jaarverslag 2003

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) doet hierbij verslag over zijn beleid en activiteiten in 2003. Het CBP zag in 2003 bevestigd dat privacy diepe wortels heeft in verdragen en richtlijnen en inmiddels ook in jurisprudentie, met name de eerste arresten van het Europese Hof voor Justitie met betrekking tot de toepasselijkheid van de Privacyrichtlijn en de interpretatie daarvan aan de hand van artikel 8 van het Europees verdrag van de rechten van de mens.

In het publieke debat klinkt vooral de roep om meer controlemaatregelen waarbij bescherming van de persoonlijke levenssfeer als obstakel wordt gezien. Het CBP is bezorgd over de erosie in dat publieke debat van het besef dat persoonsgegevens alleen verwerkt mogen worden voor zover dat werkelijk noodzakelijk is. Maatvoering bij het verzamelen, gebruiken en bewaren van persoonsgegevens blijft geboden.

Positief is de toename van het aantal functionarissen voor de gegevensbescherming bij bedrijven, instanties en andere organisaties. Ook het feit dat in 2003 belangrijke gedragscodes goedgekeurd konden worden dan wel in voorbereiding zijn genomen, voedt de verwachting dat zelfregulering een belangrijke rol zal spelen bij de naleving van de normen en regels voor de omgang met persoonsgegevens.

Met het opleggen van de eerste sancties heeft het CBP ook zichtbaar de wending naar meer handhaving gemaakt die reeds in 2002 werd aangekondigd. De organisatieverandering die werd ingezet om invulling te geven aan de nieuwe taken en (sanctionerende) bevoegdheden, is in 2003 op hoofdlijnen voltooid met de inrichting van de afdeling Interventie, bezwaar en beroep en met de start per 1 januari 2004 van de afdeling Onderzoek.

In december 2003 werd de benoeming bekend van de voorzitter van het CBP, mr. P.J. Hustinx, tot Europees Toezichthouder voor gegevensbescherming. Per 1 februari 2004 is hij in functie getreden. In maart van dit jaar is officieel afscheid van hem genomen met het symposium ‘Privacy op zijn plaats’. Peter Hustinx is benoemd tot Officier in de Orde van Oranje Nassau voor zijn verdiensten en inzet voor privacybescherming in Nederland en in Europa. De onderscheiding werd hem namens Hare Majesteit de Koningin op 22 april 2004 in Rotterdam uitgereikt door de minister van Justitie, mr. J.P.H. Donner tijdens de opening van de voorjaarsconferentie van Europese privacytoezichthouders.

mr. U. van de Pol
waarnemend voorzitter
College bescherming persoonsgegevens

samenstelling

college en raad van advies

college 2003

mr. P.J. Hustinx
voorzitter van het college

mr. dr. U. van de Pol
collegelid

drs. J.W. Broekema
collegelid

raad van advies 2003

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 2003

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

prof. A.W. Neisingh RE RA
privacyaudits

H. de Zwart RE RA RO
privacyaudits

2003 in vogelvlucht

Het recht op privacybescherming is een grondrecht, maar daarmee nog geen absoluut recht. Tot dit recht behoort de zorgvuldige omgang met persoonsgegevens. Het hierin gelegen belang zal steeds afgewogen moeten worden tegen andere belangen. In de publieke sector vindt deze belangenafweging in laatste instantie plaats in het parlement en vertaalt zich doorgaans in waarborgen voor de burger bij het verzamelen en gebruiken van zijn persoonsgegevens. Burgers kunnen zich vaak in een dergelijke afweging vinden. In beide schalen van de balans liggen immers authentieke belangen. Het dient echter geen enkel belang van burgers in een democratische rechtsstaat als overheidsinstanties willekeurig met persoonsgegevens kunnen omgaan. Een democratische belangenafweging dient dan ook te resulteren in een zorgvuldige en systematische omgang met persoonsgegevens van burgers door de overheid. Het CBP is bezorgd over de erosie in de publieke discussie van het fundamentele en in internationale verdragen vastgelegde beginsel dat het gebruik van persoonsgegevens dan wel het maken van een inbreuk op de persoonlijke levenssfeer werkelijk noodzakelijk moet zijn.

