jaarverslag 2002

INHOUD

COLLEGE BESCHERMING PERSOONSGEGEVENS

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

Het College bescherming persoonsgegevens (CBP) legt hierbij verslag over zijn beleid en activiteiten in 2002, het eerste volledige werkjaar onder de Wet bescherming persoonsgegevens (WBP). Naast continuïteit in vertrouwde activiteiten bracht 2002 ook nieuwe taken met zich mee. Verder heeft het CBP zich voorbereid op een adequate inzet van de nieuwe handhavingsbevoegdheden.

Het toezicht op privacybescherming raakt aan alle maatschappelijke sectoren. Deze breedte van het werkterrein noopt de toezichthouder tot selectiviteit bij de inzet van de beperkte middelen. De WBP legt de verantwoordelijkheid voor privacybescherming bij de organisaties die persoonsgegevens verwerken. Het CBP kon in 2002 op zeer veel plaatsen positieve inspanningen constateren om gevolg te geven aan de WBP. Voorspoedig is ook de gestage groei van het aantal functionarissen voor de gegevensbescherming tot inmiddels ruim honderd. Deze interne toezichthouders zullen naar verwachting een belangrijke eigen bijdrage leveren aan de bescherming van persoonsgegevens in grote organisaties.

Het CBP is erkentelijk dat de Minister van Justitie het bestuursreglement in het voorjaar van 2002 heeft goedgekeurd. Het reglement voorziet onder meer in waarborgen tegen vermenging van de toezichthoudende, adviserende en sanctionerende taken van het College. De regeling brengt ook de onafhankelijkheid van het CBP als toezichthouder in balans met de verantwoordelijkheid van de Minister voor de financiering van de bedrijfsvoering.

Met voldoening wordt hier vermeld dat de Minister van Justitie met steun van de Tweede Kamer deze regeling van de bestuurlijke relatie in het najaar van 2002 heeft gecompleteerd met de toekenning van een budget dat past bij de nieuwe taken en bevoegdheden. Het CBP is hierdoor in staat een noodzakelijke ontwikkeling van de organisatie te realiseren. CBP dankt een ieder, zowel binnen als buiten de organisatie, die hieraan heeft bijgedragen.

mr. P.J. Hustinx
voorzitter
College bescherming persoonsgegevens

HET COLLEGE VERGADERT

samenstelling

college en raad van advies

college 2002

mr. P.J. Hustinx
voorzitter van het college

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

drs. J.W. Broekema
lid van het college

raad van advies 2002

R. Bandell
burgemeester van Dordrecht

prof. dr. T.M.A. Bemelmans
hoogleraar bestuurlijke informatiesystemen
Technische Universiteit Eindhoven

mr. G.J.M. Corstens
raadsheer Hoge Raad

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

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

prof. mr. H. Franken
hoogleraar informaticarecht Rijksuniversiteit Leiden

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

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

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

drs. A.I.M. Kool
oud-lid Verzekeringskamer

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

drs. C.R. Rog
voorzitter commissie privacy VNO-NCW

D. Westendorp
oud-directeur Consumentenbond

buitengewone leden college 2002

drs. J.J. Borking
ICT; Privacy-Enhancing Technologies

prof. A.W. Neisingh RE RA
privacyaudits

H. de Zwart RE RA RO
privacyaudits

2002 in vogelvlucht

De politiek-maatschappelijke discussie draaide in 2002 vooral om veiligheid. In de algemene roep om meer daadkracht, toezicht en controle maakten diverse vooraanstaande bestuurders en politici van privacy een karikatuur. Privacybescherming zou meer veiligheid voor de burger in de weg staan; privacywetgeving moest daarom worden aangepakt. Het kabinet stelde in november voor een algemene identificatieplicht in te voeren voor alle burgers ouder dan 12 jaar. Met het oog op misdaad- en terrorismebestrijding zouden alle telecommunicatiegegevens van iedereen langdurig bewaard moeten blijven. Het CBP maakt zich ernstige zorgen over de gevolgen die een gemakzuchtige vlucht in meer politiebevoegdheden voor de belangen en rechten van gewone burgers kan hebben.

Het CBP maakt verder ernstig bezwaar tegen de suggestie dat juist privacybescherming de samenwerking van verschillende instanties bij het oplossen van maatschappelijke problemen zou belemmeren. Het is de overtuiging en de ervaring van het CBP dat privacybescherming een van de succesfactoren is voor een effectief overheidsoptreden. Privacyregels hoeven aan weinig legitieme overheidsdoelstellingen in de weg te staan. Wel dient vanaf het begin rekening met deze regels gehouden te worden, zowel bij het ontwerpen van organisatiestructuren, informatiesystemen en procedures als bij het opstellen van beleid.

Privacy en veiligheid

Het privacybelang van burgers wordt altijd afgewogen tegen andere zwaarwegende belangen. De Nederlandse grondwet, internationale verdragen, Europese richtlijnen en de privacywetgeving stellen eisen aan deze afweging. Dit maakt deel uit van de spelregels voor de overheid in de omgang met haar burgers. Privacyregels eisen dat goed wordt nagedacht over doel, effectiviteit en evenredigheid van overheidsmaatregelen en dat er voldoende waarborgen komen tegen misbruik. Wie de privacywetgeving op de helling wil zetten, zegt in feite dat deze vragen overbodig zijn.

Een onzorgvuldige omgang met de privacy van de burger stelt diens vertrouwen in de overheid op termijn in de waagschaal. Burgers die niets te verbergen hebben, verdienen een overheid die privacybescherming vanzelfsprekend meeneemt bij het ontwerp van maatregelen, informatiesystemen of verplichtingen voor burgers.

Het recht op 'privacy' is dus een essentieel onderdeel van de 'veiligheid' die een democratische rechtsstaat zijn burgers te bieden heeft. Wie het recht op privacy onderuit haalt, berooft de goedwillende burger van een belangrijke waarborg en zaagt aan de poten van de democratische rechtsstaat.

Identificatieplicht

In december 2002 werd een wetsvoorstel ontworpen voor een algehele identificatieplicht. Het CBP adviseerde begin 2003 het voorstel niet in te dienen. Het evenwicht tussen rechten en plichten voor burger en overheid is hier zoek. Burgers wordt een permanente verplichting opgelegd zonder motivering waarom specifieke verplichtingen niet voldoende zijn. Strafbaarstelling van het niet nakomen van de identificatieplicht leidt tot een situatie waarin iedere burger naar believen als verdachte kan worden bejegend.

De Nederlandse discussie over een beperkte of algemene identificatieplicht is zeker al twintig jaar oud. Steeds werd op goede gronden geconcludeerd dat een algemene identificatieplicht te ver ging. Aangezien in het voorstel ook geen nieuwe argumenten werden aangedragen, voldeed het kabinet niet aan de eis van het Europees Verdrag voor de Rechten van de Mens om de inbreuk op de persoonlijke levenssfeer voldoende te rechtvaardigen.

Cameratoezicht op openbare plaatsen

Publiek cameratoezicht blijft onverminderd in de belangstelling en zal wettelijk beter worden geregeld. Als middel om veiligheid en openbare orde te bevorderen werd het allerwegen geaccepteerd hoewel de eerste evaluaties van cameraprojecten de veiligheidseffecten ervan relativeren.

Tweemaal bracht het CBP in 2002 advies uit over het wetsvoorstel cameratoezicht op openbare plaatsen. Vanuit het oogpunt van rechtszekerheid is een wettelijk kader van belang. Het CBP kon zich goed verenigen met de toekenning van de bevoegdheid tot plaatsing van camera's aan de burgemeester op basis van een verordening van de raad. Een dergelijke toedeling komt overeen met de verantwoordelijkheid van de burgemeester voor de handhaving van de openbare orde.

Onder de reikwijdte van het cameratoezicht bleken ook de kerken en vergelijkbare plaatsen te vallen. Is het de bedoeling dat de overheid met het oog op de openbare orde camera's kan plaatsen in kerken, moskeeen en andere gebouwen bestemd voor de belijdenis van een levensovertuiging?

Elektronische overheid

De overheid brengt langzaam maar zeker steeds meer structuur aan in haar informatiehuishouding met het oog op een efficiënte en betrouwbare taakvervulling. Deze ontwikkeling brengt belangrijke kansen en bedreigingen met zich mee voor de bescherming van persoonsgegevens. In 2002 heeft het CBP een uitgewerkte visie neergelegd in de studie *Elektronische overheid en privacy: bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid*. De studie richt zich met name op de beleidsmakers, bespreekt privacy-ontwerpprincipes voor informatiesystemen en geeft een analyse van de speelruimte die de privacyregels bieden.

Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Het CBP heeft daarom reserves ten aanzien van het pleidooi de burger 'de regie' over zijn eigen persoonsgegevens geven. De overheid moet inderdaad zorgen voor optimale transparantie, maar er zijn evidente grenzen aan informationele zelfbeschikking. In de WBP is bewust gekozen voor een systeem van *checks and balances* waarin toestemming en verzet slechts een corrigerende rol spelen. Belangrijker is dat de overheid ook zonder regie-aanwijzingen van de burger transparant en vertrouwenwekkend werkt.

Burgerservicenummer

Het CBP heeft vanuit zijn visie op de elektronische overheid ook een bijdrage geleverd aan het advies van de interdepartementale commissie Van Thijn, *Persoonsnummerbeleid in het kader van identiteitsmanagement*. Het CBP was vertegenwoordigd in de commissie. Het kabinet onderschreef het advies en

Resultaten 2002

IN HET VORIGE JAARVERSLAG IS AANGEKONDIGD DAT IN 2002 ZOU WORDEN GESTREEFD NAAR DE VOLGENDE RESULTATEN:

- **Elektronische overheid**
  In de studie *Elektronische overheid en privacy* heeft het CBP laten zien hoe de overheid door de inzet van ICT beter kan werken met behoud en versterking van privacywaarborgen. Deze visie heeft bijgedragen aan het overheidsbeleid met betrekking tot de stroomlijning van basisgegevens en het gebruik van persoonsnummers.

- **Informatietechnologie in de zorg**
  In de studie *Privacy bij ICT in de zorg* heeft het CBP aangegeven hoe privacybescherming beter kan worden verankerd in de gezondheidszorg. De inhoud van de studie is binnen de sector breed uitgedragen. Tijdige en adequate aandacht voor privacybescherming is een kritische succesfactor bij nieuwe ontwikkelingen op dit terrein.

- **Onderzoek en statistiek**
  In de notitie *Privacy bij wetenschappelijk onderzoek en statistiek* zijn de wettelijke regels voor het gebruik van persoonsgegevens op dit gebied verhelderd. De notitie bevat ook een kader voor de ontwikkeling van een gedragscode waarin die regels naar de praktijk kunnen worden vertaald. De Koninklijke Nederlandse Academie van Wetenschappen heeft hiertoe het initiatief genomen.

- **Werknemers**
  Een nieuwe versie van de studie *Goed werken in netwerken*, een nieuwe *Raamregeling voor het gebruik van e-mail en internet* en de brochure *Privacy: checklist voor de ondernemingsraad* hebben het belang van goede privacybescherming op het werk nadrukkelijk onder de aandacht gebracht. Ook is de basis gelegd voor een publicatie over de positie van zieke werknemers.

- **Handelsinformatie**
  Het is in 2002 nog niet mogelijk gebleken om binnen de branche overeenstemming te bereiken over duidelijke normen voor een rechtmatige verwerking van persoonsgegevens en waarborgen voor een juiste naleving daarvan. De behoefte aan normen en waarborgen is bij onderzoeken opnieuw gebleken. Het CBP heeft hierin aanleiding gevonden om met meer inzet op te treden.

- **Gebruik van telecommunicatie**
  Het CBP heeft een verkennend onderzoek verricht naar de verwerking van gegevens over het gebruik van telecommunicatie. De resultaten hebben ten grondslag gelegen aan een workshop die in september 2002 is georganiseerd samen met het Instituut voor Informatierecht (UvA) en mogelijk werd gemaakt mede door de OPTA. De uitkomst is neergelegd in de studie *Verkeersgegevens* die ook voor het CBP een basis zal vormen voor verdere activiteiten op dit gebied.

kondigde aan in 2003 een voorstel te zullen uitwerken voor een 'burgerservicenummer'.

De invoering van een burgerservicenummer dient de eenduidige identificatie van gegevens van burgers voor een doelmatiger en klantgerichter overheid. Het nummer maakt de koppeling van gegevens tussen overheden mogelijk en is daardoor ook belangrijk voor opsporing en bestrijding van (identiteits)fraude.

Het beoogde sectorale persoonsnummerbeheer is in lijn met de visie van het CBP op de elektronische overheid en de voorkeur voor sector- en ketennummers. De sectoren Justitie en Zorg zullen volgens het advies aparte sectornummers gebruiken. De rechtmatige verwerking van gegevens zal bevorderd worden door de vertrouwensfuncties, die onder meer bestaan uit Privacy-Enhancing Technologies, dus technische privacywaarborgen in de informatiesystemen zelf.

Dossiers van de sociale dienst

In de sfeer van de sociale zekerheid is diepgaande controle van individuen noodzakelijk. In februari 2002 werd een dossieronderzoek uitgevoerd bij drie sociale diensten. Onderzocht werd of de gegevens in de dossiers noodzakelijk waren voor de vaststelling van het recht op bijstand (noodzakelijkheidsvereiste). Verder is nagegaan van welke instanties de sociale diensten gegevens ontvingen en aan welke instanties zij gegevens verstrekten. Het CBP heeft een positieve indruk gekregen van de wijze waarop de drie sociale diensten met persoonsgegevens omgaan, maar overweegt wel over enige tijd een handhavingsonderzoek te doen bij sociale diensten.

- **Bijzondere politieregisters**
  In 2002 zijn verbeteringen zichtbaar geworden bij de politieregisters met 'criminele inlichtingen'. Zowel het beheer als het structurele toezicht op deze registers hebben bij de meeste korpsen meer aandacht gekregen. Ook is overeenstemming bereikt over een stroomlijning van de behandeling van verzoeken om inzage door betrokkenen. De resultaten zijn binnen de politie en het Openbaar Ministerie breed uitgedragen.

- **Openbaar register van WBP-meldingen**
  Op de CBP-website is een openbaar register van ontvangen meldingen voor iedereen toegankelijk geworden. Naast een verbeterde versie van het WBP-meldingenprogramma op diskette is nu ook een melding via internet mogelijk. Het aantal meldingen is in de loop van 2002 sterk toegenomen. De CBP-website bevat ook een openbaar register van functionarissen voor de gegevensbescherming.

- **Voorafgaand onderzoek**
  Het aantal voorafgaande onderzoeken naar verwerkingen met bijzondere risico's (artikelen 31-32 WBP) is sterk toegenomen. Een overzicht zal in de loop van 2003 op de CBP-website verschijnen. Voor een aantal veel voorkomende verwerkingen zijn in overleg met belanghebbenden inmiddels standaarden ontwikkeld (bijv. sociale recherche van de Gemeentelijke Sociale Diensten).

- **Handhavingsplan**
  In 2002 is een afdeling Interventie, bezwaar en beroep in het leven geroepen. De ontwikkeling van een handhavingsplan heeft inmiddels geleid tot een aantal instrumenten die het CBP in staat stellen om zijn nieuwe bevoegdheden effectief te gebruiken. Ook is een begin gemaakt met een systematische controle op de naleving van de meldingsplicht.

Jeugdzorg: intaketeams en informatie-uitwisseling

Het Bureau Jeugdzorg zal met de invoering van de nieuwe Wet op de jeugdzorg de hulpvraag van jeugdigen vertalen in een indicatie voor de gewenste zorg. Het inrichten van één 'balie' betekent dat de verschillende soorten zorg bij de Bureaus Jeugdzorg vertegenwoordigd zullen zijn: jeugdbescherming, jeugdhulpverlening en de jeugd Geestelijke Gezondheidszorg. Het doel is een multidisciplinaire diagnostiek.
De bij deze intake betrokken hulpverleners werken vaak voor een instelling in een van de vertegenwoordigde sectoren maar fungeren ook als medewerkers van het bureau. In een dergelijke dubbele functie ontstaat in de praktijk gemakkelijk het idee dat informatie over reeds bekende cliënten voor de intake onderling mag worden uitgewisseld.
Wanneer de hulpvrager al bekend is bij een van de 'intakers', heeft deze een flink dilemma. Als in het intaketeam de 'eigen' cliënt ter sprake komt, heeft hij enerzijds te maken met zijn beroepsgeheim, anderzijds met de verwachting, mogelijk ook de neiging, om informatie over de cliënt die al eerder is verkregen bij de intake te gebruiken. Een van de betrokken hulpverleners legde de situatie voor aan het CBP.
Het inrichten van een Bureau Jeugdzorg betekent niet dat persoonsgegevens onbeperkt uitgewisseld kunnen worden. Het beroepsgeheim geldt onverkort, ook in dergelijke dubbelfuncties. Bij het eerste contact met de hulpvrager zou bijvoorbeeld kunnen worden gevraagd naar eerdere ervaringen met jeugdzorg. Door gerichte samenstelling van het intaketeam kan het dilemma vermeden worden.
Bij het eerste contact moet ook toestemming worden gevraagd om eventueel informatie in te winnen bij een eerdere behandelaar. Ook doorverwijzing vanuit de instellingen naar het intaketeam kan alleen met inachtneming van het beroepsgeheim. Toestemming van de betrokkene voor het verstrekken van gegevens aan het intaketeam betekent niet dat daarmee ook toestemming is gegeven voor verdere verstrekkingen. Steeds zal moeten worden bezien of opnieuw toestemming nodig is of dat een andere grondslag verdere verstrekking rechtvaardigt.
Het Bureau Jeugdzorg zal de gegevens bij hulpvragers kunnen verzamelen die noodzakelijk zijn voor intake en indicatiestelling. Doorverstrekking van deze gegevens, voor zover noodzakelijk voor zorgtoewijzing en zorgverlening, is onder voorwaarden ook mogelijk. Een belangrijke voorwaarde is dat hulpvragers vooraf op de hoogte zijn gebracht van de gang van zaken. Degene aan wie de gegevens verstrekt worden, moet bovendien direct betrokken zijn bij de aan de betreffende jeugdige aan te bieden zorg ●

Een nieuwe bijstandswet

Eind 2002 heeft het CBP geadviseerd over het voorstel voor een nieuwe bijstandswet, inmiddels Wet werk en inkomen geheten. De nieuwe wet zal een groot aantal bestaande wettelijke regelingen vervangen. Door gemeenten een grotere bewegingsvrijheid te geven bij de invulling van de individuele rechten en plichten en bij het aanbieden van voorzieningen beoogt het kabinet de reintegratie van werkzoekenden te versnellen.ïntegratie van werkzoekenden te versnellen.

Het CBP had de Minister van Sociale Zaken en Werkgelegenheid al verscheidene malen verzocht om heldere regels te stellen voor de overdracht van persoonsgegevens bij reintegratie.Het moest constateren dat ook dit wets-ïntegratie. Het moest constater voorstel geen helderheid geeft over hoe gegevensverwerking bij reintegratie praktisch vorm dient te krijgen. Veel lijkt overgelaten te worden aan de gemeenten. Hierin schuilt het gevaar dat er verschillen tussen gemeenten optreden bij de uitvoering van de reintegratietaak.

Sociale recherche en fraudeteams

De strijd tegen fraude bij de sociale zekerheid stond in 2002 sterk in de belangstelling. Deze fraudebestrijding wordt uitgevoerd door allerlei organisaties. Het gaat om de (gemeentelijke) sociale recherches, de Regionale Interdisciplinaire Fraudeteams (RIF) en de Sociale Inlichtingen- en Opsporingsdienst (SIOD). Het CBP heeft in het kader van de melding van enkele informatieverwerkingen een voorafgaand onderzoek verricht ter beoordeling van de rechtmatigheid van de inrichting van de verwerking. Vergelijkbaar onderzoek werd gestart naar de rechercheactiviteiten van het Uitvoeringsinstituut Werknemersverzekeringen en de Sociale Verzekeringsbank.

Het CBP heeft onderzoek gedaan naar de procesbeschrijving voor heimelijke waarneming die door één van RIF's was opgesteld, en de daaruit voortvloeiende werkwijze beoordeeld. De naleving van de procesbeschrijving bood in beginsel voldoende waarborgen voor een rechtmatige verwerking van persoonsgegevens. Afgesproken werd dat de procesbeschrijving ook voor andere RIF's als leidraad kon dienen. Een dergelijke aanpak heeft het CBP ook gevolgd ten aanzien van de sociale recherches van de gemeenten.

Belangrijke winst van de gekozen benadering kan een brede, landelijke harmonisering zijn van de werkwijze bij heimelijke waarneming van de RIF's en van de (gemeentelijke) sociale recherches. Rechtszekerheid en het nalevingsniveau van de WBP worden hierdoor bevorderd terwijl de noodzakelijke melding eenvoudiger kan worden afgehandeld.

Zwarte lijsten

Ook het bedrijfsleven zocht in 2002 nadrukkelijk naar maatregelen tegen criminaliteit. Tegen de achtergrond van onvrede over wat politie en justitie voor bedrijven konden doen, groeide de behoefte om zelf paal en perk te stellen aan wangedrag en fraude van klanten of eigen personeelsleden. Zwarte lijsten worden gezien als deel van de oplossing. Het CBP heeft in 2002 onder meer nauwkeurig gekeken naar de zwarte lijst van de gezamenlijke financiële instellingen.

Dat bedrijven bij het voeren van zwarte lijsten een gerechtvaardigd belang kunnen hebben staat eigenlijk niet ter discussie. De vraag is vooral of het belang van het bedrijf opweegt tegen de individuele consequenties van plaatsing op een zwarte lijst. Als besloten wordt een zwarte lijst in te voeren, moet het bedrijf waarborgen treffen om een dergelijk systeem zorgvuldig te gebruiken. Zonder dergelijke waarborgen is een zwarte lijst verboden.

Waarschuwingslijsten als middel tegen frauderende werknemers kregen veel publiciteit. Het CBP heeft diverse lijsten beoordeeld. De gevolgen van plaatsing worden sterk bepaald door de reikwijdte van de zwarte lijst. Deze kan gelden voor noodzakelijke functies of voor alle werknemers, voor een bedrijf al dan niet met filialen, een concern of zelfs een hele bedrijfstak. De criteria voor plaatsing moeten strikter worden wanneer de reikwijdte van de lijst toeneemt.

Goed werken in netwerken

Goede motivering en inrichting van controle kan voorkomen dat noodzakelijke fraudebestrijding de relatie met werknemers onnodig belast. Een goede afweging van belangen is hierbij de sleutel. Een verantwoorde controle op (privé)gebruik van e-mail en internet op het werk vereist een privacytoets en goed overleg met de werknemers of de instemming van de ondernemingsraad. Om een goede regeling binnen bedrijven te bevorderen publiceerde het CBP in 2002 een geactualiseerde versie van *Goed werken in netwerken*, een nieuwe *Raamregeling voor het gebruik van e-mail en internet* en de brochure *Privacy: checklist voor de ondernemingsraad*. Voor deze handreikingen bleek in 2002 grote belangstelling.

Privacy bij ICT in de zorg

In 2002 publiceerde het CBP ook de studie *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg*. Doel van de studie is een overzicht van de privacyaspecten van de toepassing van ICT in de zorg. De vele beleidsvoornemens,

experimenten en trends bij ICT in de zorg zullen leiden tot een elektronische identiteitsinfrastructuur, een elektronische informatie-infrastructuur en veranderingen in de organisatie en de financiering van de zorg. Bij de huidige ICT-toepassingen is privacy onvoldoende als ontwerpcriterium meegenomen. Tijdige én adequate aandacht voor privacybescherming in de zorg is echter een kritische succesfactor.

Bij de stelselherziening gaat het vooral om meer concurrentie tussen aanbieders van zorg en tussen zorgverzekeraars. Vergoeding van de zorg moet worden gerelateerd aan de werkelijk gemaakte kosten. Als onderdeel van de stelselwijziging zal de zogeheten Diagnose-Behandeling Combinatie(DBC)-systematiek worden ingevoerd. Bij de uitwerking van het DBC-concept dient de overheid zich rekenschap te geven van de verschillende rollen van de zorgverzekeraar en de andere partijen in de gezondheidszorg. Gedetailleerde behandelingsgegevens mogen niet zomaar worden verstrekt. De privacywetgeving en het medisch beroepsgeheim stellen dwingend grenzen aan de verwerking van (bijzondere) persoonsgegevens.

Handelsinformatiebureaus

Een ronduit onbevredigende situatie bestaat in de sector van de handelsinformatiebureaus. In 2002 heeft het CBP andermaal bij een bureau een diepgaand onderzoek moeten uitvoeren; elders in dit jaarverslag (p. 22) wordt een impressie gegeven van wat werd aangetroffen. Kennelijk is meer nodig dan incidenteel toezicht om de handelsinformatiebranche zich te laten voegen naar het wettelijke kader voor de verwerking van persoonsgegevens.

Bedrijven hebben een evident belang bij goede creditscoring en verhaalsinformatie. Dat dient echter wel in balans te worden gebracht met het algemene belang dat is gemoeid met een betrouwbaar en integer functioneren van overheden en bedrijven in hun omgang met persoonsgegevens. Een oplossing dient wellicht gezocht te worden in nadere regelgeving voor het verkrijgen van persoonsgegevens voor creditscoring en incasso.

Stadionverbod bij Feijenoord

Misdragingen van supporters, gewelddadigheden door een harde kern van hooligans, voetbalclubs zien zich al jaren genoodzaakt hier tegen op te treden. Een van de middelen die ingezet worden, is het stadionverbod. Een stadionverbod kan wel, maar niet zomaar.
Een stadionverbod kan worden opgelegd door de rechter of door een stadion c.q. voetbalvereniging, een zogenaamd civiel stadionverbod. Een door de rechter opgelegd stadionverbod geldt landelijk. Een dergelijk verbod naar aanleiding van onrechtmatig of hinderlijk gedrag valt onder de bepalingen in de Wet bescherming persoonsgegevens voor strafrechtelijke gegevens. Dat betekent dat het in principe verboden zou zijn deze gegevens te verwerken ten behoeve van derden, in dit geval dus andere clubs die het verbod moeten handhaven. Deze clubs moeten er immers van weten en de gegevens ook verwerken in hun 'zwarte lijst'.

Telecommunicatie

De telecommunicatiesector wordt geconfronteerd met uitgebreide regelgeving op grond van Europese richtlijnen, nationale wetten en jurisprudentie. Het CBP signaleerde onzekerheid in de sector bij het toepassen van de privacynormen. Het CBP zal zich in 2003 inspannen de sector op concrete punten te informeren over de geldende normen. Samen met de OPTA startte het CBP een onderzoek naar de verkoop door KPN van adresgegevens behorende bij zogenaamde 'geheime' nummers voor marketingdoeleinden. Het CBP streeft er naar de samenwerking met de OPTA op het gebied van het toezicht verder uit te werken.

