBP zich steeds meer op andersoortige, meer hoogwaardige producten en diensten kan gaan toeleggen.

genomen verstrekking, dat hem mededeling was gedaan van de indiening van de klacht, dat hem mededeling was gedaan van de gewraakte verstrekking (alleen van het voornemen daartoe) en ook niet dat consultatie van het Parket-Generaal had plaats gevonden. Dit laatste moet indien het OM twijfelt of het de betrokkenen nu wel of niet moet horen om een goede afweging van belangen te kunnen maken.
De privacywaarborgen die het in principe ongewenste doorgeven van de strafrechtelijke gegevens voor de betrokkene moeten compenseren, waren kortom niet in acht genomen. De Registratiekamer oordeelde dus dat de verstrekking van informatie aan de KvT onrechtmatig was geweest. De notaris had onder deze omstandigheden volgens het boekje van het Compasreglement vooraf gehoord moeten worden en van de beslissing tot verstrekking op de hoogte moeten worden gebracht. Reglementen zijn er niet voor niets. Nu de zorgvuldigheidsregels niet in acht waren genomen, had de verstrekking niet mogen plaatsvinden ●

Uitvoering en verantwoording

De geschetste strategie en kritische succesfactoren zullen jaarlijks worden getoetst en geconcretiseerd in een voortschrijdend meerjarenplan, met de beoogde activiteiten voor het volgende jaar en de strategische keuzes voor de drie daarop volgende jaren. Elk jaar is er daarbij ruimte voor bijsturing, maar die behoeft niet in de weg te staan aan een grote mate van continuïteit.

Het openbare jaarverslag geeft telkens aan wat van het beoogde beleid en de voorgenomen activiteiten terecht is gekomen. Het CBP legt in dat verslag jaarlijks verantwoording af over het gevoerde beleid, zoals vastgesteld in het beleidsplan. Daarbij zal tevens een beknopt overzicht worden gegeven van de beoogde resultaten in het lopende jaar. Dit past in het streven van het CBP naar een zo effectief mogelijke inzet van mensen en middelen en een resultaatgerichte beleidscyclus.

Deze inrichting van de beleidscyclus is op hoofdlijnen neergelegd in het bestuursreglement dat ingevolge artikel 56, derde lid WBP is vastgesteld. Het bestuursreglement is inmiddels op 9 april 2002 goedgekeurd door de Minister van Justitie. De uitvoering van het jaarplan zal aan de hand van kwartaalrapportages intern worden geëvalueerd en zo nodig bijgestuurd. Het bestuursreglement zal tevens voorzien in een beschrijving van werkwijzen en procedures met het oog op een goede en zorgvuldige taakuitoefening. De hierin vervatte uitgangspunten en beleidsregels zullen worden bekend gemaakt.

Het bestuursreglement voorziet in een regeling van de beheersrelatie met de Minister van Justitie waarbij de eigen verantwoordelijkheid van het CBP voor zijn taakuitoefening onverlet blijft. Via een meerjarenplanning wordt gestreefd naar duidelijkheid over behoeften en mogelijkheden, en een situatie waarin het CBP zo zelfstandig mogelijk kan functioneren. Over de besteding van middelen en de daarmee bereikte resultaten zal ook in dat kader verantwoording worden afgelegd.

activiteiten

In dit hoofdstuk worden de voornaamste trends en ontwikkelingen weergegeven per maatschappelijk veld of deelterrein waarop de Registratiekamer en het CBP in 2001 actief waren.

activiteiten

activiteiten

Openbaar bestuur

OP DE GEVEL VAN DE TWEEDE KAMER STAAT ARTIKEL 1 VAN DE GRONDWET IN BRAILLE

De mate van zorgvuldigheid waarmee overheid en instellingen persoonsgegevens uitwisselen, heeft de Registratiekamer soms grote zorgen gebaard. Vooral waar instellingen in samenwerkingsverbanden persoonsgegevens uitwisselen, kunnen zich in de praktijk gemakkelijk problemen voordoen. Niet altijd is dan duidelijk wie voor welke verwerking van persoonsgegevens verantwoordelijk is of zelfs maar kan zijn. In dergelijke situaties kan efficiënter gegevensverkeer onbedoeld ten nadele van het individu uitpakken of ronduit in strijd zijn met de wet. Deze samenwerking en uitwisseling van gegevens tussen overheidsinstellingen op allerlei terreinen zal bovendien in de nabije toekomst uitgroeien tot een vaste informatie-infrastructuur.

Elektronische overheid

Het CBP heeft in 2001 de privacyaspecten van de overheidsplannen op het gebied van de 'elektronische overheid' onderzocht. In 2002 zal het CBP haar visie op elektronische overheid en privacy publiceren. Op initiatief van een aantal departementen en het CBP is het programma Stroomlijning Basisgegevens (SBG) ontwikkeld om te komen tot een stelsel van zogenaamde authentieke registraties voor de overheid. In deze registraties, onder andere van personen, worden de diverse vitale basisgegevens beheerd die gebruikt worden bij het optreden van de overheid. Het CBP stimuleert een maximaal gebruik van de niet onaanzienlijke speelruimte binnen de geldende (privacy)regels. Bijzondere aandacht heeft het CBP voor het persoonsnummerbeleid. Persoonsnummers vormen immers een sleutelonderdeel van de 'identiteitsinfrastructuur' van de overheid.

Gemeentelijke basisadministratie

De Commissie Snellen bracht in 2001 haar voorstellen uit voor de modernisering van de Gemeentelijke basisadministratie persoonsgegevens (GBA). Het doel van de voorstellen is een snellere informatie-uitwisseling tussen de gemeentelijke basisadministratie persoonsgegevens en de geautoriseerde organisaties tot stand te brengen. In haar reactie adviseerde de Registratiekamer op tal van punten positief. Zij ondersteunde de aanbeveling van de commissie om accountantscontrole en externe EDP-audits te laten uitvoeren bij de geautoriseerde organisaties.

Het geruchtmakende voorstel van een digitale kluis behoeft echter nadere overweging. De kluis was gedacht als een online raadpleegbare, digitale verzameling gegevens met als basis de gegevens uit de bevolkingsadministratie. Iedere burger zou de kluis gebruiken voor de uitwisseling van gegevens met de overheid. Als eigenaar van de kluis zou hij bovendien extra gegevens erin kunnen opslaan voor gegevensuitwisseling met andere partijen. De burger zou hier-

mee de 'regie' over zijn eigen gegevens herwinnen. Naast diverse negatieve effecten voor de privacy is het maar de vraag of de burger baas in eigen kluis blijft. Volgens de Registratiekamer bestaan er geen mogelijkheden om de burger te beschermen tegen druk van derden om zijn gegevens beschikbaar te stellen. Het tegendeel is het geval: hoe meer de digitale kluis wordt geïnstitutionaliseerd, des te groter zal de maatschappelijke druk op de burger worden om opgeslagen gegevens ter beschikking te stellen.

Op 1 september 2001 is de Wet GBA aangepast aan de Europese privacyrichtlijn. De belangrijkste wijziging is dat geen gegevens meer mogen worden verstrekt aan commerciële bedrijven, zoals incassobureaus en handelsinformatiebureaus. Deze partijen moeten sterk wennen aan de wijziging. De Registratiekamer had hier tegen geadviseerd juist vanwege het maatschappelijk belang van incasso van geldvorderingen. Het op slot doen van de GBA zou bovendien het zoeken naar sluipwegen kunnen stimuleren. Deze vrees bleek gegrond bij het onderzoek van de Registratiekamer naar het opereren van een handelsinformatiebureau (zie p. 31). Het CBP kan zich wel vinden in het principiële uitgangspunt dat informatie die de burger verplicht aan de overheid af moet staan, niet wordt uitverkocht. In 2001 werden ook de resultaten bekend van het privacygedeelte van de verplichte periodieke GBA-audit. Veel gemeenten voldeden niet aan de gestelde normen. De inbedding van het onderwerp privacy in de dagelijkse werkprocessen van de afdeling burgerzaken is nog onvoldoende. Dat is zorgwekkend. In 2002 zullen controleonderzoeken worden afgerond bij de gemeenten die eerder door de Registratiekamer zijn onderzocht. Verder beraadt het CBP zich op een effectieve aanpak van het probleem.

Sofi-nummer in het onderwijs

In 2001 werd ook het wetsontwerp voor de invoering van persoonsgebonden nummers in het onderwijs - op basis van het sofinummer - in het parlement behandeld. De Eerste Kamer deelde de bezorgdheid van de toezichthouder over het gebruik van het sofinummer op een nieuw maatschappelijk terrein. De minister van Onderwijs, Cultuur en Wetenschappen zegde een gedragscode voor het onderwijs toe evenals de aanstelling van functionarissen voor de gegevensbescherming.

De adviezen van de Registratiekamer hebben dus geleid tot een zorgvuldiger regeling. De meest opvallende waarborgen zijn de scheiding tussen beheer en gebruik, de inschakeling van het CBS bij het gebruik van de gegevens voor statistiek of (gemeente)beleid, de uitvoerige regeling van de informatieprocessen en de beveiligingseisen. De versleuteling van het sofi-nummer verhindert de ongewenste uitwaaiering ervan. De Registratiekamer bleef bij haar sterke voorkeur voor sectorspecifieke persoonsnummers, maar had waardering voor dit signaal van het kabinet dat een uitbreiding van het bereik van het sofi-nummer aan zeer stringente eisen dient te voldoen. De noodzaak van invoering en gebruik van een persoonsnummer moet grondig onderbouwd worden en waarborgen tegen misbruik moeten bij wet worden geregeld.

"Het Sofi-nummer moet niet verworden tot een nationaal persoonsnummer"

Kilometerheffing

Mobiliteitsheffingen, zoals de kilometerheffing voor automobilisten, waarvoor persoonsgegevens over de mobiliteit digitaal worden verzameld en verwerkt, kunnen nadelige effecten hebben op de privacy van de burger. Dergelijke systemen maken het mogelijk een gedetailleerd beeld te krijgen van het verplaatsingspatroon van individuele weggebruikers. Er is een reëel risico, zo leert de ervaring, dat deze gegevens ook voor andere doeleinden dan de heffing zullen worden gebruikt. Het CBP drong daarom aan op de toepassing van Privacy-Enhancing Technologies (PET).

Dit advies is opgevolgd. In het conceptwetsvoorstel Kilometerheffing dat eind 2001 aan het CBP werd voorgelegd, werd bepaald dat kilometerheffing zal plaatsvinden via een zogenaamde mobimeter in het voertuig. De privacygevoelige positie-informatie over het voertuig op basis van satellietgegevens (GPS-techniek) wordt alleen in het voertuig zelf verwerkt. De mobimeter wordt niet uitgelezen maar doet vanuit het voertuig aangifte bij de Belastingdienst via draadloze communicatie. Bij de aangifte worden niet de gedetailleerde verplaatsingsgegevens verstrekt maar uitsluitend de totaalgegevens. Functionaliteit en privacy zijn zo beide gewaarborgd. Indien langs deze lijnen gerealiseerd, zou de mobimeter een mooi voorbeeld zijn van *privacy by design*: het systeemontwerp zelf maakt inbreuk op de privacy onmogelijk. Wel is het is van belang dat de mobimeter via beveiligde protocollen met de buitenwereld communiceert.

Het CBP benadrukt verder dat het gebruik van de gegevens uit de mobimeter voor andere doeleinden alleen mag plaatsvinden op basis van vrijwilligheid. Dat geldt dus ook voor de ontwikkeling van nieuwe diensten waarbij de locatie van weggebruiker een belangrijke rol speelt. Het conceptwetsvoorstel maakt echter de houder van het voertuig zelf verantwoordelijk voor het correct functioneren van de mobimeter. De vraag is of dat de ingebouwde privacybescherming niet ontkracht. Deze kan worden ondermijnd als bijvoorbeeld de Belastingdienst op basis van zijn algemene, ruime onderzoeksbevoegdheden, stelselmatig gedetailleerde verplaatsingsgegevens op zou vragen bij de houder van het voertuig ■

activiteiten

Politie en Justitie

De registratie van burgers bij politie en justitie en de wijze waarop informatie over hen wordt vergaard, kan ingrijpende gevolgen hebben voor hun privacy. Het CBP heeft daarom een bijzondere belangstelling hiervoor.

De registers van de Criminele Inlichtingeneenheden (CIE) vormen de grootste bedreiging voor de privacy: door de aard van de registers en omdat bijna alle grote opsporingsonderzoeken erop zijn gebaseerd. Juist daarom zou de kwaliteit en het beheer van deze registers in orde moeten zijn.

POLITIEBEAMBTEN TIJDENS EEN BROMFIETSEN-CONTROLE

Kwaliteit van de politie-informatie

Uit onderzoek in 2001 waarbij de Registratiekamer betrokken was, bleek dat het toezicht op en de kwaliteit van de registratie - juist ook bij de Criminele Inlichtingeneenheden - nog steeds beneden de maat waren. Tot dit oordeel kwam al eerder de parlementaire enquêtecommissie Opsporingsmethoden (commissie Van Traa). Juist het groeiend aantal onverdachte burgers dat in politieregisters terechtkwam, was verontrustend.

Al in 2000 werden de regels voor opname en duur van de opslag van gegevens flink aangescherpt. Verbetering van de kwaliteit en het beheer van de bijzondere politieregisters moet er toe leiden dat het aantal geregistreerden in de bijzondere politieregisters vermindert en dat de bewaartermijnen in acht worden genomen. Goede analyse van informatie op het moment van vastlegging en gedurende de opslag kan voorkomen dat onjuiste informatie zowel de privacy van de betrokkenen als een zorgvuldige opsporing de doodsteek geeft.

Deze problemen – gesignaleerd door de parlementaire enquêtecommissie en bij herhaling door de Registratiekamer – zijn terug te voeren op het ontbreken van afdoende toezicht. Uit enkele pilot-audits was gebleken dat het toezicht op de kwaliteit van de informatiehuishouding ten onrechte nog geen prioriteit kreeg van de korpsleiding en het openbaar ministerie. Toezicht stond daarom centraal op de themadagen in 2001, georganiseerd door de Raad van Advies van de CIE en de Registratiekamer een jaar na de inwerkingtreding van de Wet bijzondere politieregisters. Deze inspanningen van de betrokken partijen hebben resultaat gehad.

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft een circulaire voorbereid waarin toezicht door middel van (externe) audits wordt voorgeschreven. Het CBP heeft hierover positief geadviseerd. De circulaire is in 2002 in werking getreden. Ook het Openbaar Ministerie is opgedragen direct toezicht uit te oefenen op de kwaliteit van de bijzondere politieregisters. Problemen in de nieuwe wetgeving worden ook zichtbaar. Het gaat vooral om de bewaartermijn van informatie over onverdachte burgers en over de gegevens betreffende informanten. Dat de wetgeving als knellend wordt ervaren is een goed teken: de wet wordt nu kennelijk serieus genomen. De evaluatie van de wet zal starten in 2002.

Inzage in de bijzondere politieregisters

De bijzondere politieregisters trokken ook de aandacht door de verzoeken om inzage. Zowel de advocatuur als de geregistreerden zelf weten de toezichthouder daarvoor te vinden. De Registratiekamer heeft in 2001 veel bemiddeld bij geschillen over inzage. In de praktijk bleek dat de politie de verwijderingstermijnen vaak niet in acht neemt. De politie verwijdert bijvoorbeeld niet altijd automatisch gegevens die langer dan zes maanden zijn vastgelegd in het voorlopig register. De politie is daartoe wel wettelijk verplicht.

Bij het behandelen van inzageverzoeken doen zich steeds vaker problemen voor. Deze hebben te maken met de reikwijdte van het verzoek en het stadium waarin informatie wordt gevraagd. Het kan gaan om (tien)duizenden berichten in de registers. Advocaten doen inzageverzoeken om te weten te komen of er een onderzoek tegen hun cliënt loopt. Deze zogenaamde 'fishing expeditions' schieten echter over het doel van het inzagerecht heen. Het doel is het zichtbaar maken van informatie die over een burger is verzameld, niet het doorkruisen van de opsporing doordat politie en justitie genoodzaakt worden te vroeg informatie prijs te geven. Het CBP werkt samen met de politie aan een stroomlijning van de inzageprocedure die privacy- en opsporingsbelang opnieuw in evenwicht moet brengen. De uitkomst zal met de advocatuur worden besproken.

"Goed toezicht is essentieel voor kwaliteit opsporing"

Oneigenlijk gebruik van politiebevoegdheden

Bedrijven en instellingen krijgen in de praktijk van alledag allerlei verzoeken en vorderingen van politie en justitie om inzage en afgifte van persoonsgegevens van bijvoorbeeld klanten. Onduidelijk is vaak waarop deze verzoeken of vorderingen zijn gegrond en of bedrijven en instellingen tot medewerking verplicht zijn. Houders van persoonsregistraties berichtten de Registratiekamer regelmatig dat de politie en ook het Openbaar Ministerie op grond van artikel 96a van het Wetboek van Strafvordering (Sv) bevel gaven persoonsgegevens uit computerbestanden op schrift te verstrekken ter inbeslagneming. De gevorderde informatie varieerde van bijvoorbeeld de dagafschriften van cliënten van bankinstellingen tot de bonuskaartgegevens van klanten van Albert Heijn.