Noodzakelijkheid als leidraad

Van erosie van het noodzakelijkheidsbeginsel is sprake als politici, ambtsdragers en beleidsmakers zich niet langer de vraag stellen of het verzamelen, gebruiken en bewaren van gegevens van burgers noodzakelijk is voor een bepaald doel. Het feit dat instanties nu eenmaal beschikken over veel gegevens van burgers is op zich geen toereikende legitimatie om deze voor andere doeleinden aan te wenden, langdurig te bewaren of met andere organisaties te delen.

Deze toets aan de noodzakelijkheid laat ruimte voor het gebruik van een basisset van gegevens van burgers door diverse overheidsinstanties en daarmee verwante instellingen. Ook samenwerking tussen instanties is zeer wel mogelijk, mits daarbij telkens weer wordt vastgesteld welke gegevensuitwisseling noodzakelijk is voor de samenwerking en mits de betrokken burger goed wordt geïnformeerd. Complexer wordt de situatie bij publiek-private taakverdeling. Met name bij de overheveling of uitbesteding van onderdelen van de sociale zekerheid dient uitdrukkelijk aandacht te worden besteed aan het juiste gebruik van (veelal bijzondere) persoonsgegevens door de marktpartijen. Uitbesteding ontslaat de overheid niet van haar eigen verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens.

Controle, veiligheid en vrijheid

In het publieke debat klinkt aanhoudend de roep om meer controlemaatregelen. Nuchtere afweging en realistische taxatie van het effect van voorgestelde maatregelen lijken te bezwijken onder de reële dreiging van terroristische aanslagen en de last van ernstige criminaliteit. De symboliek van voorstellen is echter vaak vele malen groter dan de effectiviteit ervan. Steeds verder gaande controlemaatregelen zullen echter niet zonder meer leiden tot vergroting van de veiligheid van de burger, terwijl de maatschappelijke kosten voor overheid en burgers hoog zijn. Een doorslaande zorg om veiligheid zal op den duur de vrijheid van de burger aantasten.

Bezinning op nut, noodzaak en maatvoering van te nemen controlemaatregelen is nodig. Maatregelen kunnen ook tijdelijk zijn; de reikwijdte ervan kan beperkt worden tot plaatsen of tijden met een verhoogd risico. Evaluatie van de maatregelen zou standaard moeten zijn, zeker bij ingrijpende controlemiddelen zoals cameratoezicht, preventief fouilleren en identiteitscontroles. Doordachte maatregelen, een proportionele inzet en het meten van effectiviteit bij het bestrijden van terrorisme en andere vormen van ernstige criminaliteit passen een overheid die de hoeder is van onze grondrechten.

Privacy van meet af aan

Bij het aantreden van het nieuwe kabinet in 2003 heeft het CBP aandacht gevraagd voor een zorgvuldige omgang met persoonsgegevens. Op tal van punten – zorg, veiligheid, fraudebestrijding en elektronische overheidsdienstverlening – raakt het kabinetsbeleid immers aan een zorgvuldige en behoorlijke verwerking van persoonsgegevens. Als privacybescherming veronachtzaamd wordt, ontstaan aanzienlijke risico's voor de houdbaarheid in rechte van beleidsinitiatieven en overheidsoptreden. Grotere speelruimte voor succes wordt gewonnen door van meet af aan privacybescherming mee te nemen bij het ontwerp van maatregelen en informatiesystemen.

Bij voorstellen voor wet- en regelgeving die in belangrijke mate betrekking hebben op de verwerking van persoonsgegevens, dient het CBP om advies gevraagd te worden. In overleg met de departementen zijn in 2003 betere voorwaarden geschapen voor de invulling van deze verplichting.

Informatie-infrastructuur

Stroomlijning van basisgegevens dient niet uit te monden in ongebreideld verkeer van persoonsgegevens binnen de overheid. Voor grote gegevensstromen is een specifieke en duidelijke wettelijke regeling geboden, met aandacht voor onder meer de maatschappelijke noodzaak, rol- en taakverdelingen, het feitelijke gegevensverkeer en transparantie.