De voornaamste kwestie die in 2002 vanuit privacyoptiek in de sector speelde, was die van het bewaren en gebruiken van verkeersgegevens. Telecomaanbieders verzamelen enorme hoeveelheden gegevens over de telecommunicatie van individuen (vaste en mobiele telefonie en internet), zij bewaren deze gegevens ook na afloop van de communicatie en voor hen is het verdere gebruik van deze gegevens voor allerlei innovatieve diensten van groot commercieel belang. Marketing op basis van telecommunicatiegegevens is van strategische waarde. In 2002 heeft het CBP een verkennende studie gedaan naar het afrekenen en verrekenen van telecommunicatiediensten als oriëntatie op het feitelijke gebruik van verkeersgegevens.

Opsporing en verkeersgegevens

In samenwerking met het CBP organiseerde het Instituut voor Informatierecht van de Universiteit van Amsterdam in september 2002 een seminar over de technische, publiekrechtelijke en strafvorderlijke aspecten van verkeersgegevens. Het CBP pleitte ook bij die gelegenheid voor grote terughoudendheid bij de opslag van verkeersgegevens. Verkeersgegevens geven in de context zeer veel informatie. Het grondrecht op vertrouwelijke communicatie is hierdoor in het geding.

Het verbod op het verwerken van strafrechtelijke gegevens ten behoeve van derden is echter niet van toepassing als onder meer 1) de verwerking plaats vindt door verantwoordelijken met een vergunning voor particuliere beveiligingsorganisaties en recherchebureaus of 2) indien waarborgen zijn getroffen en bij de toezichthouder een voorafgaand onderzoek is aangevraagd.
De Stichting Feijenoord en het Stadion Feijenoord NV zijn samen verantwoordelijk voor het verwerken van dergelijke gegevens. Aangezien alleen het Stadion Feijenoord NV beschikt over de vereiste vergunning is in dit geval het verbod niet van toepassing wanneer voldaan is aan de tweede voorwaarde. Er moest dus bij het CBP een voorafgaand onderzoek worden aangevraagd bij de melding van de zwarte lijst en er moesten passende en specifieke waarborgen zijn getroffen.

Deze waarborgen bleken bij het voorafgaand onderzoek inderdaad aanwezig. Er zijn richtlijnen voor het opleggen van een stadionverbod met heldere criteria om willekeur te voorkomen. Stadionverboden worden opgelegd na overtreding van het toegangsreglement van het stadion. De toegangsvoorwaarden staan op het kaartje vermeld en worden aan het begin van het seizoen aan de kaarthouders toegezonden. Rondom het stadion hangen bij iedere ingang borden met voldoende informatie. Hierdoor is het voor de stadionbezoekers duidelijk wat de spelregels zijn om een stadionverbod te voorkomen. Daarnaast zijn er mogelijkheden voor inzage, correctie en aanvulling van de gegevens voor supporters die op de zwarte lijst komen.
Op grond van deze bevindingen achtte het CBP de door Feijenoord gemelde gegevensverwerking voor het opleggen van stadionverboden rechtmatig ●

Doelen 2003

In 2003 zullen met name de volgende resultaten worden nagestreefd:

- **Wetgevingsadviezen**
  Ingevolge artikel 51 lid 2 WBP moet het CBP om advies worden gevraagd over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. Het CBP zal in overleg met de betrokken departementen de randvoorwaarden ontwikkelen zodat op een adequate wijze invulling gegeven kan worden aan deze verplichting.

- **Functionarissen gegevensbescherming**
  Op grond van de artikelen 62-64 WBP zijn inmiddels meer dan honderd functionarissen voor de gegevensbescherming bij het CBP aangemeld. Het contact met dit groeiend netwerk van interne toezichthouders zal binnen het CBP zodanig worden geborgd, dat zich in de praktijk een goed samenspel tussen functionarissen en het CBP kan ontwikkelen.

- **Cameratoezicht**
  Het aantal gemeenten met cameratoezicht op openbare plaatsen is de afgelopen tijd aanzienlijk toegenomen. Het CBP zal een onderzoek uitvoeren naar de wijze waarop dit camera-toezicht in de praktijk functioneert en hoe met de privacy-aspecten daarvan in verschillende gemeenten wordt omgegaan.

- **Zieke werknemer**
  Door veranderingen in de sociale zekerheid en de samenleving is de positie van werknemers vóór, tijdens en na afloop van ziekte meer onder druk gekomen. Het CBP zal een studie publiceren waarin de privacyaspecten van deze positie centraal zullen staan en waarin de relaties met andere relevante ontwikkelingen op dit terrein zullen worden belicht.

- **Politieregisters**
  In het verlengde van eerdere activiteiten van het CBP met betrekking tot de registers van de Criminele Inlichtingen-eenheden (CIE's), zal een aantal van deze eenheden aan een nadere toets worden onderworpen. Daarbij zal mede gebruik worden gemaakt van de uitkomsten van interne evaluaties van de CIE's.

- **Telecommunicatie**
  Bij het verlenen van diensten op het gebied van de tele-communicatie doen zich in de praktijk verschillende privacy-vragen voor. In samenwerking met de OPTA zal het CBP voorlichtingsmateriaal ontwikkelen om meer duidelijkheid te verschaffen. Het CBP zal ook nadere aandacht besteden aan meldingsplicht en voorafgaande onderzoeken binnen de telecomsector.

- **Certificering**
  Op basis van de uitkomsten van het eerdere project Auditaanpak is de grondslag gelegd voor een systeem van privacycertificering. In samenwerking met aspirant-accreditatieinstellingen zal het CBP dit systeem nader ontwikkelen en gereed maken voor invoering. Doel hiervan is de naleving van privacywetgeving via zelfregulering verder te bevorderen.

- **Internetsite**
  Een goed ingerichte website is een centraal onderdeel van de voorlichtingsstrategie van het CBP. De toegankelijkheid van de CBP-website zal worden verbeterd, onder meer door de intro-ductie van themadossiers en de ontwikkeling van een aparte sectie voor vragen van betrokkenen. Op deze website zal ook het beleid van het CBP met betrekking tot de verschillende zaaksoorten worden bekendgemaakt.

- **Meldingsplicht**
  De verplichting om verwerkingen van persoonsgegevens bij het CBP te melden draagt bij aan transparantie en controleer-baarheid. De handhaving van deze verplichting zal door inzet van systematische controle ter hand worden genomen. In het verlengde daarvan zal gebruik worden gemaakt van de bevoegdheid tot het opleggen van een bestuurlijke boete bij overtredingen.

- **Formatieplan**
  Om een goede uitvoering van nieuwe taken op het terrein van toezicht en handhaving te kunnen verzekeren, zullen de organisatie en formatie van het CBP worden aangepast. In de loop van het jaar zal een nieuw formatieplan met nieuwe of aangepaste functieprofielen worden vastgesteld.

Wie wat bewaart

In de telecommunicatiesector wordt van elk en ieder gesprek een hele reeks technische gegevens – onder andere de nummers van de gelegde verbinding, duur, datum en tijdstip - vastgelegd. Dat is alleen al noodzakelijk voor het sturen van een rekening aan de klanten en voor de verrekening tussen de telecomaanbieders onderling. De verkeersgegevens mogen vervolgens een beperkte tijd bewaard worden voor het geval er discussie over een rekening ontstaat. Dit is bepaald in de Telecommunicatiewet. Deze geeft verder nog ruimte voor het verwerken van deze verkeersgegevens voor de marketing van eigen telecommunicatiediensten op voorwaarde dat de abonnee daarmee heeft ingestemd.
Een van de vele in Nederland actieve telecomaanbieders gaf in de melding van zijn verwerkingen van persoonsgegevens aan dat de verkeersgegevens maar liefst drie jaar bewaard bleven. Een dergelijke termijn is langer dan nodig voor rekeningdoeleinden en voldoet niet aan de hiervoor geldende wettelijke norm. Als voornaamste doel van het zo lang bewaren werd echter genoemd het gebruik van de gegevens voor marketing en verkoop van de eigen diensten. In de algemene voorwaarden bij de overeenkomsten met de abonnees lag dat al vast zodat de klant hiermee akkoord was gegaan.
Het CBP was van oordeel dat dit niet kon gelden als de vereiste vrije en gerichte toestemming van de klant. Een abonnee behoort een reële mogelijkheid te worden geboden zich over het specifieke gebruik van verkeersgegevens voor marketingdoeleinden uit te spreken. Bovendien werd de klant op geen enkele manier geïnformeerd over het bewaren van de gegevens en het doel daarvan. Niet duidelijk was dat de gegevens in de praktijk drie jaar bewaard bleven of dat marketingprofielen werden gemaakt.
In het kader van het onderzoek naar de melding, waaruit ook de heimelijke vastlegging van alle telefonische contacten van klanten met de helpdesk bleek, kwam het CBP tot de conclusie dat de gemelde gegevensverwerking een verwerking was zoals bedoeld in artikel 31, eerste lid, sub b WBP: gegevens vastleggen op grond van eigen waarneming zonder de betrokkene daarvan op de hoogte te stellen.
Het advies was de verwerking, die in de gemelde vorm onrechtmatig was, anders in te richten en opnieuw te melden ●

In het klimaat van na *September 11* ontstond een sterke politieke beweging om deze data voor het doel van opsporing en strafvordering zeer lang te doen bewaren. Op Europees niveau werd in 2002 door regeringen gesproken over een systematische bewaarplicht voor de verkeersgegevens van alle telefoongesprekken, faxverkeer, e-mails en overig gebruik van internet. Deze zouden bewaard moeten blijven voor politie, justitie en veiligheidsdiensten. Dit is een ernstige bedreiging van de bescherming van de persoonlijke levenssfeer.

Op 3 september 2002 liet het CBP de Minister van Justitie weten dat het een algemene bewaarplicht voor verkeersgegevens van een jaar of meer oneven-redig en in geen geval toelaatbaar achtte. Op 11 september 2002 gaven de Europese privacytoezichthouders, bijeen in Cardiff, een verklaring van dezelfde strekking uit. Europese regelgeving maakt het bewaren van verkeersgegevens voor het doel van de rechtshandhaving alleen mogelijk voor een beperkte periode en alleen voor zover noodzakelijk, passend en proportioneel in een democratische samenleving.

Privacy-Enhancing Technologies

De afgelopen jaren heeft het CBP veel geinvesteerd in de ontwikkeling en het uitdragen van het concept van de Privacy-Enhancing Technologies (PET). Het door het CBP georganiseerde PET-symposium in mei 2002 liet zien dat deze aanpak zich in de praktijk heeft bewezen en *proven technology* is geworden. PET heeft ook een belangrijke plaats gekregen in het toekomstige persoonsnummerbeleid van de overheid.

Het doel van het symposium was beleidsmakers van overheid en private sector de praktische bruikbaarheid van het PET-concept te laten zien. Door privacyregels mee te nemen in het ontwerp van het informatiesysteem kan immers een rechtmatige verwerking van persoonsgegevens (deels) gegarandeerd worden: *privacy by design*. Vanuit een oogpunt van privacybescherming is het beter dat iets niet kan, dan dat het alleen maar verboden is. Uit de zorgsector werden drie werkende informatiesystemen gepresenteerd; in het internationale gedeelte werden de ervaringen met het PET-concept in Canada en Duitsland belicht.

Certificering

De WBP-assurance producten *WBP Zelfevaluatie* en *Raamwerk Privacy Audit* vonden in 2001 en 2002 gretig aftrek evenals de CBP-studie *Beveiliging van persoonsgegevens (2001)*. Het CBP heeft in 2002 minder aandacht gegeven aan voorlichting over deze auditaanpak en heeft zijn inspanningen vooral gericht op privacycertificering. Daarbij beoogt het CBP commerciële audit-organisaties een kader te bieden voor het verlenen van privacycertificaten. In nauw overleg met de beroepsorganisaties die kunnen optreden als accreditatie-instelling, is het schema opgesteld op basis waarvan auditors geaccrediteerd kunnen worden als privacy auditor. Bij het opstellen van de certificeringseisen speelt het *Raamwerk Privacy Audit* een sleutelrol. De eerste opzet van een certificatieschema is voorbereid en enkele brancheorganisaties zijn bereid als accreditatie-instellingen op te treden voor het erkennen van auditors die de bevoegdheid krijgen om erkende privacycertificaten voor specifieke verwerkingen af te geven.

Gedragscodes

In 2002 is de Gedragscode van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie (Nefarma) als eerste gedragscode onder de WBP voorzien van een goedkeurende verklaring. Een gedragscode dient een uitwerking te geven van de WBP en andere wettelijke bepalingen voor de verwerking van persoonsgegevens specifiek voor de sector. In 2002 is ook uitvoerig overleg gevoerd over een gedragscode met de banken en verzekeraars. In januari 2003 kon deze belangrijke Gedragscode Verwerking Persoonsgegevens Financiële Instellingen worden goedgekeurd.

Ook de Nederlandse Vereniging van Handelsinformatiebureaus heeft in 2002 overleg gevoerd met het CBP over een conceptgedragscode maar resultaat werd helaas nog niet bereikt. Dit klemt te meer gezien de situatie in de sector. Met de branchevereniging van particuliere beveiligings- en recherchebureaus – een onvoldoende gereglementeerde en sterk groeiende sector – werd gewerkt aan een gedragscode evenals met de brancheorganisatie voor reintegratiebedrijven (Borea) en de Koninklijke Beroepsvereniging van Gerechtsdeurwaarders. De verwachting is dat deze gedragscodes in 2003 zullen worden goedgekeurd.

Wetgevingsadvisering

In lijn met het viersporenbeleid stelt het CBP zich pro-actief op als adviseur en onderhoudt het actief contact met de overheid en andere organisaties. In het najaar van 2002 is het CBP gesprekken met de ministeries gestart om de wettelijke adviesfunctie van het CBP onder de aandacht te brengen. Er bleek bij de ministeries niet alleen onbekendheid met de nieuwe regelgeving maar ook onzekerheid over de reikwijdte van de verplichting. Het CBP streeft ernaar de adviesverplichting deel uit te laten maken van de wetgevingsprocedure. Dit moet leiden tot een meer structurele invulling van de adviestaak van het CBP en tot een intensivering van de werkzaamheden op dit terrein.

Sleutelen aan modelcontracten

Multinationals sturen heel wat persoonsgegevens rond tussen Europa en de rest van de wereld. Voor doorgifte van persoonsgegevens aan landen buiten Europa zonder passende privacybescherming is veelal een vergunning nodig. Het CBP beoordeelt de vergunningaanvraag en adviseert de minister over het verlenen ervan. Daarbij kunnen bedrijven een doorgifte regelen op basis van modelcontracten goedgekeurd door de Europese Commissie. Wanneer een modelcontract ongewijzigd wordt gebruikt, wordt in principe de vergunning verleend.

Het CBP ontving een vergunningaanvraag van een multinational waarvan de Nederlandse vestiging financiële diensten verleent. De Nederlandse vestiging wilde gegevens doorgeven aan een zusterorganisatie in de VS, die op zou treden als 'bewerker'. Een bewerker verwerkt persoonsgegevens op instructie en onder verantwoordelijkheid van de opdrachtgever. Het bedrijf had het Europese modelcontract voor doorgifte aan een bewerker gebruikt en daarbij gewijzigd.

Het contract voorzag ook in overdracht van taken en onderaanbesteding door de Amerikaanse bewerker aan anderen. Dat betekent dus een verdere doorgifte van persoonsgegevens waarvoor de Nederlandse vestiging verantwoordelijk blijft. Ook deze derde partijen dienden dus gebonden te worden aan het contract met de verantwoordelijke. De mogelijkheid van de Nederlandse verantwoordelijke om de verwerking van de Amerikaanse bewerker te controleren was ingeperkt. Een audit zou alleen mogelijk zijn als er sprake zou zijn van (onder meer) een risico van ernstig nadeel voor de betrokkene. De mogelijkheid om de bewerker te controleren is echter een belangrijke garantie voor een adequate bescherming. Op basis van het modelcontract kan een betrokkene ook de bewerker voor geleden schade via de Nederlandse rechter aansprakelijk stellen als de gegevensexporteur niet meer aansprakelijk kan worden gesteld. Deze bepaling biedt de betrokkene dus een ruimere mogelijkheid zijn recht te halen en was niet opgenomen in het contract. De bepaling die stelt dat na vergunningverlening het contract niet kan worden gewijzigd, was door de aanvrager geclausuleerd: dit was toegestaan tenzij dit negatieve gevolgen zou hebben voor de bescherming van persoonsgegevens. De ratio van de contractuele waarborgen is echter het garanderen van adequate privacybescherming aan de betrokkenen. Afspraken in het contract die hiervoor bepalend zijn, kunnen dus niet worden gewijzigd nadat de vergunning is verleend. De aanvrager volgde de voorstellen door het doorgiftecontract op deze punten aan te passen. Het CBP bracht daarop een positief advies uit aan de Minister van Justitie, die vervolgens de vergunning voor doorgifte verleende ●

Het College bescherming persoonsgegevens heeft in 2002 voor het eerst een volledig jaar gewerkt op basis van een nieuwe wet en met nieuwe taken en bevoegdheden. Na een schets van de strategische visie en het meerjaren-perspectief zal in dit hoofdstuk daarom vooral aandacht worden besteed aan het beleid van het CBP op het niveau van deze taken en bevoegdheden.

Beleid van de toezichthouder

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

Strategisch belang

De op 1 september 2001 in werking getreden Wet bescherming persoonsgegevens geeft uitvoering aan Richtlijn 95/46/EG. Deze richtlijn beoogt enerzijds bescherming te bieden aan fundamentele rechten en vrijheden van natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens, en anderzijds een vrij verkeer van persoonsgegevens binnen de Europese Unie tot stand te brengen.

De hoofdlijnen van de richtlijn zijn inmiddels verankerd in artikel 8 van het EU Handvest voor de grondrechten. Dit geeft uitdrukking aan de waarde die aan de speciale rechtsbescherming op dit terrein toekomt. Het strategische belang hiervan wordt vergroot door het feit dat voor steeds meer diensten, producten en processen in onze samenleving persoonsgegevens benut worden. Een effectieve doorwerking van privacybescherming in de praktijk is nodig om de rechten en vrijheden van de burger veilig te stellen.

Tegelijk valt op dat belangrijke onderdelen van de actuele beleidsagenda, zoals verbetering van veiligheid, zorg en onderwijs, voor hun verwezenlijking mede afhankelijk zijn van een doelmatig en rechtmatig gebruik van ICT. In die zin is een tijdige inbedding van privacyrandvoorwaarden bij de ontwikkeling van systemen en benodigde wetgeving te zien als een kritische succesfactor. In zijn jaarverslag over 2001 heeft het CBP er reeds op gewezen, dat hetzelfde geldt voor een reeks van andere onderwerpen. De speelruimte die gecreeerd kan worden door 'privacy' vanaf het eerste begin mee te nemen in het ontwerp van informatiesystemen en processen, wordt veelal onderschat.

De implementatie van de richtlijn in de Nederlandse wetgeving moge formeel een feit zijn, de doorwerking daarvan in de praktijk zal een proces van veel langere adem vergen, waarin toezicht en handhaving door het CBP een grote rol zullen moeten spelen. In verband daarmee zal het CBP niet alleen als deskundige adviseur, maar ook als toezichthouder en handhaver een adequate bijdrage moeten kunnen leveren.

Beleidsplan

Om aan zijn taken in de komende jaren op een doeltreffende en resultaatgerichte wijze uitvoering te kunnen geven, heeft het CBP na overleg met zijn Raad van Advies een meerjarig beleidsplan met een voortschrijdend karakter vastgesteld. Dit beleidsplan waarvan de hoofdlijnen in het jaarverslag over 2001 zijn uiteengezet gaat uit van:

- een geintegreerde aanpak van de verschillende taken in het kader van een 'viersporenbeleid' van privacybewustwording, normontwikkeling, technologie en handhaving;
- de stimulering van eigen verantwoordelijkheid van belanghebbenden, eerstelijnsorganisaties, sectorale verbanden en andere stakeholders;
- een toenemende aandacht voor handhaving door uitvoering van onderzoeken naar de naleving van de WBP en het waar nodig opleggen van sancties (bijv. bestuurlijke boeten en bestuursdwang).

Deze strategie betekent een geleidelijke accentverschuiving naar het spoor van de handhaving en een sterkere tweedelijnspositie voor het CBP, die samen moeten leiden tot een 'vliegwieleffect'. Naar mate meer organisaties zich verantwoordelijk gaan voelen voor de privacybescherming, zal de totale aandacht daarvoor toenemen en kan het CBP zich richten op die onderdelen van zijn taak die het meest op zijn weg liggen en het meest zijn aandacht behoeven.

Privacy bedreigt de veiligheid niet

De burgemeester van Rotterdam betoogde in 2002 met kracht dat zijn stad niet veilig te maken was voor gewone burgers zonder aanpassing van de privacy-wetgeving. Dat was daarom het eerste punt van zijn actieplan 'Tien punten voor een veilige stad', dat hij op 4 november presenteerde.
Bij de integrale aanpak van overlast zou het stadsbestuur oplopen tegen "doorgeschoten" privacy-wetgeving. Doorgeschoten, omdat er grenzen zijn aan de informatie-uitwisseling tussen de betrokken instanties en omdat de rechter een bepaald gebruik van persoonsgegevens kan verbieden. De burgemeester gaf daarbij twee voorbeelden: de aanpak van lastige verslaafden en de aanpak van malafide huiseigenaren.
Bij een integrale aanpak van verslaafden is informatie-uitwisseling tussen hulpverlening en politie en justitie echter wel degelijk mogelijk. Het vereist alleen een zorgvuldige afweging. Het wettelijk beschermd beroepsgeheim van hulpverleners laat niet toe een medisch dossier aan de politie te geven. Het beroepsgeheim geeft wel ruimte om informatie over (mogelijke) hulpverlening met politie en justitie uit te wisselen als dat ook in het belang van de cliënt is. Toestemming van de cliënt hiervoor zou ideaal zijn, maar uitwisseling kan ook op grond van een door de hulpverleners gemaakte afweging van de in het geding zijnde belangen. In Amsterdam zijn bij de bestrijding van extreme overlast structurele afspraken hierover gemaakt met hulpverlenende instanties.
Bij de aanpak van malafide huiseigenaren is uitwisseling tussen instanties ook mogelijk, zoals bijvoorbeeld in de Amsterdamse 'Zoeklicht'-acties al gebeurt.
Het CBP heeft zich in 2002 ook al positief uitgelaten over aanpak en uitvoering van het Rotterdamse Alijda-project in de wijk Spangen. Samenwerking tussen overheidsinstanties is mogelijk daar waar hun taken en bevoegdheden op elkaar aansluiten of overlappen. Deze samenwerking zal doorgaans ook uitwisseling van informatie kunnen en mogen betreffen. Het beste is voor informatieverwerking op deze grondslag tevoren een reglement of een doordachte procesbeschrijving op te stellen.
Strafrechtelijke informatie, met name over het strafblad, is aan bijzondere wettelijke beperkingen gebonden. De Minister van Justitie bereidt een wet voor die bepaalt voor welke doelen en onder welke voorwaarden het Openbaar Ministerie informatie mag verstrekken over onder meer iemands strafblad. Gelet op het overgangsrecht dient deze wet in 2004 van kracht te zijn ●

Het CBP ziet het in dit kader als zijn taak om zelfregulering door maatschappelijke verbanden te stimuleren. De WBP past in dit opzicht goed bij het overheidsbeleid om een middenweg te volgen tussen overheid, markt en samenleving, waarbij op veel terreinen in feite sprake is van 'co-regulering'. Dat betekent tevens dat het CBP in staat moet zijn om op een duidelijke en daadkrachtige wijze zijn adviserende en toezichthoudende rol in dit geheel te spelen.

Het CBP heeft met voldoening mogen constateren dat deze overwegingen gehoor hebben gevonden bij de Minister van Justitie. Na overleg met de Tweede Kamer is immers besloten het budget van het CBP voor 2003 substantieel te verhogen.

De verhouding met de Minister van Justitie is mede onderwerp van het bestuursreglement dat ingevolge artikel 56, derde lid WBP door het CBP in maart 2002 is vastgesteld en kort daarop door de minister is goedgekeurd (zie Stcrt. 2002, nr. 76). Hierbij is voorzien in een regeling van de beheersrelatie met de Minister van Justitie waarbij de eigen verantwoordelijkheid van het CBP voor zijn taakuitoefening onverlet blijft. Via meerjarenplanning wordt gestreefd naar een situatie waarin het CBP zo zelfstandig mogelijk kan functioneren. Over de besteding van middelen en de bereikte resultaten zal in dat kader verantwoording worden afgelegd.

Taakuitoefening

De WBP strekt zich uit over veel sectoren van de samenleving. Het CBP heeft als toezichthouder voorts te maken met de Wet politieregisters, de Wet gemeentelijke basisadministratie persoonsgegevens en andere bijzondere wetten, die al dan niet in samenhang met de WBP van toepassing zijn. Dit leidt ertoe dat het CBP in de praktijk ook te maken heeft met beleidsgebieden van de meeste andere departementen. Het CBP heeft zijn werkzaamheden verdeeld over een aantal aandachtsgebieden, die in het volgende hoofdstuk afzonderlijk aan de orde komen: Openbaar bestuur, Politie en Justitie, Arbeid en Sociale zekerheid, Zorg en Welzijn, Handel en Diensten, Telecommunicatie, Technologie en Audit, en Internationaal.

Op deze terreinen is het CBP in principe steeds belast met een aantal taken, die in de meeste gevallen direct voortvloeien uit de Europese richtlijn. Op een deel van die taken wordt hieronder nader ingegaan. Een beknopt overzicht is opgenomen in het hoofdstuk Organisatie (zie pagina 52).

Wetgevingsadviezen

De verplichting het CBP om advies te vragen over nieuwe wetgeving is in Richtlijn 95/46/EG expliciet voorzien. In artikel 51, tweede lid WBP is deze verplichting toegespitst op voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. Daarbij gaat het niet alleen om de WBP of andere privacywetten en hun uitvoeringsbesluiten, maar om alle wetten en besluiten waarin het verzamelen, vastleggen, uitwisselen of anderszins verwerken van persoonsgegevens een belangrijke rol spelen, of die op dat terrein belangrijke gevolgen kunnen hebben. In het najaar van 2002 heeft het CBP contact opgenomen met de wetgevingsdirecties van alle departementen om deze verplichting onder de aandacht te brengen en concrete afspraken te maken over de invulling daarvan.

In het kader van zijn adviestaak gaat het CBP na of rekening is gehouden met de WBP en andere relevante privacywetten, en indien daarvan is afgeweken, of dit past binnen de richtlijn. Waar ruimte bestaat voor nadere invulling, toetst het CBP of de regeling voldoende duidelijk is en voldoende rekening houdt met privacybelangen. In voorkomende gevallen gaat het CBP na of voldaan is aan artikel 10 Grondwet en artikel 8 EVRM. Zijn bevindingen legt het CBP meestal neer in een schriftelijk advies. Ook komt het voor dat al dan niet in een vroeg stadium mondeling overleg wordt gepleegd, of dat vanuit Tweede of Eerste Kamer wordt gevraagd om een nadere inbreng. Het CBP kan zo bijdragen aan een betere wetgeving.