Deze vorderingen zijn onrechtmatig. Artikel 94 Sv vermeldt de gronden voor inbeslagneming door de politie. Informatie die in computerbestanden is opgeslagen, valt niet onder dat artikel. Voor het onderzoeken en verkrijgen van dit soort gegevens geeft artikel 125i Sv de rechter-commissaris een specifieke en exclusieve bevoegdheid. De politie kan dus gegevens uit computerbestanden niet op rechtmatige wijze vorderen om in beslag te nemen. Deze uitdrukkelijke verdeling van bevoegdheden wordt omzeild als de politie op grond van artikel 96a Sv een houder beveelt gegevens op een diskette op te slaan en ter inbeslagneming uit te leveren. In de praktijk gebeurt het echter wel en deze handelwijze brengt een bedrijf dat hiermee wordt geconfronteerd in een lastige

positie. Meermalen heeft de Registratiekamer vastgesteld, dat de politie een bedrijf voorhoudt een strafbaar feit te plegen als niet onmiddellijk tot de verzochte uitlevering wordt overgegaan. Onder deze druk zijn heel wat bedrijven gezwicht om vervolgens op onrechtmatige wijze gegevens te verstrekken. Uiteindelijk zouden zij hiervoor verantwoordelijk gehouden kunnen worden.

Naar aanleiding van de klachten heeft de Registratiekamer de minister van Justitie schriftelijk om een standpunt in deze kwestie verzocht. Inmiddels heeft de minister zich uitgesproken tegen een dergelijke wijze van informatie-inwinning. Het College van procureurs-generaal had de minister eerder desgevraagd bericht dat artikel 96a Sv daarvoor inderdaad geen deugdelijke basis biedt. Voor zover er geen specifieke wettelijke regeling is voor het vorderen van persoonsgegevens, kan de houder van een persoonsregistratie op grond van artikel 11, tweede lid, van de Wet persoonsregistraties (Wpr) slechts worden gevraagd om de betreffende gegevens te verstrekken, aldus de minister.

De brief van de Registratiekamer vormde voor de minister aanleiding om het College van procureurs-generaal te verzoeken een nieuwe gedragslijn nader uit te werken. Deze gedragslijn dient te bepalen dat registratiehouders conform de wet worden verzocht de betreffende gegevens te verstrekken. Ook de WBP kent een bevoegdheid voor bedrijven en instellingen om mee te werken aan strafvordering door het verstrekken van persoonsgegevens. Dat blijft echter een lastige positie aangezien de beoordeling door deze partijen zelf moet gebeuren.

Commissie Mevis

De Commissie Strafvorderlijke gegevensvergaring (Commissie Mevis) heeft de kwestie van de politiebevoegdheden onderzocht. Zij stelt voor politie en justitie vergaande bevoegdheden te geven tot het vorderen van inlichtingen bij bedrijven en overheidsinstellingen. In beginsel wordt een ieder verplicht om aan politie en justitie iedere informatie te vestrekken van welke aard dan ook. Het CBP acht een duidelijke wettelijke regeling nodig die alle belanghebbenden meer rechtszekerheid biedt. De belangen van een zorgvuldige en effectieve opsporing zullen in balans moeten worden gebracht met belangen van partijen die gedwongen worden gegevens te verstrekken en ook met die van de grote groepen onverdachte personen over wie gegevens verkregen zullen gaan worden. De Commissie Mevis is er naar het oordeel van het CBP onvoldoende in geslaagd deze balans te treffen.

De commissie wil veel te vergaande informatieverplichtingen opleggen aan alle mogelijke partijen, informatieverplichtingen die geen verband houden met hun eigenlijke taken of doelstellingen. Daarmee zou elk bedrijf of overheidsinstelling in feite kunnen worden verplicht te fungeren als verlengstuk van justitie of politie doordat opsporingshandelingen moeten worden verricht. In een advies aan de minister van Justitie heeft het CBP erop aangedrongen de bevoegdheden in het wetsontwerp nauwkeuriger te bepalen en met meer waarborgen te omgeven.

Screening

Onderzoek naar de integriteit van een persoon buiten deze betrokkene om, ofwel screening, betekent een inbreuk op de privacy van degene die onderzocht wordt. Een dergelijke inbreuk op iemands persoonlijke levenssfeer is alleen gerechtvaardigd binnen duidelijke juridische kaders en wanneer er passende waarborgen zijn. Dat dit in de praktijk niet altijd zo gaat, blijkt wel uit de volgende zaak.

Voor de functie van assistent milieupolitieman en dierenwachter bij de gemeente Heerlen werd een sollicitant aan een screening op betrouwbaarheid onderworpen en op grond van de resultaten afgewezen. De betrokkene verzocht de Registratiekamer om een onderzoek naar de wijze waarop het regionaal politiekorps Limburg Zuid en de gemeente Heerlen het screeningsonderzoek hadden uitgevoerd. Onderzocht is hoever het integriteitonderzoek is gegaan, of de daarbij behorende gegevensverstrekkingen op de juiste rechtsgronden hebben plaatsgevonden en of de sollicitant voldoende rechtswaarborgen hierbij zijn geboden. De Registratiekamer heeft uiteindelijk geconcludeerd dat de persoonsgegevens van de betrokkene bij dit integriteitonderzoek niet op zorgvuldige en rechtmatige wijze door de gemeente en de politie zijn verwerkt.

De uitkomst van het onderzoek door de Registratiekamer is voor de korpsbeheerder aanleiding geweest om alsnog adequate richtlijnen voor het screenen op te laten stellen. Bovendien heeft de korpsbeheerder laten weten te zullen overleggen met de bij de screening betrokken personen en instanties om te bekijken of de betrokkene alsnog een passende baan of een andere genoegdoening kan krijgen. (Aan betrokkene is inmiddels een nieuwe baan aangeboden.) De gemeente Heerlen is in overweging gegeven een behoorlijk integriteitbeleid op te stellen voor het screenen van personen die onder regie van de politie aan het werk gaan .

DNA in strafzaken

De Registratiekamer heeft in december 2000 de minister van Justitie geadviseerd in verband met het wetsvoorstel "Wijziging van de regeling DNA-onderzoek in strafzaken i.v.m. het vaststellen van uiterlijk waarneembare persoonskenmerken uit celmateriaal" (Kamerstuk 28072). De Registratiekamer riep daarbij op tot het organiseren van een discussie tussen de bij de materie betrokken deskundigen en organisaties: een debat over de grenzen van het gebruik van DNA-onderzoek naar uiterlijk waarneembare kenmerken.

Het advies van de Registratiekamer is opgevolgd en op 21 mei 2001 is een expertmeeting gehouden over het conceptwetsvoorstel. De Registratiekamer heeft daaraan deelgenomen. De expertmeeting heeft ertoe geleid dat de afgrenzing van uiterlijk waarneembare persoonskenmerken duidelijker is verwoord. De uitkomsten van de expertmeeting tezamen met de adviezen over het conceptwetsvoorstel werden bij de verdere uitwerking van het wetsvoorstel gebruikt. Inmiddels is het aangepaste voorstel op 31 oktober 2001 aangeboden aan de Tweede Kamer.

De belangrijkste wijzigingen houden in dat de uiterlijk waarneembare persoonskenmerken die volgens de huidige stand van de techniek met een voldoende mate van exactheid uit het celmateriaal kunnen worden afgeleid, op het niveau van wet worden aangewezen. Een grens moet worden getrokken bij informatie die de betrokkene zelf al bekend is. Sluipende uitbreiding met andere persoonskenmerken waarvan de afleiding uit DNA minder zeker is, wordt daarmee onmogelijk. Dat is ook in lijn met het advies van de Registratiekamer.

Havank: vingerafdrukken

De politiedatabase Havank bevat zowel de vingerafdrukken van criminelen als van asielzoekers. In 2001 kwam in het nieuws dat de politie bij de controle van gevonden vingerafdrukken routinematig ook de vingerafdrukken van asielzoekers betrok. De vingerafdrukken van de asielzoekers zonder documenten worden in eerste instantie echter ter identificatie vastgelegd en niet vanwege een verdenking. Toch werden alle asielzoekers routinematig behandeld alsof er een verdenking op hen rust. Dit gebruik is strijdig met het doel van de vastlegging van de gegevens van de asielzoekers. Alleen als uitdrukkelijk een asielzoeker wordt verdacht van een strafbaar feit kan deze zoekactie plaatsvinden. Asielzoekers mogen evenmin als andere mensen zomaar als verdachte worden beschouwd. De minister vroeg in deze zaak advies van het CBP.

Het CBP heeft erop gewezen dat het onderbrengen van beide groepen in één database extra waarborgen vereist. Justitie heeft het advies ter harte genomen en werkt momenteel aan een daadwerkelijke scheiding ■

activiteiten

Arbeid en sociale zekerheid

INFORMATIE-TERMINAL BIJ EEN CENTRUM VOOR WERK EN INKOMEN (CWI)

De werknemer ziet zijn werkplek meer en meer geautomatiseerd. Dat betekent ook dat hij wordt omringd door systemen die geschikt zijn als personeelsvolgsysteem: het digitale toegangspasje, de beveiligingscamera, GSM, RSI-programma's en andere software. De controle op het gebruik van e-mail en internet stond in 2001 maatschappelijk volop in de belangstelling. Op Europees niveau werd gezocht naar een meer uniforme interpretatie van de regels voor de verwerking van persoonsgegevens in de relatie tussen de werkgever en werknemer. Het CBP heeft in 2001 ook de regelgeving rond de reïntegratie van de zieke werknemer met argusogen gevolgd.

Nieuwe fundamenten in de sociale zekerheid

In 2001 is verder gewerkt aan de nieuwe fundamenten voor de uitvoeringsstructuur van de sociale zekerheid. De overheid wil bevorderen dat overheidsinstellingen op het terrein van de sociale zekerheid efficiënter en vooral effectiever functioneren. Niet het verstrekken van uitkeringen, maar het helpen van arbeidsongeschikten aan een baan moet voorop staan. Reïntegratie is hierbij een kernbegrip. De afgelopen jaren heeft dit geleid tot een stroom van nieuwe wetsvoorstellen en regelgeving.

Deze voorstellen zijn ook aan het CBP en de Registratiekamer voorgelegd voor advies met het oog op de bescherming van de persoonsgegevens. De informatie-uitwisseling rond reïntegratie is daarbij het meest gevoelige punt. Het CBP heeft geadviseerd te zorgen voor grote transparantie en helderheid van de gegevensstromen. Het moet voor alle betrokken personen, instellingen en bedrijven duidelijk zijn welke informatie, tussen welke partijen voor welke doeleinden mag worden uitgewisseld. Dit kan worden bereikt door duidelijke regelgeving waarin met name de doelen van verstrekking afdoende gespecificeerd worden.

Sinds 1 januari 2002 hebben de eerste wijzigingen van de uitvoeringsstructuur hun beslag gekregen door de inwerkingtreding van de Wet SUWI (Structuur Uitvoering Werk en Inkomen). Dat

betekent dat het komende jaar gekeken zal worden hoe de bescherming van de privacy binnen de sociale zekerheid in de praktijk uitwerkt.

Reïntegratie

Bij de stelselwijzigingen heeft reïntegratie van arbeidsongeschikten een belangrijke plaats gekregen. Het proces van reïntegratie bij arbeidsongeschiktheid wordt steeds vaker uitbesteed aan particuliere bedrijven. Vanaf 2003 wordt een werkgever zelfs verplicht om een reïntegratiebedrijf in te schakelen wanneer de zieke werknemer niet meer kan terugkeren in de eigen functie en er ook geen andere passende functie binnen zijn bedrijf beschikbaar is.

Mede vanwege de kwetsbare positie van de te reïntegreren werknemer en de gevoelige persoonsgegevens die hierbij een rol spelen, volgt het CBP dit onderwerp nadrukkelijk. In verscheidene wetgevingsadviezen heeft het CBP de noodzaak benadrukt van specifieke regelgeving – bij voorkeur vastgelegd in wetgeving – voor de gegevensuitwisseling bij reïntegratie. Ondanks toezeggingen van de minister van Sociale Zaken en Werkgelegenheid moest het CBP constateren dat deze niet zijn nagekomen. Het CBP houdt vast aan het oordeel dat dit een ernstige omissie is, die de met de uitvoering belaste instanties voor aanzienlijke problemen zal plaatsen.

Ook bij de gegevensuitwisseling in het eerste ziektejaar heeft het CBP de bescherming van de privacy zo vroeg mogelijk op de agenda willen zetten. Met betrokken partijen zijn contacten gelegd om de te verwachten problemen te inventariseren. In 2001 heeft het CBP als adviseur deelgenomen aan een breed samengestelde werkgroep, geïnitieerd door verzekeraar Achmea, over de gegevensuitwisseling bij verzuim en reïntegratie. In vervolg op deze gezamenlijke analyse van praktijkvoorbeelden heeft het CBP in het najaar van 2001 een hoorzitting over gegevensuitwisseling in het eerste ziektejaar georganiseerd. Drie nagespeelde praktijksituaties wierpen een scherp licht op de lacunes, onduidelijkheid of tegenstrijdigheid in de wet- en regelgeving. Conclusie: het reïntegratieproces vereist voor een goed verloop meer duidelijkheid in de vorm van wetgeving of protocollen.

"Gegevensuitwisseling bij reïntegratie is onvoldoende geregeld"

Uitvoering Algemene bijstandswet

Op verzoek van de minister van Sociale Zaken en Werkgelegenheid (SZW) heeft het CBP geadviseerd over de privacyaspecten van de conceptcirculaire 'Uitbesteding onderdelen uitvoering Algemene bijstandswet'. Aan de orde is de vraag of en zo ja in hoeverre uitbesteding van de uitvoering van de Algemene bijstandswet aan particuliere bedrijven mogelijk is. In de praktijk lossen gemeenten uitvoeringsproblemen onder meer op door werkzaamheden op te dragen aan personeel dat niet in dienst is bij de gemeente. Dit wordt 'inbesteden' genoemd en kan verschillende vormen aannemen: van het inhuren van uitzendkrachten om administratieve achterstanden weg te werken tot een contract met een particulier bedrijf over het aantal door dit bedrijf te beoordelen bijstandsaanvragen. Het CBP heeft geadviseerd om de verschillende vormen van 'inbesteding' nader te analyseren en op basis hiervan regels te ontwikkelen. Het gaat immers om veel en gevoelige persoonsgegevens van de betrokken burgers.

De minister van SZW heeft inmiddels zijn standpunt dat de verstrekking van bijstandsuitkeringen een echte overheidstaak is in de praktijk tot gelding gebracht. De privatisering van de sociale dienst in de gemeente Maarssen is tegengegaan. Naar het oordeel van de minister is de toekenning van uitkeringen bij uitstek een publieke taak die door ambtenaren moet worden uitgevoerd. Uitvoerende taken, zoals de administratie mogen wel worden afgestoten.

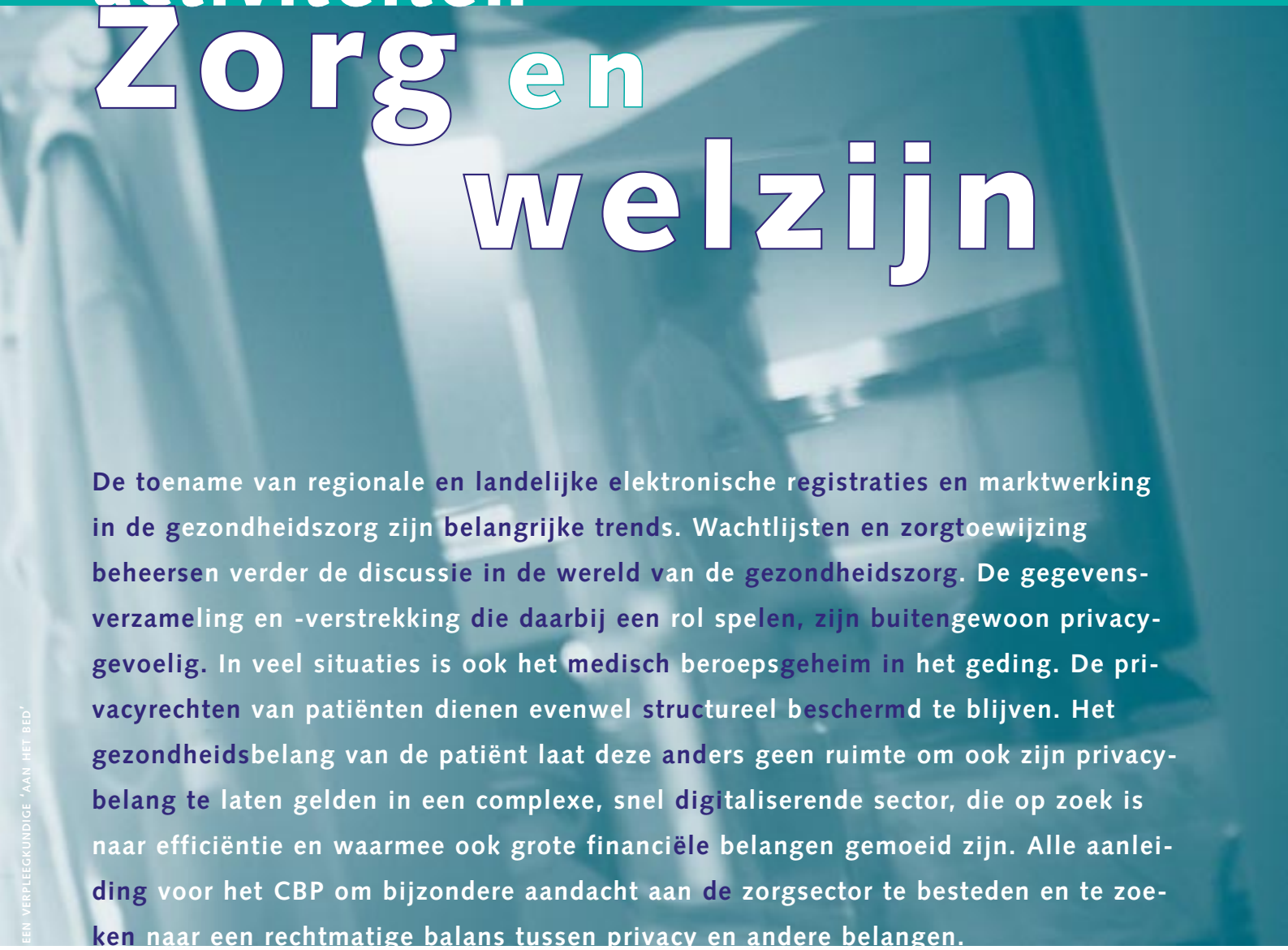
Controle op e-mail en internetgebruik

Op het terrein van de arbeidsverhoudingen werden in 2001 veel vragen gesteld aan de Registratiekamer en het CBP juist over de controle op het gebruik dat werknemers van e-mail en internet maken. Al in december 2000 publiceerde de Registratiekamer de studie *Goed werken in netwerken* met vuistregels voor een goede regeling van de controle door werkgevers op het email- en internetgebruik van hun werknemers. Een tweede herziene druk zal in april 2002 verschijnen.