In 2003 werd vervolg gegeven aan het advies *Persoonsnummerbeleid* van de zogenaamde Tafel Van Thijn over het inrichten van een overkoepelende informatie-infrastructuur voor de overheid. Bij de ontwikkeling van een plan voor de invoering was het CBP zowel op stuurgroep- als op werkgroepniveau intensief betrokken. Het CBP heeft onder meer een bijdrage geleverd aan de voorstellen voor een Nationale Vertrouwensfunctie, een organisatie die tot taak zal krijgen de burger inzicht te geven in alle gegevensstromen op basis van het burgerservicenummer. Vertrouwen van de burger in de elektronische overheid is essentieel. Het CBP zal daarom bestaande en nieuwe gegevensverwerkingen toetsen en in de toekomst een ombudsfunctie op dit terrein vervullen.

Gemeenten

De gemeente is voor de burger een belangrijke overheid waarmee hij veel te maken heeft. Gemeenten verwerken daarom ook veel persoonsgegevens van burgers. Door ontwikkeling in de taken en het bestuur van de gemeente neemt de verantwoordelijkheid voor de bescherming van persoonsgegevens nog toe. Het is daarom van groot belang dat gemeenten hun informatiehuishouding op orde hebben, ook ten behoeve van de bescherming van de persoonsgegevens van hun ingezetenen.

Resultaten 2003

In het vorige jaarverslag is aangekondigd dat in 2003 zou worden gestreefd naar de volgende resultaten:

- **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 heeft bij vrijwel alle departementen aandacht gevraagd voor de adviesplicht en afspraken kunnen maken zodat op adequate wijze invulling kan worden gegeven aan deze verplichting.

- **Functionarissen gegevensbescherming**
  Het aantal functionarissen voor de gegevensbescherming (FG), dat bij het CBP werd aangemeld op grond van de artikelen 62-64 WBP, groeide met 51 tot 148 eind 2003. Het CBP droeg bij aan de organisatie van een contactdag voor FG's werkzaam bij gemeenten en alle FG's hebben een contactpersoon binnen het CBP. Het samenspel tussen de toezichthouder en de functionarissen voor de gegevensbescherming is in ontwikkeling.

- **Cameratoezicht**
  Het CBP publiceerde in 2003 de resultaten van het onderzoek naar de wijze waarop bij Nederlandse gemeenten het cameratoezicht op openbare plaatsen in de praktijk functioneert en hoe met de privacyaspecten daarvan in verschillende gemeenten wordt omgegaan: *Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten.*

- **Zieke werknemer**
  Al enkele jaren wordt getracht de instroom van zieke werknemers in de WAO te beperken. Dit heeft geleid tot een toenemende behoefte aan informatie over de zieke werknemer die direct raakt aan diens privacy. Het CBP heeft in 2003 het onderzoek afgerond naar de privacyaspecten van de complexe regelgeving en de belangrijkste gegevensstromen omtrent de zieke werknemer. De publicatie van de studie is vertraagd.

- **Politieregisters**
  In het verlengde van eerdere activiteiten met betrekking tot de registers van de Criminele Inlichtingeneenheden (CIE's), is het CBP gestart met een steekproefsgewijze doorlichting van de praktijk bij 8 van deze eenheden. In de geselecteerde dossiers werd onderzocht in hoeverre de regels voor de informatieverwerking daadwerkelijk waren gevolgd. Het onderzoek zal in 2004 worden afgerond.

Bij analyse van de eerste 13.000 meldingen van verwerkingen van persoonsgegevens onder de Wet bescherming persoonsgegevens (WBP) bleek dat onder meer bij gemeenten het aantal meldingen sterk achterbleef bij de verwachtingen; zeker 60 gemeenten bleken de meldingsplicht consequent te negeren. In een steekproef heeft het CBP vervolgens bij een aantal gemeenten gecontroleerd of zij voldaan hadden aan de meldingsplicht. In december 2003 is aan een eerste gemeente een boete opgelegd voor het niet nakomen van de meldingsplicht.