Gedragscodes

Zelfregulering door middel van gedragscodes voor bepaalde sectoren is een belangrijk instrument om de algemene normen van de WBP naar de praktijk te vertalen en daarvoor binnen een sector zelf de verantwoordelijkheid te dragen. Bij de beoordeling van gedragscodes ingevolge artikel 25 WBP moet het CBP nagaan of de initiatiefnemers voldoende representatief zijn voor de betrokken sector en of deze sector in de code voldoende nauwkeurig is omschreven.

Indien dit het geval is, kan het CBP verklaren dat de gedragscode, gelet op de bijzondere kenmerken van de sector, een juiste uitwerking vormt van de WBP of van andere wettelijke bepalingen over de verwerking van persoonsgegevens. Het CBP stelt zich op het standpunt dat een gedragscode op grond hiervan niet alleen in overeenstemming moet zijn met de wet, maar ook een

concrete uitwerking daarvan dient te bevatten die bijdraagt aan een goede toepassing. In 2002 heeft het CBP een brochure uitgebracht met een toelichting op de eisen waaraan gedragscodes moeten voldoen. Deze brochure is over alle relevante sectoren verspreid en staat ook op de CBP-website.

Melding en voorafgaand onderzoek

Het CBP heeft in de loop van 2002 meer middelen beschikbaar gesteld om op een eenvoudige wijze aan de meldingsplicht te voldoen. Naast een verbeterde versie van het WBP-meldingsprogramma op diskette is nu ook een melding via internet mogelijk. De ontvangen meldingen worden door het CBP getoetst op volledigheid en globaal op aannemelijkheid. Zo nodig wordt gevraagd om een melding aan te vullen of te verbeteren. De overige meldingen worden opgenomen in een openbaar register dat op de CBP-website voor iedereen toegankelijk is. Een nader onderzoek naar de juistheid van een melding wordt alleen ingesteld als daartoe aanleiding bestaat.

Enkele in artikel 31 WBP omschreven categorieën van verwerkingen met bijzondere risico's zijn onderworpen aan een voorafgaand onderzoek naar de rechtmatigheid. Tijdens een vooronderzoek van vier weken wordt dan eerst nagegaan, of het inderdaad gaat om één van de bedoelde verwerkingen en of er aanleiding is om te besluiten tot een nader onderzoek van ten hoogste dertien weken. Dit is bijvoorbeeld niet het geval, als blijkt dat gebruik is gemaakt van een goedgekeurde standaard. Het CBP streeft er dan ook naar om waar mogelijk tot zulke standaarden te komen. Een overzicht van tot dusver opgedane ervaringen op dit gebied zal in de loop van 2003 op de CBP-website beschikbaar komen.

Zo lek als een mandje

Handelsinformatiebureaus leveren doorgaans twee soorten diensten: creditscoring en rapportage van verhaalsinformatie. Een zogenaamde creditscore is een schatting of een consument zijn rekeningen kan betalen. Leveranciers vragen hierom voordat een product op krediet wordt geleverd. De bureaus kijken naar kenmerken zoals het inkomen, de auto, de buurt en gegevens over eerdere betalingsproblemen. Bij een betalingsachterstand bekijken zij voor de leverancier of een debiteur zijn schuld nog kan voldoen. Zij rapporteren deze informatie aan de crediteur om het verhalen van de schuld mogelijk te maken.

Sommige handelsinformatiebureaus gaan zeer indringend te werk. Dit bleek al uit eerdere onderzoeken. In 2002 werd een klacht ingediend door iemand die het rapport met verhaalsinformatie over hem per ongeluk in handen had gekregen. De verhaalsrapportage over de klager bevatte het Sofi-nummer van klager. Bij uitkeringsinstellingen en diverse banken was informatie verkregen waaronder rekeningnummers, saldi, kredietfaciliteiten en bezit van aandelen. De klager was ook geobserveerd in zijn omgeving. Merk, type en kleur van zijn auto waren bekend; bij de Rijksdienst voor het Wegverkeer was ook informatie gevraagd en gekregen. Het bureau bleek desgevraagd van mening dat bij alle instanties informatie mocht worden gevraagd. Het leek kennelijk vanzelfsprekend dat de informatie ook werd verstrekt. Het CBP heeft in 2002 onaangekondigd een onderzoek ter plaatse gedaan. Hierbij werden vele duizenden documenten voor nader onderzoek meegenomen evenals de relevante digitale administratie. De eerste bevindingen maakten duidelijk dat er in feite geen instanties waren waar dit bureau geen informatie kon krijgen. Dit leidde tot rapportages met passages als: "De heer <naam> heeft van 1 september 1999 tot 1 mei 2002 een WAO-uitkering van CADANS te ***

Bijzondere gegevens

Artikel 16 WBP bevat een verbod op de verwerking van bepaalde categorieën van persoonsgegevens (zoals godsdienst, ras, politieke gezindheid, gezondheid en strafrechtelijk verleden), tenzij de wet voorziet in een uitdrukkelijke grondslag. Ingevolge artikel 23, eerste lid, onder e WBP kan het CBP een ontheffing verlenen, indien dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer. Uit de wetsgeschiedenis blijkt dat het hierbij alleen kan gaan om nauwkeurig omschreven gevallen met een beperkte reikwijdte. Besluiten van algemene strekking zijn voorbehouden aan de wetgever in formele zin. Daarbij komt dat een ontheffing naar het oordeel van het CBP alleen in aanmerking komt als andere mogelijkheden, zoals de uitdrukkelijke toestemming van de betrokkene, redelijkerwijs geen uitkomst bieden.

Doorgifte naar derde landen

De regeling in de artikelen 76-78 WBP voor het gegevensverkeer met landen buiten de Europese Unie vloeit rechtstreeks voort uit de Europese richtlijn en is voor Nederland een nieuw verschijnsel. Het CBP heeft daarom in een vroeg stadium geinvesteerd in het scheppen van duidelijkheid over de betekenis van de betrokken bepalingen en de voorwaarden waaronder de Minister van Justitie op grond van artikel 77, tweede lid WBP een vergunning zou kunnen verlenen voor een doorgifte van persoonsgegevens naar een derde land zonder een passend beschermingsniveau. Het CBP brengt hierover steeds advies uit aan de minister. In overleg met de Minister van Justitie is dan ook beleid ontwikkeld dat zijn neerslag heeft gevonden in een beleidsnota, een brochure en een informatieblad die op de CBP-website zowel in het Nederlands als in het Engels beschikbaar zijn. Het CBP is voorts zeer actief bij het overleg in EU-verband over nieuwe instrumenten om het internationale gegevensverkeer op een doelmatige en flexibele wijze te ondersteunen, met behoud van alle nodige waarborgen voor de persoonlijke levenssfeer.

ontvangen. De uitkering werd verstrekt onder registratienummer: <nummer>. Zijn Sofi-nummer is: <nummer>. De uitkering bedroeg laatstelijk 791,05 euro netto per maand. CADANS heeft de WAO-uitkering op laatstgenoemde datum beëindigd omdat men de man minder dan 15% arbeidsongeschikt acht. Verder is bekend geworden dat aangevraagde om een herkeuring heeft verzocht dat zeer waarschijnlijk eind mei zal plaatsvinden" (geanonimiseerd citaat).
Het bleek dat routinematig niet-openbare informatie werd ingewonnen bij justitiële bronnen en bij de Belastingdienst. Ook uitkeringsinstellingen, banken, nutsbedrijven, woningbouwverenigingen, zorgverzekeraars bleken direct of via via toegankelijk. Een dergelijke praktijk kan niet anders dan het vertrouwen in de dienstverlening en de informatiesystemen van overheid en bedrijfsleven ondermijnen. Het CBP heeft het onderzoek in 2003 afgerond en inmiddels actie genomen ●

.NET Passport controle

.NET Passport is een dienst van Microsoft die een bedrijf in staat stelt een bezoeker van zijn website te identificeren en (een deel van) diens gegevens te raadplegen. Het is een zogenaamde online-authenticatiedienst die ervoor zorgt dat bedrijven weten met wie zij online in zee gaan. Voor de consument die zich bij de dienst heeft aangemeld, is het voordeel dat deze zich maar eenmaal hoeft aan te melden bij .NET Passport met één wachtwoord en loginnaam in plaats van apart bij allerlei sites. Ook hoeft niet alle persoonlijke informatie steeds weer te worden ingevoerd; aan het webpaspoort is immers een flink aantal gegevens gekoppeld. Gebruik van bij het systeem aangesloten websites wordt daardoor efficiënter. Informatie, producten en diensten kunnen gemakkelijker op maat worden aangeboden.
.NET Passport veroorzaakte een groeiend onbehagen over de ondoorzichtige verzameling van grote hoeveelheden persoonsgegevens zonder merkbare waarborgen. De veel bekritiseerde dominante marktpositie van Microsoft wakkerde de discussie nog aan. Inmiddels kende de dienst al 40 miljoen accounts van EU-burgers. Gezien het belang van online-authenticatie voor soepele transacties op het internet, besloten de privacytoezichthouders in de landen van de Europese Unie de krachten te bundelen en gezamenlijk – in de zogenaamde Artikel 29-werkgroep in Brussel - de privacyaspecten van de dienst te onderzoeken.
In juni 2002 verscheen een eerste verklaring waarin de punten werden opgesomd die uitgezocht moesten worden: onder andere het informeren van de consument, diens toestemming voor het verzamelen en doorgeven van persoonsgegevens, de hoeveelheid en kwaliteit van de verwerkte gegevens, hoe de consument zijn privacy-

Bemiddeling en klachtbehandeling

Op grond van artikel 47 WBP is het CBP belast met de behandeling van verzoeken om bemiddeling bij geschillen over de uitoefening van het recht op kennisneming en verbetering van persoonsgegevens en over de uitoefening van het recht op verzet. Belanghebbenden kunnen er ook voor kiezen om hun zaak voor te leggen aan de rechter, of gebruik te maken van een geschillenregeling in een door het CBP goedgekeurde gedragscode. Voorts kan het CBP op grond van artikel 60 WBP op verzoek van een belanghebbende een onderzoek instellen naar de naleving van het bepaalde bij of krachtens de wet. Daartoe beschikt het CBP over de nodige onderzoeksbevoegdheden op grond van de WBP en de Algemene wet bestuursrecht.

In beide gevallen gaat het om een bevoegdheid van het CBP en niet om een verplichting. Bij de beoordeling van dergelijke verzoeken gaat het CBP dan ook niet alleen na of is voldaan aan de formele voorwaarden om het verzoek in behandeling te nemen, maar ook of er wel voldoende grond bestaat om aan het verzoek te voldoen. Daarbij wordt bijvoorbeeld nagegaan of verzoeker zijn klacht reeds voldoende duidelijk heeft kenbaar gemaakt aan de verantwoordelijke, en of er voor hem andere en meer voor de hand liggende wegen zijn om zijn belangen te behartigen. Het CBP draagt in elk geval zorg voor een duidelijke motivering van de beslissing en de nodige informatie om betrokkene verder te helpen. De uitgangspunten en beleidsregels die worden gehanteerd bij bemiddeling en klachtbehandeling zullen in de loop van 2003 op de website van het CBP worden bekend gemaakt.

Ambtshalve onderzoeken

Ingevolge artikel 60 WBP heeft het CBP ook de bevoegdheid om uit eigen beweging een onderzoek in te stellen naar de naleving van de wet. In de praktijk komt het geregeld voor, dat het CBP niet direct besluit tot het instellen van een onderzoek, maar eerst de verantwoordelijke om informatie verzoekt. Ook bij klachten is dit vaak de gang van zaken. Niet zelden blijkt deze informele voorronde voldoende om het probleem op te lossen. In andere gevallen heeft het CBP een duidelijker beeld van het probleem gekregen zodat een meer gerichte aanpak van het onderzoek mogelijk is.

rechten (met name dat op verwijdering van gegevens) kon uitoefenen en de beveiliging van de gegevens. Na uitgebreid overleg met Microsoft op 29 januari 2003 kwam de werkgroep met richtlijnen voor online-authenticatiediensten en een verklaring waaruit bleek dat Microsoft had toegezegd zijn .NET Passport te zullen aanpassen. Gebruikers van .NET Passport zullen op korte termijn beter worden geïnformeerd. Ook zullen zij meer kunnen beslissen over het gebruik van hun eigen gegevens door Microsoft en de verstrekking van deze gegevens aan deelnemende websites. Microsoft zal daartoe onder meer technische wijzigingen in het systeem doorvoeren.
De Europese privacytoezichthouders zullen nauwlettend toezien of Microsoft zijn toezeggingen nakomt en in het algemeen de ontwikkeling van online-authenticatie-systemen blijven volgen ●

Bij het uitvoeren van ambtshalve onderzoeken zijn verschillende mogelijkheden bruikbaar, variërend van een briefwisseling tot een diepgaand onderzoek ter plaatse met bijstand van de politie, of een verkennend onderzoek in een bepaalde sector, waarbij bepaalde organisaties binnen die sector in aanmerking komen voor vervolgonderzoek. Het CBP zal in de komende tijd vaker van het hele palet van mogelijkheden gebruik maken op basis van systematische analyse van privacyrisico's en jaarlijks vast te stellen prioriteiten.

Bestuurlijke boetes

Er is een begin gemaakt met een systematische controle op de naleving van de meldingsplicht. Indien de feitelijk geconstateerde situatie niet overeen kwam met het verwachtingsbeeld op basis van de bij het CBP beschikbare kennis van een sector en de toepasselijke vrijstellingen van de meldingsplicht, is dat aan de betrokken sector kenbaar gemaakt. In de loop van 2003 zullen verdere controles worden gehouden en zal ook gebruik worden gemaakt van de bevoegdheid tot oplegging van een bestuurlijke boete bij overtreding van de meldingsplicht. De beleidsregels voor de boeteoplegging zullen op de website van het CBP worden bekend gemaakt.

Dwangsom en bestuursdwang

Het CBP heeft de voorwaarden ontwikkeld om gebruik te maken van de bevoegdheid tot het opleggen van een dwangsom of het toepassen van bestuursdwang bij overtredingen buiten het terrein van de meldingsplicht. Het ligt echter voor de hand om daartoe pas over te gaan, als daarvoor in een bepaald geval een duidelijke aanleiding bestaat. In het algemeen zal deze situatie zich eerst voordoen, indien een verantwoordelijke na een voltooid onderzoek blijft weigeren aan de conclusies daarvan gevolg te geven. Om die reden zal het CBP in beginsel niet ingaan op verzoeken om direct tot toepassing van dwangmaatregelen over te gaan. Dergelijke verzoeken zullen worden getoetst aan de criteria voor het in behandeling nemen van klachten en het instellen van onderzoeken.

Publiciteitsbeleid

Het CBP levert een grote inspanning om adequate voorlichting over een reeks van privacyrelevante onderwerpen voor verschillende doelgroepen beschikbaar te stellen en toegankelijk te houden. Een goed ingerichte website vormt een centraal onderdeel van de voorlichtingsstrategie. Daartoe behoort ook het verstrekken van informatie over de taakuitoefening van het CBP. Belangrijke uitspraken worden sinds kort ook via e-mail onder de aandacht gebracht. Het CBP streeft ernaar om op de website een overzicht te bieden van het beleid dat wordt gehanteerd bij de uitvoering van de verschillende taken. Daarbij zal ook worden ingegaan op het publiciteitsbeleid met betrekking tot de diverse zaaksoorten.

Mensenrechten en topinkomens

In mei van 2002 speelde het initiatief wetsvoorstel van de GroenLinks-fractie 'Openbaarheid topinkomens'. Een wijziging van de Wet op de ondernemingsraden zou openbaarheid verschaffen over de hoogte van inkomens van topkader, bestuurders en toezichthouders van ondernemingen. Het gaf de ondernemingsraad het informatierecht over de hoogte en inhoud van arbeidsvoorwaardelijke regelingen en afspraken met werknemers, bestuurder(s) en leden van toezichthoudende organen. Dit zou binnen de onderneming de discussie stimuleren over verschillen in inkomensontwikkeling. De maatschappelijke discussie had volgens de toelichting het belang van openbaarheid van topinkomens per persoon duidelijk gemaakt. Dat belang diende te prevaleren boven een inbreuk op de privacy.

Het VNO-NCW achtte het belang van privacy ondergeschoven in de discussie en wees erop dat het CBP hierover behoorde te adviseren. De vaste kamercommissie voor Sociale Zaken organiseerde daarop een hoorzitting waar het CBP de privacyaspecten uiteenzette. Naderhand heeft het CBP de GroenLinks-fractie ook schriftelijk geadviseerd.

Artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) eist dat iedere beperking van het grondrecht op eerbiediging van de persoonlijke levenssfeer op een wettelijke grondslag berust. Zo'n wet dient ook effectieve waarborgen te bevatten tegen ongeoorloofde inbreuken. Verder is een beperking van het recht op privacy in een democratische samenleving slechts gerechtvaardigd voor een zwaarwegend maatschappelijk belang. De inbreuk op de belangen van betrokkene mag bovendien niet onevenredig zijn in verhouding tot het doel en dat doel moet niet op een andere, voor de betrokkene minder nadelige wijze, kunnen worden gerealiseerd.

Het CBP adviseerde daarom uitdrukkelijk te motiveren op basis van welk zwaarwegend maatschappelijk belang, conform artikel 8 EVRM, de inbreuk op de persoonlijke levenssfeer wordt gerechtvaardigd. Verder zou beargumenteerd moeten worden dat de openbaarmaking aan de ondernemingsraad verenigbaar is met de oorspronkelijke doeleinden waarvoor deze gegevens verzameld zijn (de salaris- en personeelsadministratie). Tevens zou helder moeten worden voor welk doel de ondernemingsraad deze persoonsgegevens zou krijgen. GroenLinks heeft het wetsvoorstel in december 2002 aangepast zodat onder andere inkomens van het topkader niet individueel openbaar gemaakt worden, maar worden samengevoegd in groepen van minimaal vijf ●

activiteiten

Openbaar bestuur

De overheid brengt steeds meer structuur aan in haar informatiehuishouding. Langzaam maar zeker creëert zij een elektronische identiteits- en informatie-infrastructuur voor een efficiënte en betrouwbare taakvervulling. Deze ontwikkeling brengt belangrijke kansen en bedreigingen met zich mee voor de bescherming van persoonsgegevens.

In 2002 heeft het CBP een uitgewerkte visie op de privacybescherming bij de 'elektronische overheid' neergelegd: de studie Elektronische overheid en privacy. Het CBP heeft vanuit deze visie ook een bijdrage geleverd aan de totstandkoming van het advies van de commissie Van Thijn, Persoonsnummerbeleid, dat het kabinet begin 2003 heeft overgenomen.

Wetgevingsadvisering

Privacyregels hoeven weinig legitieme overheidsdoelstellingen te belemmeren. Wel dient vanaf het begin rekening met deze regels gehouden te worden, zowel bij het ontwerpen van organisatiestructuren, informatiesystemen en procedures als bij het opstellen van beleid. In lijn met het viersporenbeleid stelt het CBP zich daarom pro-actief op als adviseur en onderhoudt het actief contact met overheid en andere organisaties. Het CBP kan privacy als toezichthouder 'achteraf' beschermen, als adviseur kan het bijdragen aan de inbedding van privacybescherming in de opzet van projecten en systemen en van wet en regelgeving.

In het najaar van 2002 is het CBP gesprekken met de wetgevingsdirecties van de ministeries gestart om de wettelijke adviesfunctie van het CBP onder de aandacht te brengen. Op grond van de WBP dient de toezichthouder om advies te worden gevraagd "over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens". Er was niet alleen onbekendheid met de nieuwe regelgeving maar ook onzekerheid over de reikwijdte van de verplichting.

Met enkele ministeries konden al concrete afspraken worden gemaakt over de praktische invulling van deze verplichting. Het CBP streeft ernaar de adviesverplichting deel uit te laten maken van de wetgevingsprocedure. Dit moet leiden tot een meer structurele invulling van de adviestaak van het CBP en tot een intensivering van de werkzaamheden op dit terrein.

Elektronische overheid en privacy

De in juli 2002 gepubliceerde studie *Elektronische overheid en privacy: bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid* richt zich met name op de beleidsmakers die de informatie-infrastructuur van de elektronische overheid ontwikkelen. Het CBP wil hieraan mede richting geven. De studie bespreekt privacy-ontwerpprincipes voor informatiesystemen en geeft een analyse van de speelruimte die de privacyregels bieden.

Persoonsnummers spelen een belangrijke rol in de identiteitsinfrastructuur. De studie voert aan dat algemene nummers moeilijk te beheren zijn. Er zijn goede argumenten voor het gebruik van verschillende sector- en ketennummers naast elkaar. Een dergelijke aanpak kan tegelijkertijd gezien worden als een bijdrage aan infrastructurele privacyborging. Alleen wanneer privacy op een robuuste manier wordt ingebouwd, is zij ook op langere termijn te garanderen.

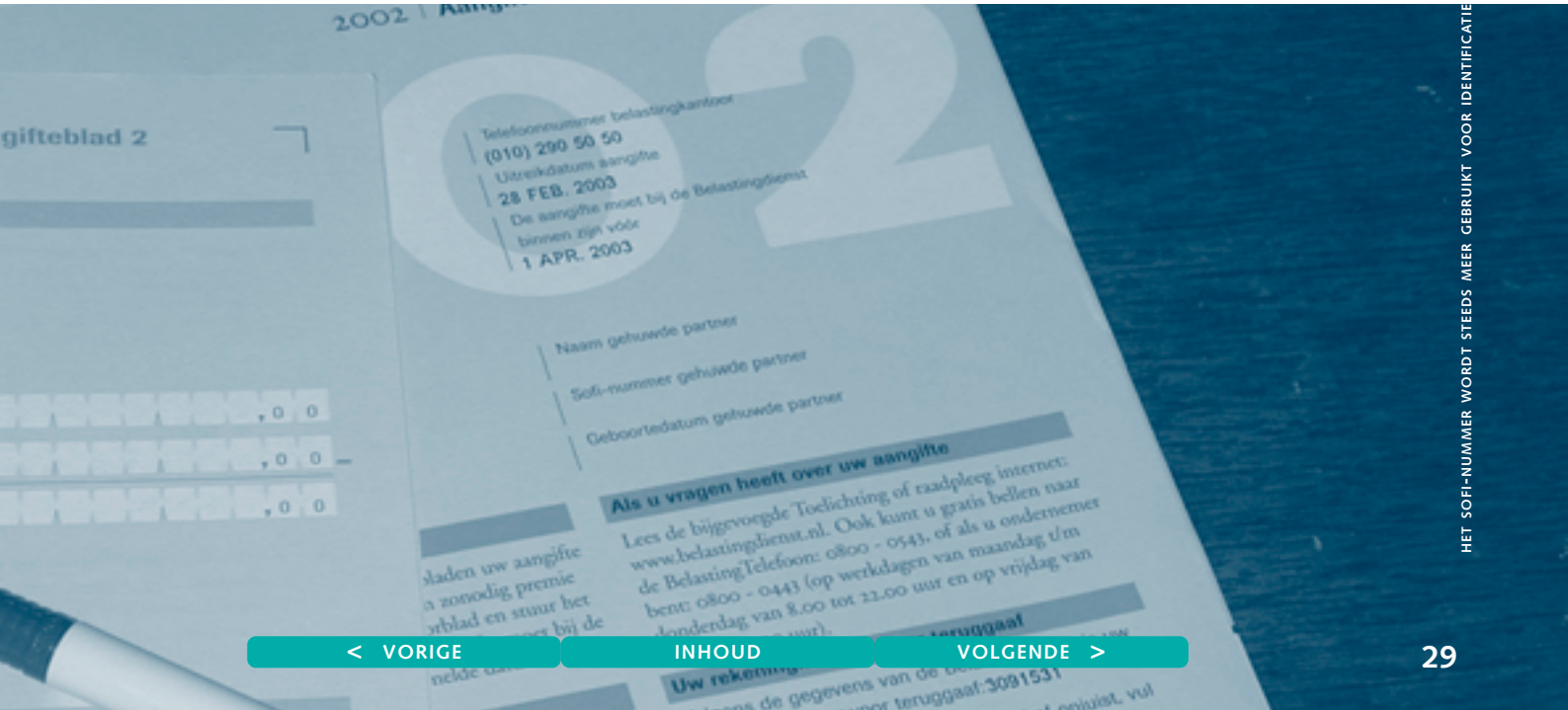
Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Er wordt daarom vaak voor gepleit de burger zoveel mogelijk 'de regie' over zijn eigen persoonsgegevens te geven; dat zou zowel inzicht als zeggenschap bieden. De overheid moet inderdaad zorgen voor optimale transparantie, maar er zijn grenzen aan informationele zelfbeschikking. In de WBP is bewust gekozen voor een systeem van checks and balances waarin toestemming en verzet slechts een corrigerende rol spelen. Belangrijker is dat de overheid ook zonder regie-aanwijzingen van de burger transparant en vertrouwenwekkend werkt. Het CBP wil met deze studie een bijdrage leveren aan de totstandkoming van een informatie-infrastructuur voor de overheid die terecht het vertrouwen van de burger geniet.

Burgerservicenummer

Het CBP heeft in 2002 ook een bijdrage geleverd aan het advies van de interdepartementale commissie Van Thijn, *Persoonsnummerbeleid in het kader van identiteitsmanagement*, dat de kaders schetst voor het toekomstig gebruik van persoonsnummers door de overheid. Het CBP was vertegenwoordigd in de commissie. Het kabinet onderschreef het advies en kondigde aan in 2003 een voorstel te zullen uitwerken voor een 'burgerservicenummer'.

In 2001 waarschuwde de Registratiekamer naar aanleiding van de introductie van het onderwijsnummer nog voor een ongewenste uitwaaiering van het Sofi-nummer. Ook heeft het CBP een sterke voorkeur voor sector- of ketengebonden nummers. Het kon zich echter vinden in de uiteindelijke weging van doelen en criteria omdat het concept een aantal wezenlijke waarborgen van privacybescherming bevat.

Het door de commissie voorgestelde beleidskader kent vier basiselementen: de invoering van een burgerservicenummer (gebaseerd op het huidige Sofi-nummer), sectoraal persoonsnummerbeheer, overkoepelend persoonsnummerbeheer en de zogenaamde vertrouwensfuncties.



HET SOFI-NUMMER WORDT STEEDS MEER GEBRUIKT VOOR IDENTIFICATIE

De invoering van een burgerservicenummer dient de eenduidige identificatie van gegevens van burgers. Het is nodig voor een doelmatiger en klantgerichter overheid. Het nummer maakt de koppeling van gegevens tussen overheden mogelijk en is daardoor ook belangrijk voor opsporing en bestrijding van (identiteits)fraude. Samen met het overkoepelend persoonsnummerbeheer zouden hiermee gebrekkige identificatie en identiteitsfraude teruggedrongen kunnen worden. Dat is ook wenselijk vanuit een oogpunt van privacybescherming.

Het sectorale persoonsnummerbeheer is in lijn met de visie van het CBP op de elektronische overheid en de voorkeur voor sector- en ketennummers. In veel sectoren zal het sectornummer overigens gelijk zijn aan het burgerservicenummer. Deze algemene regel geldt niet voor de overheidssectoren die bijzondere persoonsgegevens zoals medische of strafrechtelijke gegevens verwerken. De sectoren Justitie en Zorg zullen volgens het advies van het CBP aparte sectornummers gebruiken met een koppeling naar het burgerservicenummer.