Hoever mag de werkgever gaan om zijn werknemers te controleren? Technisch is onvoorstelbaar veel mogelijk. Niet de technische mogelijkheden, maar de noodzaak om te controleren moet echter bepalend zijn voor de mate en de vorm van de controle. De werkgever moet hierbij rekening houden met de privacybelangen van de werknemers. De Wet op de ondernemingsraden geeft de ondernemingsraad daarom het recht van instemming bij de invoering van een personeelsvolgsysteem. De Registratiekamer ontwikkelde een privacychecklist om ondernemingsraden de helpende hand te bieden bij het maken van deze afweging van bedrijfsbelangen en privacybelang. Ook deze checklist zal in april 2002 in een herziene versie verschijnen.

Het CBP kiest deze stimulerende rol juist om zelfregulering en het nemen van de eigen verantwoordelijkheid door werkgevers en werknemers binnen organisaties te bevorderen. De inspanningen die een organisatie zich moet getroosten om de controle op e-mail en internetgebruik goed te regelen, vertalen zich daarbij al snel in kwaliteitsverbetering op allerlei gebied zoals een beter beheer van informatiesystemen en duidelijkheid en vertrouwen in de werksfeer. Als toezichthouder wil het CBP met de vuistregels voor de controle op e-mail en internetgebruik de wettelijke normen in de dagelijkse praktijk ingang doen vinden: maximale transparantie voor betrokkenen, minimale verwerking van persoonsgegevens en alleen op een gerechtvaardigde grondslag ■

activiteiten Zorg en welzijn



De toename van regionale en landelijke elektronische registraties en marktwerking in de gezondheidszorg zijn belangrijke trends. Wachtlijsten en zorgtoewijzing beheersen verder de discussie in de wereld van de gezondheidszorg. De gegevensverzameling en -verstrekking die daarbij een rol spelen, zijn buitengewoon privacygevoelig. In veel situaties is ook het medisch beroepsgeheim in het geding. De privacyrechten van patiënten dienen evenwel structureel beschermd te blijven. Het gezondheidsbelang van de patiënt laat deze anders geen ruimte om ook zijn privacybelang te laten gelden in een complexe, snel digitaliserende sector, die op zoek is naar efficiëntie en waarmee ook grote financiële belangen gemoeid zijn. Alle aanleiding voor het CBP om bijzondere aandacht aan de zorgsector te besteden en te zoeken naar een rechtmatige balans tussen privacy en andere belangen.

EEN VERPLEEGKUNDIGE 'AAN HET BED'

Wachtlijsten en zorgtoewijzing

Al in 2000 heeft de Registratiekamer de minister en de staatssecretaris van VWS en Zorgverzekeraars Nederland erop gewezen dat de toezichthouder ernstige twijfel koesterde of de gegevensverstrekking in verband met zorgtoewijzing en wachtlijstbeheer een rechtmatige grondslag had. De kritische kanttekeningen waren vooral gericht op de voorgenomen landelijke AWBZ-brede zorgregistratie, waarin gegevens tot op individueel niveau identificeerbaar zouden worden. Uiteindelijk heeft de staatssecretaris van VWS in 2001 toegezegd dat bij de landelijke gegevensverzameling geen gegevens in de database worden opgenomen die tot personen herleidbaar zijn. Bovendien zal iedere nieuwe fase van het project aan het CBP worden voorgelegd.

Ziekenhuisbacterie

Aan de Registratiekamer werd gevraagd of een centrale registratie per regio van MRSA-besmette patiënten toelaatbaar is gelet op het medisch beroepsgeheim en de Wet bescherming persoonsgegevens (WBP). MRSA is een besmettelijke ziekenhuisbacterie. Het doel van de regionale MRSA-registratie is het voorkomen van (verdere) besmetting van andere patiënten en personeel door de aangesloten ziekenhuizen te waarschuwen zodra een met de ziekenhuisbacterie besmette patiënt wordt ingeschreven.

De Registratiekamer moest concluderen dat een centrale MRSA-registratie per regio, zonder toestemming van de patiënt, niet in overeenstemming is met het medisch beroepsgeheim en de privacywetgeving. In de eerste plaats is er geen wettelijk voorschrift om het medisch beroepsgeheim in de zin van artikel 7:457 BW te doorbreken. MRSA valt namelijk niet onder de Infectieziektenwet. Ten tweede is er geen sprake van rechtstreekse betrokkenheid bij de behandelingsovereenkomst. Alleen personen die rechtstreeks bij de behandeling zijn betrokken mogen onderling informatie uitwisselen. En in de derde plaats is er geen sprake van een 'conflict van plichten'. In noodgevallen kan een arts zijn beroepsgeheim doorbreken, maar daarvan is hier geen sprake. Het gaat immers om een stelselmatige registratie.

Hoewel deze geïmproviseerde doorbreking van het medisch beroepsgeheim dus niet door de beugel kon, was daarmee de ziekenhuisbacterie nog niet aangepakt. De Registratiekamer heeft daarom de aanbeveling gedaan de kwestie in een bredere con-

text te bekijken en voor te leggen aan de Gezondheidsraad zodat een oplossing gevonden kan worden die ook recht doet aan de privacy van de patiënt.

Medisch beroepsgeheim en letselschade

Bij de afhandeling van letselschade dienen doorgaans ook medische gegevens van de benadeelde (de patiënt) tussen diverse partijen te worden uitgewisseld: bijvoorbeeld artsen, verzekeringsmaatschappijen en rechtsbijstandverzekeraars. In eerste instantie vraagt de verzekeringsmaatschappij de benadeelde om zijn behandelende artsen te machtigen medische gegevens aan de verzekeraar te verstrekken. Bij onduidelijkheid over schuldvragen neemt de rechtsbijstandverzekeraar de afhandeling van de zaak over. De rechtsbijstandverzekeraar vraagt dan opnieuw machtigingen aan de benadeelde.

"Structurele bescherming van privacy bij zorgtoewijzing is geboden"

De Registratiekamer deed uitspraak over de vraag of de medisch adviseur van de schadeverzekeraar en die van de rechtsbijstandverzekeraar in het kader van de afhandeling van dezelfde schade niet te beschouwen zijn als 'functionele eenheid' in de zin van de gedragsregels van de KNMG waarbinnen ook zonder machtiging gegevens mogen worden uitgewisseld.

Zowel de privacywetgeving – na 1 september 2001 de WBP - als de regels betreffende het beroepsgeheim van de arts zijn van belang. Verstrekking van gegevens aan een derde is niet toegelaten als een ambts- of beroepsgeheim zich daartegen verzet. Ook de medisch adviseur is als arts tot zekere hoogte gebonden aan een beroepsgeheim. Uitsluitend met toestemming kan informatie verstrekt worden aan derden. Het beroepsgeheim is echter niet absoluut.

De medisch adviseur kan informatie beschikbaar stellen aan personen die noodzakelijkerwijze betrokken zijn bij het doel waarvoor de medische gegevens zijn gevraagd, c.q. verstrekt, de 'functionele eenheid'. Daarmee wordt de groepering van personen bedoeld die als team op directe of gelijkgerichte wijze betrokken is bij het doel waarvoor medische gegevens worden gevraagd c.q. verstrekt. Anderen dan de behandelend arts of de medisch adviseur krijgen alleen toegang tot relevante medische gegevens als zij behoren tot dezelfde functionele eenheid.

Bij overdracht van gegevens door de medisch adviseur van de ene verzekeringsmaatschappij aan de andere is van werken als een 'team' niet echt sprake. Wel zijn beide adviseurs op gelijkgerichte wijze betrokken bij hetzelfde doel, de afhandeling van een letselschade. Naar analogie met andere situaties concludeerde de Registratiekamer dat impliciete toestemming kan worden verondersteld bij overdracht van de afhandeling van eenzelfde letselschade door de medisch adviseur van de verzekeraar aan de rechtsbijstandsverzekeraar. Voorwaarde is dat de verzekerde/benadeelde is geïnformeerd en geen bezwaar heeft gemaakt. Deze constructie biedt tevens voldoende waarborgen om de verstrekking, als verdere verwerking in de zin van de Wet bescherming persoonsgegevens, te zien als verenigbaar met het doel waarvoor de gegevens zijn verzameld.

Jeugdzorg

Het conceptvoorstel voor de Wet op de jeugdzorg voorziet in de instelling van provinciale 'bureaus jeugdzorg'. Deze bureaus zullen de toegang zijn voor de verschillende vormen van jeugdzorg. Ook zijn in het conceptvoorstel bepalingen opgenomen over de verwerking van persoonsgegevens voor beleidsdoeleinden.

Juist omdat aan de bureaus jeugdzorg zeer uiteenlopende taken worden toebedeeld, waarvoor de verwerking van een groot aantal gevoelige persoonsgegevens nodig zal zijn, heeft de Registratiekamer de staatssecretaris van Justitie in 2001 geadviseerd het toezicht op de bureaus met name te richten op het gebruik van persoonsgegevens. Individuele zorg en de ontwikkeling van beleid zijn gerelateerde maar wel wezenlijk verschillende doelen. Bij de verwerking en verstrekking van gegevens voor beleidsdoeleinden adviseerde het CBP een goede wettelijke regeling. Aangezien de Advies- en Meldpunten Kindermishandeling ook in de bureaus jeugdzorg zullen worden ingebed, adviseert het CBP de verwerking van deze persoonsgegevens af te scheiden van andere gegevensverwerkingen.

Onderzoek

Het CBP onderzocht in samenwerking met Zorg Onderzoek Nederland (ZoN/MW) toekomstige ontwikkelingen in de zorg. In het zogenaamde 'juridisch laboratorium', dat mede aan de hand van proefsites juridische vraagstukken rond elektronische patiëntendossiers onderzoekt. In samenwerking met ZoN/MW zijn er over vraagstukken rond de bescherming van patiëntengegevens talrijke publicaties uitgebracht. In 2002 zal het CBP zijn visie op privacy en de rol van informatie- en communicatietechnologie in de zorg publiceren ■

activiteiten

Handel en diensten

EEN DRUKKE MIDDAG BIJ DE PLAATSELIJKE SUPERMARKT

De spanning tussen bedrijfsbelang en privacybelang van consumenten is een constante in de sector van handel en diensten. Hoe meer informatie over iemand bekend is, hoe nauwkeuriger diens profiel. Hierdoor kunnen gericht potentiële klanten worden aangeschreven en zijn mogelijke risico's beter in te schatten. De gevolgen voor de consument kunnen variëren van het ontvangen van 'onschuldige' – en soms zelfs zeer nuttige – direct mail tot het niet kunnen verkrijgen van hypotheken of verzekeringen. Willen marketeers alles weten om te verkopen, crediteuren willen alles weten om de rekening te innen en verzekeraars om hun risico's te beperken. De consument lijkt soms vogelvrij maar heeft wel degelijk recht op respect voor zijn privacy, ook een schuldenaar. Als toezichthouder zocht en zoekt het CBP naar het evenwicht tussen gerechtvaardigde bedrijfsbelangen en het recht op privacy van consumenten. Opkomen voor eigen rechten door de consument en zelfregulering door het bedrijfsleven dragen wezenlijk bij aan het tot stand brengen van dit evenwicht.

Gedragscode voor banken en verzekeraars

In 2001 is overleg gevoerd met de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars over de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen. De banken en verzekeraars stelden een gezamenlijke gedragscode op. Naar verwachting zal deze in 2002 aan het CBP ter goedkeuring worden voorgelegd. Ook heeft met dienstverleners overleg plaatsgevonden over de aanpassing van het protocol 'Incidenten-waarschuwingssysteem financiële instellingen' aan de Wet bescherming persoonsgegevens (WBP). Ook dit protocol zal in de loop van 2002 aan het CBP ter goedkeuring worden voorgelegd.

Adressenhandel

De komst van de WBP zorgde voor onzekerheid en wrevel in de direct marketingbranche. Er bestond lange tijd onduidelijkheid over de exacte regels bij adressenhandel onder de WBP. Het CBP bracht daarom in 2001 de studie *Klant te Koop, privacyregels voor adressenhandel* uit. Tijdens de jaarlijkse Direct Marketingdagen in

Maastricht is het rapport na een forumdiscussie aangeboden aan de voorzitter van de brancheorganisatie, de DMSA. Het CBP beoogde met het rapport niet alleen de branche duidelijkheid te bieden maar ook een overtuigend betoog neer te zetten dat de lucratieve adressenhandel uit de stiekeme hoek moet. Respect voor de privacy van consumenten is niet alleen wettelijke noodzaak maar ook goed koopmanschap.

Belangrijk voor een maatschappelijk breed geaccepteerde adressenhandel zijn transparantie en het recht van verzet. De klant moet weten wat er met zijn gegevens gebeurt en moet bezwaar kunnen maken. Zowel de consumenten als de bedrijven die handelen in adressen, hebben er baat bij dat de regels van de WBP zorgvuldig worden toegepast.

Informatieplicht

In de WBP is de plicht om consumenten te informeren over het gebruik van hun persoonsgegevens aangescherpt. Op de Direct Marketingdagen in Maastricht waar het CBP ook met een stand vertegenwoordigd was, kwamen hier veel vragen over binnen. Wat moet de cliënt wanneer verteld worden als een bedrijf zijn gegevens verkregen heeft?

Ook De Nederlandsche Bank werd geconfronteerd met de informatieplicht toen DNB iedere ingezetene van Nederland ouder dan zes jaar de Eurokit wilde toesturen. De WBP schrijft voor dat de bank in principe een ieder had moeten informeren op het moment dat zijn gegevens waren verkregen (in dit geval van de Belastingdienst), tenzij de betrokkene hier reeds van op de hoogte zou zijn. In de praktijk zou dit hebben betekent dat De Nederlandsche Bank iedereen een brief had moeten sturen met de mededeling dat er binnenkort een brief zou komen van de DNB (waarvoor die adresgegevens nodig waren).

DNB beriep zich op de uitzondering in de WBP die stelt dat de informatieplicht niet van toepassing is als het informeren van de betrokkene onmogelijk blijkt of onevenredige inspanning kost. Het CBP achtte het verdedigbaar dat DNB zich hier in dit geval op beriep. De informatieplicht is echter wel een waarborg dat betrokkenen hun rechten kunnen uitoefenen. Het CBP stelde daarom dat DNB wellicht in een eerder stadium het publiek had kunnen informeren, eventueel via de Belastingdienst. Het beroep op het feit dat de informatieplicht onevenredige inspanning kost, ontsloeg de DNB immers ook niet volledig van de informatieplicht. Het geeft DNB slechts de ruimte om de nakoming van de informatieplicht uit te stellen tot het moment van mailen.

Handelsinformatiebureau

In 2000 deed de Registratiekamer op grond van ernstige en herhaalde klachten een inval bij een handelsinformatiebureau. In 2001 werd het onderzoek afgesloten. De Registratiekamer moest constateren dat er op grote schaal onrechtmatig persoonsgegevens werden verkregen en verstrekt. Het handelsinformatiebureau doorbrak bewust de wettelijke geheimhoudingsverplichting van anderen. Niet alleen het bureau zelf overtrad de wet door onrechtmatig verkregen informatie aan derden te verstrekken maar het bureau zette ook organisaties aan tot het onrechtmatig verstrekken van informatie. Bij diverse instanties zoals sociale diensten, zorginstellingen, uitzendbureaus en nutsbedrijven werd op diverse manieren informatie opgevraagd en vaak ook verkregen. Het CBP heeft het onderzoek gebruikt om op diverse plaatsen orde op zaken te stellen. Het betrokken bedrijf heeft uiteraard de eigen werkwijze moeten aanpassen aan de wet om te waarborgen dat persoonsgegevens op een rechtmatige wijze worden verwerkt. Het CBP zal in 2002 controleren of het bedrijf de beschreven werkprocessen ook daadwerkelijk in praktijk brengt.

Het onderzoek heeft ook geleid tot intensievere contacten met de Nederlandse Vereniging van Handelsinformatiebureaus. Het CBP heeft het belang van zelfregulering met kracht naar voren gebracht. Dit heeft geleid tot het met spoed opstellen van een nieuwe gedragscode, die naar verwachting in 2002 aan het CBP zal worden voorgelegd.