Cameratoezicht door gemeenten

Bij alle gemeenten heeft het CBP in 2003 een onderzoek laten verrichten naar de inzet van cameratoezicht. Doel van het onderzoek *Cameratoezicht in de openbare ruimte* was een overzicht te verkrijgen van de wijze waarop cameratoezicht in de praktijk functioneert en hoe met de privacyaspecten van cameratoezicht in de verschillende gemeenten wordt omgegaan. Uit het onderzoek bleek dat één op de vijf gemeenten camera's inzet voor openbare orde, toezicht en veiligheid. Meer dan de helft van de gemeenten met cameratoezicht heeft echter de effectiviteit ervan niet geëvalueerd. Ruim de helft van de gemeenten benut het cameratoezicht in het kader van samenwerking tussen instanties en organisaties. Meestal gaat het om samenwerking met de politie bij opsporing, maar ook samenwerking met bedrijven en andere organisaties komt regelmatig voor. De kaders waarbinnen dit gebeurt, bleken echter vaak niet duidelijk.

Rotterdam: Persoonsgebonden aanpak mogelijk

Eind 2002 bestreed het CBP de opvatting van het stadsbestuur van Rotterdam dat aanpassing van de privacywetgeving nodig was voor een veilige stad.

- **Telecommunicatie**
  Het CBP heeft aandacht besteed aan de meldingsplicht binnen de telecommunicatiesector en adviseerde over de nieuwe Telecommunicatiewet. Eind 2003 heeft het CBP de sector schriftelijk geconsulteerd inzake nummeridentificatie met het oog op een verheldering van de normen voor de praktijk.

- **Certificering**
  Op basis van de uitkomsten van het eerdere project Auditaanpak is de grondslag gelegd voor een systeem van privacycertificering. Doel hiervan is de naleving van privacywetgeving via zelfregulering verder te bevorderen. In samenwerking met de toekomstige accreditatie-instellingen NOREA en NIVRA heeft het CBP dit systeem in 2003 vrijwel gereed gemaakt voor invoering.

- **Meldingsplicht**
  De verplichting om verwerkingen van persoonsgegevens bij het CBP te melden, draagt bij aan transparantie en controleerbaarheid. Op basis van het openbaar register heeft het CBP in 2003 een analyse van de meldingen uitgevoerd met het oog op de handhaving van deze verplichting. Uiteindelijk is in een drietal sectoren en bij de gemeenten nader onderzoek ingesteld dat eind 2003 heeft geleid tot de eerste bestuurlijke boetes.

- **Internetsite**
  De toegankelijkheid van de CBP-website is verbeterd, onder meer door de introductie van themadossiers en een nieuwsbrief via e-mail. De groeiende omvang van de website en de noodzaak het beleid inzake de nieuwe taken van het CBP inzichtelijk te maken, leidden ertoe dat in 2003 begonnen is met een herontwerp van de website. De voorgenomen aparte sectie voor praktische vragen van betrokkenen is niet gerealiseerd en zal worden meegenomen in het herontwerp.

- **Formatieplan**
  Om een goede uitvoering van nieuwe taken op het terrein van toezicht en handhaving te kunnen verzekeren, zijn de organisatie en formatie van het CBP aangepast. Op basis van het nieuwe formatieplan functioneert sinds 1 januari 2003 de afdeling Interventie, bezwaar en beroep. De vernieuwing van de organisatiestructuur kon in 2003 worden afgerond met de oprichting per 1 januari 2004 van de afdeling Onderzoek. De bijbehorende functieprofielen werden voor zover mogelijk in 2003 gerealiseerd.