De rechtmatige verwerking van gegevens zal sterk bevorderd worden door de vertrouwensfuncties, die onder meer bestaan uit Privacy-Enhancing Technologies, dus technische privacywaarborgen in de informatiesystemen zelf. De door de commissie geformuleerde uitgangspunten leggen verder een grote nadruk op transparantie van de overheid en het informeren van de burger.

Gemeentelijke informatiehuishouding

Gezien de huidige en toekomstige spilfunctie van de Gemeentelijke basisadministratie (GBA) in de informatie-infrastructuur van de overheid wijst het CBP op het belang van de zorg voor privacybescherming bij deze gemeentelijke diensten. Alle overheidsinstellingen zullen in de toekomst, naar het zich laat aanzien, het GBA als authentieke bron voor identificerende persoonsgegevens van ingezetenen gebruiken. Dat is althans de visie van de regiecommissie voor het Programma Stroomlijning Basisgegevens waarin het CBP de afgelopen drie jaar deelnam.

Een dergelijke spilfunctie vereist ook een scherp bewustzijn van het belang van privacybescherming. In het jaarverslag over 2001 noemde het CBP het zorgwekkend dat privacy nog onvoldoende was ingebed in de werkprocessen van de afdelingen burgerzaken. Er zijn geen signalen dat de situatie in 2002 over het geheel beter is. Ook hebben nog steeds niet alle gemeenten de verplichte reglementen voor de interne en externe gegevensverstrekkingen aangepast aan de WBP.

In 2002 heeft het CBP wel bij het vervolgonderzoek op de GBA-audits van 1999 in Breda en Almelo kunnen constateren dat deze gemeenten de privacybescherming van hun bevolkingsadministratie op orde hebben. In beide gemeenten zijn de eerdere aanbevelingen uitgevoerd, is er een groeiend privacybewustzijn en is duidelijk geinvesteerd in de beveiliging van persoonsgegevens.

Eind 2002 bleek een groot aantal gemeenten vergelijkenderwijs niet of nauwelijks de eigen verwerkingen die onder de WBP vallen gemeld te hebben ondanks nadrukkelijke voorlichting door het CBP. In januari 2003 heeft het CBP in een brief herinnerd aan deze meldingsplicht en gewezen op mogelijke handhavingsacties ■

Politie en Justitie

De politiek-maatschappelijke discussie over politie en justitie draaide in 2002 om veiligheid. Tegen de achtergrond van de roep om meer daadkracht, toezicht en controle poneerden diverse bestuurders en politici een karikaturale tegenstelling tussen veiligheid en privacy. Grif werd aangenomen dat privacybescherming uitwisseling van gegevens en uitbreiding van bevoegdheden verhinderde. Voor deze bestuurders stond privacy als een heilig huisje meer veiligheid in de weg. Terwijl in januari 2002 de regering nog een incidentele identificatieplicht verdedigde, stelde het nieuwe kabinet in november voor een algemene identificatieplicht in te voeren voor alle burgers ouder dan 12 jaar. Ook zouden alle verkeersgegevens van telecommunicatie van een ieder langdurig bewaard moeten worden. Het CBP maakt zich ernstige zorgen over de gevolgen die een gemakzuchtige vlucht in meer bevoegdheden voor belangen en rechten van gewone burgers kan hebben.

Privacy en veiligheid

Het CBP heeft in het najaar van 2002 deze zorgen ook gedeeld met verantwoordelijke partijen en de Tweede Kamer. Ook in de pers heeft het gewaarschuwd van privacybescherming geen karikatuur te maken. Het is onjuist te suggereren dat in Nederland het recht op privacy heilig is.

In de praktijk krijgt het grondrecht van burgers op 'privacy' betekenis in situaties waarin het nodig is de privacy van burgers in te perken, bijvoorbeeld bij controles en toezicht door de overheid. De vraag is dan naast of dat moet gebeuren, vooral hoe dat moet gebeuren en hoe kan worden gezorgd voor een juist gebruik van bevoegdheden.

Het privacybelang wordt dus afgewogen tegen andere zwaarwegende belangen. De Nederlandse grondwet, internationale verdragen, Europese richtlijnen en de privacywetgeving stellen eisen aan deze afweging. Dit maakt deel uit van de spelregels voor de overheid in de omgang met haar burgers. Privacyregels eisen dat goed wordt nagedacht over doel, effectiviteit en evenredigheid van overheidsmaatregelen en dat er voldoende waarborgen komen tegen misbruik. Wie de 'privacywetgeving' op de helling wil zetten, zegt in feite dat deze vragen overbodig zijn.

De wat naeve reactie 'Ik heb toch niets te verbergen?' van de argeloze man of vrouw in de straat stemt optimistisch. De reactie wijst vooral op vertrouwen in de overheid. Dat is een groot goed. Een onzorgvuldige omgang met de privacy van de burger stelt dat vertrouwen op termijn in de waagschaal. Burgers die niets te verbergen hebben, verdienen een overheid die privacybescherming vanzelfsprekend meeneemt bij het ontwerp van maatregelen, informatiesystemen of verplichtingen voor burgers.

Het recht op 'privacy' is dus een essentieel onderdeel van de 'veiligheid' die een democratische rechtsstaat zijn burgers te bieden heeft. Wie het recht op privacy onderuit haalt, berooft de goedwillende burger van een belangrijke waarborg en zaagt aan de poten van de democratische rechtsstaat.

Identificatieplicht

Het wetsvoorstel incidentele identiteitscontroles van januari 2002 voorzag in het tijdelijk invoeren van een verplichting tot identificatie en een bevoegdheid hierop controle uit te oefenen in situaties waarin sprake is van terroristische dreiging. Het CBP kon zich vinden in deze beperkte uitbreiding van de bestaande identificatieplicht. De term 'concreet gevaar' in de wettekst diende wel aangescherpt te worden. Een vergaande bevoegdheid als de (incidentele) identiteitscontrole kan immers volgens het Europees Verdrag van de Rechten van de Mens (EVRM) alleen ingeroepen worden in geval van een acuut gevaar voor de algemene veiligheid of bij een risico van ernstige ontwrichting van de rechtsorde.

In december 2002 werd het CBP om advies gevraagd over een algehele identificatieplicht. Het CBP adviseerde begin 2003 het voorstel niet in te dienen. Het schoot ernstig tekort in de onderbouwing van de noodzaak van de maatregel. Het voorstel stond bovendien haaks op de uitgangspunten voor het algemene beleid inzake identificatie.

De Nederlandse discussie over een beperkte of algemene identificatieplicht is zeker al twintig jaar oud. Steeds werd geconcludeerd, bijvoorbeeld door het kabinet Lubbers II, dat een algemene identificatieplicht te ver ging. Eind 2001 trok ook het kabinet Kok II deze conclusie op basis van een degelijke analyse. De identificatieplicht werd gerechtvaardigd geacht in een aantal specifieke situaties waarin de overheid de burger inderdaad als potentiële verdachte beschouwt, bijvoorbeeld bij de controle op 'zwart rijden' in het openbaar vervoer.

Het voorstel voor een algemene identificatieplicht ging voorbij aan deze breed gedragen analyse en tegenargumenten werden bewust genegeerd. Aangezien ook geen nieuwe argumenten werden aangedragen, voldeed het kabinet niet aan de eis van het EVRM om de inbreuk op de persoonlijke levenssfeer voldoende te rechtvaardigen.

De Raad van Hoofdcommissarissen achtte bovendien invoering van een identificatieverplichting niet zinvol zonder de mogelijkheid van zelfstandige controles, die ook systematisch moesten worden vastgelegd. Daarmee is de burger dus altijd verdachte. Het gebruik van deze bevoegdheid zou verder goed geregistreerd moeten worden om discriminerend optreden van de politie te kunnen corrigeren. Het wetsvoorstel zou dus een politiebevoegdheid kunnen scheppen die leidt tot een aanzienlijke uitbreiding van de registratie van onverdachte burgers of oncontroleerbaar blijkt bij nalatigheid rond de registratie.

In het voorstel voor een algemene identificatieplicht is het evenwicht tussen rechten en plichten voor burger en overheid zoek. De overheid legt haar burgers een permanente verplichting op zonder te motiveren waarom specifieke verplichtingen niet voldoende zijn. Strafbaarstelling van het niet nakomen van de identificatieplicht leidt tot een situatie waarin de burger naar believen als verdachte kan worden bejegend. De dagelijkse draagplicht en de toonplicht bij (algemene) controles zullen de relatie tussen burger en overheid op de proef stellen. De vraag of dit alles maatschappelijk en rechtsstatelijk aanvaardbaar is, werd in het voorstel niet afdoende beantwoord.

Privacybescherming in de praktijk

Onder het roerige oppervlak van de politieke discussie lag een kalmere werkelijkheid van constructief overleg en advisering. Met de brancheverenging van particuliere beveiligings- en recherchebureaus – een onvoldoende gereglementeerde en sterk groeiende sector – werd gewerkt aan een gedragscode, die in 2003 goedgekeurd zal kunnen worden.

De nota 'Openbaar tenzij' van de Procureurs Generaal van februari 2002 waarin de voorlichting in strafzaken werd gereglementeerd, stelde dat het Openbaar Ministerie (OM) geen gegevens meer zou verstrekken die herleidbaar waren tot de persoon van de verdachte. Het OM acht zich hiertoe gedwongen

door inwerkingtreding van de WBP. Het concept gaf een onjuiste uitleg van de WBP en de WOB, maar het CBP onderschreef wel de hoofdlijn van het OM dat de voorlichting zich meer op zaken dan op personen dient te richten. Het CBP werd in het vervolgtraject betrokken.

Samen met politie en OM werd toegewerkt naar een praktische stroomlijning van inzageverzoeken van burgers. Politie en CBP werkten ook samen bij de ontwikkeling van modelreglementen voor de permanente en de tijdelijke politieregisters. Dit bevordert de eenduidigheid in de informatiehuishouding van de politie en vermindert daarnaast de administratieve lasten. Voor de privacy-functionarissen van de politie werd een bijeenkomst in januari 2003 voorbereid. Het CBP droeg verder bij aan de gedachtevorming over antecedentenonderzoek voor politiepersoneel, de vorming van een DNA-databank en de landelijke informatisering van de politie (NPOL).

Met de Raad van Advies voor de Centrale Inlichtingen Eenheden (CIE) werd opnieuw een praktijkgerichte conferentie georganiseerd. Een belangrijk resultaat van het overleg met de CIE's is de plicht tot een regelmatige zelfevaluatie met externe toetsing. Het CBP-advies deze benadering voor alle politieregisters te kiezen, werd onderschreven door het kabinet. In 2003 zal het CBP een aantal CIE's bezoeken.

De Nederlandse Vereniging van Strafrecht Advocaten diende in 2002 een klacht in over schending van het beroepsgeheim van advocaten door het tappen van telefoongesprekken met cliënten. De bestaande regels en instructies zouden op dit punt tekort schieten. Met het oog op de toekomst vroeg het CBP in een hoorzitting de betrokken partijen om een toelichting. Schriftelijke uitwisseling van standpunten nam vervolgens geruime tijd in beslag. In 2003 zal het CBP een oordeel geven over de geldende instructies en de bestaande praktijk en voorstellen doen voor een betere bescherming van het beroepsgeheim.

Samenwerkingsverbanden

Het Ministerie van Justitie publiceerde in samenwerking met het Ministerie van Binnenlandse Zaken de *Handreiking voor gemeenten over privacyaspecten bij criminaliteitspreventie*. De handreiking biedt praktische mogelijkheden om op verantwoorde wijze gegevens voor preventie van jeugdcriminaliteit uit te wisselen. Het CBP juicht de handreiking toe maar wijst erop dat de beschrijving van de toepasselijke regelgeving niet volledig is. De toepasselijkheid van de Wet op de geneeskundige behandelingsovereenkomst en andere regelingen die een geheimhoudingsverplichting in het leven roepen, wordt onvoldoende duidelijk.

Medio 2002 oordeelde het CBP positief over aanpak en uitvoering van het Rotterdamse Alijda-project waarin onder meer malafide huiseigenaren worden aangepakt. Samenwerking tussen overheidsinstanties is mogelijk daar waar hun taken en bevoegdheden op elkaar aansluiten. Een verantwoorde taakuitoefening maakt dan ook de uitwisseling van noodzakelijke informatie mogelijk. Bij de aanpak van verslaafden draaide het om de samenwerking met hulpverlenende instanties. Naar het oordeel van het CBP verhindert het beroepsgeheim echter niet bepaalde hulpverleningsinformatie mede in het belang van de cliënt te delen. Het CBP zal in 2003 uitgebreider aandacht besteden aan gegevensuitwisseling in samenwerkingsverbanden

Doorgifte naar de Nederlandse Antillen en Aruba

Het wetsvoorstel over de uitwisseling van gegevens uit de Justitiële Documentatie tussen Nederland en de Nederlandse Antillen en Aruba ten behoeve van opname in documentatiesystemen maakt het mogelijk dat binnen het Koninkrijk der Nederlanden kennis kan worden genomen van de justitiële antecedenten van een persoon die deze heeft opgebouwd in het land van herkomst.
De Nederlandse Antillen en Aruba kennen echter geen specifieke privacywetgeving. Voldoende waarborgen ten aanzien van de bescherming van de persoonlijke levenssfeer zijn dan vereist, zeker voor een structurele uitwisseling van gegevens waarbij de Justitiële Documentatie van de rijksdelen min of meer op elkaar worden aangesloten. Bovendien worden bijzondere gegevens uitgewisseld waarvoor in Nederland maar niet in de Nederlandse Antillen en Aruba een bijzonder regime geldt. Het CBP adviseerde daarom het wetsvoorstel te voorzien van passende en structurele waarborgen.

Cameratoezicht op openbare plaatsen

Publiek cameratoezicht blijft onverminderd in de belangstelling en zal wettelijk beter geregeld worden. Als middel om veiligheid en openbare orde te bevorderen, werd het allerwegen geaccepteerd zo niet omarmd hoewel de eerste evaluaties van cameraprojecten de veiligheidseffecten ervan relativeerden. Het CBP leverde een bijdrage aan de Landelijke Cameradag eind 2002, waar vooral gemeenten zich oriënteerden. Voor 2003 werd een onderzoek naar cameratoezicht bij een aantal gemeenten aangekondigd.

Tweemaal bracht het CBP in 2002 advies uit over het wetsvoorstel cameratoezicht op openbare plaatsen. Vanuit het oogpunt van rechtszekerheid achtte het CBP een wettelijk kader voor cameratoezicht op openbare plaatsen van belang. Het CBP kon zich goed verenigen met de toekenning van de bevoegdheid tot plaatsing van camera's aan de burgemeester op basis van een verordening van de raad. Een dergelijke toedeling komt overeen met de verantwoordelijkheid van de burgemeester voor de handhaving van de openbare orde.

De noodzakelijkheid van het cameratoezicht werd voldoende onderbouwd, zij het dat de criteria voor de noodzaak telkens in concreto zullen moeten worden vastgesteld. Voor de verlenging van het cameratoezicht zou de burgemeester een verslag over de doeltreffendheid en de effecten moeten maken voor de raad. Een duidelijke evaluatieplicht dwingt de raad zich daadwerkelijk over de noodzaak van verlenging van plaatsing van camera's uit te spreken. Het inzage- en correctierecht van betrokkenen, de in beeld gebrachte personen, was niet nader uitgewerkt. Het CBP adviseerde hieraan aandacht te besteden.

Onder de reikwijdte van het cameratoezicht bleken ook de kerken en vergelijkbare plaatsen te vallen op grond van de gekozen definitie van 'openbare plaats'. Door de wijziging van de Gemeentewet worden plaatsen die de rechthebbende bestemt voor de belijdenis van levensovertuiging, niet meer uitgesloten van het begrip openbare plaats. In het kader van cameratoezicht ten behoeve van (primair) de openbare orde dient deze invulling van het begrip nader onderbouwd te worden. Is het de bedoeling dat de overheid camera's kan plaatsen in kerken, moskeeën en andere gebouwen bestemd voor de belijdenis van een levensovertuiging? ■

Arbeid en sociale zekerheid

Fraudebestrijding is in 2002 hét toverwoord geworden, zowel in de sociale zekerheid als in de arbeidsrelatie. In het vigerende klimaat werd ingezet op strengere controles en sociale recherche bij de bestrijding van fraude in de sociale zekerheid. Het CBP rondde een onderzoek naar dossiers van sociale diensten af, beoordeelde de praktische inrichting van sociale recherches en adviseerde over herziening van wet- en regelgeving inzake de bijstand.

Zwarte lijsten als middel tegen frauderende werknemers kregen veel publiciteit en vroegen veel aandacht van het CBP. De praktijk van de reïntegratie van zieke werknemers en uitkeringsgerechtigden bleek in 2002 nog steeds onvoldoende geregeld. Om een goed beeld van de praktijk te krijgen werd een onderzoek gestart naar de privacysituatie van de zieke werknemer.

Dossiers van de sociale dienst

Een dossieronderzoek in februari 2002 uitgevoerd bij drie sociale diensten beperkte zich tot twee vragen. Er is gekeken of de gegevens in de dossiers noodzakelijk waren voor de vaststelling van het recht op bijstand (noodzakelijkheidsvereiste). Verder is onderzocht van welke instanties de sociale dienst gegevens ontvangt en aan welke instanties de sociale dienst gegevens verstrekt. Consulenten dienen per geval te bepalen welke gegevens noodzakelijk zijn voor de uitvoering van de bijstandswet. In de onderzochte dossiers bevonden zich weinig niet ter zake doende gegevens. In enkele gevallen had de behandelaar zich onvoldoende afgevraagd of het noodzakelijk was de gegevens in het dossier op te nemen.

De sociale diensten bleken in eerste instantie uit te gaan van de gegevens die de cliënt overlegt. Bij aanleiding tot vragen werden andere instanties geraadpleegd, soms instanties die niet in de Algemene bijstandswet worden genoemd. De verantwoordelijkheid voor de gegevensverstrekking ligt primair bij de verstrekkende instantie. De sociale dienst is echter verplicht om zelf na te gaan of de desbetreffende partij inlichtingen mag geven. Soms bleken medewerkers zonder toestemming van de cliënt navraag te hebben gedaan bij personen en instanties die gebonden zijn aan een beroepsgeheim. Dit is in strijd met de privacywetgeving: onrechtmatig verkregen gegevens mogen niet worden verwerkt. Soms was onduidelijk waar bepaalde informatie geverifieerd was.

Het CBP heeft een positieve indruk gekregen van de wijze waarop de drie sociale diensten met persoonsgegevens omgaan. Wel is gebleken dat duidelijke werkinstructies voor het personeel en informatie aan de cliënt noodzakelijk zijn. Het CBP overweegt over enige tijd een handhavingsonderzoek te doen bij sociale diensten.

Sociale recherche en fraudeteams

De strijd tegen fraude bij de sociale zekerheid wordt uitgevoerd door allerlei organisaties. Het gaat om de (gemeentelijke) sociale recherches, de Regionale Interdisciplinaire Fraudeteams (RIF) en de Sociale Inlichtingen- en Opsporingsdienst (SIOD). Uit de aard van hun taak worden ook gegevens van betrokkenen verwerkt die door heimelijke waarneming zijn verkregen. Het CBP heeft in het kader van de melding van hun gegevensverwerkingen daarom een vooraf-gaand onderzoek verricht ter beoordeling van de rechtmatigheid van de inrichting van de verwerking. Vergelijkbaar onderzoek was eind 2002 nog gaande naar de rechercheactiviteiten van het Uitvoeringsinstituut Werknemersverzekeringen en de Sociale Verzekeringsbank.

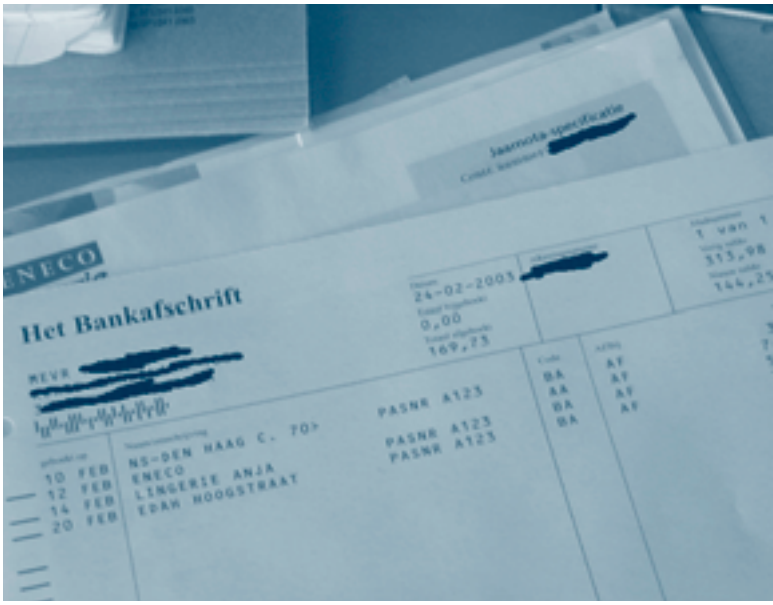
De per 1 januari 2002 opgerichte SIOD is verantwoordelijk voor opsporing van zware fraude in de sociale zekerheid en verricht vooral algemene criminaliteitsanalyses. Met name wanneer niet tot vervolging wordt overgegaan, zijn voor de SIOD de waarborgen uit de WBP van belang, zoals het informeren van betrokkenen, het recht op inzage en correctie en redelijke bewaartermijnen. Het CBP achtte de verwerking rechtmatig met enkele kanttekeningen juist op het gebied van deze waarborgen. Een uitwerking van de werk-processen was dus nog noodzakelijk.

RIF's zijn samenwerkingsverbanden tussen (al naar gelang het project) colleges van burgemeester en wethouders, uitvoerings-instellingen van de sociale zekerheid, de belastingdienst, arbeids-inspectie of de politie en het Openbaar Ministerie in een regio. Deze teams werken samen in onderzoeken naar allerlei vormen van fraude op het terrein van de sociale en fiscale wetgeving. De aan-pak is gericht op de integrale naleving van alle arbeids-, sociale zekerheids- en fiscale wetgeving.

Het CBP heeft onderzoek gedaan naar de procesbeschrijving voor heimelijke waarneming die door één van RIF's was opgesteld. Het CBP heeft het gehanteerde normenkader en de daaruit voort-vloeiende werkwijze beoordeeld op rechtmatigheid. Het CBP kwam tot het oordeel dat naleving van de procesbeschrijving in beginsel voldoende waarborgen bood voor een rechtmatige verwerking van persoonsgegevens. Voorwaarde is wel dat de omschreven werkwijze steeds nader wordt geconcretiseerd per projectplan. Afgesproken werd bovendien dat de procesbeschrijving ook voor andere RIF's bij de melding van gegevensverwerkingen waarbij de gegevens (deels) via heimelijke waarneming werden verkregen, als leidraad kon dienen.

Een vergelijkbare aanpak heeft het CBP gevolgd ten aanzien van de sociale recherches van de gemeenten. De procesbeschrijving 'Heimelijke waarneming door sociale diensten' werd opgesteld door Stimulansz, een stichting die gemeenten adviseert bij de uitvoering van de bijstandswet, in afstemming met vertegenwoordigers van het Landelijk Contact Sociaal Rechercheurs en rechercheurs van enkele gemeenten. Het CBP keurde de procesbeschrijving in 2002 goed met de kanttekening dat gemeenten de werkwijze, zoals omschreven in de procesbeschrijving, steeds concreet dienen vast te leggen in werkprocessen.

Belangrijke winst van de gekozen benadering kan een brede, landelijke harmonisering zijn van de werkwijze bij heimelijke waar-neming van de RIF's en van de (gemeentelijke) sociale recherches. Rechtszekerheid en het nalevingsniveau van de WBP worden hier-door bevorderd terwijl voor alle betrokken partijen de noodzakelijke melding eenvoudiger kan worden afgehandeld.



Lacunes in regelgeving reintegratie

In mei 2002 heeft het CBP een werkconferentie georganiseerd over gegevensverkeer bij reintegratie. Het bleek dat met name de verwerking van medische gegevens problemen geeft. Ook de waar-borgen die in de Wet SUWI zijn neergelegd (reglement en audit) voor de verwerking van persoonsgegevens door reintegratie-bedrijven, moeten nog worden uitgewerkt. De huidige regels voor het gegevensverkeer bij reintegratie hebben alleen betrekking op de

publieke en wettelijke taak. Deze regels gelden bijvoorbeeld niet voor het gegevensverkeer tussen een werkgever en een particuliere herverzekeraar. De wetgeving biedt een grondslag voor de verstrekking van persoonsgegevens van de te reintegreren persoon door de opdrachtgever (werkgever, gemeente of UWV) aan het reintegratiebedrijf. Over de verdere verwerking door het reintegratiebedrijf, de 'teruglevering' aan de opdrachtgever en de consequenties hiervan is weinig tot niets geregeld.

Het CBP heeft tijdens de conferentie nogmaals het belang benadrukt van heldere regelgeving zodat het voor alle partijen duidelijk wordt welke gegevens in welk kader mogen worden verwerkt. Naar het oordeel van het CBP moet de Minister van Sociale Zaken en Werkgelegenheid zijn verantwoordelijkheid nemen ook voor dit onderdeel van het reintegratieproces en dus de wetgeving aanvullen.

Een nieuwe bijstandswet

Het CBP heeft vervolgens eind 2002 geadviseerd over het voorstel voor een nieuwe bijstandswet, inmiddels Wet werk en inkomen geheten. De nieuwe wet zal een groot aantal bestaande wettelijke regelingen vervangen. De kern van het wetsvoorstel is dat gemeenten meer (financiële) verantwoordelijkheid krijgen voor de bijstandsverlening.

In de nieuwe situatie is het college van Burgemeester en Wethouders (B&W) verantwoordelijk; de gemeenteraad ziet dan toe op de uitvoering van het bijstandsbeleid door de gemeente. Door gemeenten een grotere bewegingsvrijheid te geven bij de invulling van de individuele rechten en plichten en bij het aanbieden van voorzieningen beoogt het kabinet de reintegratie van werkzoekenden te versnellen.

Het CBP is in het advies ingegaan op de verhouding van het wetsvoorstel tot de bestaande circulaires, het reintegratiebeleid, de gewijzigde toezichtstructuur, de inrichting van de administratie, de wijzigingen in de inlichtingenplicht en het gesloten verstrekkingenregime en de informatievoorziening aan de Minister van Sociale Zaken en Werkgelegenheid.