"Adressenhandel moet uit de stiekeme hoek "

Gerechtsdeurwaarders

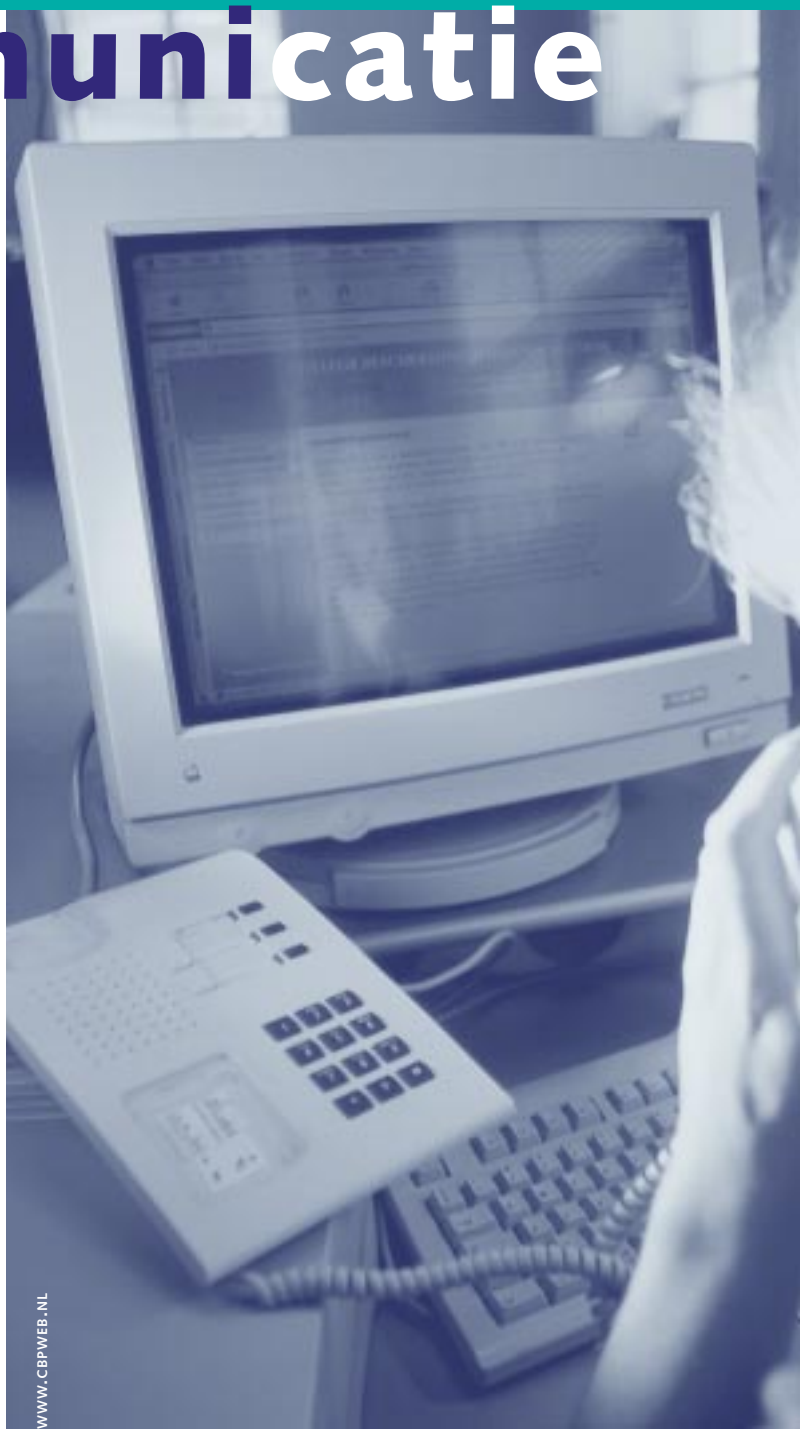
Het onderzoek bij het handelsinformatiebureau toonde ook aan dat opdrachtgevers (waaronder gerechtsdeurwaarderskantoren) op onrechtmatige wijze persoonsgegevens verstrekten aan het bureau. Het CBP heeft deze opdrachtgevers hierop gewezen. De betrokken kantoren hebben toegezegd hun werkwijze te verbeteren. Het onderzoek heeft ook geleid tot intensivering van de gesprekken met de Koninklijke Beroepsvereniging van Gerechtsdeurwaarders en met het ministerie van Justitie als toezichthouder.

Medio 2001 is de Gerechtsdeurwaarderwet in werking getreden. Op grond van de Deurwaarderswet zijn onder meer de 'Verordening beroeps- en gedragsregels gerechtsdeurwaarders' en de 'Administratieverordening' van kracht geworden. De Administratieverordening gebiedt een administratieve scheiding van de deurwaarders- en de incassopraktijk, die veel kantoren combineren. Het CBP is nauw betrokken geweest bij de totstandkoming van deze verordeningen en heeft daarbij kunnen putten uit de opgedane kennis van de praktijk. De verordeningen bieden de deurwaarderskantoren een basis om te komen tot beheersmaatregelen die kunnen waarborgen dat persoonsgegevens rechtmatig worden verwerkt ■

activiteiten

Telecommunicatie

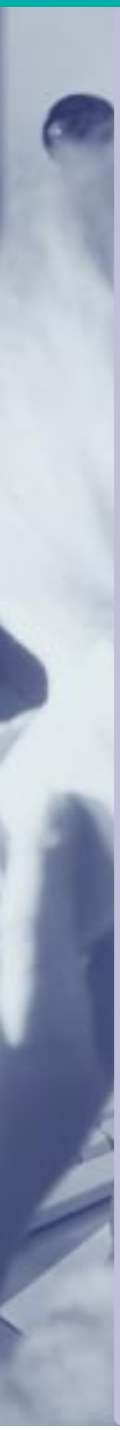
Ondanks het barsten van de internetbel en de ontnuchtering na de hype, heeft communicatie over open netwerken zoals het internet de toekomst. Veiligheid en betrouwbaarheid van deze communicatie worden daarom steeds belangrijker. Internet is onderdeel van de telecommunicatie, een maatschappelijke sector die sterk in beweging is. Om toezicht te kunnen houden op de privacyaspecten van de telecommunicatie analyseerde het CBP in 2001 een sleuteltechniek in de sector op privacyaspecten. Ook adviseerden Registratiekamer en CBP over voorstellen op het gebied van opsporing en telecommunicatie die het grondrecht op vertrouwelijke communicatie ernstig in het gedrang brengen.



Sleutels van vertrouwen

Veiligheid en betrouwbaarheid van internetcommunicatie gaat concreet om vragen als 'Wie zit er achter deze website?', 'Is de afzender van deze e-mail wie hij zegt te zijn?', 'Mag deze persoon wel namens zijn bedrijf bestellingen doen?', 'Wordt mijn e-mail alleen gelezen door de geadresseerde?' 'Is er niet gerommeld met het bedrag van deze elektronische factuur?', 'Kan een klant een via de website gedane bestelling later zomaar ontkennen?'. Een belangrijke techniek bij het bieden van garanties voor veilige en betrouwbare telecommunicatie is de openbare-sleutel-cryptografie, die de laatste tijd sterk aan populariteit wint. De techniek kan zowel gebruikt worden voor het afschermen van berichten voor onbevoegden als voor het zetten van een digitale handtekening. Het gebruik ervan vereist dat de sleutel op betrouwbare wijze gekoppeld is aan de identiteit of andere attributen van de houder ervan. De infrastructuur die nodig is om dit te faciliteren heet een public-key infrastructuur (PKI). Een *trusted third party* (TTP) staat binnen een PKI in voor de genoemde koppeling. De TTP doet dat door zelf gebruik te maken van een elektronische handtekening. Een digitaal certificaat is een door een TTP uitgegeven en digitaal ondertekend elektronisch document dat het verband legt tussen een openbare sleutel en attributen van de houder ervan.

In 2001 publiceerde het CBP het rapport *Sleutels van vertrouwen* over de privacyaspecten van TTP's en digitale certificaten. Drie belangrijke thema's zijn 1) anonimiteit en pseudonimiteit, 2) digitale sporen, 3) het verspreiden van informatie in een PKI (zie kader en ook pagina 34).



1 Anonimiteit en pseudonimiteit

Het is meestal wenselijk dat de identiteit bekend is van iemand die een digitale handtekening zet. Dat wil echter nog niet zeggen dat deze identiteit dan ook vermeld moet worden op het certificaat dat bij de handtekening hoort. Vaak is het voldoende dat de identiteit van de houder is te achterhalen als dat echt nodig is, bijvoorbeeld in geval van fraude. Modellen voor certificaten die bijvoorbeeld door het gebruik van pseudoniemen de privacy beschermen, verdienen meer aandacht. Het CBP ziet hier een rol voor de TTP's.

2 Digitale sporen

Traditionele identiteitsgegevens als naam-adres-woonplaats zijn een onvoldoende basis voor het betrouwbaar koppelen van persoonsgegevens. Zulk koppelen komt de kwaliteit van de gegevens ten goede, maar kan ook grote privacyrisico's inhouden. Om die reden is de invoering van een algemeen persoonsgebonden nummer voor dat doel onwenselijk. Persoonsnummers die gebonden zijn aan bepaalde maatschappelijke sectoren kunnen hier mogelijk uitkomst bieden. Voorkomen moet worden dat openbare sleutels of, nog gevaarlijker, biometrische templates gaan fungeren als alternatieve persoonsgebonden nummers.

3 Informatieverspreiding in een PKI

De meest gebruikelijke manier om certificaten te verspreiden is via een openbare directory. Dat mag alleen met toestemming van de certificaathouder, die ook een reëel alternatief moet hebben. De toestemming moet vrijwillig gegeven zijn en dient te zijn gebaseerd op juiste, duidelijke en volledige informatie. Het op grote schaal openbaar zijn van certificaten biedt tal van mogelijkheden voor het opbouwen van gedetailleerde profielen. Om die reden verdient privé-verspreiden serieuze aandacht als alternatief. De inrichting van een openbare directory moet ongeoorloofd gebruik van de erin opgenomen informatie zoveel mogelijk verhinderen.

Opsporing en telecommunicatie

Bij het opsporen van criminelen speelt de telecommunicatiesector een belangrijke rol. Er moet worden meegewerkt aan het aftappen van telefoongesprekken, er moeten inlichtingen worden verstrekt over het communicatieverkeer en over de personen die daaraan deelnemen. Politie en justitie ervaren de wettelijke grenzen die ze daarbij in acht moeten nemen nogal eens als onterechte beperkingen van hun handelingsvrijheid. Bij de wetgever vindt deze visie in ruime mate gehoor.

De Commissie Mevis heeft in 2001 voorgesteld politie en justitie vergaande bevoegdheden te geven tot het opeisen van informatie bij bedrijven en overheidsinstellingen. Het CBP heeft de Minister van Justitie geadviseerd de bevoegdheden preciezer te bepalen en met meer waarborgen te omgeven. Aan personen of instanties van wie gegevens worden gevorderd, moet de mogelijkheid worden geboden de vordering door de rechter te laten toetsen voordat de gegevens worden verstrekt. Bedrijven of overheidsinstellingen moeten niet gaan fungeren als verlengde arm van justitie of politie, door zelf de opsporing ter hand te nemen.

De noodzaak om een duidelijke wettelijke basis te scheppen voor de bevoegdheid tot het vorderen gebruikersgegevens, wordt door het CBP onderschreven. Het gaat hierbij in verreweg de meeste gevallen om het vorderen van naam- en adresinformatie van uit printertaps verkregen telefoonnummers en om het verkrijgen van geheime telefoonnummers door politie, justitie en de inlichtingendiensten.

Hoewel de Commissie Mevis als vertrekpunt nam dat na de telecommunicatiesector die in de afgelopen jaren al wettelijk tot vergaande vormen van medewerking was verplicht, nu andere maatschappelijke sectoren aan de beurt waren, liet ze doorschemeren dat haar nieuwe voorstellen straks ook voor de telecommunicatiesector zullen gaan gelden. Zo wordt voortdurend haasje over gespeeld met bevoegdheden: de meest vergaande bevoegdheden zijn de maat voor andere sectoren. (Zie ook pagina 24).

"Grondrecht op vertrouwelijke communicatie in het gedrang"

Grondrechten in het digitale tijdperk

In het wetsvoorstel Vorderen gegevens telecommunicatie waarover de Registratiekamer al eerder advies uitbracht, werd aan verkeersgegevens categorisch de bijzondere bescherming van artikel 13 Grondwet onthouden. Het CBP meent dat er alle reden is voor grote terughoudendheid bij het verplichten van de telecommunicatiesector tot het bewaren van gegevens in het algemeen. Historische gegevens over het communicatiegedrag of de beschikbaarheid van locatiegegevens bij mobiele telefonie zijn inmiddels op grote schaal voorhanden. Dat raakt ook onverdachte personen.

Dat de Grondwet in het digitale tijdperk niet meer kan spreken van het 'telegraafgeheim' zal duidelijk zijn. De voorstellen tot modernisering van het grondrecht op vertrouwelijke communicatie vinden dan ook brede instemming. Het CBP heeft gereageerd op het standpunt van het kabinet over het eindrapport van de Commissie Grondrechten in het digitale tijdperk.

Het kabinetsvoorstel voor een nieuw artikel 13 Grondwet schiet in hoge mate tekort bij het beschermen van het recht van ieder vertrouwelijk te kunnen communiceren. Het grondrecht dient niet beperkt te worden tot de inhoud van het berichtenverkeer, maar moet zich ook uitstrekken tot de gegevens over het telecommunicatieverkeer (verkeersgegevens) ■

Technologie en audit

De digitale revolutie beïnvloedt meer dan wat ook de manier waarop de samenleving met informatie en dus ook met persoonsgegevens omgaat. Het College bescherming persoonsgegevens investeert daarom al jaren in onderzoek naar de bedreigingen en kansen die informatie-en communicatietechnologie scheppen voor de bescherming van de persoonlijke levenssfeer.

Een adequate beveiliging van persoonsgegevens in het digitale domein is daarbij de meest voor de hand liggende benadering.

In 2001 publiceerde de Registratiekamer *Beveiliging van persoonsgegevens*, dat een kader biedt voor de implementatie van de Wet bescherming persoonsgegevens bij informatiesystemen. Gedegen privacy-audit-instrumenten zijn daarbij nodig voor de beoordeling en controle van informatiesystemen.
Bij beveiliging gaat het erom met technische en organisatorische maatregelen persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. De studie geeft ook het belang aan van een tweede benadering, de toepassing van privacy bevorderende technologieën.

Privacy-Enhancing Technologies

Privacy-Enhancing Technologies (PET) voorkomen de onnodige verwerking van persoonsgegevens in informatiesystemen zonder dat verlies van functionaliteit optreedt. In plaats van de wet toe te passen op het systeem, wordt de wet in het systeem ingebouwd: *privacy by design*. Ronduit futuristisch is op dit gebied het Europese PISA-project waaraan het CBP deelneemt. De ambitie van het project Privacy Incorporated Software Agents is het ontwikkelen van ontwerpspecificaties voor autonome software agents die de 'eigenaren' in staat zullen stellen allerlei elektronische transacties te (laten) verrichten met behoud van zeggenschap over hun persoonsgegevens.

Het CBP ziet digitale privacy als een wezenlijke succesfactor in het realiseren van de beloftes van e-commerce, e-health en e-government zoals het begin 2001 nog vol zelfvertrouwen genoemd werd. Helaas constateert het CBP dat privacyregels vaak als obstakel worden gezien voor de digitale ambities van bedrijfsleven en overheid. Miskend wordt dan dat vertrouwen in de digitale relatie bij consument en burger staat en valt met de wijze waarop met zijn gegevens wordt omgesprongen. Het is de vaste overtuiging van het CBP dat dit vertrouwen gebaat is bij maximale transparantie en minimale verwerking van persoonsgegevens.

Digitale certificaten en privacy

De behoefte aan betrouwbare en vertrouwelijke elektronische communicatie en transactie is groot en groeiend. Zekerheid over de identiteit van de betrokken partijen is daarbij essentieel. Daarvoor is een speciale infrastructuur nodig, een zogenaamde *public-key infrastructure* (PKI). Een belangrijke rol binnen zo'n infrastructuur spelen *trusted third parties* (TTP's). Zij vergewissen zich van de identiteit of andere kenmerken van iemand en geven ter bevestiging daarvan vervolgens een digitaal certificaat uit. Deze digitale certificaten zullen in de nabije toekomst een cruciale rol spelen bij het realiseren van betrouwbare en veilige digitale relaties.

Nederland staat aan de vooravond van grootschalige invoering van TTP's, zowel publiek als privaat. De taskforce PKI-overheid ontwerpt een PKI voor communicatie en transacties met de overheid. Het project TTP.NL is een zelfreguleringsinitiatief van aanbieders en afnemers van TTP-diensten. Beide initiatieven kunnen een belangrijke positieve bijdrage leveren aan het tot stand

komen van een goede infrastructuur en daarmee aan de bescherming van de privacy on-line. Willen TTP's hun voortrekkersrol als aanbieders van privacy-enhancing technology waarmaken, dan dienen zij goed om te gaan met persoonsgegevens.

De Registratiekamer bracht daarom in 2001 het rapport *Sleutels van vertrouwen* uit, de eerste uitwerking van de implicaties van de Europese privacyrichtlijn en de Nederlandse wet bescherming persoonsgegevens voor de TTP-sector. Daarbij moest steeds de balans gezocht worden tussen het belang van een goede ondersteuning van elektronische communicatie en transactie en anderzijds het recht op bescherming van de persoonlijke levenssfeer (zie ook pagina 32).

Biometrische identificatie

Ook het gebruik van biometrische kenmerken voor een eenduidige identificatie van personen staat sterk in de belangstelling. De komst van biometrische identificatie is een belangrijke trend binnen de beveiliging van andere gegevens. Verantwoorde inzet van dit identificatiemiddel betekent wel dat deze biometrische persoonsgegevens zelf goed beschermd dienen te worden.