'Smoelenboek'

Het komt regelmatig voor dat de politie bestanden aanlegt van personen zonder de directe aanleiding van een strafbaar feit maar wel met een concreet doel. Het gaat om (digitale) verzamelingen van persoonsgegevens waarmee mensen te herkennen zijn, meestal foto's met naam, adres, persoonsbeschrijvingen. Deze gegevens waren al opgenomen in een politieregister en worden dan opnieuw gebruikt. Zo'n bestand wordt in de politiepraktijk een 'smoelenboek' genoemd en het wordt in de regel gemaakt voor een beperkte groep van opsporingsambtenaren, bijvoorbeeld voor een wijkteam.
Het aanleggen van zo'n bestand mag. Er is zelfs een modelreglement op van toepassing, het reglement Aandachtsvestigingen. In 2003 adviseerde het CBP alle korpsbeheerders hierover. Privacywetgeving vereist dat er voldoende waarborgen zijn voor de kwaliteit van een smoelenboek. Rechtmatigheid vanuit het oogpunt van privacy en bruikbaarheid voor de politietaak liggen hier in elkaars verlengde. Een ongerichte collectie gegevens helpt op straat niet, een duidelijk doel en heldere selectiecriteria leveren wel een effectief instrument op. Privacynormen vereisen voor het verzamelen van persoonsgegevens eveneens een goed omschreven doel; duidelijke selectiecriteria zijn vereist om te voorkomen dat meer gegevens worden verwerkt dan noodzakelijk. Belangrijk zijn verder de actualiteit van de gegevens, digitale opslag in verband met een goed beheer en een beperking aan de duur dat de gegevens in het smoelenboek worden opgenomen.
Een bruikbaar digitaal smoelenboek van bijvoorbeeld de meest actieve autokrakers kan worden samengesteld op van grond van concrete selectiecriteria. Om te beginnen moet het gaan om een bepaald gebied, bijvoorbeeld een wijk. Verder moet de persoon blijkens de politieregisters meer dan tien keer verdacht zijn geweest van diefstal uit een auto door middel van braak. Deze diefstallen vonden plaats in het betreffende gebied in het tijdsbestek van de afgelopen 24 maanden. Indien bekend wordt ook de zogenaamde 'modus operandi' opgenomen, de typische manier van werken van de betreffende autokraker, bijvoorbeeld inbraak via de achterklep van de auto. Via autorisatie wordt deze selectie alleen beschikbaar gesteld aan een specifieke groep opsporingsambtenaren, in dit geval een wijkteam. Vervolgens wordt elke drie maanden gekeken of de personen nog rechtmatig in het smoelenboek staan. Deze waarborgen voor 'de privacy' zijn ook waarborgen voor de bruikbaarheid van het smoelenboek in de politiepraktijk door de duidelijke selectiecriteria en het actueel houden van de gegevens ●

In vervolg hierop heeft het CBP in 2003 overleg gevoerd met de partijen die betrokken zijn bij de diverse projecten voor een integrale aanpak van circa 700 drugsverslaafden die voor overlast zorgen of crimineel gedrag vertonen en doorgaans ook medische zorg en sociale hulp mijden. Aan dit samenwerkingsverband nemen onder meer deel de politie, de hulpverlening en de reclassering. Van de betrokken verslaafden worden gegevens over hun contacten met zowel de politie als de hulpverlening uitgewisseld. De gedeelde informatie wordt opgeslagen in een basisdossier. Op basis van het dossier wordt vervolgens besloten tot een bepaalde aanpak, de zogenaamde zorg-, drang- of dwangtrajecten.

De discussie binnen het samenwerkingsverband spitste zich toe op de grenzen die het beroepsgeheim van de zorgverleners stelt. Het CBP heeft in het overleg erop gewezen dat zorgverleners dienen vast te houden aan hun wettelijke plicht te handelen in het belang van de cliënt. Indien het naar hun professionele oordeel in het belang van de cliënt is dat zij informatie delen met andere instanties, is dat in principe mogelijk. Deze benadering gaf aanleiding tot een breder debat over de reikwijdte van het medisch beroepsgeheim onder regie van de Inspectie voor de Gezondheidszorg. In de loop van 2003 hebben de betrokken partijen de regels voor de informatie-uitwisseling uitgewerkt en kon het Informatiesysteem PGA gemeld worden bij het CBP.