Het CBP heeft de Minister verscheidene malen verzocht om heldere regels te stellen voor de overdracht van persoonsgegevens bij reintegratie. Het moest constateren dat ook dit wetsvoorstel geen helderheid geeft over hoe gegevensverwerking bij reintegratie praktisch vorm dient te krijgen. Veel lijkt overgelaten te worden aan de gemeenten. Hierin schuilt het gevaar dat er verschillen tussen gemeenten optreden bij de uitvoering van de reintegratietaak. Het CBP is van oordeel dat voor zowel de gemeenten, de cliënten als de reintegratiebedrijven duidelijk moet worden welke (categorieën van) gegevens daadwerkelijk noodzakelijk zijn voor de uitvoering van de bijstandswet en dus over en weer tussen het reintegratiebedrijf en de sociale dienst mogen worden uitgewisseld. Uitvoering van wettelijke verplichtingen zal doorgaans een toereikende grondslag kunnen zijn. Toestemming van de betrokkene dient voor bijzondere situaties te worden gereserveerd.

Gedragscode reintegratiebedrijven

De brancheorganisatie voor reintegratiebedrijven (Borea) is in 2002 begonnen met de ontwikkeling van een gedragscode in de zin van artikel 25 WBP. Het CBP onderschrijft van harte het door Borea genomen initiatief. Als toezichthouder kan het na toetsing van de gedragscode een goedkeurende verklaring afgeven. Voorwaarde is dat de regels van de code, gelet op de bijzondere kenmerken van de sector waarin de Borea werkzaam is, een juiste uitwerking vormen van de WBP of van andere wettelijke bepalingen voor de verwerking van persoonsgegevens. De verwachting is dat in 2003 de gedragscode zal worden goedgekeurd.

Frauderende werknemers

Waarschuwingslijsten, meestal zwarte lijsten genoemd, werden in 2002 gepresenteerd als middel tegen frauderende werknemers. Het CBP heeft diverse partijen in algemene zin geadviseerd over hun voornemens.

Bedrijven en bedrijfstakken kunnen een gerechtvaardigd belang hebben bij het gebruik van een waarschuwingslijst. Het blijft echter een gevoelig instrument. Het aanleggen van een waarschuwingssysteem is pas te rechtvaardigen wanneer de schade een zodanige omvang heeft bereikt dat een beperking op het recht van de persoonlijke levenssfeer noodzakelijk is. De verantwoordelijke moet kunnen motiveren waarom dit zware middel in zijn situatie gerechtvaardigd is, met andere woorden, waarom het bedrijfs(tak)belang zwaarder weegt dan het privacybelang van de betrokken medewerkers. Een gedegen motivering van de grondslag is dus essentieel om een zwarte lijst rechtmatig te kunnen aanleggen.

Het gerechtvaardigd belang van een waarschuwingslijst is mede afhankelijk van de gevolgen van de plaatsing op de lijst voor de betrokkene, dat wil zeggen de mate waarin betrokkenen, door plaatsing op de lijst, afgesneden worden de toegang tot een deel van de arbeidsmarkt. Een eenmalig vergrijp van geringe omvang mag niet leiden tot plaatsing op een dergelijke lijst. Arbeid is immers één van de sociale grondrechten en dat dient zwaar te wegen.

De gevolgen van plaatsing worden sterk bepaald door de reikwijdte van de zwarte lijst. Deze kan gelden voor noodzakelijke functies of voor alle werknemers, voor een bedrijf al dan niet met filialen, een concern of zelfs een hele bedrijfstak. De criteria voor plaatsing moeten strikter worden wanneer de reikwijdte van de lijst toeneemt. Bij een concernbrede registratie kan een waarschuwingslijst immers aanzienlijk verstrekkender gevolgen voor de betrokkenen krijgen. De toegang tot de arbeidsmarkt wordt dan verder ingeperkt.

Een zwarte lijst die voor een (aanzienlijk deel van de) bedrijfstak geldt, dient aan nog strengere eisen te voldoen. Een nog zwaarder (bedrijfstak)belang dient een dergelijke inbreuk op de persoonlijke levenssfeer van betrokkene te rechtvaardigen. De verantwoordelijke zal zwaardere waarborgen moeten instellen om een zorgvuldig gebruik te garanderen en de rechten van de betrokkenen te beschermen. Alleen werknemers die echte vergrijpen hebben gepleegd, komen in aanmerking voor plaatsing op een dergelijke brede waarschuwingslijst.

Controle op gebruik van e-mail en internet op het werk

Goede motivering en inrichting van waarschuwingslijsten kan voorkomen dat noodzakelijke fraudebestrijding de relatie met werknemers onnodig belast. Een goede afweging van belangen is hierbij de sleutel evenals bij overige controle op werknemers. Een verantwoorde controle op (privé)gebruik van e-mail en internet op het werk vereist een vergelijkbare privacytoets en goed overleg met de werknemers of de instemming van de ondernemingsraad. Om een goede regeling binnen bedrijven te bevorderen publiceerde het CBP in 2002 een geactualiseerde versie van *Goed werken in netwerken*, een nieuwe *Raamregeling voor het gebruik van e-mail en internet* en de brochure *Privacy: checklist voor de ondernemingsraad* ■

WIE WEET WELKE MEDICIJNEN U GEBRUIKT?

Zorg en welzijn

De maatschappelijke discussie over de zorg is in 2002 verder verscherpt. Een algemene roep om grotere efficiëntie, minder bureaucratie en meer marktwerking stuurt het debat. Grote verwachtingen worden gekoesterd van een verdergaande informatisering van de zorg en de zorgsector, die uitwisseling van gegevens op alle niveaus moet faciliteren. De behoefte patiëntgegevens uit te wisselen in samenwerkingsverbanden binnen de zorg en met partijen daarbuiten groeit.
De ontwikkelingen in de informatie- en telecommunicatietechnologie (ICT) maken dat ook mogelijk. Commerciële aanbieders van diensten zoeken een plaats in de sector. De zorgverzekeraars krijgen een meer prominente rol in de toewijzing en bekostiging van de zorg. Ook groeit het aantal databases voor medisch onderzoek. Verontrustend is dat privacybescherming bij het ontwerp van de informatiesystemen vaak onvoldoende wordt meegenomen. Veel problemen zouden immers in de ontwerpfase voorkomen kunnen worden.

Gezien de kwetsbare positie van de patiënt zal het CBP sterk toezien op de bescherming van patiëntgegevens en de naleving van geheimhoudingsverplichtingen.

Privacy bij ICT in de zorg

In 2002 publiceerde het CBP de studie *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg*. Doel van de studie is een overzicht van de privacyaspecten van de toepassing van ICT in de zorg.

De vele beleidsvoornemens, experimenten en trends bij ICT in de zorg zullen leiden tot een elektronische identiteitsinfrastructuur, een elektronische informatie-infrastructuur, een grotere rol voor internet en veranderingen in de organisatie en de financiering van de zorg. Bij de huidige ICT-toepassingen is privacy onvoldoende als ontwerpcriterium meegenomen. Tijdige én adequate aandacht voor privacybescherming in de zorg is echter een kritische succesfactor. Bij de stelselherziening gaat het vooral om meer concurrentie tussen aanbieders van zorg en tussen zorgverzekeraars. Vergoeding van de zorg moet worden gerelateerd aan de werkelijk gemaakte kosten.

Als onderdeel van de stelselwijziging zal de zogeheten Diagnose-Behandeling Combinatie (DBC)-systematiek worden ingevoerd. Bij de uitwerking van het DBC-concept dient de overheid zich rekenschap te geven van de verschillende rollen van de zorgverzekeraar en de andere partijen in de gezondheidszorg. Gedetailleerde behandelingsgegevens mogen niet zomaar worden verstrekt. De privacywetgeving en het medisch beroepsgeheim stellen dwingend grenzen aan de verwerking van (bijzondere) persoonsgegevens.

Samenwerking in de jeugdzorg

Het CBP adviseerde in 2001 over de informatiehuishouding van de bureaus voor jeugdzorg, waarin de verschillende vormen van jeugdzorg samenwerken bij diagnose en doorverwijzing. In 2002 bleek deze samenwerking in de praktijk toch de nodige vragen op te roepen rond de uitwisseling van cliëntgegevens. De hulpverleners uit de diverse sectoren fungeren immers ook vaak als medewerkers van het bureau. In een dergelijke situatie ontstaat gemakkelijk het idee dat informatie over reeds bekende cliënten onderling mag worden uitgewisseld. Het CBP adviseerde het betrokken bureau en wees op de plicht het beroepsgeheim in acht te nemen. Een praktische en rechtmatige samenwerking is echter wel degelijk mogelijk; zie de casus in dit jaarverslag op pagina xx.

Aanpak van kindermishandeling

In 2002 adviseerde het CBP positief inzake het Ontwerpbesluit advies- en meldpunten kindermishandeling. Hierbij worden onder andere regels gegeven voor het niet bekendmaken van de identiteit van de persoon die een vermoeden van kindermishandeling heeft gemeld of van de persoon van wie informatie voor het onderzoek is verkregen. Het Ontwerpbesluit (artikel 10) beoogt een bepaalde rechtszekerheid te garanderen bij de behandeling van het inzagerecht en het recht op informatie van de betrokkene. Daarbij wil men ook voorkomen dat de identiteit van een melder of informant via derden bekend raakt.

Er worden verschillende categorieën van melders onderscheiden. De regeling komt erop neer dat geen inlichtingen worden verstrekt over de herkomst van de persoonsgegevens als dat een bedreiging kan vormen voor de minderjarige of de hulpverlener of als dat tot een verstoring kan leiden van de vertrouwensrelatie tussen professional en het gezin. Over een melder buiten de professionele sfeer worden op diens verzoek geen inlichtingen verstrekt.

Gedragscode farmaceutische industrie

In 2002 is de Gedragscode van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie (Nefarma) als eerste gedragscode onder de WBP voorzien van een goedkeurende verklaring. De gedragscode geeft een juiste uitwerking van de WBP en andere wettelijke bepalingen voor de verwerking van persoonsgegevens specifiek voor de sector. De farmaceutische industrie stelt er groot belang aan te hechten dat een zorgvuldig evenwicht wordt

bewaard tussen de verantwoordelijkheid voor ontwikkeling en marktbegeleiding van geneesmiddelen enerzijds en de bescherming van persoonsgegevens anderzijds.

Commerciële DNA-tests

Het CBP heeft in 2002 een onderzoek ingesteld naar twee bedrijven die verwantschapstests op basis van genetisch materiaal aanbieden. In beginsel worden 'testkits' toegezonden aan de aanvrager waarmee wangslijm kan worden afgenomen. In de meeste gevallen gaat het om vaderschapstests. Een en ander bleek niet goed geregeld.

Erfelijkheidsgegevens mogen slechts verwerkt worden met betrekking tot degene bij wie deze gegevens zijn verkregen en slechts met uitdrukkelijke toestemming. De bedrijven bleken zich van deze bijzondere beperking niet bewust. Bijgevolg werden betrokkenen hierover ook onvoldoende geinformeerd.

Voor een kind onder de zestien jaar is voor de test toestemming van zijn wettelijk vertegenwoordiger vereist. Eén ouder is in principe bevoegd het kind te vertegenwoordigen, mits van bezwaren van de andere ouder niet gebleken is. Bij vaststelling van het biologische vaderschap mag niet aangenomen worden dat de andere ouder daar altijd mee instemt. Een verstandige werkwijze is dat de bedrijven een schriftelijke verklaring verlangen waarin staat dat de eventuele andere gezaghebbende ouder of voogd geen bezwaar heeft tegen de test.

Zorgfacturering via internet

Het bedrijf A stelt zich ten doel via internet een efficiënte gegevensuitwisseling mogelijk te maken tussen zorgverleners en zorgverzekeraars voor de financiële afhandeling van zorg. Alle (gezondheids) gegevens die voor declaratieafwikkeling worden verwerkt, zijn (tijdelijk) opgeslagen in één centrale database. Het personeel van het bedrijf heeft geen toegang tot de gegevens. Het bedrijf positioneert zich als bewerker en niet als verantwoordelijke. Het handelt dus uitsluitend op instructie en onder verantwoordelijkheid van zijn opdrachtgevers, namelijk de zorgverleners en de zorgverzekeraars.

Bedrijf A heeft zijn systeem overeenkomstig de aanbevelingen van het CBP ingericht. Het bedrijf heeft gezorgd voor juridische en technische waarborgen voor een rechtmatige verwerking en heeft bovendien gekozen voor een jaarlijkse externe privacyaudit. Voornaamste zorg van het CBP is dat de tijdelijke opslag van gegevens bij groei of uitbreiding van de dienstverlening kan leiden tot onrechtmatige patiëntenregisters.

Dit voorbeeld illustreert vooral twee aspecten van ICT in de zorg. Ten eerste de grote (juridische) complexiteit van dergelijke verwerkingen. Zie voor de details het eindoordeel in deze zaak op de website van het CBP (z2000-1250). Belangrijker is dat rechtmatige verwerking van gezondheidsgegevens met het oog op een efficiëntere zorg, heel wel mogelijk is indien van begin af aan privacybescherming bij de opbouw van systemen wordt meegenomen ■

Handel en diensten

In de sector handel en diensten ging het in 2002 vooral om maatregelen tegen criminaliteit. Tegen de achtergrond van onvrede over wat politie en justitie voor bedrijven konden doen, groeide de behoefte om zelf paal en perk te stellen aan wangedrag en fraude van klanten of eigen personeelsleden. Zwarte lijsten werden gezien als deel van de oplossing.

Onveranderd bleef het wankele evenwicht tussen het belang van het bedrijfsleven bij het verwerken van klantgegevens en het recht op privacy van de consument. Belangrijke winst was de voortgang in de ontwikkeling van een aantal gedragscodes. Ronduit verontrustend was de situatie die onderzoek aan het licht bracht bij een handelsinformatiebureau.

Zwarte lijsten

De KLM voert een zwarte lijst van agressieve reizigers. Horeca-ondernemers hopen via een signaleringssysteem eetpiraten en andere oplichters te weren. Banken en verzekeraars hebben een register voor fraudeurs. Ook de juweliers werken aan een signaleringslijst. Een grote winkelketen wil met een zwarte lijst voorkomen dat bij het ene filiaal ontslagen personeel bij een ander filiaal weer wordt aangenomen. De Raad voor de Nederlandse Detailhandel ontwerpt voor alle leden een zwarte lijst van medewerkers die gefraudeerd hebben. Het CBP achtte de aangemelde systemen deels rechtmatig, deels onrechtmatig.

Het belang van een bedrijf bij zwarte lijsten staat eigenlijk niet ter discussie. De vraag is vooral of het belang van het bedrijf opweegt tegen de individuele consequenties van plaatsing op een zwarte lijst. Naast de ernst van de zaak weegt mee hoe essentieel de voorziening is waarvan iemand wordt uitgesloten. Ook moet het doel niet op een minder ingrijpende manier bereikt kunnen worden.

Als besloten wordt een zwarte lijst in te voeren, moet het bedrijf waarborgen treffen om een dergelijk systeem zorgvuldig te gebruiken. De kans ten onrechte op de lijst te worden gezet moet zo klein mogelijk zijn. Iedereen die op een zwarte lijst wordt gezet, moet hierover zo mogelijk worden geinformeerd. Inzage moet geregeld zijn en mag slechts incidenteel geweigerd worden. Feitelijk onjuiste informatie dient gecorrigeerd te worden. Ook moet duidelijk zijn afgesproken hoe lang de vermelding op de zwarte lijst blijft bestaan.

Zwarte lijst van financiële instellingen

Banken en verzekeraars verwerken persoonsgegevens die van grote invloed kunnen zijn op de wijze waarop personen beoordeeld of behandeld worden. In 2002 werd daarom veel aandacht besteed aan de zelfregulering van de sector en een verkenning van samenwerking met de Autoriteit Financiële Markten. Het CBP heeft bovendien nauwkeurig gekeken naar de zwarte lijst van de gezamenlijke financiële instellingen.

In het zogenaamde Incidentenwaarschuwingssysteem financiële instellingen worden onder andere strafrechtelijke gegevens over frauderende klanten en personeelsleden verwerkt en ook gedeeld met andere financiële instellingen. Het CBP diende daarom een zogenaamd voorafgaand onderzoek in te stellen. In het kader van het overleg met de sector heeft het CBP bij één bank de verwerking van strafrechtelijke gegevens getoetst om te beoordelen of het 'Protocol Incidentenwaarschuwingssysteem' in de praktijk voldoende waarborgen bood. Het voorafgaand onderzoek naar de zwarte lijsten van andere financiële instellingen zou dan gestandaardiseerd kunnen worden. Het voordeel hiervan was - naast een lastenverlichting voor alle partijen - een uniforme aanpak in de sector. Dit pilot onderzoek is afgesloten met een positieve verklaring. Het protocol dient wel steeds in werkinstructies geconcretiseerd te worden.

De gedragscode financiële instellingen

Organisaties die een bepaalde sector vertegenwoordigen, kunnen voor hun leden een gedragscode vaststellen. Het CBP kan op verzoek de gedragscode toetsen en een goedkeurende verklaring uitgeven.

In 2002 is uitvoerig overleg gevoerd met de banken en verzekeraars over een gedragscode. Deze is uiteindelijk in januari 2003 goedgekeurd. In de verklaring stelt het CBP dat de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen met de bijbehorende toelichting een nadere en juiste uitwerking bevat van de WBP en andere wettelijke bepalingen betreffende de verwerking van persoonsgegevens. De gedragscode draagt daarmee bij aan een grotere doorzichtigheid van het gebruik van persoonsgegevens in de financiële sector.

ILVM. FOTOJURIST TE HIER EEN ANDERE FOTO AFGEBEELD DAN IN HET GEDRUKTE JAARVERSLAG.

Belangrijk in de gedragscode is de doelbinding, ook binnen de instellingen. Persoonsgegevens die voor bepaalde activiteiten zijn verkregen, mogen binnen dezelfde instelling voor andere activiteiten worden verwerkt, mits dit niet op gespannen voet staat met het oorspronkelijke doel waarvoor de gegevens verzameld zijn.

De opportuniteit van de gedragscode bleek uit de vragen en klachten die het CBP in september 2002 kreeg over een mailing van de Postbank en de ING Bank. Hierin werd het voornemen meegedeeld om de relatiegegevens voortaan in één centraal systeem vast te leggen. Het onderzoek is in 2003 afgerond met de conclusie dat de mailing onvoldoende informatie gaf over het doel van het klantenbestand en de daarvoor te gebruiken gegevens.

Marketing en melding

In de afgelopen jaren is een viertal studies gepubliceerd met als doel de bescherming van consumentengegevens in de marketingsfeer te bevorderen. In 1999 verscheen *Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden*. In juni 2000 verscheen *Klant in het web. Privacywaarborgen voor internettoegang* en in september 2000 *Herkomst van de klant. Privacyregels voor etnomarketing.* In september 2001 werd *Klant te koop. Privacyregels voor adressenhandel* gepubliceerd en gepresenteerd op het jaarcongres van de toenmalige brancheorganisatie DMSA.

Ondanks deze uitgebreide voorlichting en ondersteuning bij de ontwikkeling van praktische normen, laat de respons in de sector echter te wensen over. De privacytoets van het gerechtvaardigde marketingbelang van bedrijven leidt lang niet altijd tot adequate waarborgen, al was het maar in de vorm van heldere informatie voor de consument. De sector presteerde eveneens onder de maat bij de tijdige melding van verwerkingen bij het CBP. In 2003 zal daarom de wijze van handhaving van de meldingsplicht nader overwogen worden.

Handelsinformatiebureaus

Een ronduit onbevredigende situatie bestaat in de sector van de handelsinformatiebureaus. De Nederlandse Vereniging van Handelsinformatiebureaus heeft in 2002 weliswaar overleg gevoerd met het CBP over een conceptgedragscode maar resultaat werd nog niet bereikt. Dit klemt te meer aangezien de bescherming van persoonsgegevens geen groot gewicht in de schaal legt in de sector als geheel.

Sinds 1996 heeft de Registratiekamer enkele malen een onderzoek ingesteld naar een handelsinformatiebureau. In 1999 bleek dat aan een bureau gegevens werden verstrekt uit persoonsregistraties waarvoor een strikte geheimhoudingsplicht gold. Een groot onderzoek in 2001 leidde tot de conclusie dat het onderzochte bureau de wettelijke geheimhoudingsverplichting van anderen bewust doorbrak, hoewel het op de hoogte was van de geldende regelgeving. Het bureau zette ook organisaties aan tot het onrechtmatig verstrekken van informatie. Bij diverse instanties zoals sociale diensten, zorginstellingen, uitzendbureaus en nutsbedrijven werd informatie opgevraagd en vaak ook verkregen. In 2002 is een controleonderzoek bij dit bureau gestart.

In 2002 heeft het CBP bij weer een ander bureau een diepgaand onderzoek uitgevoerd en kwam tot globaal dezelfde conclusies; de casus op pagina xx geeft een impressie van dit onderzoek. Kennelijk is meer nodig dan incidenteel toezicht om de handelsinformatiebranche zich te laten voegen naar het wettelijke kader voor de verwerking van persoonsgegevens. Bedrijven hebben een evident belang bij goede creditscoring en verhaalsinformatie. Dat dient echter wel in balans te worden gebracht met het algemene belang dat is gemoeid met een betrouwbaar en integer functioneren van overheden en bedrijven in hun omgang met persoonsgegevens. Een oplossing dient wellicht gezocht te worden in nadere regelgeving voor het verkrijgen van persoonsgegevens voor creditscoring en incasso ■

GLASVEZEL, BACKBONE VAN HET DATAVERKEER

Telecommunicatie

De telecommunicatiesector wordt geconfronteerd met een uitgebreide regelgeving op grond van Europese richtlijnen, nationale wetten en jurisprudentie. Naast de algemene privacyregels kent de sector ook bijzondere regels. Juist de samenhang tussen de algemene en bijzondere regels is niet altijd helder. Het CBP signaleerde onzekerheid in de sector bij het toepassen van de privacynormen en neemt klachten over het tekortschieten van informatie serieus. Het CBP, toezichthouder op de sector naast de OPTA, zal zich in 2003 daarom inspannen de sector op concrete punten, zoals bijvoorbeeld nummeridentificatie, te informeren over de geldende normen.

De voornaamste kwestie die in 2002 vanuit privacyoptiek in de sector speelde, was die van het bewaren en gebruiken van verkeersgegevens. Telecomaanbieders verzamelen enorme hoeveelheden gegevens over de telecommunicatie van individuen (vaste en mobiele telefonie en internet), zij bewaren deze gegevens ook na afloop van de communicatie en voor hen is het verdere gebruik van deze gegevens voor allerlei innovatieve diensten van groot commercieel belang. Marketing op basis van telecommunicatiegegevens is van strategische waarde.

De verkeersgegevens, de gegevens nodig om de verbinding tot stand te brengen en te onderhouden, geven veel informatie over de betrokkenen. De telecom-aanbieders zagen zich in het klimaat van na September 11 geconfronteerd met een sterke politieke beweging om deze data voor het doel van opsporing en straf-vordering zeer lang te doen bewaren. Dit is een ernstige bedreiging van de bescherming van de persoonlijke levenssfeer.

Verkeersgegevens

In de huidige telecommunicatiesystemen vervangt het signaleringssysteem al lang de telefoniste met het schakelbord: computers zoeken de beste route, leggen de verbinding en onderhouden deze. De gegevens die hiervoor nodig zijn, worden doorgaans verkeersgegevens genoemd. Een deel van de verkeersgegevens wordt geruime tijd bewaard voor het afrekenen van de geleverde diensten. De gegevens worden verder opgeslagen voor netwerkbeheer, fraudedetectie en marketing van diensten.

Welke gegevens nu precies als verkeersgegevens te beschouwen zijn, verschilt per telecommunicatiedienst. Mobiel telefoonverkeer bijvoorbeeld genereert ook gegevens over de locatie van telefoons. De verwachting is dat deze locatiegegevens een centrale rol zullen spelen in toekomstige telecommunicatiesystemen. Zij kunnen gebruikt worden om extra diensten aan gebruikers te leveren, bijvoorbeeld voor routeplanning en logistiek, hulpverlening en beveiliging, marketing en verkoop.

In 2002 heeft het CBP een verkennende studie gedaan naar het afrekenen en verrekenen van telecommunicatiediensten als oriëntatie op het gebruik van verkeersgegevens. Ook de verkeersgegevens moeten immers veelal als persoonsgegevens beschouwd worden. Een goed beeld van de praktijk van gegevensverwerking in de telecommunicatie is nodig voor constructieve normontwikkeling met en effectief toezicht op de sector. Het ligt in de rede de samenwerking met de OPTA daarbij verder uit te werken.

Geheime nummers

Het CBP en de OPTA, toezichthouders op de naleving van de Telecommunicatiewet (Tw), startten na klachten in juli 2002 een onderzoek naar het beleid van KPN inzake 'geheime nummers'. De toezichthouders wilden van de grootste aanbieder van telefonie in Nederland weten hoe de abonnees geinformeerd worden over dit beleid en hoe het bedrijf vorm geeft aan de rechten van de abonnee. OPTA en CBP besloten ook het verstrekken van adresgegevens aan derden voor reclamedoeleinden bij het onderzoek te betrekken.

Het onderzoek stelt drie hoofdvragen: de rechtmatigheid van het beschikbaar stellen van persoonsgegevens van abonnees met een geheim nummer voor commerciële, ideële of charitatieve doeleinden; ten tweede welke informatie KPN abonnees geeft over het geheime nummer en hun rechten; ten derde de keuzemogelijkheden die KPN abonnees biedt bij het commerciële gebruik van abonneegegevens. Het onderzoek zal in 2003 worden afgerond.

Klantcontact en marketing

Voor abonnees en gebruikers zijn de gegevensverwerkingen achter een telefoongesprek of een e-mail goeddeels ondoorzichtig. De complexiteit van de technologieën alsmede de ondoorzichtigheid van de samenwerkingsvormen tussen aanbieders, maken het vrijwel onmogelijk om zicht te houden op wat nu eigenlijk met gegevens gebeurt. Transparantie is echter een noodzakelijke voorwaarde willen klanten hun (privacy)rechten kunnen uitoefenen. De houding van de sector is nu eerder: wat niet weet wat niet deert.

Het CBP heeft in 2002 een zogenaamd voorafgaand onderzoek gedaan bij een telecomaanbieder die in zijn callcenter de telefoongesprekken met klanten vastlegde. Daarnaast werden verkeersgegevens langere tijd bewaard en gebruikt voor marketingdoeleinden. Telefoongesprekken met klanten bleken standaard te worden opgenomen en gedurende drie maanden bewaard voor training van het personeel en daarnaast ook wel voor bewijsvoering en klachtafhandeling. Deze verwerking werd onrechtmatig geacht zowel jegens het personeel als jegens de klanten, onder meer omdat daarover aan hen geen enkele informatie werd verstrekt.

Ook het feitelijk tot drie jaar bewaren van verkeersgegevens werd niet rechtmatig geacht, onder meer omdat er geen bewaartermijn was vastgesteld voor gegevens nodig voor de afrekening.

Een periode van drie jaar is voor dat doel langer dan noodzakelijk. De abonnee werd evenmin een reële mogelijkheid geboden zich over het gebruik van verkeersgegevens voor marketing uit te spreken.