In maart 2001 rondde de Registratiekamer een onderzoek af naar een toegangscontrolesysteem voor horeca- en sportgelegenheden, waarbij gebruik werd gemaakt van digitale opnames van het gezicht van bezoekers. Van eventuele raddraaiers kon ook een digitale zwarte lijst worden aangelegd op basis van de biometrische kenmerken. Juist gezichtskenmerken bevatten echter rasgegevens en zijn daarmee als bijzondere persoonsgegeven aan te merken. Een ontheffing van het verbod om rasgegevens te verwerken is mogelijk indien die verwerking geschiedt met het oog op de identificatie van de betrokkene en slechts voor zover de verwerking voor dit doel onvermijdelijk is. Dat was in dit geval aannemelijk. Voor de koppeling tussen dit gebruik en het gebruik van de gegevens voor marketingdoeleinden zonder vrije keuze van de betrokkenen was echter geen rechtvaardiging te vinden. Het betrokken bedrijf nam alle aanbevelingen over, onder andere die over de bewaartermijn, de gescheiden opslag voor marketingdoeleinden en de versleuteling van gegevens.

De minister van Binnenlandse Zaken en Koninkrijksrelaties stelde in 2001 voor de Paspoortwet zo te wijzigen dat biometrische identificatie ook bij reisdocumenten mogelijk wordt met als belangrijkste doel het voorkomen van identiteitsfraude.

Het CBP was – in het advies van oktober 2001 aan de minister – er niet van overtuigd dat de tijd al rijp is voor een wettelijke basis voor de toepassing van biometrie in reisdocumenten. Mocht de minister hiertoe toch willen overgaan dan zouden de gegevens in ieder geval zodanig moeten worden gecompartimenteerd dat onbevoegd gebruik onmogelijk wordt gemaakt. Overneming in andere systemen moet daardoor worden uitgesloten.

Het CBP achtte het niet noodzakelijk om biometrische gegevens op te nemen in de administraties van de autoriteiten die bevoegd zijn tot de afgifte van reisdocumenten. Centrale opslag wordt hiermee vermeden. De opslag in decentrale databases laat bovendien allerlei ander mogelijk gebruik toe. Tenslotte vroeg het CBP in zijn advies nadrukkelijk aandacht voor de beveiliging van de biometrische gegevens.

"Vertrouwen door maximale transparantie en minimale verwerking van persoonsgegevens"

Audit-instrumenten

Vooruitlopend op de invoering van de WBP heeft de Registratiekamer al eind 1999 het initiatief genomen om in een samenwerkingsverband een aantal audit-instrumenten te ontwikkelen. Het beschikbaar maken van deze hulpmiddelen past in de strategie van het CBP om zelfregulering te stimuleren. De instrumenten stellen organisaties in staat om de kwaliteit van de genomen maatregelen voor de bescherming van persoonsgegevens te (laten) beoordelen.

Het samenwerkingsverband bestaat uit marktpartijen, zoals audit- en adviesorganisaties, koepelorganisaties van auditors, werknemers-, werkgevers- en consumentenorganisaties en de ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties. Eind 2001 is gestart met een onderzoek naar de mogelijkheid privacy-auditors ook te certificeren.

De samenwerking heeft geresulteerd in drie audit-instrumenten die in 2001 energiek onder de aandacht zijn gebracht: *Quickscan, WBP-Zelfevaluatie* (eventueel met review) en *Raamwerk Privacy Audit*. Voor de *WBP-Zelfevaluatie* bestond in 2001 een grote belangstelling. Met dit instrument kan een organisatie zelfstandig en in betrekkelijk korte tijd de kwaliteit van de maatregelen voor de bescherming en beveiliging van persoonsgegevens beoordelen.

Het *Raamwerk Privacy Audit* is bedoeld voor het opstellen van een werkplan voor het uitvoeren van een privacy-audit door een (privacy)deskundige auditor. De privacy-audit geeft de leiding van een organisatie met een hoge mate van zekerheid een objectief oordeel over de naleving van de wettelijke bepalingen en daarmee ook inzicht in de sterke en zwakke punten van de bescherming van persoonsgegevens ■

Internationaal

Een integrale benadering van privacybescherming is niet meer mogelijk zonder rekening te houden met ontwikkelingen in het internationale vlak. Persoonsgegevens worden steeds vaker uitgewisseld via internationale netwerken, met name internet, en opgeslagen in internationale databases. Daarbij doet zich in veel gevallen de vraag voor welk nationaal recht op een verwerking van toepassing is.

Als consequentie van de Europese integratie hebben activiteiten op Europees niveau een steeds grotere invloed op het nationale beleid. Omdat de WBP uitvoering geeft aan Richtlijn 95/46/EG, is de betekenis van wettelijke bepalingen mede afhankelijk van beslissingen die in Brussel, Luxemburg of Straatsburg worden genomen. Het CBP is op grond van artikel 61, zesde lid, WBP verplicht om aan de toezichthoudende autoriteiten van de andere lidstaten alle medewerking te verlenen, voor zover dat voor de uitvoering van hun taken noodzakelijk is.

Het CBP neemt dan ook deel aan verschillende vormen van internationale samenwerking. In de meeste gevallen ligt de nadruk daarbij op advisering over wetgeving of afstemming van beleid. Binnen de derde pijler van de EU is ook sprake van gemeenschappelijk toezicht op de verwerking van persoonsgegevens op het terrein van politie en grensbewaking. In concrete zaken wordt daarnaast steeds vaker via bilaterale contacten tussen nationale toezichthouders samengewerkt.

DOUANESCHEPEN IN DE HAVEN VAN ROTTERDAM

Artikel 29 Werkgroep

De Werkgroep van nationale toezichthouders als bedoeld in artikel 29 van Richtlijn 95/46/EG heeft tot taak advies uit te brengen over privacykwesties in het kader van de Europese besluitvorming. Ook de feitelijke afstemming van het beleid van de nationale toezichthouders vindt hier plaats. In 2001 werd daartoe zesmaal plenair vergaderd, telkens voor twee dagen, en een intensief programma afgewerkt. (Zie ook pagina 50.)

Het CBP heeft deelgenomen aan de subgroep belast met de behandeling van een Europese gedragscode op het gebied van privacy en direct marketing, opgesteld in het kader van de Europese brancheorganisatie FEDMA. De goedkeuring van deze gedragscode door de werkgroep lijkt in de loop van 2002 mogelijk.

Het CBP heeft ook deelgenomen aan de subgroep Employment over privacy op de werkplek. In september 2001 werd een algemeen kaderdocument aanvaard, dat naar verwachting zal worden gevolgd door een aanbeveling over monitoring van e-mail en internet op de werkplek.

Het CBP heeft tenslotte intensief bijgedragen aan het werk van de subgroep die is belast met de beoordeling van contractuele bepalingen voor gegevensverkeer met derde landen. In de loop van 2001 heeft de Europese Commissie een tweetal contracten goedgekeurd. Het CBP neemt ook deel aan het panel van nationale toezichthouders dat in het leven is geroepen voor de behandeling van klachten tegen bedrijven die meedoen aan de 'Safe Harbour'-regeling met de Verenigde Staten.

Schengen en Europol

In het kader van de derde pijler van de EU zijn gemeenschappelijke controle-autoriteiten die bestaan uit vertegenwoordigers van de nationale toezichthouders, in het leven geroepen voor het Schengen Informatiesysteem (SIS) en voor de gegevensbestanden van Europol. Sinds kort is een soortgelijke controle-autoriteit ingesteld voor het Douane Informatiesysteem (DIS). Daarnaast is er een onafhankelijke beroepsinstantie voor geschillen over de uitoefening van het recht op kennisneming en verbetering van gegevens bij Europol. Ten behoeve van deze vier instanties is een gemeenschappelijk secretariaat ingericht. Een medewerker van het CBP is in de loop van 2001 aangesteld tot hoofd van dit secretariaat. De plenaire vergaderingen, al dan niet voorbereid door subgroepen, vinden in principe vijf keer per jaar plaats. Het CBP heeft in 2001 een brochure uitgebracht over het SIS en de rechten van betrokkenen. Deze is op Schiphol en bij andere grensdoorlaatposten verkrijgbaar.

Raad van Europa

Het CBP vertegenwoordigt Nederland in de adviescommissie van het Dataprotectieverdrag van de Raad van Europa uit 1981, waarbij thans 27 landen partij zijn. Dit verdrag heeft mede aan de basis gestaan van de privacyrichtlijn van de Europese Unie. Toetreding tot dit verdrag is voor landen die lid willen worden van de EU een belangrijke eerste stap tot implementatie van de privacyrichtlijn.

In 2001 heeft het CBP bijgedragen aan een conferentie in Warschau ter viering van het twintigjarige bestaan van het Dataprotectieverdrag. Centraal stond de vraag of, en zo ja hoe, het verdrag moet worden herzien. De conclusie was dat het Dataprotectieverdrag nog steeds een belangrijke rol speelt, met name voor wat betreft de derde pijler van de Europese Unie. De privacyrichtlijn is hierop niet van toepassing.

In 2001 is een additioneel protocol bij het verdrag aangenomen dat door de adviescommissie is opgesteld. In dit protocol worden partijen verplicht om een toezichthoudende autoriteit in te stellen die in volledige onafhankelijkheid werkt, wat een belangrijke voorwaarde is voor een effectieve gegevensbescherming. Daarnaast stelt het protocol regels voor de doorgifte van persoonsgegevens aan 'derde' landen. Het belang hiervan neemt toe met de intensivering van het internationale gegevensverkeer. Daarom heeft de adviescom-

missie in 2001 gewerkt aan het ontwikkelen van richtlijnen voor het opstellen van contracten die gegevensverkeer met derde landen mogelijk maken.

Doorgifte van persoonsgegevens naar derde landen

Nieuwe regels voor het gegevensverkeer met landen buiten de Europese Unie zijn ook in werking getreden met de WBP. Het CBP heeft in het verslagjaar deze regels en zijn beleid hieromtrent uiteengezet in een nota die op de website (www.cbpweb.nl) staat. Met name de procedure voor het aanvragen van een vergunning voor doorgifte van gegevens naar derde landen op basis van een contract heeft in dit stuk veel aandacht gekregen. Deze procedure is opgesteld in nauw overleg met het ministerie van Justitie, dat de vergunning verleent na advies van het CBP.

Samenwerking met andere toezichthouders

Samenwerking met toezichthoudende autoriteiten in andere landen draagt bij aan een verdergaande harmonisatie van de privacybescherming, zowel in Europa als daarbuiten. In een tijd van intensivering van internationale informatiestromen is een goede coördinatie tussen nationale toezichthouders daarnaast een noodzakelijke waarborg voor een effectieve bescherming van burgers.

Tijdens de lenteconferentie van de Europese toezichthouders in Athene heeft het CBP een aantal presentaties verzorgd. Onder andere werd in samenwerking met de Belgische zusterorganisatie, het werk van de Artikel 29 Werkgroep met betrekking tot het internet gepresenteerd. Ook besteedde het CBP in dit forum aandacht aan het PISA-project voor de ontwikkeling van nieuwe technologieën waarbij privacybescherming in de structuur is ingebouwd. Dit project waarin het CBP samenwerkt met een aantal private partners, wordt gefinancierd door de Europese Unie.

De jaarlijkse wereldconferentie van toezichthoudende autoriteiten, die kort na 11 september 2001 in Parijs plaatsvond, stond in het teken van het belang van een goed evenwicht tussen veiligheid en privacybescherming, juist in tijden waarin de veiligheid onder druk staat. In dit licht werd ook de discussie gevoerd tijdens de workshop over de bestrijding van cybercrime, die werd voorgezeten door het CBP.

De in 2000 gestarte halfjaarlijkse workshops voor medewerkers van toezichthoudende autoriteiten in de EU, die zijn gericht op praktische onderwerpen, werden in 2001 succesvol gecontinueerd. In dit jaar is tevens een besloten internetplatform in gebruik genomen, dat gebruikt wordt voor de samenwerking tussen Europese toezichthouders bij de behandeling van internationale klachten en informatie-uitwisseling.

Het CBP was leider van deze website en heeft tijdens de twee workshops uitleg gegeven over de wijze waarop de website de toezichthouders in hun werkzaamheden van dienst kan zijn. Dankzij deze mogelijkheid tot coördinatie is het CBP in staat geweest om samen met de zusterorganisaties op een snelle en effectieve wijze een aantal internationale klachten te behandelen. Tevens heeft het CBP via dit overlegforum bijgedragen aan snelle en intensieve informatie-uitwisseling tussen de toezichthoudende autoriteiten ■

eBay: doorgifte van klantgegevens naar de VS

iBazar, een bedrijf dat veilingwebsites exploiteerde in verschillende EU-landen, waaronder Nederland, werd in 2001 overgenomen door het Amerikaanse bedrijf eBay, dat de grootste veilingsite ter wereld beheert.

Om de overgang van iBazar-gebruikers naar het eBay-systeem zo gemakkelijk mogelijk te laten verlopen, wilde eBay de klantgegevens van iBazar Nederland verplaatsen naar de Verenigde Staten. De doorgifte zou plaats vinden tenzij klanten bezwaar zouden maken tegen het verplaatsen van hun gegevens. Deze aanpak wordt 'opt-out' genoemd: de betrokkene heeft de keus om uit te stappen. De gegevens zouden in de VS pas gebruikt worden nadat de klant toestemming had gegeven. Deze aanpak wordt 'opt-in' genoemd: de betrokkene heeft de keus om in te stappen. Binnen de Europese Unie zijn er geen bijzondere problemen met de doorgifte van persoonsgegevens van het ene land naar het andere. Voor doorgifte naar landen buiten de Europese Unie – de zogenaamde derde landen - gaat dat niet zomaar. De Europese privacyrichtlijn 95/46/EG vereist voor doorgifte van persoonsgegevens een passend beschermingsniveau. Dit ontbreekt in de VS terwijl er natuurlijk een grote behoefte is om persoonsgegevens uit te wisselen. De EU heeft daarom besloten dat er een passend beschermingsniveau is als Amerikaanse bedrijven zich houden aan de 'safe harbour'-regels, een privacyregeling van het Amerikaanse Ministerie van Handel. eBay nam echter niet deel aan de 'Safe Harbour'-regeling.
De Registratiekamer wees iBazar/eBay er op dat de geplande doorgifte van de klantgegevens niet rechtmatig was. De doorgifte was niet nodig voor het uitvoeren van een overeenkomst: in de verkoop aan eBay waren de klanten van iBazar immers geen partij. En er was ook geen sprake van toestemming van de klanten. Toestemming impliceert een wilsuiting: de klant stemt bewust in met doorgifte. In de opt-out benadering wil de klant echter (als hij er op tijd aan denkt) dat zijn gegevens niet worden doorgegeven. De geplande doorgifte kon dus niet rechtmatig doorgaan. Het zou anders zijn als iBazar alsnog toestemming van de klant zou vragen. Vreemd genoeg gebeurde dat wel bij de overdracht van klantgegevens van iBazar Frankrijk. eBay volgde daarop de aanbeveling van de Registratiekamer en vroeg toestemming aan alle klanten voor de doorgifte ●

DNA, HET ULTIEME PERSOONSGEGEVEN, IS VERWERKT IN HET LOGO VAN HET CBP.

Organisatie

Het jaar 2001 was voor de organisatie een enerverend, elektriserend en bijzonder jaar door de invoering van de nieuwe Wet bescherming persoonsgegevens (WBP). De Registratiekamer transformeerde tot College bescherming persoonsgegevens. Taken op grond van de oude Wet persoonsregistraties (WPR) werden uitgevoerd naast de voorbereiding op de nieuwe wet.

Productie

De taken van de Registratiekamer op grond van de WPR zijn voor een groot deel overgegaan in de taken van het CBP. Daarnaast zijn er nieuwe taken en bevoegdheden met de WBP bijgekomen. De uitvoering van deze taken is de productie waarover de organisatie verantwoording aflegt. Onderstaand overzicht presenteert de productie geordend op hoofdzaken. De voornaamste ontwikkelingen die de tabel zichtbaar maakt, zijn de stijging – opnieuw – van het aantal wetgevingsadviezen en de stug doorgroeiende vraag naar informatie over de bescherming van persoonsgegevens.

	1999	2000	2001
Wetgevingsadviezen	25	35	43
Gedragscodes	3	6	1
Reglementen WpolR en WPR tot 1-9-01	111	88	50
Voorafgaand onderzoek	0	0	12
Voorlichtingsverzoeken	687	910	1.204
Internationale zaken	17	10	13
Bemiddeling en klachten	367	323	290
Ambtshalve onderzoeken	32	17	24
Aanmeldingen WPR tot 1-9- 01	60.928	65.977	66.572
WBP meldingen	0	0	591
Telefonisch spreekuur	4.464	4.277	4.979

OVERZICHT VAN DE PRODUCTIE 1999 - 2001

In het kader van het stimuleren van de bewustwording en de normontwikkeling op het gebied van privacy hebben medewerkers van het CBP in 2001 circa 180 lezingen en presentaties gegeven voor een groot aantal organisaties. De thema's waren onder meer de nieuwe Wet bescherming persoonsgegevens, de auditinstrumenten, privacy bevorderende technologie, privacyaspecten van biometrie en direct-marketing.

Overgang naar de WBP

In 2001 is een tiental projecten uitgevoerd – deels met hulp van externe partijen – om de organisatie voor te bereiden op de overgang naar de WBP. Hiervoor was ook extra budget beschikbaar.