Melding

Het CBP heeft naar aanleiding van deze zaak in juli 2002 de telecomaanbieders geinformeerd over de sectorspecifieke kanten van de meldingsplicht onder de WBP. Verwerkingen van persoonsgegevens voor openbare telecommunicatiediensten komen niet in aanmerking voor een vrijstelling. Om onnodige problemen te voorkomen bij de eventuele aanvraag van een voorafgaand onderzoek naar de melding, adviseerde het CBP de telecombedrijven een aantal gedragslijnen te volgen. Deze gedragslijnen hebben tot doel een rechtmatige verwerking en correcte melding te bevorderen. Het CBP zal in 2003 de opgedane ervaringen bundelen in een document bedoeld voor overleg met de sector en voor de ontwikkeling van een beleidskader voor toezicht in de sector.

Opsporing en verkeersgegevens

In samenwerking met het CBP organiseerde het Instituut voor informatierecht van de Universiteit van Amsterdam in september 2002 een seminar over de technische, publiekrechtelijke en strafvorderlijke aspecten van verkeersgegevens. Het seminar resulteerde in maart 2003 in een publicatie.

Het CBP pleitte ook bij die gelegenheid voor grote terughoudendheid bij de opslag van verkeersgegevens. Verkeersgegevens geven in de context zeer veel informatie over het gedrag van mensen. Verkeersgegevens kunnen ook veel aanwijzingen geven over de inhoud van de communicatie. Het grondrecht op vertrouwelijke communicatie is hierdoor in het geding.

Op Europees niveau werd in 2002 door regeringen gesproken over een systematische bewaarplicht voor de verkeersgegevens van alle telefoongesprekken, faxverkeer, e-mails en overig gebruik van internet. Deze zouden bewaard moeten blijven voor politie, justitie en veiligheidsdiensten. Op 3 september 2002 liet het CBP de Minister van Justitie weten dat het een algemene bewaarplicht voor verkeersgegevens van een jaar of meer onevenredig en in geen geval toelaatbaar achtte. Een bewaarplicht van een jaar of meer vormt een onrechtmatige inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer, zoals omschreven in artikel 8 van het Europees Verdrag voor de Rechten van de Mens. De bescherming van verkeersgegevens is verder ook vastgelegd in de Europese Richtlijn inzake privacy en elektronische communicatie.

Op 11 september gaven de Europese privacytoezichthouders, bijeen in Cardiff, een verklaring van dezelfde strekking uit. Europese regelgeving maakt het bewaren van verkeersgegevens voor het doel van de rechtshandhaving alleen mogelijk voor een beperkte periode en alleen voor zover noodzakelijk, passend en proportioneel in een democratische samenleving ■

PSEUDO-IDENTITEITEN

Technologie en audit

De afgelopen jaren heeft het CBP veel geïnvesteerd in de ontwikkeling en het uitdragen van het concept van de Privacy-Enhancing Technologies (PET).
In 2002 bleek het rendement van deze investering. Het door het CBP georganiseerde PET-symposium in mei 2002 liet zien dat deze aanpak zich in de praktijk heeft bewezen en proven technology is geworden. PET heeft ook een belangrijke plaats gekregen in het toekomstige persoonsnummerbeleid van de overheid.
De belangstelling voor de auditinstrumenten bleef in 2002 zeer groot, ongetwijfeld ook gestimuleerd door de meldingsplicht. Het CBP heeft in 2002 zijn inspanningen vooral gericht op privacycertificering. Daarbij beoogt het CBP commerciële audit-organisaties een kader te bieden voor het verlenen van privacycertificaten. Het CBP is in 2002 tevens begonnen met een evaluatie van de eigen investeringen in technologie. Daarnaast is de rol van technologie en auditing opnieuw bezien in het kader van de organisatieontwikkeling van het CBP.

Privacy-Enhancing Technologies

Op 23 mei 2002 vond in de Ridderzaal te Den Haag het symposium *Privacy by design* plaats over de toepassing van Privacy-Enhancing Technologies in informatiesystemen. Het symposium was een eerbewijs aan de inspirerende bijdrage van John Borking aan het denken over technology en privacy. John Borking was van 1994 tot 2001 plaatsvervangend voorzitter van de Registratiekamer en vervolgens tot 2002 lid van het College bescherming persoonsgegevens.

Het doel van het symposium was beleidsmakers van overheid en private sector de praktische bruikbaarheid van het PET-concept te laten zien. Door privacyregels mee te nemen in het ontwerp van het informatiesysteem kan immers een rechtmatige verwerking van persoonsgegevens (deels) gegarandeerd worden: *privacy by design*. Vanuit een oogpunt van privacybescherming is het beter dat iets niet kan, dan dat het alleen maar verboden is. Uit de zorgsector werden drie werkende informatiesystemen gepresenteerd: het systeem van de geestelijke gezondheidszorg Flevo-Veluwe (Meerkanten), het Landelijk Alcohol en Drugs Informatiesysteem (keteninformatisering voor verslaafdenzorg) en het Nederlandse Brandwonden Informatiesysteem.

In het internationale gedeelte werden de ervaringen met het PET-concept in Canada en Duitsland belicht. In Sleeswijk-Holstein wordt geprobeerd via marktpartijen het PET-concept met behulp van een 'privacy-keurmerk' voor producten ingang te doen vinden en zo privacybescherming te stimuleren. Uit de afsluitende bijdrage van Nederland~ICT sprak eveneens een groot vertrouwen dat privacybescherming in de vorm van PET bij voldoende vraag ook een commercieel product kan zijn. De overheid als ICT-grootverbruiker werd gevraagd hier het initiatief te nemen.

Belangrijk voor de toekomst van PET in Nederland zijn inderdaad de ontwikkelingen rond de elektronische overheid. De elektronische identiteits- en informatie-infrastructuur die aan het ontstaan is, zal voorzien worden van PET. Dit sluit aan op de WBP en de kamerbreed aangenomen motie dat de overheid de toepassing van onder meer Privacy-Enhancing Technologies ter hand neemt. In het advies *Persoonsnummerbeleid* van de commissie Van Thijn (zie ook p. 29) zijn PET onderdeel van 'vertrouwensfuncties': naast klassieke waarborgen dus ook technische waarborgen voor geautoriseerd berichtenverkeer tussen geauthentiseerde communicatiepartijen, voor de integriteit en de vertrouwelijkheid van dit berichtenverkeer, voor de transparantie ervan, en voor het bieden van de mogelijkheid met pseudo-identiteiten te werken.
In het Burgerservicenummer-model zullen dus technische en organisatorische maatregelen gerealiseerd worden om invulling te geven aan het PET-concept. Er zijn bovendien enkele goede voorbeelden van PET-implementaties op sectorniveau die in het burgerservicenummer-model een ruimere verspreiding zullen krijgen. Nu het PET-concept genoegzaam bekend is geworden, zal het CBP de aandacht minder richten op de introductie van het concept en meer op de advisering rond de toepassing van uitwerkingen van PET.

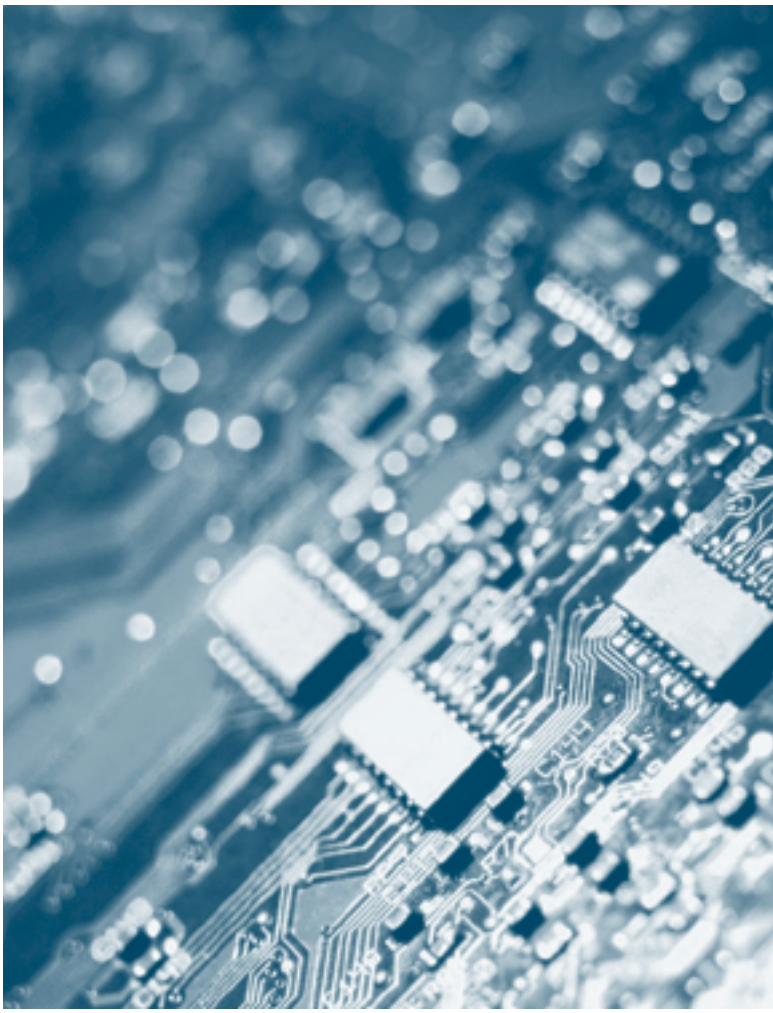
Certificering

De WBP-assurance producten *WBP Zelfevaluatie* en *Raamwerk Privacy Audit* vonden in 2001 en 2002 gretig aftrek evenals de CBP-studie *Beveiliging van persoonsgegevens* (2001). Een en ander bevestigde de ingeslagen weg naar privacycertificering. Met het doel in Nederland te komen tot een privacycertificaat is in het verlengde van het Samenwerkingsverband Audit Aanpak door het Samenwerkingsverband Certificering in 2002 grote vooruitgang gemaakt met de concretisering van een geheel van afspraken dat het mogelijk maakt organisaties te kwalificeren met een privacycertificaat voor specifieke verwerkingen. In nauw overleg met de beroepsorganisaties die kunnen optreden als accreditatie-instelling is het schema opgesteld op basis waarvan auditors geaccrediteerd kunnen worden als privacy auditor. Bij het opstellen van de certificeringseisen speelt het *Raamwerk Privacy Audit* een sleutelrol.

De eerste opzet van een certificatieschema is voorbereid en onder meer de brancheorganisaties Koninklijk NIVRA en NOREA zijn bereid als accreditatie-instellingen op te treden voor het erkennen van auditors die de bevoegdheid krijgen om erkende privacycertificaten af te geven.

Inzet van technologie en auditing

Technologische en auditondersteuning van de onderzoeken van het CBP bleef in 2002 belangrijk en zal dat ook blijven. In 2002 deden auditors en technologen van het CBP verschillende onderzoeken of droegen daaraan bij. Het ging om het gezamenlijke Europese onderzoek naar .Net Passport van Microsoft, deelname aan roadmapprojecten ingebracht in het zesde Kaderprogramma van de Europese Unie (PAMPAS en RAPID), de bijdrage aan audits van Europol-systemen, de betrokkenheid bij de ontwikkeling van een nationaal informatiesysteem voor de politie, het dossieronderzoek



bij enkele sociale diensten, controleaudits bij een incassobureau en een handelsinformatiebureau en de bijdrage aan het diepgaande CBP-onderzoek in 2002 naar, wederom, een handelsinformatiebureau.

Het CBP is in 2002 tevens begonnen met een evaluatie van de eigen investeringen in technologie en auditing. Het technologisch veld is zeer groot en sterk in beweging. Een zelfstandige onderzoeksrol op dit gebied is voor het CBP niet weggelegd. De eigen investering in het bestuderen van MIX – een PET-concept voor telecommunicatiesystemen – is in 2002 afgerond. Toekomstige deelname aan een geavanceerd technologisch project als het project Privacy-Incorporated Software Agents ligt minder voor de hand. Voor PISA is in 2002 een eerste versie van een handleiding opgeleverd met een vertaling van normen uit de EU-privacyrichtlijn in beschrijvingen van concrete softwarecomponenten. In 2003 zal het project worden afgerond met het bouwen van een proefomgeving die ook door het CBP getoetst zal worden.

Anderzijds zal blijvend genvesteerd moeten worden in technologische kennis om als adviseur en toezichthouder voldoende beslagen ten ijs te komen. Voor de komende tijd is de verwachting dat technologiethema's als mobiel internet, digital rights management, toepassing van biometrie en identiteitsvraagstukken de aandacht van het CBP zullen vragen. In de kern gaat het steeds om het uitwerken van privacynormen in de technische inrichting van systemen. Het CBP zal vanaf 2003 deze brugfunctie tussen recht en techniek op een wat andere wijze gaan invullen. Het CBP wil meer het accent leggen op het informeren en adviseren van de partijen die informatiesystemen voor verantwoordelijken ontwikkelen. Beoogd wordt vanuit een tweedelijnspositie de commerciële 'eerste lijn' te adviseren met het oog op de ontwikkeling van de (markt)waarde van privacybescherming. Het streven samen met andere partijen een certificeringssystematiek ingang te doen vinden, sluit hierop aan ■

GEGEVENS REIZEN SNELLER DAN KOFFERS

Internationaal

Toenemend internationaal gegevensverkeer brengt met zich mee dat een effectieve bescherming van die gegevens een steeds grotere internationale dimensie dient te krijgen. Voor het CBP betekent dit dat het veel aandacht besteedt aan de internationale aspecten van de privacywetgeving. Het gaat met name om vragen rond het toepasselijke recht en de doorgifte van persoonsgegevens naar landen buiten de Europese Unie. Internationalisering van gegevensverkeer, in samenhang met de integratie en toekomstige uitbreiding van de Europese Unie, dwingen de toezichthoudende autoriteiten tot onderlinge samenwerking. De nationale privacywetgeving van de Europese lidstaten is de implementatie van de Europese Richtlijn 95/46/EG en de betekenis van wettelijke bepalingen is daarmee mede afhankelijk van beslissingen op Europees niveau. Afstemming van beleid en gezamenlijke advisering zijn van belang om tot effectief en geharmoniseerd toezicht te komen. Ook bilaterale samenwerking tussen toezichthouders in concrete zaken speelt een steeds grotere rol.

Het CBP neemt dan ook deel aan diverse vormen van internationale samenwerking en draagt tevens bij aan het gemeenschappelijke toezicht op het terrein van politie en grensbewaking.

Internationaal gegevensverkeer

In 2002 heeft het CBP intensief contact gehad met Nederlandse en buitenlandse organisaties over hun internationale gegevensverkeer, zowel in het kader van zijn voorlichtende taak als met het oog op de advisering aan de Minister van Justitie bij de vergunningverlening voor doorgifte naar derde landen. De eerste vergunningen op basis van artikel 77 lid 2 WBP zijn inmiddels door de Minister verleend.

Veel partijen maken gebruik van de door de Europese Commissie goedgekeurde modelcontracten. De meeste vergunningaanvragen betreffen personeelsgegevens die worden opgeslagen in een internationale database die ter beschikking staat van een concern. Met name als er veel partijen zijn betrokken bij een doorgifte kan het gebruik van contracten tot complexe situaties leiden. In overleg met betrokken partijen denkt het CBP na over mogelijkheden om de voorwaarden voor deze doorgiften te vereenvoudigen, met behoud van het niveau van de waarborgen. In dit verband is er ook met collega-toezichthouders gewerkt aan mogelijkheden voor intensivering en coördinatie van de samenwerking rond de vergunningverlening.

Europese Unie

Het afgelopen jaar is er ook in de Artikel 29-werkgroep veel aandacht geweest voor de grensoverschrijdende aspecten van gegevensbescherming. Deze groep is het onafhankelijke overlegorgaan van Europese nationale toezichthouders, die zijn bestaansgrond vindt in artikel 29 van Richtlijn 95/46/EG. De groep adviseert de Europese Commissie over privacykwesties en binnen de groep vindt ook afstemming en harmonisatie van nationaal beleid plaats. Hiertoe komt de groep meerdere malen per jaar bijeen in Brussel.

In dit verband is het CBP nauw betrokken geweest bij de beoordeling van de contractuele bepalingen voor doorgifte die door de Internationale Kamer van Koophandel (ICC) met een aantal partijen zijn ontwikkeld. Ook heeft het CBP meegewerkt aan de totstandkoming van een werkdocument van de Artikel 29-werkgroep over de toepasselijkheid van de Europese privacywetgeving in de context van het gebruik van internet door niet-EU-websites (zie ook pagina 64).

Binnen het kader van de groep heeft het CBP, in samenwerking met een aantal collega-toezichthouders, met Microsoft overlegd over de online-authenticatiedienst .NET Passport (zie ook de casus op pagina xx). Hierop heeft het bedrijf toegezegd zijn authenticatiesysteem te wijzigen om te voldoen aan de Europese regelgeving. Concreet heeft dit tot gevolg dat gebruikers beter worden geinformeerd en meer zeggenschap krijgen over het gebruik van hun gegevens door Microsoft en deelnemende websites binnen en buiten de EU.

In reactie op berichten dat de Verenigde Staten in het kader van het nationale veiligheidsbeleid luchtvaartmaatschappijen verplichten passagiersgegevens uit de reserveringssystemen te

verstrekken aan de Amerikaanse autoriteiten, heeft de groep een kaderstellend advies opgesteld over de rechtmatigheid van deze gegevensverstrekking. Daarmee werd een belangrijke bijdrage geleverd aan de Europese besprekingen met de Amerikaanse autoriteiten.

In september 2002 nam het CBP, samen met vele partijen uit alle geledingen van de maatschappij, deel aan de conferentie die de Europese Commissie organiseerde in het kader van de evaluatie van de Europese privacyrichtlijn. Uit de vele discussies, met bijdragen van het CBP op het gebied van Privacy-Enhancing Technologies en videobewaking, bleek dat de principes en hoofdlijnen van de richtlijn breed worden onderschreven. Ook hier werd aandacht gevraagd voor harmonisatie en Europese samenwerking en voor flexibiliteit in het kader van het gegevensverkeer met derde landen.

Samenwerking met andere toezichthouders

In het kader van de Complaints Workshop, de halfjaarlijkse workshop voor medewerkers van Europese toezichthouders, heeft het CBP een inventarisatie gemaakt van het doorgiftebeleid van de deelnemende landen. Dit heeft inzicht geboden in de nationale wetgeving en werkwijze van de deelnemers en is daarmee een basis voor verdere samenwerking. In deze interactieve workshop, die is gericht op praktische aspecten van de dagelijkse werkzaamheden van toezichthouders, participeerden nu voor het eerst ook de toezichthouders uit de landen die in 2004 toetreden tot de EU. Via het besloten internetplatform dat de deelnemers aan de workshop ter beschikking staat, heeft het CBP bijgedragen aan samenwerking bij de behandeling van nationale en internationale zaken.

Tijdens de Lenteconferentie van Europese toezichthouders, waaruit de Complaints Workshop voortkomt, heeft het CBP zijn auditmethode en certificeringsproject gepresenteerd. Audits en certificering kunnen een belangrijke bijdrage leveren aan zelfregulering en handhaving.

Veiligheid en verkeersgegevens

In 2002 is de nieuwe Richtlijn 2002/58/EG over privacy en elektronische communicatie tot stand gekomen. Het bewaren van verkeersgegevens voor opsporingsdoeleinden is onder strikte voorwaarden als mogelijkheid voorzien. Lidstaten hebben de wens verkeersgegevens voor langere tijd voor deze doeleinden te bewaren. Tijdens de Wereldconferentie in Cardiff hebben de Europese toezichthouders op Nederlands initiatief een verklaring aanvaard over de ontoelaatbaarheid van het bewaren van verkeersgegevens voor een langere termijn dan enkele maanden.

De Wereldconferentie was tevens bij uitstek de gelegenheid om verschillende beelden van privacy te toetsen. Deelnemers vanuit bedrijfsleven, wetenschap, maatschappelijke organisaties en overheid discussieerden over de overeenkomsten en tegenstellingen in hun visies op onderwerpen als de rol van de toezichthouder en veiligheid en privacy in het informatietijdperk. In een tijd waarin de wereld een ‘global village’ wordt genoemd waarbij persoonsgegevens wereldwijd kunnen rondgaan, is deze uitwisseling van visies een belangrijke bijdrage aan een goede internationale samenwerking bij de bescherming van de persoonlijke levenssfeer en andere rechten en vrijheden van burgers.

Schengen, Europol en Douane

Het CBP is met de andere nationale toezichthouders ook vertegenwoordigd in de gemeenschappelijke controle-autoriteiten die in het leven zijn geroepen voor het Schengen Informatiesysteem (SIS) en de gegevensbestanden van Europol. Deze autoriteiten komen regelmatig bijeen en worden ondersteund door een gemeenschappelijk secretariaat. Een soortgelijke autoriteit is werkzaam voor het Douane Informatiesysteem (DIS). Daarnaast is er een onafhankelijke beroepscommissie voor geschillen over de uitoefening van het recht op kennisneming en verbetering bij Europol.

De gemeenschappelijke controle-autoriteiten voor Schengen en Europol hebben in 2002 adviezen uitgebracht over voorstellen in de Raad van Ministers tot aanpassing van de verdragen om een verbreding van het gegevensverkeer mogelijk te maken. Op een aantal punten is deze inbreng ter harte genomen. Ook is geadviseerd over gegevensverkeer met derde landen, waaronder de Verenigde Staten.

Raad van Europa

De wortels van de Europese privacybescherming liggen in het Dataprotectieverdrag van de Raad van Europa uit 1981, waarbij thans 29 landen partij zijn. Het CBP vertegenwoordigt Nederland in de adviescommissie van dit verdrag. Ook in dit bredere verband is er veel aandacht voor de internationale dimensies van privacybescherming. Na de aanvaarding van het additionele protocol in 2001, waarin onder andere regels zijn opgenomen voor doorgiften van persoonsgegevens aan landen die niet partij zijn bij het verdrag, zijn in 2002 door de adviescommissie richtlijnen vastgesteld voor het opstellen van contractuele bepalingen voor doorgifte naar deze landen.

Het CBP nam in december deel aan de conferentie van de Raad van Europa. Vanuit een praktische invalshoek werd daar het viersporenbeleid van het CBP gepresenteerd. De conferentie was gericht op de oprichting en ontwikkeling van privacytoezichthouders in de landen die nieuw toetreden tot de Raad ■

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

Organisatie

In 2002 heeft het CBP een organisatieverandering ingezet om invulling te geven aan de nieuwe taken en (sanctionerende) bevoegdheden en de daarmee samenhangende noodzakelijke waarborgen. Een extern advies heeft hiervoor de basis gelegd. Ondanks de verslechterende economische omstandigheden hebben de Minister van Justitie en de Tweede Kamer het belang van effectief toezicht op de naleving van de WBP onderstreept door het budget van het CBP voor 2003 substantieel te verhogen.

Productie

Het jaar 2002 stond in het teken van een aanscherping van de werkwijze van de organisatie in lijn met de Algemene wet bestuursrecht. Nieuwe werkprocessen werden ontwikkeld en geimplementeerd. Een aantal zaaksoorten dat het CBP in het kader van de WBP behandelt, is beduidend complexer, legt een groter beslag op medewerkers en heeft een langere doorlooptijd dan voorheen.

Onder de productie van het CBP worden de afgehandelde 'zaken' verstaan. De verschillende zaaksoorten zijn gerelateerd aan de wettelijke taken van het CBP (zie het kader). Zaaksoorten kennen doorgaans meerdere behandelniveaus. Bij de intake van zaken wordt bepaald wat het behandelniveau zal zijn: frontoffice, backoffice of college (sterzaken). Het behandelniveau geeft de complexiteit van de te behandelen zaak aan en in de werkprocesbeschrijving wordt aangegeven wat de bijbehorende werkwijze dient te zijn, wie daarbij betrokken is en wie gemandateerd is voor de afdoening.

Het overzicht van de productie in 2002 is geaggregeerd op het niveau van zaaksoort. Ter vergelijking zijn ook de cijfers van 2000 en 2001 weergegeven, althans voor zover mogelijk, aangezien door de invoering van de WBP nieuwe zaaksoorten zijn gecreëerd. In de productietabel is goed zichtbaar wat het effect is van de implementatie van de WBP bij organisaties en bedrijven: zeer weinig meldingen in 2001 en een groot aantal voorafgaande onderzoeken.

De wijze waarop burgers, bedrijven en organisaties contact zoeken met het CBP is door de groei van het gebruik van internet en e-mail duidelijk gewijzigd. Door de inrichting van een 'e-mailpiket' naast het telefonisch spreekuur, kon het aantal voorlichtingsverzoeken dat formeel in behandeling werd genomen, in 2002 worden teruggebracht. Het aantal verzoeken om informatie dat per e-mail binnen kwam, nam echter wel toe. Het grote aantal vragen dat door burgers, organisaties en professionals bij het CBP wordt neergelegd, blijft daarom een punt van aandacht. Door effectieve inzet van de website wordt getracht het aantal verzoeken om voorlichting binnen de perken te houden.

	2000	2001	2002
Wetgevingsadviezen	35	43	26
Gedragscodes	6	1	5
Reglement WPR (tot 1 sept 2001) en WpolR	88	50	40
WBP-meldingen vanaf 1 sept 2001	n.v.t.	591	8.454
Voorafgaand onderzoek	n.v.t.	12	90
Voorlichtingsverzoeken	910	1.204	686
Internationale zaken	10	13	33
Bijzondere gegevens	n.v.t.	0	0
Gegevensverkeer derde landen	n.v.t.	0	10
Bemiddeling en klachten	323	290	282
Ambtshalve onderzoek	17	24	11
Boete	n.v.t.	n.v.t.	0
Dwangsom	n.v.t.	n.v.t	0
Bestuursdwang	n.v.t.	n.v.t.	1
Beroep	n.v.t.	n.v.t.	1
Bezwaar	n.v.t.	0	4
Wet openbaarheid bestuur	0	0	19
Publieksvoorlichting (telefonisch spreekuur)	4.277	4.979	5.715
Vragen WBP-melding (telefonisch spreekuur)	n.v.t	0	2.500
Publieksvoorlichting (via e-mail)	n.v.t.	291	1.890
Klachten over het CBP	0	0	9

OVERZICHT VAN DE PRODUCTIE IN 2000-2002

Taken van het CBP

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

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

- **Reglementen**
  De WBP voorziet, 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 in principe slechts in behandeling als daarvoor een bijzondere reden bestaat.
  Ingevolge de Wet politieregisters zijn reglementen in bepaalde gevallen onderworpen aan een toetsing vooraf in het kader van een hoorprocedure. Tezamen met de portefeuillehouder privacy van de politie vanuit de Raad van hoofdcommissarissen heeft het CBP een werkwijze ontwikkeld voor de harmonisatie van de inhoud van de reglementen en het stroomlijnen van de procedure voor goedkeuring. Door deze werkwijze kan het aantal procedures voor goedkeuring en het aantal meldingen van tijdelijke registers worden beperkt.

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

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

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

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

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

- **Doorgifte naar derde landen**
  Op grond van artikel 77 lid 2 WBP heeft het CBP de taak om de Minister van Justitie te adviseren over het toekennen van een vergunning voor het doorgeven van persoonsgegevens naar een land buiten de EU dat geen waarborgen voor een passend beschermingsniveau biedt. Het gezamenlijk beleid van de Minister en het CBP is eind vorig jaar bekend gemaakt. De verzoeken van bedrijven met internationale belangen om een vergunning beginnen nu goed op gang te komen. De behandeling van verzoeken door het CBP is er op gericht de Minister van Justitie van een gedegen advies te voorzien zodat besluitvorming snel kan plaatsvinden.
  Ook de samenwerking tussen de toezichthoudende autoriteiten wordt intensiever. Met zekere regelmaat bereiken het CBP dan ook verzoeken om bijstand van buitenlandse zusterinstellingen. Via een gemeenschappelijke, besloten website kunnen de eenvoudigste verzoeken snel worden afgewikkeld. In een aantal gevallen zijn nadere onderzoekshandelingen nodig.

- **Bemiddeling en klachtenbehandeling**
  Het CBP is op grond van artikel 47 WBP belast met de behandeling van verzoeken om bemiddeling bij geschillen over de uitoefening van het recht op inzage of correctie van persoonsgegevens en over de uitoefening van het recht op verzet. Deze procedure is mede bedoeld om de rechter te ontlasten. Belanghebbenden kunnen er ook voor kiezen om hun zaak voor te leggen aan de civiele of administratieve rechter, of gebruik maken van een geschillenregeling in een goedgekeurde gedragscode. Als het CBP de bemiddeling heeft beëindigd, kan de zaak alsnog aan de rechter worden voorgelegd. De rechter kan besluiten om (opnieuw) het advies van het CBP in te winnen.
  Verder kan het CBP op grond van artikel 60 WBP op verzoek van een belanghebbende een onderzoek instellen naar de naleving van het bepaalde bij of krachtens de wet. Daartoe beschikt het CBP over de nodige onderzoeksbevoegdheden op grond van de WBP en de Algemene wet bestuursrecht. Bij het aannemen van dergelijke verzoeken voert het CBP een restrictief beleid. De mogelijkheid van toetsing door de Nationale Ombudsman stelt echter hoge eisen aan deze afweging.

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

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

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

WBP-meldingen

Het melden van bestaande en nieuwe verwerkingen onder de WBP kwam in 2002 vertraagd op gang. Gezien de prognose voor het aantal meldingen (circa 25.000) mag geconcludeerd worden dat de implementatie van de WBP bij een te groot aantal organisaties en bedrijven nog niet is doorgevoerd.

Het WBP-meldingenproces vroeg veel aandacht van de organisatie, zowel administratief als inhoudelijk. Het toegenomen gebruik van e-mail en internet heeft het CBP kunnen benutten voor grotere efficiëntie bij de melding. Het elektronische meldingsprogramma kan eenvoudig van de website worden gedownload en via e-mail weer worden aangeleverd bij het CBP. Hiervan is veelvuldig gebruik gemaakt. Na afloop van het overgangsjaar per 1 september 2002 heeft een eerste analyse plaatsgevonden op het naleven van de WBP-meldingsverplichting. Brancheorganisaties en overheidsorganen zijn op basis van deze eerste analyse aangeschreven als het ontvangen aantal meldingen achterbleef bij de verwachting ten aanzien van de branche. Het CBP zal in het vervolg periodiek het WBP-meldingenbestand analyseren en de naleving van deze verplichting beoordelen.

Klachten over het CBP

In de Algemene wet bestuursrecht is geregeld dat iedereen over de wijze waarop een bestuursorgaan zich tegenover hem of haar heeft gedragen een klacht kan indienen bij dat orgaan. Deze klachten moeten op een zorgvuldige wijze worden behandeld. Verder moeten bestuursorganen zorgen voor registratie en publicatie van bij hen ingediende schriftelijke klachten. Bijgevoegd overzicht geeft het aantal ingediende schriftelijke klachten weer met de wijze van afdoening.

	2002
Totaal aantal klachten	9
Klachten ongegrond verklaard	4
Klachten gegrond verklaard	2
Minnelijke regeling/geen oordeel/ingetrokken/andere wijze van afdoening/nog in behandeling	3

KLACHTEN OVER HET CBP 2002

Verzoeken om heroverweging en klachten over het CBP worden vaak ingediend omdat men het niet eens is met de weigering van het CBP om een onderzoek in te stellen op verzoek van belanghebbende. Men is het er niet mee eens dat de klacht van belanghebbende geen prioriteit krijgt of dat het CBP deze niet van voldoende zwaarwegend belang acht om over te gaan tot een handhavingsonderzoek.

Organisatieontwikkeling

De ontwikkeling en verandering van de organisatie is ook in 2002 planmatig aangepakt. Zo zijn er projecten uitgevoerd die direct bijdragen aan de verbetering van het primaire proces, zoals het realiseren van de mogelijkheid om via e-mail elektronisch een WBP-melding te doen en het toegankelijk maken van de informatie uit het openbare register van meldingen via internet. Voor deze projecten heeft het Ministerie van Economische Zaken in het kader van het verlichten van de administratieve lasten en de toegankelijkheid van de overheid voor de burger een subsidie verstrekt.

Andere projecten dragen indirect bij aan de verbetering van het primaire proces en de organisatieontwikkeling zoals de ontwikkeling van werkprocessen, de implementatie van de WBP in de eigen organisatie, een herinrichting van de website gericht op transparantie en informatievoorziening en het onderzoek naar vorming, bewaring en vernietiging van dossiers in het kader van het Project Invoering Verkorting Overbrengingstermijn (PIVOT).

Formatieontwikkeling

Medio 2002 heeft een extern bureau advies uitgebracht over de wijze waarop het CBP de komende jaren invulling kan geven aan de nieuwe taken, (sanctionerende) bevoegdheden en de daarmee samenhangende waarborgen. De ondernemingsraad kon zich in dit advies op hoofdlijnen vinden. Dit heeft er toe geleid dat in september 2002 een begin werd gemaakt met de inrichting van de nieuwe afdeling Interventie, bezwaar en beroep. De kwartiermaker, casu quo het beoogd hoofd voor deze afdeling, is gestart met het in kaart brengen van de verschillende aspecten van rechtsbescherming en handhaving. Op termijn wordt ook een afdeling Onderzoek voorzien.

Ondanks de verslechterende economische omstandigheden hebben de Minister van Justitie en de Tweede Kamer het belang van toezicht op de naleving van de WBP onderstreept door het budget van het CBP voor 2003 substantieel te verhogen. De ingezette formatieontwikkeling kan daardoor worden voortgezet.

	2000	2001	2002
Personeel	2.338,20	2.693,60	2.853,40
Materieel	623,2	1.225,80	1.762,10
Totaal	2.961,40	3.919,40	4.615,50

BUDGETTOEKENNING 2000-2002 (BEDRAGEN MAAL 1000 EURO)

Medewerkers

De gemiddelde bezetting is in 2002 gelijk gebleven ten opzichte van 2001, ondanks het feit dat er 15 nieuwe medewerkers zijn aangetrokken. De uitstroom wordt mede veroorzaakt door de grote belangstelling van andere organisaties (onder andere het aanstellen van functionarissen voor de gegevensbescherming) naar de specifieke kennis die het CBP in huis heeft.

	2000		2001		2002	
	m	v	m	v	m	v
In dienst	4	6	5	8	6	9
Uit dienst	6	4	6	6	5	2
Bezetting einde jaar m / v	23	28	22	30	23	37
Bezetting einde jaar totaal	51		52		60	
Mobiliteit	21%		23%		13%	
In tijdelijke dienst	9		9		11	
Fulltime in dienst	42		43		49	
Gemiddelde bezetting (fte's)	47,8		49,6		49.6	
Bezetting einde jaar totaal (fte's)	49,4		50,7		54,3	

FORMATIE 2000-2002

De uitstroom van kennis brengt met zich mee dat de organisatie veel moet investeren in kennisborging voor de organisatie en in kennisontwikkeling bij nieuwe medewerkers. Individuele medewerkers gaan naar verschillenden opleidingen en daarnaast worden er groepstrainingen *in company* aangeboden. Zo is de WBP-training voor nieuwe medewerkers opnieuw gegeven en hebben medewerkers een cursus gericht op de Algemene wet bestuursrecht gevolgd.

	2000		2001		2002	
	m	v	m	v	m	v
Uitzendkrachten	–	–	0	0,49	0	1,25
Stagiaires	–	–	0,07	0,69	0	0,75

OVERZICHT MEDEWERKERS BUITEN FORMATIE 2000-2002

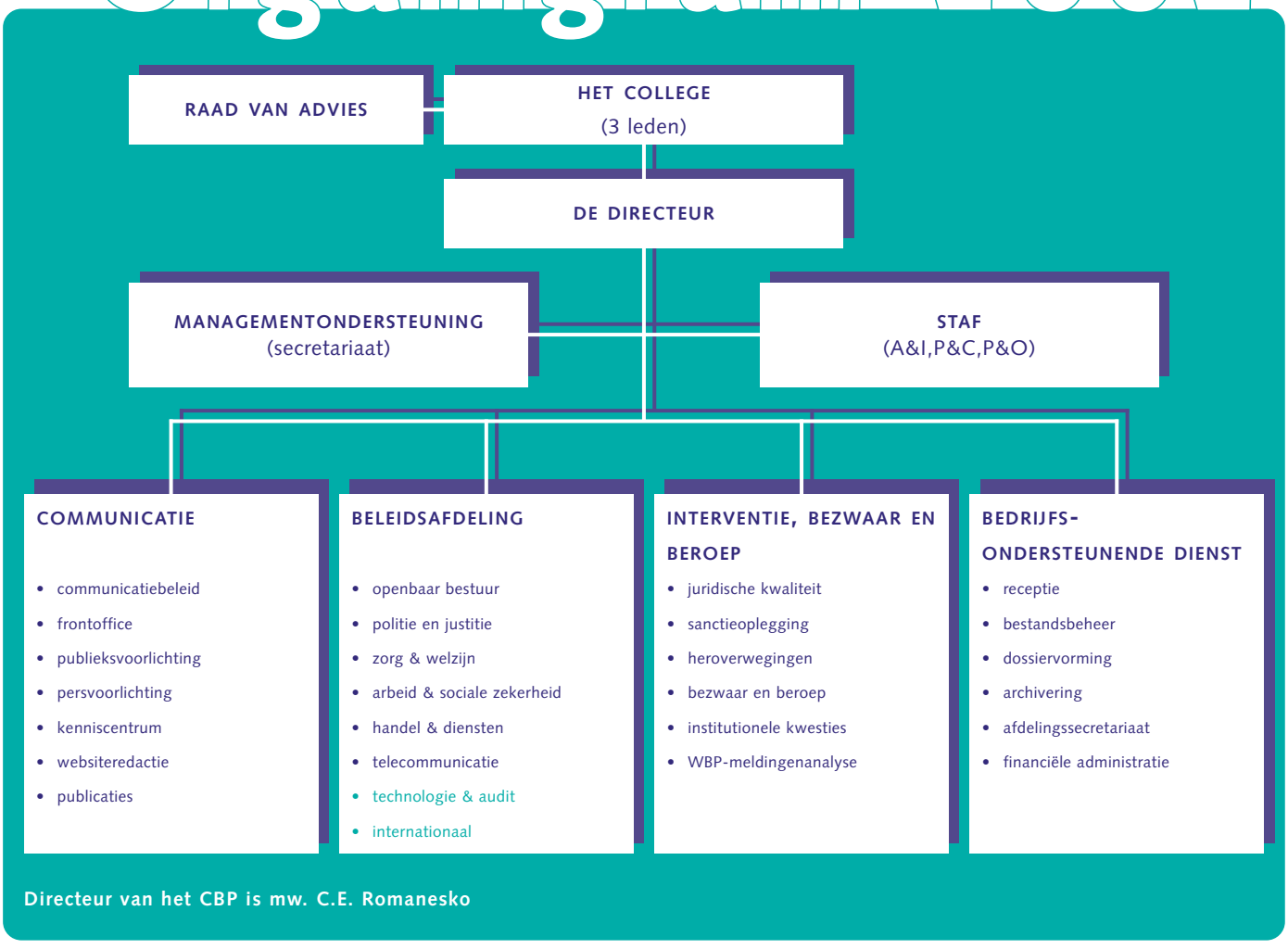
Het ziekteverzuim is gedaald van 8,15 % in 2000 naar 6,27 % in 2002. In het Sociaal-Medisch-Team wordt periodiek afgestemd met de bedrijfsarts en de personeelsfunctionaris en zonodig gezocht naar passende oplossingen. Voor het eerst in lange tijd kent het CBP geen langdurig zieken meer.

Een aandachtspunt blijft de werkdruk. Het CBP heeft in 2002 op verzoek van de ondernemingsraad aan een Arbo-dienst de opdracht gegeven tot het uitvoeren van een werktevredenheidsonderzoek in het kader van een risico-inventarisatie en evaluatie. De resultaten zullen begin 2003 worden meegenomen bij de verdere organisatie- en formatieontwikkeling. In 2002 is aandacht besteed aan verbetering van de werkplekken. Een deel van het meubilair is vervangen en de toegang tot internet en het e-mailverkeer op elke werkplek is sterk verbeterd. Ook de informatievoorziening vanuit het kenniscentrum, een onderdeel van de afdeling communicatie, is meer gestructureerd en beter toegankelijk voor medewerkers.

	2000	2001	2002
Totaal ziekteverzuim excl. zwangerschap	8,15%	6.97%	6,27%
Waarvan langdurig verzuim	4,01%	3.78%	0
Ouderschapsverlof	2	2	3
Verlof zwangerschap/bevalling	1	2	0
Kinderopvangplaatsen	2	2	4
Opleiding (euro's x 1000)	40	56	99
% t.o.v. personele budget	1,47 %	2,05 %	3,47%

ZIEKTEVERZUIM EN OVERIGE PERSONELE INFORMATIE 2000-2002

Organigram 2002



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

bijlagen

wetgevingsadviezen

Wetsvoorstel vorderen gegevens financiële sector
21 januari 2002

Wetsvoorstel tot wijziging van hoofdstuk 11 van de Telecommunicatiewet
29 januari 2002

Aanscherping op de Wet financiering van giften aan politieke partijen door natuurlijke personen
4 februari 2002

Wetsvoorstel cameratoezicht wijziging Gemeentewet
5 februari 2002

Wetsvoorstel incidentele identiteitscontroles
6 februari 2002

Autorisatieaanvraag inzake woningbehoeftenonderzoek en Balkan-onderzoek
21 februari 2002

Wijziging van de Wet op de kansspelen inzake het organiseren van kansspelen op het internet
7 maart 2002

Wetsvoorstel justitiële gegevens
10 april 2002

Voorstel wetswijziging diverse onderwijswetten inzake het gebruik van het Sofi-nummer
15 april 2002

Wetsvoorstel kansspelen op internet
15 april 2002

Uitwisseling van gegevens uit Justitiële Documentatie met de Nederlandse Antillen en Aruba
16 april 2002

Wetsvoorstel Ambtenaren Integriteit
22 april 2002

Advies gegevensuitwisseling tussen het College van zorgverzekeringen en de Pensioen- en Verzekeringskamer in het kader van de deskundigheids- en betrouwbaarheidstoets
14 mei 2002

Amvb beleidsinformatie Wet op de jeugdzorg
10 juni 2002

Wetsvoorstel openbaarheid topinkomens
20 juni 2002

Verzoek ter uitvoering van artikel 67 derde lid onder c van het Besluit GBA
7 oktober 2002

Besluit DNA-onderzoek in strafzaken
9 oktober 2002

Wetsvoorstel tot wijziging Wet op de rechtsbijstand houdende aanpassing aan het fiscale inkomens- en vermogensbegrip
16 oktober 20002

Ontwerpbesluit advies- en meldpunten kindermishandeling
16 oktober 2002

Instellingsbesluit criminele inlichtingen eenheid FIOD-ECD
5 december 2002

Wetsvoorstel cameratoezicht op openbare plaatsen
6 december 2002

Wetsvoorstel Algemene bijstandswet (nu: Wet werk en inkomen)
10 december 2002

Wetsvoorstel implementatie nieuwe richtlijnen Telecommunicatiewet
10 december 2002

Wetsvoorstel kilometerheffing
11 december 2002

Ontwerpbesluit gebruik persoonsgebonden nummers in het onderwijs (Wet op het voortgezet onderwijs)
20 december 2002

Wetsontwerp van de Wet aansprakelijkheidsverzekering motorrijtuigen en de Wet toezicht verzekeringsbedrijf 1993 richtlijn 2000/26/EG
20 december 2002

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

onder de WBP

Gedragscode Verwerking Persoonsgegevens Financiële Instellingen; geldig tot 27 januari 2008 (Stcrt. 2003, 23)

Gedragscode inzake het verwerken van persoonsgegevens van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie (Nefarma); geldig tot 2 september 2007 (Stcrt. 2002, 167)

onder de WPR

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 vastgesteld voor politieregisters

Aandachtsvestigingen	(Stcrt. 2002, 243)
Arrestanten	(Stcrt. 2002, 243)
Arrestatiebevelen	(Stcrt. 2002, 243)
Bedrijfsprocessensysteem BPS	(Stcrt. 2002, 243)
Bedrijven informatiesysteem en waarschuwingsadressen	(Stcrt. 2002, 243)
Bekeuringenafhandelingssysteem	(Stcrt. 2002, 243)
Beperkingen besturen motorrijtuigen	(Stcrt. 2002, 243)
Bureau financiële ondersteuning	(Stcrt. 2002, 243)
Fraudebestrijding	(Stcrt. 2002, 243)
Gegevensuitwisseling milieucriminaliteit	(Stcrt. 2002, 243)
Gevonden en verloren goederen	(Stcrt. 2002, 243)
Graffitibestrijding	(Stcrt. 2002, 243)
In beslag genomen goederen	(Stcrt. 2002, 243)
In bewaring genomen goederen	(Stcrt. 2002, 243)
Inbraakbestrijding	(Stcrt. 2002, 243)
Informantenregister	(Stcrt. 2002, 100)
Informantenregister openbare orde	(Stcrt. 2002, 238)
Internationale rechtshulp politie	(Stcrt. 2002, 243)
Jeugd- en zedenzaken	(Stcrt. 2002, 243)
Kabinetszaken	(Stcrt. 2002, 243)
Meldkamer	(Stcrt. 2002, 243)
Milieudelicten	(Stcrt. 2002, 243)
Multipol	(Stcrt. 2002, 243)
Openbare orde en informatie	(Stcrt. 2002, 238)
Openbare orde taken Regionale inlichtingendienst	(Stcrt. 2002, 243)
Opkopers en helingbestrijding	(Stcrt. 2002, 243)
Overvallenbestrijding	(Stcrt. 2002, 243)
Permanent autoteam	(Stcrt. 2002, 243)
Processen-verbaal en rapporten	(Stcrt. 2002, 243)
Recidive	(Stcrt. 2002, 243)
Rijverboden	(Stcrt. 2002, 243)
Schietwapen incidentenregistratie- en informatiesysteem	(Stcrt. 2002, 243)
Signalen van mensenhandel	(Stcrt. 2002, 13)
Technische recherchezaken	(Stcrt. 2002, 243)
Vakantiecontrolekaarten	(Stcrt. 2002, 243)
Vandalismebestrijding	(Stcrt. 2002, 243)
Verdovende middelen	(Stcrt. 2002, 243)
Voorlopig register	(Stcrt. 2000, 198)
Zware criminaliteit	(Stcrt. 2000, 198)

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

bijlagen

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

06 March 2002 - **Fifth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in Third Countries covering the year 2000** (Document 10557/02, WP 54)

29 May 2002 - **Working document on the surveillance of electronic communications in the workplace** (Document 5401/01, WP 55)

30 May 2002 - **Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites** (Document 5035/01, WP 56)

30 May 2002 - **Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe** (Document 10761/02, WP 57)

30 May 2002 - **Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6** (Document 10750/02, WP 58)

2 July 2002 - **Working document - First orientations of the Article 29 Working Party concerning on-line authentication services** (Document 11203/02, WP 60)

2 July 2002 - **Opinion 3/2002 on the data protection provisions of a Commission proposal for a Directive on the harmonisation of the laws, regulations and administrative provisions of the Member States concerning credit for consumers** (Document 11190/02, WP 61)

2 July 2002 - **Working document on functioning of the Safe Harbor Agreement** (Document 11194/02, WP 62)

3 October 2002 - **Opinion 4/2002 on adequate level of protection of personal data in Argentina** (Document 11081/02, WP 63)

11 October 2002 - **Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data** (Document 11818/02, WP 64)

3 October 2002 - **Working document on Black Lists** (Document 1118/02, WP 65)

24 October 2002 - **Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States** (Document 11647/02, WP 66)

Deze documenten zijn te vinden op het internetadres: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

onderzoeksrapporten 1996 - 2002

2002

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

Privacy bij wetenschappelijk onderzoek en statistiek. Kader voor een gedragscode, mei 2002

Sociale diensten: bijstandsdossier en privacy, februari 2002

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 persoons-gegevens,** 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 patiënten-registratie,** 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 rijksverkeers-inspectie,** 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 telefoon-gesprekken van werknemers,** november 1996
- **Privacy-audit Handelsinformatiebureau,** juli 1996

bijlagen

achtergrondstudies en verkenningen (1994 - 2002)

In de serie Achtergrondstudies en verkenningen zijn verschenen:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

brochures

Gedragscodes. Bescherming van persoonsgegevens door zelfregulering
oktober 2002

Derde landen. De doorgifte van persoonsgegevens naar landen buiten de Europese Unie/ Third countries. Transfers of Personal Data to Countries outside the European Union
september 2002

Privacy: checklist voor de ondernemingsraad
april 2002

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

Functionaris voor de gegevensbescherming. Een handreiking
augustus 2001

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

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

informatiebladen

Zwarte lijsten, november 2002
Cameratoezicht: richtlijnen en vuistregels voor verantwoordelijken in bedrijven en organisaties, augustus 2002
Cameratoezicht: rechten van de betrokkene, augustus 2002
Het melden van een gegevensverwerking, augustus 2002
Bewaartermijnen, juli 2002
Camera's op de werkplek, april 2002
Verstrekken van personeelsgegevens aan derden, april 2002
Doorgifte naar derde landen, januari 2002
De sociale dienst en uw persoonsgegevens, november 2001
Het gebruik van kentekengegevens en uw privacy, oktober 2001
Als de politie u vragen stelt over uw klanten of werknemers, oktober 2001
Belangrijkste verschillen tussen de Wet persoonsregistraties en de Wet bescherming persoonsgegevens (betrokkene), september 2001
Belangrijkste verschillen tussen de Wet persoonsregistraties en de Wet bescherming persoonsgegevens (verantwoordelijke), september 2001
Bemiddeling door het College bescherming persoonsgegevens, september 2001
De functionaris voor de gegevensbescherming, september 2001
Het toetsen van uw kredietwaardigheid (creditscoring), september 2001
Rechten van de betrokkene, september 2001
Uw klacht en het College bescherming persoonsgegevens, september 2001
Uw persoonsgegevens beveiligd, september 2001
Geadresseerde reclame, september 2001
Voorafgaand onderzoek, september 2001
Vrijstellingen, augustus 2001

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 kranten, tijdschriften en vakbladen 2002

Artz, S.M., en G.W. van Blarkom, **De wet bescherming persoonsgegevens en biometrie: privacy een technisch vraagstuk?**, Jaarboek fraudebestrijding 2002, p. 52-60.

Helden, W.J. van, en N. M. van Seumeren, **Het vinden van feiten,** Viszie, mei 2002, p. 7.

Hooghiemstra, T.F.M., **Privacy bij ICT in de zorg: Bescherming van persoonsgegevens als kritische succesfactor,** Zorg Management Magazine, november 2002, p. 40-44.

Hustinx, P.J., **Privacy bedreigt veiligheid niet,** NRC Handelsblad, 5 november 2002, opiniepagina.

Hustinx, P.J., **Co-regulation or self-regulation by public and private bodies - the case of data protection,** Freundesgabe für Alfred Büllesbach 2002, p. 283-288 (www.alfred-buellesbach.de).

Kenny, S., en J.J. Borking, **The Value of Privacy Engineering,** The Journal of Information, Law and Technology, 2002.

Kenny, S., and L. Korba*, **Privacy Rights Management for Digital Rights Management,** Computers & Security, november 2002.

Lieon, S., en S.M. Artz, **Controle op e-mail- en internetgebruik van werknemer,** Security Management, onafhankelijk vakblad voor professionele beveiliging, december 2002, p. 25-27.

Lieon, S., **E-mail en internet,** OR Informatie, 2 oktober 2002, p. 4-7.

Lieon, S., **De OR waakt over de privacy op het werk,** De Ondernemingsraad, juni 2002, p. 38-40

Munster-Frederiks, mr. M.Th. van, **Privacy: checklist voor de ondernemingsraad,** OR Informatie, 2 oktober 2002, p. 8-15.

Pol, U. van de, en W.J. van Helden, **Zwarte lijsten zonder waarborgen onwettig,** Noord-Hollands Dagblad, 29 oktober 2002, p. 4.

Pol, U. van de, **Toezicht en kwaliteit nog beneden de maat: terugblik één jaar bijzondere politieregisters,** in: B. Andriesse, mr. U. van de Pol en J.B.A. de Wit, Criminele Informatie; Afscherming of openheid? ('Wat bijzonder is, moet bijzonder blijven'), Den Haag 2002, p. 109-120.

Pol, U. van de, **OM mag persoonsgegevens wel vrijgeven,** Volkskrant, 9 maart 2002.

Fontein, drs. M.A.H., **Mogen overheden, bedrijfsleven en andere instanties naar de etnische afkomst van burgers vragen en deze gegevens registreren?,** in: mr. drs. C.A. Tazelaar, Multicultureel Nederland in 70 vragen, Den Haag 2002, p. 171-173.

Het CBP heeft in 2002 inhoudelijk en financieel bijgedragen aan het tot stand komen van R. Hes, A.H. Ekker en B.J. Koops, **Verkeersgegevens. een juridische en technische inventarisatie.** L.F. Asscher en A.H. Ekker red.; Instituut voor informatierecht, UvA, 2003. Het boekje is een uitwerking van presentaties en discussie tijdens de workshop Verkeersgegevens georganiseerd door het Instituut voor Informatierecht (UvA) en het College bescherming persoonsgegevens.

* Niet werkzaam bij het CBP.

Review of 2002

Security was the primary focus of political and public debate in 2002. Amid the general calls for greater decisiveness, supervision and control, various prominent administrators and politicians made a caricature of privacy. Privacy protection was portrayed as an impediment to public safety; privacy legislation therefore required reform. In November, the administration proposed that everyone over the age of twelve should have a legal obligation to identify themselves. It was also suggested that, with a view to aiding the fight against crime and terrorism, all telecommunication traffic data should be retained for an extended period. The Dutch Data Protection Authority (DPA) is very concerned that a simplistic introduction of greater police powers could seriously undermine the rights and interests of ordinary citizens.

Furthermore, the Dutch DPA strongly refutes the notion that privacy protection acts as a barrier to the resolution of social problems by hindering cooperation between various authorities. It is the Dutch DPA's conviction, borne out by experience, that privacy protection is one of the success factors for effective government.