	1999	2000	2001 excl WBP	2001 incl WBP
Personeel	4.869	5.245	6.006	6.006
Materieel	1.421	1.178	1.808	2.986
Totaal	6.290	6.423	7.814	8.992

BUDGETTOEKENNING 1999-2001 (BEDRAGEN FL. X 1000)

Nieuwe bevoegdheden brachten vanzelfsprekend een zwaardere plicht tot verantwoording, transparantie en operationele betrouwbaarheid met zich mee. Die noodzaak vertaalde zich onder andere in de ontwikkeling van een Bestuursreglement en de installatie van een Raad van Advies. De benoeming van de leden van de Raad van Advies is sterk bevorderd juist met het oog op

een breed draagvlak voor de bescherming van de persoonsgegevens. Het bestuursreglement is inmiddels vastgesteld en de leden van de Raad van Advies zijn door de Minister van Justitie benoemd. De eerste vergadering met de Raad van Advies - over het Beleidsplan 2002-2005 - heeft inmiddels plaatsgevonden.

Ook de verdere uitwerking en vastlegging van de interne werkprocessen was noodzakelijk. Deze werkprocessen dienden of aangepast te worden aan de WBP of nieuw ontworpen te worden. Het project werkprocessen heeft inmiddels een 'receptuur' opgeleverd voor de belangrijkste WBP-processen zoals bemiddeling en klachten, voorlichting en wetgevingsadviezen. In 2002 zullen de overige werkprocessen worden aangevuld en volgt een evaluatie van de receptuur. Nieuw is ook het in 2001 vrijwel afgeronde werkproces voor de doorgifte van persoonsgegevens aan landen buiten de Europese Unie. Het CBP adviseert in deze de Minister van Justitie over de vergunningverlening.

De wettelijke plicht de verwerking van persoonsgegevens te melden bij het CBP betekent voor organisaties en voor het CBP een niet onaanzienlijke administratieve last. Met veel inzet en grote betrokkenheid van velen (intern en extern) zijn bedrijven, diensten en overheden vanaf 15 augustus in staat gesteld een WBP-Meldingsprogramma aan te vragen. Dit programma maakt het mogelijk op een gebruiksvriendelijke manier een WBP-melding op te stellen en in te zenden op een diskette. Daarnaast voorziet het programma in een elektronische handreiking voor de bepaling of men meldingsplichtig is of niet. Vanzelfsprekend is ook in een papieren WBP-meldingsformulier met handleiding voorzien. Tijdens de overgang van de WPR-meldingen naar de WBP-meldingen zijn inzenders zowel schriftelijk als telefonisch bijgestaan. Er zijn dan ook tijdens de overgang geen noemenswaardige problemen ontstaan.

De ontwikkeling van nieuwe expertise vond plaats in de projecten voor kennisontwikkeling bij de eigen medewerkers. Verder werd het project voor de ontsluiting van de wetsgeschiedenis en de ontwikkeling van de interne WBP-documentatie, vrijwel afgerond. Het beheer hiervan is inmiddels overgedragen aan de lijn. Kennisontwikkeling zal echter flinke investeringen blijven vergen.

Het project Handhaving heeft een eerste verkenning opgeleverd van de consequenties voor ambtshalve onderzoeken onder de WBP in relatie tot daaraan voorafgaande processen zoals klachtbehandeling en bemiddelingsverzoeken en de daarop volgende interventie en sanctionerende processen. In 2002 zullen de

	1999	2000		2001	
		m	v	m	v
In dienst	15	4	6	6	4
Uit dienst	9	6	4	5	3
Bezetting einde jaar m / v		24	27	26	26
Bezetting einde jaar totaal	45,9	51		52	
Gemiddelde bezetting in fte's	47,9	47,8		49,6	
Formatie in fte's per 31 dec	49,4	49,4		55,4	
Gemiddelde formatie	49,4	49,4		51,4	
Mobiliteit	31%	21%		20%	
In tijdelijke dienst		9		9	
Fulltime in dienst		62,7%		61,5%	

FORMATIE 1999-2001

sanctionerende processen nog verder moeten worden uitgewerkt inclusief de organisatorische consequenties in verband met de gewenste functiescheiding.

In het project Voorlichting vond de aanpassing en ontwikkeling van WBP-voorlichtingsmateriaal plaats, dat bovendien in een nieuwe huisstijl gestoken moest worden. De brochure *Functionaris voor de gegevensbescherming* is ontwikkeld om de eigen verantwoordelijkheid van organisaties voor de bescherming van persoonsgegevens te stimuleren. Veel aandacht is besteed aan de website, www.cbpweb.nl. Niet alleen is de content aangepast aan de nieuwe wet, maar ook is de site ingericht voor de verspreiding van het elektronische WBP-meldingsprogramma en voorzien van functionaliteit om het Vrijstellingsbesluit toegankelijker te maken voor bedrijven en andere organisaties, de

	1999	2000	2001
Totaal ziekteverzuim excl. zwangerschap	8,73%	8,15%	6.97%
Waarvan langdurig verzuim	5,47%	4,01%	3.78%
Ouderschapsverlof	0	2	2
Verlof zwangerschap/bevalling	0	1	2
Kinderopvangplaatsen	3	2	2
Opleiding (in fl. x 1000)	70	88	123
% t.o.v. personele budget	1,44 %	1,47 %	2,05 %

ZIEKTEVERZUIM EN OVERIGE PERSONELE INFORMATIE 1999-2001

Handreiking Vrijstellingsbesluit. Van voorlichtingsbijeenkomsten over de gevolgen van de WBP is door een kleiner aantal brancheverenigingen en andere organisaties gebruik gemaakt dan verwacht mocht worden uit de hiervoor gehouden enquête.

Medewerkers

In samenspraak met het personeel zijn competenties voor de bestaande functies uitgewerkt. Dit proces heeft geresulteerd in het Formatieplan 2001 waarbij ook de functieprofielen zijn vastgesteld. Het proces heeft tevens geresulteerd in het uitspreken van wederzijdse verwachtingen en persoonlijke ambities. Het CBP heeft voor de begeleiding en ondersteuning van dit proces een P&O adviseur voor 0,5 fte beschikbaar gemaakt.

De toenemende aandacht in het publieke domein voor privacy en de verantwoordelijkheid die de WBP in deze bij organisaties en bedrijven legt, heeft tot gevolg dat de uitstroom van met name beleidsmedewerkers groot is. Dit is positief voor de missie van het CBP en voor de ontplooiingsmogelijkheden van de medewerkers. Het is ook zorgelijk gezien de noodzaak kennis voor de organisatie te behouden. Het CBP zag zich in 2001 daarom genoodzaakt tot een forse inspanning voor werving en selectie, die pas in 2002 vruchten zal afwerpen. Duidelijk is de noodzaak gebleken het CBP als werkgever opvallender te profileren.

Door de vele extra werkzaamheden en toenemende productie nam de werkdruk toe. De ondernemingsraad heeft in 2001 nadrukkelijk aandacht gevraagd

voor de hoge – soms te hoge – belasting. De hoge werkdruk deed zich vooral voelen door de noodzaak om snel nieuwe expertise rond de WBP voor het eigen functioneren op te bouwen naast de lopende werkzaamheden en de toenemende vraag om informatie over de WBP. Gelukkig liep het verzuim ondanks de hoge werkdruk verder terug tot 6,97%. De oorzaken van het ziekteverzuim bleken voor een beperkt deel gerelateerd aan het werk. Het CBP heeft 2,05% van de personele uitgaven in 2001 besteed aan externe opleidingen; daarnaast was er een intern project voor kennisontwikkeling.

Begin 2001 is op aandringen van de ondernemingsraad voorlichting gegeven door de Arbodienst over het voorkomen van RSI-klachten. De werkplekken zijn onder de loep genomen en zo nodig aangepast. Tevens is afgesproken om een zogenaamd workspaceprogramma voor pc-gebruik ter voorkoming van RSI-klachten aan te bieden.

Taken van het CBP

• Wetgevingsadviezen

Op grond van artikel 51, tweede lid, van de 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.

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.

• Gedragscodes

Het CBP werkt graag mee aan de totstandkoming van sectorale gedragscodes zoals bedoeld in artikel 25 WBP.

• Reglementen

De WBP voorziet anders dan de WPR, 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 daarom in behandeling als dat opportuun is.

Reglementen voor politieregisters zijn op grond van de Wet politieregisters wel onderworpen aan een toetsing vooraf. Het CBP bevordert de opstelling van modelreglementen. De hoorprocedures kunnen daardoor achterwege blijven.

• Melding en voorafgaand onderzoek

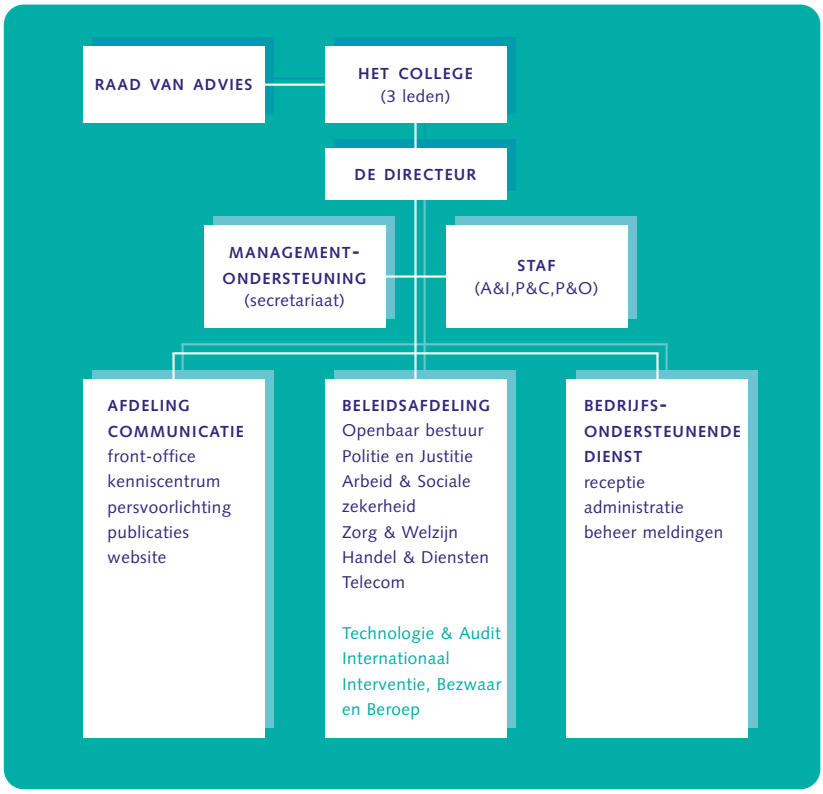
Tot 1 september 2001 werden meldingen van persoonsregistraties op grond van de WPR verwerkt. Ingevolge de WBP moeten per 1 september geautomatiseerde verwerkingen van persoonsgegevens vooraf worden gemeld bij het CBP of een functionaris voor de gegevensbescherming, tenzij het Vrijstellingsbesluit voorziet in een vrijstelling. Bepaalde categorieën van verwerkingen waaraan bijzondere risico's zijn verbonden, zijn krachtens de WBP onderworpen aan een voorafgaand onderzoek. Het onderzoek loopt meestal uit op 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. Verzoeken met een standaardkarakter worden behandeld door het frontoffice als deel van de publieksvoorlichting. Verzoeken om voorlichting kunnen ook aanleiding zijn voor verdergaande behandeling, een diepgaande studie of een principiële standpuntbepaling.

• 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 e, 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.



Directeur van het CBP is
mw. ing. C.E. Romanesko

• Doorgifte naar derde landen

Op grond van artikel 77, tweede lid 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 derde land (dat wil zeggen buiten de Europese Unie en Europese Economische Ruimte) dat geen waarborgen voor een passend beschermingsniveau biedt.

• Internationale zaken

Op grond van artikel 51, eerste lid, 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, 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.

• 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 of over de uitoefening van het recht op verzet. 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.

• 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.

• Handhaving

Indien overheden, bedrijven, andere organisaties of individuele verantwoordelijken in gebreke blijven bij de melding van hun verwerking van persoonsgegevens kan een boete worden opgelegd. Bij overtreding van de wet of daarop gebaseerde regelingen kan het CBP overgaan tot bestuursdwang of tot een last onder dwangsom.

bijlagen

wetgevingsadviezen

Voorstel tot 'Wijziging van de regeling van het DNA onderzoek in strafzaken in verband met het vaststellen van uiterlijke persoonskenmerken aan de hand van celmateriaal' 8 januari 2001

Advies Reglement justitiële jeugdinrichtingen
19 januari 2001

Wijziging besluit GBA
25 januari 2001

Kiezen op afstand
29 januari 2001

Wetsvoorstel kenbaarheid publiekrechtelijke beperkingen
29 januari 2001

Wijziging Besluit inlichtingen Strafregisters
14 februari 2001

Aanpassing Besluit politieregisters
1 maart 2001

Grondrechten in het digitale tijdperk (commissie Franken) ambtshalve
6 maart 2001

Wetsvoorstel Bereikbaarheid en mobiliteit (WBM) ambtshalve
14 maart 2001

Wijziging van de Telecommunicatiewet
27 maart 2001

Wijziging Besluit inlichtingen strafregisters
5 april 2001

Concept-wetsvoorstel Structuur Uitvoering Werk en Inkomen (SUWI)
19 april 2001

Kliq-wet
19 april 2001

Gegevensuitwisseling zorg- en hulpverlenende instanties
19 april 2001

De rechterlijke procedure bij geschillen om kennisneming van politiegegevens
1 mei 2001

Klantcontactpunten huursubsidie EOS III
10 mei 2001

Rapport van de commissie Modernisering GBA (commissie Snellen)
31 mei 2001

Conceptwetsvoorstel Wet op de Jeugdzorg
1 juni 2001

Aanpassingswet Europese richtlijn elektronische handel
20 juni 2001

Voorontwerp Wet elektronisch bestuurlijk verkeer
2 juli 2001

Wetswijziging inzake gebruik van sociaal-fiscaal nummer
25 juni 2001

Nieuwe procedure eerste aanvraag huursubsidie
23 juli 2001

Wetsvoorstel vorderen gegevens telecommunicatie
25 juli 2001

Conceptbesluit SUWI en Concept-besluit Inlichtingenbureau
7 augustus 2001

Meldingsregeling WBP
15 augustus 2001

Concept-voorstel Wet op het CBS
21 augustus 2001

Verwerking van persoonsgegevens door deurwaarders
22 augustus 2001

Handreiking privacyaspecten bij criminaliteitspreventie
24 september 2001

Wet publiekrechtelijke registratie zeeschepen
10 oktober 2001

Basisregister reisdocumenten
15 oktober 2001

Toezicht op het beheer van de bijzondere politieregisters
16 oktober 2001

Wijziging Paspoortwet in verband met invoering biometrie
17 oktober 2001

Besluit eisen elektronische handtekeningen
22 oktober 2001

Rapport Commissie Strafvorderlijke gegevensvergaring (commissie Mevis)
7 november 2001

Aanpassing Wet geneeskundige behandelingsovereenkomst (WGBO)
12 november 2001

Concept-wetsvoorstel tot wijziging van de Wet justitiële gegevens inzake verstrekkingen OM
22 november 2001

Veegwet WBP (informeel)
22 november 2001

Toetsing notitie inzake maximale versterking van de effectiviteit van opsporing en toezicht
3 december 2001

Concept Privacykader Algemene bijstandswet
11 december 2001

Ministeriële regeling Procesgang eerste ziektejaar
12 december 2001

Concept ministeriële regeling SUWI
12 december 2001

Wijziging Besluit politieregisters
18 december 2001

Uitwerking EU-Richtlijn in nationale wetgeving
20 december 2001

Vrijwel alle adviezen vanaf 1996 kunt u raadplegen op de website: www.cbpweb.nl. (Adviezen uit de periode 1991-1996 zijn ook opgenomen in de bundel *Persoonsgegevens beschermd, van WPR naar WBP.* Den Haag, Sdu uitgevers, 1999.)

bijlagen

gedragscodes waarvoor een Verklaring van Overeenstemming onder de WPR is verleend

Gedragscode persoonsregistraties van de Branchevereniging voor Informatietechnologie COSSO; geldig tot 17 januari 1994 (Stcrt. 1991, 12)

Gedragscode Direct Marketing Instituut Nederland; geldig tot 2 oktober 1995 (Stcrt. 1992, 194)

Privacy Code van de Organisatie van Adviesbureaus voor Werving en Selectie (OAWS); geldig tot 28 november 1995 (Stcrt. 1990, 232)

Privacy Gedragscode van de Nederlandse Postorderbond; geldig tot 1 april 1996 (Stcrt. 1993, 60)

Gedragscode persoonsregistraties van de Vereniging van Onderzoeks Instituten in gedrags- en maatschappijwetenschappen; geldig tot 8 mei 1996, (Stcrt. 1991, 88)

Privacy-gedragscode van de Vereniging van Marktonderzoekbureaus en de Nederlandse Vereniging van Marktonderzoekers; geldig tot 12 juni 1996 (Stcrt. 1991, 111)

Gedragsregels in verband met de bescherming van de persoonlijke levenssfeer van de Nederlandse Associatie van de Farmaceutische Industrie (Nefarma); geldig tot 13 oktober 1997 (Stcrt. 1992, 198)

Gedragscode van de Vereniging van Fabrikanten en Importeurs van Diergeneesmiddelen in Nederland (FDIN); geldig tot 3 december 1997, (Stcrt. 1992, 235)

Gedragscode van de Nederlandse Vereniging van Handelsinformatiebureaus; geldig tot 25 juni 1998; (Stcrt. 1993, 118)