There are very few legitimate government objectives whose realisation may be impeded by privacy rules. Provided, that is, that such rules are taken into account from the outset in the design of organisational structures, information systems and procedures and the formulation of policy.

Privacy and security

The citizen's interest in privacy must always be weighed up against other important interests. International treaty law, European directives and our own country's constitution and privacy legislation define the parameters within which this should take place. These parameters form part of the framework of ground rules on a government's behaviour towards its citizens. Privacy rules require that careful consideration is given to the object, effectiveness and proportionality of government action and that sufficient safeguards exist against the abuse of power. To set privacy legislation aside is to accept that such controls and safeguards are not required.

Lack of respect for the privacy of the individual ultimately erodes public faith in government. Citizens who have nothing to hide deserve a government that consistently takes privacy protection into account when formulating policy, designing information systems or defining the responsibilities of the individual.

Hence, the right to privacy is fundamental to the security that a democratic constitutional state affords its citizens. Removal of the right to privacy denies the honest citizen an important safeguard and undermines democracy itself.

Compulsory identification

In December 2002, legislation was proposed, providing for the introduction of compulsory identification. Early in 2003, the Dutch DPA advised against bringing a bill before parliament. The proposed legislation fails to strike an appropriate balance between the rights and obligations of the individual and those of the government.
A permanent obligation would be placed upon the citizen without any evidence that specific obligations are not sufficient. Criminalising failure to identify oneself would create a situation in which any member of the public was liable to be regarded as a suspect.

The question of whether a limited or general obligation to identify oneself should be introduced has been debated in the Netherlands for the last twenty years. Hitherto, it has always been concluded that a general requirement would be unduly onerous. Given that the current proposal is not based on fresh arguments in this regard, its implementation would constitute a contravention of the European Convention on Human Rights, which requires that any infringement of individual privacy must be adequately justified.

Camera surveillance of public places

Public camera surveillance remains a topical issue and is in need of better statutory regulation. Such surveillance has become generally accepted as a legitimate means of furthering security and public order, although initial evaluations of CCTV projects suggest that the security benefits are not as great as has sometimes been suggested. During the course of 2002, the Dutch DPA published two advisory reports regarding the Camera Surveillance of Public Places Bill. In the interests of legal clarity, a statutory framework is important. The Dutch DPA fully supported the proposal that the authority to install cameras should be given to mayors by order in council. Such authority is consistent with a mayor's responsibility to maintain public order.

The proposed legislation would permit the installation of CCTV in churches and comparable locations. Is it the intention that the government should have the power to place surveillance cameras in churches, mosques and other places of worship in the name of public order?

Electronic government

The government's management of information is gradually becoming more structured, as the authorities seek to operate as efficiently and reliably as possible. This development brings significant threats to and opportunities for the protection of personal information. In 2002, the Dutch DPA set out its vision in a study report entitled *Elektronische overheid en privacy: bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid* (Electronic government and privacy: the protection of personal data in the government's information infrastructure). Intended primarily for policy-makers, the report discusses privacy-design principles for information systems and analyses the scope allowed by the privacy rules.

Trust is a vital precondition for a functional information infrastructure. The Dutch DPA therefore has reservations about the plea for every citizen to have control over his or her personal data. The government should undoubtedly ensure optimal transparency, but there are practical limits on the scope for informational self-determination. The Personal Data Protection Act deliberately provides for a system of checks and balances, in which consent and objection merely play a corrective role. What is more important is that the government should of its own accord operate in a transparent manner that promotes trust.

Results secured in 2002

In last year's annual report, it was announced that in 2002 priority would be given to securing the following results:

- **Electronic government**
  In its study report *Elektronische overheid en privacy* (Electronic government and privacy), the Dutch DPA set out how government can use ICT to work more efficiently and effectively, while preserving or enhancing privacy safeguards. This vision has contributed to the government's policy on the streamlining of population records and the use of personal ID numbers.

- **ICT in healthcare**
  In its study report *Privacy bij ICT in de zorg* (Privacy and the use of ICT in the healthcare sector), the Dutch DPA indicated how privacy protection can be more effectively institutionalised in the healthcare sector. The report's recommendations have been widely publicised within the sector. Taking proper account of privacy issues at an early stage is a critical success factor in the context of new developments in this field.

- **Research and statistics**
  The policy document *Privacy bij wetenschappelijk onderzoek en statistiek* (Privacy in the context of scientific research and statistics) clarifies the legal rules governing the use of personal data in this field. The document also provides a framework for the development of a code of conduct to serve as guidance on compliance with the rules in practical situations. The Royal Dutch Academy of Science has taken the initiative in this regard.

- **Employees**
  An updated version of *Goed werken in netwerken* (Working well in networks), a new *Raamregeling voor het gebruik van e-mail en internet* (Framework for the use of e-mail and the Internet) and a brochure entitled *Privacy: checklist voor de ondernemingsraad* (Privacy: checklist for the works council) were published, emphasising the importance of proper privacy protection at work. In addition, the groundwork was done for the publication of a document on the position of workers who have fallen ill.

- **Trade information**
  It did not prove possible in 2002 to achieve consensus within the trade information sector regarding clear guidelines on the lawful processing of personal data or a mechanism for ensuring compliance with such guidelines. This was in spite of the fact that the need for standards and safeguards was emphasised by the findings of Dutch DPA investigations. Given this situation, the Dutch DPA has decided to take firmer action.

- **Telecommunications use**
  The Dutch DPA has conducted exploratory research into the processing of data on the use of telecommunications. The findings served as a basis for a workshop organised in September 2002 in conjunction with the Institute for Information Law and supported by the Netherlands OPTA (*Onafhankelijke Post en Telecommunicatie Autoriteit*, Independent Post and Telecommunications Authority). The research findings were recorded in a publication entitled *Verkeersgegevens* (Traffic Data), which will also be used as a basis for further activities in this field.

Public service numbers

Using its vision of electronic government as a starting point, the Dutch DPA contributed to the report produced by the interdepartmental Van Thijn Committee, entitled *Persoonsnummerbeleid in het kader van identiteitsmanagement* (Personal ID number policy in the context of identity management). The Dutch DPA was represented on the committee. The administration accepted the report's recommendations and announced its intention to put forward proposals for a 'public service number' in 2003.

The introduction of a public service number system would facilitate the clear association of data with the individual citizen and thus support efficient client-oriented government. The use of a number would enable the linkage of data held by different authorities and would therefore help in the detection and prevention of (identity) fraud.

The planned sector-based control of personal ID numbers is consistent with the Dutch DPA's vision of electronic government and its preference for sector and chain numbers. Under the proposals, for example, the justice sector and the healthcare sector would each have their own number systems. Furthermore, the lawful processing of data will be facilitated by the trust functions, which include Privacy-Enhancing Technologies, i.e. technical measures built into the information systems to safeguard privacy.

- **Special police records**
  An improvement was discernible during 2002 in the protection of privacy in connection with the records of 'criminal investigations' by the police. More attention is now being given to both the control and the structural supervision of such records by most forces. Agreement was also reached regarding the streamlining of the procedure for dealing with requests for the disclosure of information by people to whom such records relate. The conclusions were widely publicised within police circles and the public prosecution service.

- **Public register of notifications**
  The Dutch DPA website now provides public access to a register of personal data processing activities notified to the authority. An improved version of the software for submitting notifications on diskette has been released and Internet notifying is now possible. The number of notifications received rose sharply in the course of 2002. The register of data protection officers can also now be consulted via the Dutch DPA's website.

- **Prior checks**
  The number of prior checks into personal data processing activities involving special risks (articles 31 and 32 of the Dutch Personal Data Protection Act) rose markedly in 2002. An overview of these investigations will be posted on the Dutch DPA's website in the course of 2003. In conjunction with the relevant stakeholders (social security investigation teams, municipal social services departments, etc), standards have now been developed covering various common processing activities.

- **Enforcement plan**
  In 2002, an Intervention, Complaints and Appeals Department was set up. The development of an enforcement plan has since led to the creation of a number of tools that enable the Dutch DPA to make effective use of its new powers. The first steps have also been taken towards the systematic checking of compliance with the obligation to notify personal data processing activities.

Social security files

Operation of the social security system requires extensive checks to be made on individual clients. In February 2002, a file investigation was carried out at three social security offices. This involved inspecting client files to establish whether the information held was actually necessary for the assessment of individual clients' entitlement to benefit (i.e. whether the necessity principle was being complied with). In addition, steps were taken to establish where the social security offices obtained information and with whom they shared information. The Dutch DPA formed a positive impression of the way the three offices handled personal data, but is considering making supervisory visits to social security offices in the future.

New social security legislation

At the end of 2002, the Dutch DPA published its response to the proposed new social security legislation, since dubbed the Work and Income Bill. The new legislation is to replace a variety of existing laws and regulations. By giving municipal authorities greater freedom in the definition of individual rights and obligations and in the provision of services, the administration hopes to promote the reintegration of people seeking employment.

The Dutch DPA had previously asked the Minister of Social Affairs and Employment on a number of occasions to draw up clear rules on the sharing of personal data in the context of reintegration. However, the bill does not indicate how in practice data should be processed in connection with reintegration. It appears that a great deal has been left to the discretion of individual municipalities. There is consequently a danger that differences will arise between municipalities in terms of the way reintegration activities are organised.

Social security investigation and fraud teams

Efforts to combat social security fraud received a lot of attention in 2002. A variety of organisations are involved in the investigation of such fraud: (municipal) social security investigation teams, *Regionale Interdisciplinaire Fraudeteams* (Regional Interdisciplinary Fraud (RIF) teams) and the Sociale Inlichtingen- en Opsporingsdienst (Social Security Investigation and Detection Service, SIOD). Having been notified of certain data processing operations, the Dutch DPA carried out a prior check to assess whether the activities were organised on a lawful basis. Similar checks were initiated into the investigative activities of the Uitvoeringsinstituut Werknemersverzekeringen (Employee Insurance Scheme Executive Body) and the Sociale Verzekeringsbank (Social Insurance Bank).

The Dutch DPA assessed the process definition for covert observation drawn up by one of the RIF teams, as well as the associated working practices. In principle, the process definition was considered to provide adequate safeguards for the lawful processing of personal data. It was agreed that the process definition would be made available to other RIF teams by way of example. A similar approach was taken by the Dutch DPA in relation to municipal social security investigation teams.

It is hoped that the strategy adopted can lead to general nationwide harmonisation of the covert observation practices used by RIF teams and (municipal) social security investigation teams. This will be beneficial in terms of legal clarity and compliance with the Personal Data Protection Act, while also simplifying the necessary notification of data processing activities.

Blacklists

Crime-prevention was also very much on the agenda of the business community in 2002. Dissatisfied with the protection offered by the police and judiciary, businesses sought their own means of combating misconduct and fraud by customers and personnel. Among the tools adopted was the blacklist. Against this background, one of the Dutch DPA's focuses during 2002 was the maintenance of a shared blacklist by the financial services industry.

It is undeniable that a business may have a legitimate interest in operating a blacklist. However, it is important to consider whether the significance of that interest is sufficient to justify the consequences of inclusion for the blacklisted individual. If a business decides to introduce a blacklist, steps must be taken to ensure that the system is operated fairly. Without proper safeguards, a blacklist is unlawful.

The use of warning lists to address employee fraud attracted considerable publicity. The Dutch DPA examined a number of lists. The consequences of blacklisting depend to a considerable extent on the scope of the blacklist. Such a list may be used purely in connection with sensitive functions, or for all appointments; it may be used only within a particular business or chain, or it may be shared by an affiliated group of companies or throughout a particular industry. The wider the scope of the list, the stricter the inclusion criteria must be.

Working well in networks

Careful justification and organisation of checks can ensure that necessary fraud prevention measures do not undermine the relationship between employer and employee. The key is achieving an appropriate balance between the interests at stake. Responsible supervision of the (private) use of e-mail and the Internet at work requires a privacy test and good workforce consultation or the cooperation of the works council. With a view to promoting equable measures within employment organisations, in 2002 the Dutch DPA published an updated version of *Goed werken in netwerken* (Working well in networks), a new *Raamregeling voor het gebruik van e-mail en internet* (Framework for the use of e-mail and the Internet) and a brochure entitled *Privacy: checklist voor de ondernemingsraad* (Privacy: checklist for the works council). All these publications attracted a great deal of attention in 2002.

Privacy and the use of ICT in the healthcare sector

In 2002, the Dutch DPA also published a study report entitled *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg* (Privacy and the use of ICT in the healthcare sector. Data protection in healthcare information infrastructures). The report was intended as an overview of the privacy issues associated with the use of ICT in the care sector. The numerous proposed policies, experiments and trends relating to the use of ICT in healthcare will lead to the formation of an electronic identity infrastructure, an electronic information infrastructure and changes in the organisation and funding of healthcare. Most of today's ICT applications have not been designed with sufficient thought for privacy. Within the healthcare sector, success depends to a significant extent on taking proper account of privacy at an early stage.

Healthcare reforms are aiming at greater competition amongst care providers and amongst health insurers. The amount paid for care must be related to the actual costs.

In the context of these reforms, the so-called Diagnose-Behandeling Combinatie (Diagnosis-Treatment Combination, DTC) system is to be adopted. It is important that the government ensures that this system's design takes account of the different roles played by health insurers and the other parties involved in healthcare. Detailed treatment information should not be disclosed without careful consideration. The privacy laws and the principle of medical confidentiality impose strict limitations on the processing of (certain forms of) personal data.

Trade information agencies

A thoroughly unsatisfactory situation exists in the trade information agencies sector. The Dutch DPA had to perform another major investigation at such an agency in 2002. Clearly something more than incidental checks are required to bring this industry into line with the law on the processing of personal data. The business community has a self-evident interest in good credit rating and debt-recovery information. However, a balance has to be found between this interest and society's general interest in the reliable and fair use of personal data by the authorities and by the business community. The best solution is likely to lie in further regulations on the way personal data are obtained for credit rating and debt collection purposes.

Telecommunications

The telecommunications sector has to contend with a variety of regulatory controls in the form of European directives, national legislation and jurisprudence. The Dutch DPA realises that uncertainty exists within the sector regarding the application of privacy standards. In 2003, the Dutch DPA accordingly intends to provide telecommunications companies with practical advice regarding such matters. In conjunction with the Netherlands Independent Post and Telecommunications Authority (OPTA), the Dutch DPA has initiated investigations into the sale by KPN Telecom of address data linked to so-called 'ex-directory' numbers for marketing purposes. The Dutch DPA hopes to extend its cooperation with the OPTA on supervisory issues.

The privacy issue that exercised the industry most in 2002, was the retention and use of traffic data. Telecom service providers gather huge volumes of data on the activities of private individuals (use of landlines, mobile phones and the Internet). Such data are retained after the communication activities cease and can be of great commercial value to providers in the context of a wide variety of innovative services. Telecommunications data are strategically valuable for marketing purposes. In 2002, the Dutch DPA undertook an exploratory study into charging and settlement within the telecommunications industry and made preparations for an investigation into the actual use of traffic data.

Investigation and traffic data

With support from the Dutch DPA, the Institute for Information Law at the University of Amsterdam organised a seminar in September 2002 concerning the technical, criminal and public-law issues surrounding traffic data. At the seminar, the Dutch DPA again called for a cautious approach to the retention of traffic data. Taken in context, traffic data can be highly informative. Hence, the constitutional provisions regarding confidential communication are of relevance in relation to its use.

In the post-September 11 climate, strong political support developed for the prolonged retention of such data for use by investigative agencies. At the European level, inter-governmental discussions were held in 2002 regarding the possibility of compulsory systematic retention of all telephone, fax, e-mail and Internet traffic data. The suggestion was that such data would have to be made available to the police, the Public Prosecutor and the security services. Such a move would be a serious threat to the privacy of the individual.

On 3 September 2002, the Dutch DPA informed the Minister of Justice that it would consider a general obligation to retain traffic data for a year or more to be disproportionate and wholly unacceptable. A joint statement to similar effect was issued on 11 September 2002 by Europe's data protection authorities, meeting at the time in Cardiff. European regulations allow traffic data to be retained for law-enforcement purposes only for a limited period and insofar as retention may be considered necessary, appropriate and proportional in a democratic society.

Privacy-Enhancing Technologies

In recent years, the Dutch DPA has invested substantially in developing and propagating the concept of Privacy-Enhancing Technologies (PET). At the PET symposium organised by the Dutch DPA in May 2002, the message was that PET had proven its worth in practice. Meanwhile, PET has been accorded a significant role in the government's planned personal ID number policy.

The aim of the symposium was to demonstrate the practical benefits of PET to policy-makers in the public and private sectors. By designing information systems to take account of privacy rules, it is possible to ensure – or at least go a significant way towards ensuring – that personal data are processed in a lawful way. In other words, one can achieve privacy by design. A situation in which privacy-compromising action is impossible is preferable to a situation where such action is prohibited. Symposium participants were told about three PET-protected information systems already in use in the Netherlands' healthcare sector, and about application of the PET concept in Canada and Germany.

Certification

The Personal Data Protection Act assurance products *WBP Zelfevaluatie* (Personal Data Protection Act Self-Evaluation) and *Raamwerk Privacy Audit (Privacy Audit Framework)* proved popular in 2001 and 2002, as did the Dutch DPA study report *Beveiliging van persoonsgegevens* (The protection of personal data) (2001). However, the Dutch DPA put less emphasis on publicising this approach in 2002, focusing primarily on privacy certification instead. In this context, the object has been to provide commercial audit organisations with a framework for privacy certification. In close consultation with those representative organisations that act as accreditation bodies, a scheme has been developed for the accreditation of privacy auditors. Certification criteria have been formulated using the *Privacy Audit Framework* as a primary reference. A preliminary structure has been developed for a certification scheme and a number of representative organisations have agreed to act as accreditation bodies, so that auditors may be accredited to issue privacy certificates for particular processing activities.

Targets for 2003

The main targets that the Dutch DPA will pursue in 2003 are as follows:

- **Advice on legislative proposals**
  Article 51, paragraph 2, of the Personal Data Protection Act states that the Dutch DPA has to be consulted about any proposed legislation or general administrative regulations which relates exclusively or to a significant extent to the processing of personal data. In consultation with the relevant government departments, the Dutch DPA will develop parameters to ensure that this statutory requirement is complied with.

- **Data protection officers**
  In accordance with articles 62 to 64 of the Personal Data Protection Act, more than a hundred data protection officers have now been registered with the Dutch DPA. Contact with this growing body of internal supervisors will be consolidated by the Dutch DPA so that there is effective practical interaction between the authority and the individuals concerned.

- **Camera surveillance**
  A growing number of municipalities have been installing camera surveillance systems in public places. The Dutch DPA will investigate how this supervision operates in practice and how privacy issues have been taken into account by the municipalities concerned.

- **Sickness leave**
  Changes to the social security system and in society at large have affected the position of an employee before, during and following a period of sick leave. The Dutch DPA will publish a study report dealing with the privacy issues surrounding the position of employees who take sick leave and with other relevant developments.

- **Police records**
  Following on from the Dutch DPA's earlier activities in connection with the records kept by Criminele inlichtingeneenheden (Criminal Investigation Units, CIEs), checks will be performed at the offices of a number of these units. These checks will draw partly upon the findings of the CIEs' internal evaluations.

- **Telecommunications**
  In practice, the provision of telecommunications services raises a number of privacy-related issues. In collaboration with the OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit, Independent Post and Telecommunications Authority), the Dutch DPA will develop information material to assist service providers. The Dutch DPA will also focus on the obligation to notify data processing activities and on prior checks in the telecoms industry.

- **Certification**
  Output from the earlier Audit Approach Project forms a basis for the development of a system of privacy certification. In conjunction with organisations interested in acting as accreditation bodies, the Dutch DPA will develop this system further and prepare for its implementation. In doing so, the authority hopes to promote compliance with privacy legislation by self-regulation.

- **Website**
  A well-designed website is a central element of the Dutch DPA's communication strategy. The accessibility of the Dutch DPA's website will be improved by, for example, the use of theme files and the creation of a separate section for data subjects' frequently asked questions. The site will also give details of the Dutch DPA's policy in relation to its various tasks.

- **Notification obligation**
  The obligation to notify the Dutch DPA regarding personal data processing activities is important in relation to transparency and accountability. With a view to enforcing compliance with the obligation, systematic checks will be performed. In addition, the authority will make use of its power to impose administrative penalties in the event of non-compliance.

- **Staffing plan**
  In order to ensure the authority's ability to discharge its new responsibilities in the field of supervision and enforcement, the Dutch DPA's structure and staffing arrangements will be reviewed. In the course of the year, a new staffing plan will be drawn up, incorporating new or modified job profiles.

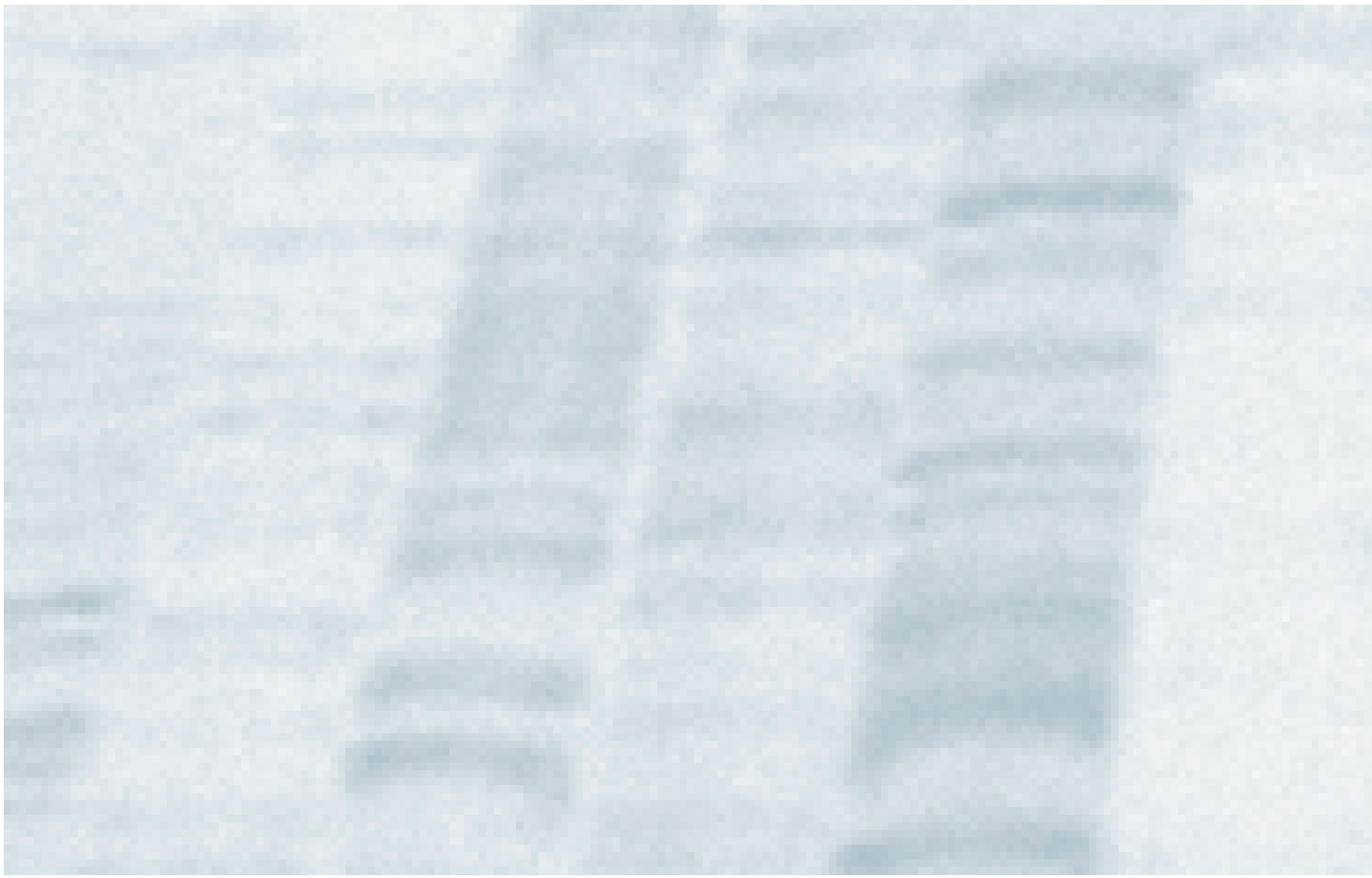
Codes of conduct

In 2002, the *Gedragscode van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie* (Code of Conduct of the Netherlands Association of Research-Oriented Pharmaceutical Companies) became the first code of conduct to be formally approved under the Personal Data Protection Act. To secure approval, a code of conduct needs to reflect the provisions of the act and any other sector-specific rules governing the processing of personal data. Detailed discussions were also held with the banks and insurance companies in 2002 regarding the introduction of a similar code. The *Gedragscode Verwerking Persoonsgegevens Financiële Instellingen* (Code of Conduct for the Processing of Personal Data by Financial Institutions) was ultimately approved in January 2003. The Dutch DPA regards the introduction of this code as a significant development.

The year under review also saw the start of discussions between the Nederlandse Vereniging van Handelsinformatiebureaus (Netherlands Association of Trade Information Agencies) and the Dutch DPA regarding a draft code of conduct. Unfortunately, however, the talks came to nothing yet. Given the situation within the industry, this outcome gave the Dutch DPA particular cause for concern. Nevertheless, progress towards the development of codes of conduct was made with three other bodies: the organisation representing private investigators and security firms (whose industry is growing rapidly but is poorly regulated), the reintegration consultants' umbrella organisation (Borea) and the Koninklijke Beroepsvereniging van Gerechts-deurwaarders (Royal Association of Court Bailiffs). In all three cases, it is anticipated that codes of conduct will be approved in 2003.

Advice on legislative proposals

In line with its four-track policy, the Dutch DPA has been pro-active in the provision of advice to government and other organisations. In the autumn of 2002, the Dutch DPA started talks with the ministries with a view to emphasising its statutory advisory role. It appeared that the ministries were not only unfamiliar with the new regulations, but also uncertain as to the extent of the obligation to seek advice. The Dutch DPA would like to see the legislative procedure modified to take formal account of the need to obtain advice. This would put the Dutch DPA's advisory activities on a more institutional footing and lead to an intensification of activities in this field.



COLOFON

Jaarverslag 2002

College bescherming persoonsgegevens, Den Haag, april 2003.

Met medewerking van:
J.H.M. Baart, M.A.H. Fontein,
P.J. Hustinx, G.O. van de Klashorst,
P. Krul, C.E. Romanesko, B. den Uyl,
V. Vermaas en de beleidsafdeling.

Eindredactie: G.O. van de Klashorst

Ontwerp: Proforma, strategie, ontwerp en management (Miriam Monster)
Vertaling: DBF Communicatie (Alphen a/d Rijn)
Druk: Sdu Grafisch Bedrijf bv (Den Haag)

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

Advies, bemiddeling, onderzoek en interventie

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

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

Voor meer informatie kunt u kijken op de website: www.cbpweb.nl.