Privacy Gedragscode van de Nederlandse Vereniging van Banken; geldig tot 16 oktober 1998 (Stcrt. 1995, 207)

Gedragscode Gezondheidsonderzoek van de Federatie van Medisch Wetenschappelijke Verenigingen; geldig tot 14 juli 2000; (Stcrt. 1995, 140)

Gedragscode verwerking persoonsgegevens verzekeringsbedrijf (Verbond van Verzekeraars); geldig tot 5 maart 2001 (Strct. 1998, 44)

Gedragscode van het Nationaal Chipcard Platform; geldig tot 18 september 2001 (Stcrt. 1996, 195)

modelreglementen voor politieregisters, vastgesteld sinds 1994

Aandachtsvestigingen	(Stcrt. 1994, 78)
Arrestanten	(Stcrt. 1994, 78)
Arrestatiebevelen	(Stcrt. 1994, 78)
Bedrijfsprocessensysteem BPS	(Stcrt. 1994, 78)
Bedrijven informatiesysteem en waarschuwingsadressen	(Stcrt. 1994, 78)
Bekeuringenafhandelingssysteem	(Stcrt. 1994, 78)
Beperkingen besturen motorrijtuigen	(Stcrt. 1994, 78)
Bureau financiële ondersteuning	(Stcrt. 1996, 125)
Fraudebestrijding	(Stcrt. 1994, 78)
Gegevensuitwisseling milieu	(Stcrt. 1998, 102)
Gevonden en verloren goederen	(Stcrt. 1994, 78)
Graffitibestrijding	(Stcrt. 1994, 78)
Herkenningsdienst	(Stcrt. 1994, 78)
Inbeslaggenomen goederen	(Stcrt. 1994, 78)
Inbraakbestrijding	(Stcrt. 1994, 78)
In bewaring genomen goederen	(Stcrt. 1994, 78)
Informantenregister	(Stcrt. 2000, 198)
Internationale rechtshulp politie	(Stcrt. 1994, 144)
Jeugd- en zedenzaken	(Stcrt. 1994, 78)
Kabinetszaken	(Stcrt. 1994, 78)
Meldkamer	(Stcrt. 1994, 78)
Milieudelicten	(Stcrt. 1994, 78)
Multipol	(Stcrt. 1994, 78)
Openbare orde Regionale inlichtingendienst	(Stcrt. 1996, 125)
Opkopers en helingbestrijding	(Stcrt. 1994,78)
Overvallenbestrijding	(Stcrt. 1994, 78)
Permanent autoteam	(Stcrt. 1994, 78)
Processen-verbaal en rapporten	(Stcrt. 1994, 78)
Recidive	(Stcrt. 1994, 78)
Rijverboden	(Stcrt. 1994, 78)
Schietwapen incidentenregistratie en informatiesysteem	(Stcrt. 1994, 78)
Signalen van mensenhandel	(Stcrt. 2002, 13)
Technische recherchezaken	(Stcrt. 1994, 78)
Vakantiecontrolekaarten	(Stcrt. 1994, 78)
Vandalismebestrijding	(Stcrt. 1994, 78)
Verdovende middelen	(Stcrt. 1994, 78)
Voorlopig register	(Stcrt. 2000, 198)
Wijziging herkenningsdienst	(Stcrt. 1996, 125)
Zware criminaliteit	(Stcrt. 2000, 198)

In 2002 zullen verschillende modelreglementen aangepast worden aan de inmiddels veranderde wetgeving en getoetst worden aan de behoeften van de praktijk. Tevens is te verwachten dat het CBP in 2002 voor verschillende nieuwe modelreglementen een verklaring van geen bezwaar zal afgeven.

bijlagen

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

26 January 2001 - **Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the transfer of personal data to third countries under Article 26(4) of Directive 95/46** (Document 5102/00 – WP 38).

26 January 2001 – **Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act** (Document 5109/00 – WP 39).

26 January 2001 - **Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000** (Document 5095/00 – WP 40).

22 March 2001 - **Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime** (Document 5001/01 – WP 41).

22 March 2001 - **Recommendation 1/2001 on Employee Evaluation Data** (Document 5008/01 – WP 42).

17 May 2001 - **Recommendation 2/2001 on certain minimum requirements for collecting personal data online in the European Union** (Document 5020/01 – WP 43).

17 May 2001 - **Opinion 5/2001 on the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH** (Document 5003/00 – WP 44).

17 May 2001 - **Fourth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the Community and in Third Countries covering the year 1999** (Document 5019/01 – WP 46).

13 September 2001 - **Opinion 7/2001 on the Draft Commission Decision (version 31 August 2001) on Standard Contractual Clauses for the transfer of personal data to data processors established in third countries under Article 26(4) of Directive 95/46** (Document 5061/01 – WP 47).

13 September 2001 - **Opinion 8/2001 on the processing of personal data in the employment context** (Document 5062/01 – WP 48).

13 September 2001 - **Working Document on IATA Recommended Practice 1774 Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo** (Document 5032/01 – WP 49).

5 November 2001 - **Opinion 9/2001 on the Commission Communication on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"** (Document 5074/01 – WP 51).

13 December 2001 - **Decision 1/2001 on the participation of representatives of Data Protection Supervisory Authorities from the candidate countries in Article 29 Data Protection Working Party meetings** (Document 5080/01 – WP 52).

14 December 2001 - **Opinion 10/2001 on the need for a balanced approach in the fight against terrorism** (Document 5403/01 – WP 53).

Deze documenten zijn te vinden op het onderstaande internetadres: http://europa.eu.int/comm/internal-market/en/dataprot/wpdocs/index.htm

onderzoeksrapporten 1996 - 2001

Elektronische overheid en privacy 10 december 2001

Onrechtmatige handelwijze van een (handels)-informatiebureau juli 2001

Zorg voor gegevens bij indicatiestelling augustus 2000

Politiegegevens beschermd – Een toelichting op het gesloten verstrekkingenregime van de Wet politie-registers juni 2000

Het verstrekken van gegevens door de Belastingdienst aan CAK BZ 27 april 2000

Screening van politiepersoneel moet volgens de regels 9 februari 2000

Controle e-mailverkeer door werkgever 27 december 1999

Is Landelijk Alcohol en Drugs Informatiesysteem een persoonsregistratie? 19 november 1999

Onderzoek naar handelsinformatiebureau Goderie van Groen november 1999

Uitbesteding taken Algemene Bijstandswet 8 september 1999

Werken met gegevens – gegevensuitwisseling tussen CWI's en uitzendbureaus augustus 1999

Bijstandsdossiers en bescherming persoonsgegevens 10 juli 1999

Vastleggen en verstrekken van call detail records 24 juni 1999

Verzekeringsmaatschappij verplicht Arbo-dienst tot registratie en rapportage gegevens 14 juni 1999

Verstrekken van gegevens door deurwaarders 30 juni 1999

Handhavingsteams en persoonsgegevens april 1999

Dealer mag zonder toestemming alleen gegevens aan een auto-importeur verstrekken voor service-ondersteuning 15 februari 1999

Privacyaudit Gemeentelijke Basisadministratie gemeenten Almelo, Breda en Langedijk 5 februari 1999

Privacyaudit Nationaal Schengen Informatiesysteem december 1998

Doorzenden voorlichtingsrapport reclassering na toestemming 21 december 1998

Medicatiebewaking door centrale patiëntenregistratie 27 oktober 1998

Beroepscode psychologen 14 juli 1998

Reglementering en beveiliging persoonsregistraties door ministeries 9 juli 1998

Gegevens over honden en het verstrekken daarvan 8 juli 1998

Gegevens uit controle door de rijksverkeersinspectie 23 juni 1998

Persoonsgebonden clubcard II 28 mei 1998

Persoonsgebonden clubcard 11 februari 1998

Meldpunt Ongebruikelijke Transacties juli 1997

Videocamera's Wallen Amsterdam 21 mei 1997

In beeld gebracht – privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging 27 januari 1997

Als de telefoon wordt opgenomen – regels voor het registreren, meeluisteren en opnemen van telefoongesprekken van werknemers november 1996

Privacy-audit Handelsinformatiebureau juli 1996

Rapporten kunt u doorgaans raadplegen op de website: www.cbpweb.nl.

bijlagen

achtergrondstudies en verkenningen (1994 - 2001)

In de serie Achtergrondstudies en verkenningen zijn verschenen:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

brochures

De Wet bescherming persoonsgegevens, het College bescherming persoonsgegevens
augustus 2001

De functionaris voor de gegevensbescherming
augustus 2001

Mag het een bitje minder zijn? Over Privacy-Enhancing Technologies
december 2001

Privacy: checklist voor de ondernemingsraad
april 2002

informatiebladen

- Geadresseerde reclame
- Verstrekken van personeelsgegevens aan derden
- Camera's op de werkplek
- Het gebruik van kentekengegevens en uw privacy
- Het toetsen van uw kredietwaardigheid (credit-scoring)
- Bemiddeling door het College bescherming persoonsgegevens
- Uw klacht en het College bescherming persoonsgegevens
- De sociale dienst en uw persoonsgegevens
- Belangrijkste verschillen tussen de Wet persoonsregistraties en de Wet bescherming persoonsgegevens voor de betrokkene
- Belangrijkste verschillen tussen de Wet persoonsregistraties en de Wet bescherming persoonsgegevens voor de verantwoordelijke
- Rechten van betrokkene
- Het melden van een gegevensverwerking
- Vrijstellingen
- Voorafgaand onderzoek
- De functionaris voor de gegevensbescherming
- Uw persoonsgegevens beveiligd
- Doorgifte naar derde landen
- Als de politie u vragen stelt over uw klanten of werknemers

Het CBP heeft in 2001 inhoudelijk en financieel bijgedragen aan het tot stand komen van Lex van Almelo, *Ik heb toch niets te verbergen. Privacybescherming in het informatietijdperk* (Sdu Uitgevers, Den Haag 2001). Het boek verscheen op 1 september ter gelegenheid van het van kracht worden van de Wet bescherming persoonsgegevens.

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

bijlagen

publicaties in vakbladen en tijdschriften 2001

Alonso Blas, D., **European DPAs new approach to online privacy**, International Newsletter, Privacy Laws & Business, nr 57, February 2001, p. 12-18.

Alonso Blas, D., **Mechanisms for implementation and international co-operation in the context of data protection: existing mechanisms and mechanisms to be established**, Report prepared as "rapporteur" for The Council of Europe Conference Council of Europe convention 108: present and future, in Warsaw, November 2001 (www.coe.fr), p. 54-68.

Alonso Blas, D., **Towards a uniform application of the European Data Protection rules: the role of the Article 29 Working Party,** Privacy & Informatie, Koninklijke Vermande, jg. 4 2001, nr. 1, p.4-8.

Alonso Blas, D., **Universal effects of the European Data Protection Directive, A decade of research @ the crossroads of law and ICT**, Dumortier, J., F. Robben and M. Taeymans (editors), Larcier, Brussel 2001, p. 23-33.

Borking J.J., **Checklist administratieve organisatie (dl. IV)** in: J.M.A.Berkvens en J. Holvast (red.), De Nieuwe privacywet, Schriftelijke Praktijk Cursus, Eindhoven 2001, p.1-55.

Borking, J.J., **Darf es ein bitchen weniger sein?** Datenschutz und Datensicherheit 2001, nr. 10, p. 607-615.

Borking, J.J., **E-Privacy, wat nu**, in: P.B. Cliteur, It ain't necessarily so, Deventer 2001, p. 285-296.

Borking, J.J., **Geschillenoplossing van offline naar online**, Computerrecht 2001, nr. 5, oktober 2001, p. 240-244.

Borking, J.J. en Charles D. Raab*, **Laws, Pets and other Technologies for Privacy Protection**, Journal of Informatics, Law and Technology (JILT), January 2001 (http://elj.warwick.ac.uk/jilt/01- 1/borking.html)

Borking, J.J., **Mag het een bitje minder zijn? Over Privacy Enhancing Technologies (PET) en de juridische basis van hun gebruik**, Compact, KPMG Information Risk Management / ten Hagen & Stam, Groningen, 2001, nr. 4, p. 8-15.

Borking, J.J., **Mediation**, in: H. Franken e.a., Recht en Computer, Deventer 2001, p. 462-483.

Borking, J.J., Pet: **Het privacy probleem structureel opgelost**, Informatiebeveiliging nr. 5, september 2001, p. 4-8.

Borking, J.J., Pet: **Inzetbaarheid bewezen**, Informatiebeveiliging nr. 5, september 2001, p. 20-24.

Borking, J.J., **Privacy een vol ei of een lege dop**, Emerce (Be an E-leader, dl. 3), 2001, p. 1-2.

Borking, J.J., **Privacy Incorporated Software Agent (PISA)**, Datenschutz und Datensicherheit 2001, nr. 7, p. 411-416.

Borking J.J., **Privacy Incorporated Software Agents**, in: H. Federrath, Designing Privacy Enhancing Technologies, Berlin 2001, p. 130-140.

Borking, J.J., **Proposal for building a privacy guardian for the electronic age**, Privacy Incorporated Software Agent, IT Monitoring, 2001 nr 2. en nr. 3, p. 4-5 en p. 4-5.

Eijk, M.M.M. van, en W.J. van Helden, **WBP en adressenhandel**, In Sight, jg. 2, nr. 4, p. 33-35.

Fontein, M.A.H., **Wet bescherming persoonsgegevens**, Migratie & Integratie, 17.2/100, p. 1-40, aanvulling 13, november 2001.

Gils, H.G.Th. van* en J.P.M.J. Leerentvelt, **Auditor en privacy**, Compact, KPMG Information Risk Management / ten Hagen & Stam, Groningen, 2001, nr. 4, p. 43-48.

Gräve, A.C., **Consequenties van de Wbp voor de bestuurlijke informatievoorziening**, Compact, KPMG Information Risk Management / ten Hagen & Stam, Groningen, 2001, nr. 4, p. 16-21.

Heij, A.C.M. de, **Het WBP-vrijstellingsbesluit,** Privacy & Informatie, Koninklijke Vermande, Lelystad, 2001, nr. 2, p. 59-63.

Helden, W.J. van, **Herkomst van de klant, privacyregels voor ethnomarketing**, Onderzoek, NVMI, maart 2001, p. 34-36.

Hooghiemstra, T.F.M., **Biometrie en privacy: kansen en bedreigingen**, (Smart)Cards in Business, 2001, nr. 1, p. 38-39.

Hooghiemstra, T.F.M., **Patiënten en internet**, Tijdschrift voor Gezondheidsrecht 2001, nr. 7, p. 434 – 445.

Hooghiemstra, T.F.M., en A. ter Linden, **Recht en EPD's in de GGZ**, Nederlands Tijdschrift voor Medische Administratie, jg. 27, 2001, nr. 104, p. 40-44.

Hooghiemstra, T.F.M., **Teksten en toelichting op de Wet bescherming persoonsgegevens** (Koninklijke Vermande, Lelystad, 2001).

Hustinx, P.J., **Article 8 of the Charter: Fundamental data protection and the interaction with Directives 95/46/EC and 97/66/EC,** in: Nizza, die Grundrechte-Charta und ihre Bedeutung für die Medien in Europa / Nice, the Charter of Fundamental Rights and their Importance for the Media in Europe, Schriftenreihe des Instituts für Europäisches Medienrecht (EMR), nr. 23, Nomos Verlagsgesellschaft, Baden-Baden, 2001, p. 89-102.

Hustinx, P.J., **Nieuwe zekerheden voor persoonsgegevens**, Notariaat Magazine, KNB/ Koninklijke Vermande, Den Haag, 2001, nr. 1, p. 16.

Hustinx, P.J., **Privacy, data protection and informational self-determination**, Papers Spring Conference of European Data Protection Commissioners, Athens, 10-11 May 2001, Hellenic Data Protecion Authority, CD-rom.

Hustinx, P.J., **Wet bescherming persoonsgegevens: continuïteit en verandering**, Compact, KPMG Information Risk Management / ten Hagen & Stam, Groningen, 2001, nr. 4, p. 3-7.

Pol, U van de, **Niemand gunt terroristen een ontwrichting van de rechtsstaat**, Nederlands Juristenblad 2001, p. 1893.

Pol, U van de, **Toekomstig toezicht op bescherming van persoonsgegevens; van Registratiekamer naar College bescherming persoonsgegevens**, NJCM-bulletin 2001, p. 1141-1157.

Pol, U van de, **Uitspraak op internet, Media en strafrecht**, KUB, Deventer 2001, p. 159-179.

Pol, U van de, en M. van Stratum, **Corruptiebestrijding met gebruik van persoonsgegevens**, Corruptie: van taboe naar sociale verandering, EUR 2001, p. 51-69.

Pol, U van de, en M. van Stratum, **Privacyregels bij de verwerking van persoonsgegevens ten behoeve van de bestuurlijke aanpak van de georganiseerde criminaliteit**, De bestuurlijke aanpak van (georganiseerde) criminaliteit in Amsterdam, Gemeente Amsterdam, november 2001, p. 53-60.

Zandee, C.G., **Jeugdzorg en jeugdbescherming**, Perspectief, augustus 2001, p. 13.

* In 2001 niet werkzaam bij de Registratiekamer of het CBP.

Review of 2001

More than anything else, the digital revolution influences the way society handles information, including personal data. Citizens and consumers welcome the benefits of digital service provision with open arms. But, at the same time, they worry about the security and confidentiality of on-line services and contacts. Focused on the pursuit of commercial or political objectives, enterprises and governmental organisations are often inclined to regard the protection of privacy as an inconvenience. At the same time, there is a failure to recognise the potential benefits of taking privacy into account from the outset when designing information systems and processes.

Privacy is in fact a success factor. Whether one is concerned with running an electronic government help desk, checking the way employees use e-mail, police powers of investigation, exchanging medical data in connection with employee reintegration, passing on customer information to non-EU countries or selling address information for direct marketing purposes, commercial or administrative success cannot be obtained without ensuring that personal data is handled scrupulously and correctly. Because, unless privacy is adequately protected, it will not be possible to win the trust of the citizen or consumer.

Against this background, the Dutch Data Protection Authority (CBP) presented a study report entitled *Klant te koop, privacyregels voor adressenhandel (Customer for sale: privacy rules for list broking)* to the chairman of the DMSA, the direct marketing industry's representative organisation, at the latter's 2001 Direct Marketing Days. The report was intended to address uncertainties within the industry and to make it clear that the law allowed considerable scope for the buying and selling of address data.

Similarly, it was felt that greater clarity regarding the rules on the transfer of personal data would be beneficial to the business community, which has an interest in the smooth and lawful exchange of information with countries outside the EU. The CBP accordingly published its *Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act* in 2001. As well as dealing with the various issues in turn, the report explained the CBP's role in the permit process for the benefit of enterprises and organisations involved in the transfer of data outside the EU.

Privacy and ICT

In 2001, the CBP also conducted research into the threats to privacy and the opportunities for privacy protection associated with information and communication technology (ICT). The Data Protection Authority published a report entitled *Beveiliging van persoonsgegevens (The Protection of Personal Data)*, which provides a framework for organising information systems to comply with the Dutch Data Protection Act. During the course of the year, considerable exposure was also given to the privacy audit tools developed in collaboration with the public and private sectors for use in the assessment and auditing of information systems.

In addition, the CBP worked hard to publicise the benefits of privacy-enhancing technologies. Such technologies prevent the unnecessary processing of personal data in information systems, and thus serve to bring about *'privacy by design'*. One particularly futuristic initiative in this field is the European PISA Project, in which the CBP has been participating. PISA – Privacy Incorporated Software Agents – was set up with the aim of developing design specifications for autonomous software 'agents', whose 'owners' would be able to perform or authorise electronic transactions of various kinds while retaining control of their personal data.

In the near future, the Netherlands can expect to see the arrival of numerous public and private 'trusted third parties' (TTPs). As the issuers of digital identity certificates, these entities will play a key role. In 2001, the Data Protection Authority accordingly published a report entitled *Sleutels van vertrouwen (The Keys to Trust)*: an initial examination of the implications of the European Privacy Directive and the Dutch Data Protection Act for the TTP sector.

Electronic government

The degree of care exercised by government bodies and other institutions when exchanging personal data has sometimes caused the Data Protection Authority considerable concern. Particularly where a number of institutions exchange personal data on a collaborative basis, it is not always clear who is or may be the controller for which data processing activities. Under such circumstances, efficient data processing can conflict with the subjects' interests and may even be against the law. Before long, collaboration and data exchange between government bodies will have developed to the point where a formal information infrastructure exists. So in 2001, the CBP initiated an investigation of the privacy issues associated with 'electronic government', which will culminate in the publication later this year of a paper setting out its views.

Police records

The gathering of information and the maintenance of records by the police and judicial authorities can have far-reaching consequences for the privacy of the data subjects. The CBP therefore takes a keen interest in this field. The records kept by criminal investigation units (CIEs) represent a particularly serious threat to privacy. Nevertheless, the quality both of the registration activities and of their supervision remained disappointing in 2001. The CBP has, however, noted the gradual development of a willingness to improve matters on the part of the police and judicial authorities. Since the end of the year, a circular issued by the Minister of the Interior and Kingdom Relations has come into effect, requiring the introduction of (external) auditing.

Investigative powers

In the past, companies and other organisations were often asked or ordered by the police and judicial authorities to disclose or allow access to computerised personal data (regarding customers, for example). In many cases, however, such orders were unlawful. The companies in question were consequently placed in a difficult position. Having received numerous complaints, the Data Protection Authority wrote to the Minister of Justice asking for guidance in this area. The Minister has since spoken out against this form of information gathering.
In 2001, the question of police powers was considered by the Committee on the Gathering of Information in Criminal Investigations (the 'Mevis Committee'). The committee suggested that the police and the Public Prosecutions Department should be given extensive powers, enabling them to

Results secured in 2001

IN LAST YEAR'S ANNUAL REPORT, IT WAS ANNOUNCED THAT IN 2001 PRIORITY WOULD BE GIVEN TO SECURING THE FOLLOWING RESULTS:

- **Information campaigns**

Information campaigns linked to the introduction of the Data Protection Act were organised in collaboration with the Ministry of Justice and the Ministry of the Interior and Kingdom Relations. The Data Protection Authority took care of the campaign aimed at representative organisations in the various sectors, focusing on the particular needs of each industry.

- **Website & information material**

The CBP's website (www.cbpweb.nl) has been redesigned and made more accessible. Further improvements are planned for 2002. A comprehensive review of the information on the site has been undertaken, and additional material posted. All the authority's publications are available free of charge on the site.

- **Self-regulation**

A leaflet has been published to help organisations interested in appointing a 'data protection officer', as referred to in Sections 62 and following of the Data Protection Act. Several dozen registrations have since been received and processed. Assessment guidelines have also been drawn up for organisations that are considering the introduction of a code of conduct, as referred to in Section 25 of the Act, and a leaflet is now under development.

- **Data protection & PET**

The report *Beveiliging van persoonsgegevens (The Protection of Personal Data)* explains how a controller should go about providing appropriate protection, as required by Section 13 of the Data Protection Act. A separate leaflet has been produced, dealing with the use of privacy-enhancing technologies (PET). Preparations are also being made for a symposium on this topic.

- **Auditing**

In conjunction with representative organisations and market players, a system for assessing the quality of the data protection arrangements within an organisation has been developed. The products of

require businesses and government departments to assist their enquiries by providing information. The CBP has opposed such a move, however, arguing that statutory regulations are required to ensure that the rights of all interested parties are more clearly defined. Neither commercial nor governmental organisations are simply investigative extensions of the police or the Public Prosecutions Department. Investigative bodies need to show greater sensitivity in the way they handle information. The proposals presently under consideration would result in information being made available regarding many people who were not suspected of any wrongdoing; this would amount to a considerable extension of police and judicial authority, despite the fact that the bodies in question have so far failed to abide by the existing rules.

Confidential communication

If the Telecommunications Data Requisitions Bill were to become law, data concerning telecommunications would be categorically excluded from the constitutional protection afforded to confidential communications. The CBP has always contended that the legislature should be cautious about requiring telecommunications companies to retain data. The authority could not therefore support the government's proposal that Article 13 of the Constitution should be amended, as recommended by the Committee for the Assessment of Constitutional Rights in the Digital Age. The CBP felt that constitutional protection should not be restricted to the content of communications, but should extend to 'traffic data', i.e. information about the communications.

Worker supervision

ICT is increasingly prominent in the modern workplace. One consequence of this is that workers now make daily use of equipment – digital access cards, security cameras, GSM phones, RSI programs and other software – which lends itself to their own supervision. The monitoring of workers' e-mail and Internet use was a very topical issue in 2001. In its contributions to the public debate, the CBP emphasised that each organisation should develop a set of monitoring arrangements, tailored to its particular circumstances. For this purpose, the authority made a range of tools available, which will be offered to organisations again in 2002, but has not involved itself directly in worker supervision.

Occupational disability

During the course of the year, close attention was paid by the CBP to social security-related issues, particularly the reintegration of workers after

this project – *Quickscan, WBP Zelfevaluatie (Data Protection Act Self-evaluation)* and Raamwerk *Privacy Audit (Privacy Audit Framework)* – have been posted on the CBP website and put into use in the field. The possibility of setting up a certification system will be examined in the context of a follow-up project.

- **Data Protection Act reports**

In anticipation of the new Data Protection Act coming into force, special software was developed for use by anyone who has to report the processing of personal data to the CBP in accordance with the Act. With the software, the user can draw up a standardised report and submit it on diskette. The program comes with guidelines designed to help the user decide whether an activity is exempt from the reporting requirement. These guidelines can also be consulted on the CBP website. New report forms and explanatory information have also been developed.

- **Enforcement**

Provisional versions of the processes for issuing orders and imposing penalties have been developed and are now being introduced. The policies and principles that the CBP is to follow in the exercise of its powers in these areas will be published in the course of 2002.

- **Working methods and procedures**

The working methods and procedures that the CBP is to follow in the performance of its other duties and the exercise of its other powers have been defined and are being introduced in stages. The underlying principles and policies will be published in the course of 2002.

- **Third countries**

A policy statement on data transfers to third countries (as referred to in Sections 76 and 77 of the Data Protection Act) has been posted on the CBP website. A leaflet and information sheet on the same topic are also available from the site. Dutch and English-language printed versions are currently being prepared.

- **Management and organisation**

A management charter has been developed and since approved by the Minister of Justice. An organisational and staffing plan has also been drawn up, on the basis of which a system of competence management will be introduced.

Targets for 2002

THE MAIN RESULTS THAT THE CBP WILL PURSUE IN 2002 ARE AS FOLLOWS:

- **Electronic government**

The use of ICT can make the government more accessible, more effective and more client-oriented, while also reducing the administrative burden for companies and institutions. The CBP will publish a review of the privacy issues associated with electronic government, with a view to assisting the identification of promising solutions and opportunities for improvement.

- **ICT in healthcare**

Changes are also taking place in the healthcare sector, which could have far-reaching consequences for privacy protection. The CBP will seek to contribute to balanced progress in this field by preparing a publication devoted to the use of ICT in the sector.

- **Research and statistics**

As interest in results and effects increases, more scientific and statistical research is undertaken. The CBP will produce a framework document setting out the legal rules on the use of personal data in the context of scientific and statistical research.

- **Workers**

Privacy at work will be addressed, with the release of new versions of the report on the supervision of workers' use of e-mail and the Internet, and of the privacy checklist for staff councils. Preparations will also be made for the publication of information regarding the position of employees on sick leave.

- **Trade information**

Research has revealed a need for clarification of the legal situation as regards the processing of personal data by trade information agencies. The CBP will work towards the availability of clear guidelines on the lawful processing of personal data drawn up for use by those active in this field.

- **Telecommunications use**

The CBP will undertake exploratory research into the processing of

periods of occupational disability. The first structural changes took effect on 1 January 2002, when the SUWI (Work and Income Implementation Structure) Act came into force. The CBP urged the government to ensure the total transparency of the data flows associated with the Act. It should be clear to everyone involved – individuals, institutions and companies – just what information can lawfully be exchanged, between whom and for what purposes. Clarity in these matters can be achieved by the
careful formulation of regulations defining the permissible aims of information provision.

Increasingly, the occupational reintegration of people who have been unfit for work for extended periods is contracted out to private companies. When advising the government on various legislative issues, the CBP has repeatedly underlined the need for specific regulations – preferably based in legislation – covering the exchange of information in the context of reintegration activities. Someone who is being reintegrated is in a vulnerable position, and the data that is being exchanged is essentially of a medical nature. The evident conflict between the need to protect privacy and the need to help people back to work is such that the providers of reintegration services would benefit from guidance. To date, however, no such guidance has been made available.

Care referral

ICT is ever more commonplace in the healthcare sector. It is not only regional and national electronic registers and market forces that are relevant in this context; waiting lists and care referrals have also been the subjects of intense debate. Indeed, the collection and distribution of highly sensitive data are involved in both cases. In many instances, medical confidentiality is at issue. Furthermore, a patient's right to privacy requires structural protection. Otherwise, in a complex and rapidly automating sector where efficiency is prioritised and sizeable financial interests are at stake, the patient's need for care will tend to preclude the assertion of his or her right to privacy.

personal data concerning telecommunications use, in particular billing data. The findings will be presented at a workshop for experts and representatives of organisations active in the sector.

- **Special police records**

The police's control of the records of 'criminal investigations' could be improved, with a view to enhancing both privacy protection and the investigation of crime. The CBP would like to see better structural supervision of such records and more efficient arrangements for processing requests for access to such records.

- **Public register of WBP reports**

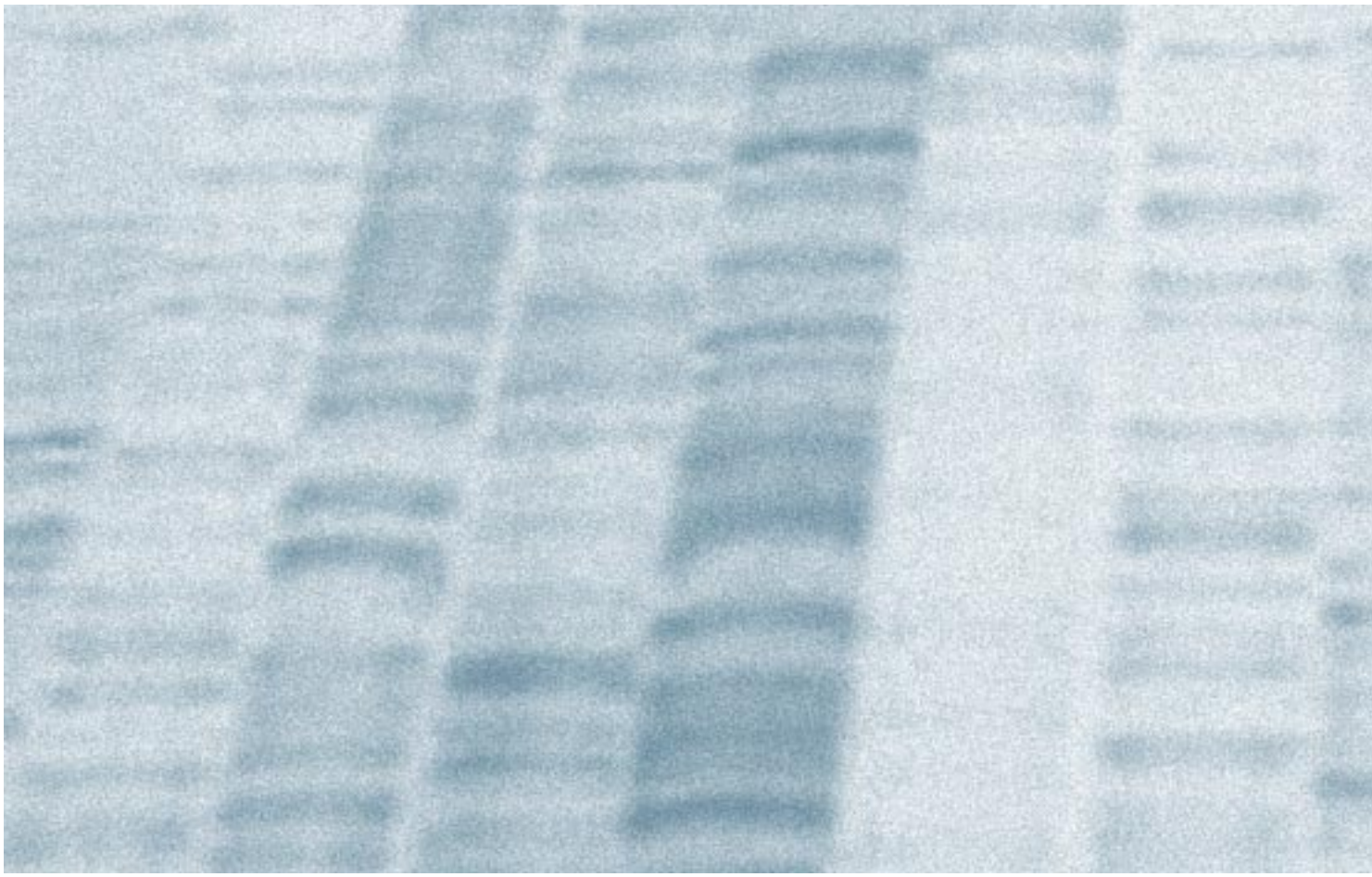
An open-access public register of data processing activities reported to the CBP in accordance with the new Data Protection Act (WBP) will be set up on the authority's website. An improved version of the software for submitting reports on diskette will be released and Internet reporting will be enabled.

- **Preliminary investigation**

Details of the experience gained with the preliminary investigation of processing activities that entail special risks (as referred to in Sections 31 and 32 of the Data Protection Act) will be published on the CBP website. Where possible, standards on common processing operations will be developed in conjunction with the interested parties.

- **Enforcement plan**

The CBP will create the conditions for the systematic monitoring of compliance with the statutory reporting requirements. These conditions will be described in an enforcement plan, which will also give details of various other activities in the field of supervision, investigation and intervention.



COLOFON

Jaarverslag 2001

College bescherming persoonsgegevens, Den Haag, mei 2002.

Met medewerking van:
S.M. Artz, J.H.M. Baart, E.T.H.M. Bool,
M.M.M. van Eijk, M.A.H. Fontijn, W.J. van Helden,
T.F.M. Hooghiemstra, B.J.P. Hulsman
P.J. Hustinx, P. Krul, L.E. van Laviere,
S. Lieon, U. van de Pol, C.E. Romanesko,
A. Tempelman, J.A.G. Versmissen en J. de Zeeuw

Eindredactie: G.O. van de Klashorst

Ontwerp: Proforma, strategie, ontwerp en management (Miriam Monster)
Druk: Sdu Grafisch Bedrijf bv, Den Haag
Fotografie: Dieter Schütte, Rotterdam
Fotografie college: Martijn Beekman, Den Haag

Het College bescherming persoonsgegevens (CBP) – onder de Wet bescherming persoonsgegevens (WBP) de opvolger van de Registratiekamer – houdt 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 zo-nodig 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 uit-voering 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 website: www.cbpweb.nl.