Onvoldoende toezicht op uitvoering WWB

De kern van de nieuwe Wet werk en bijstand (WWB) is dat gemeenten meer (financiële) verantwoordelijkheid krijgen voor de bijstandsverlening. Het CBP heeft zich in 2002 en in 2003 meerdere malen uitgesproken over de inrichting van het toezicht op de uitvoering van de WWB. Er is een kloof tussen de formele regeling dat de Inspectie Werk en Inkomen (IWI) toeziet op de rechtmatigheid van de uitvoering (inclusief de verwerking van persoonsgegevens) en de praktische uitwerking waarin het IWI niet de nodige informatie ontvangt om structureel toezicht uit te oefenen. Deze kloof is niet gedicht bij de behandeling van het wetsontwerp in de beide Kamers. De uitwerking van het toezicht is voor wat betreft de verwerking van (persoons)gegevens verder niet in overeenstemming met het standpunt van de staatssecretaris van Sociale Zaken en Werkgelegenheid tijdens de parlementaire behandeling. Het CBP maakt zich zorgen over dit gebrek aan verantwoordingsplicht voor de gemeenten.

Politie en privacy

De bijdrage van een aantal hoofdcommissarissen aan de publieke discussie over veiligheid was niet in balans. Privacybescherming werd bij herhaling als obstakel voor het politiewerk, als belemmering voor betere resultaten aangewezen. Toonaangevende politiemensen leken te miskennen dat de politie kan beschikken over zeer veel bronnen van informatie over burgers. Privacybescherming verplicht de politie daarmee op verantwoorde en controleerbare wijze om te gaan. De typering van het grondrecht op privacy als 'schuilplaats van het kwaad' door de korpschef van Groningen was ver over de schreef.

Het CBP onderkent dat de politie een grote en legitieme informatiebehoefte heeft en kon zich op hoofdlijnen vinden in de voorgenomen uitbreiding van de bevoegdheid van justitie en politie om persoonsgegevens op te vragen bij maatschappelijke instellingen en bedrijven als dat voor de opsporing noodzakelijk is. Het wetsvoorstel is gebaseerd op de voorstellen van de commissie Mevis (2001) en schept vooral duidelijkheid voor het bedrijfsleven. Naar het oordeel van het CBP is wel een contragewicht nodig. Niet alleen dient informatie gericht en selectief verzameld en gebruikt te worden, maar er dient ook toezicht op de informatiehuishouding van de politie te zijn, onder andere in de vorm van periodieke en onafhankelijke controles achteraf. De minister van Justitie heeft dit ook toegezegd in het kabinetsstandpunt over de voorstellen van de commissie Mevis. Het CBP heeft aangedrongen op een spoedige invoering van deze periodieke audits op alle politieregisters.

Criminele inlichtingeneenheden

In 2003 is het CBP begonnen met een eerste serie onderzoeken bij de criminele inlichtingeneenheden (CIE's) van acht politiekorpen in aanvulling op de door de politie georganiseerde zelfevaluatie en onafhankelijke review van 2002. CIE's voeren een aantal bijzondere registers, die ook opsporingsinformatie over niet-verdachte personen bevatten. Onafhankelijk, extern toezicht is daarom van wezenlijk belang. Alleen het CBP kan als externe toezichthouder kennisnemen van de inhoud van de dossiers. Bij deze serie onderzoeken ging het om steekproefsgewijze doorlichting van de praktijk. In de geselecteerde dossiers werd onderzocht in hoeverre de regels voor de informatieverwerking daadwerkelijk waren gevolgd. In 2004 zullen de onderzoeken worden afgerond.

Advocaten afgeluisterd

Uit het CBP-onderzoek naar het afluisteren en registreren van gesprekken van burgers met hun advocaten bleek dat het beroepsgeheim van advocaten onvoldoende gerespecteerd werd. Het stelselmatig opnemen, registreren, uitwerken en kennisnemen van deze vertrouwelijke communicatie door de politie en het Openbaar Ministerie is strijdig met de bij wet en verdrag erkende bijzondere positie van beroepsgeheimhouders. Het is daarmee ook in strijd met de Wet politieregisters en de Wet bescherming persoonsgegevens. Politie en justitie waren doorgeschoten bij het afluisteren en registreren van gesprekken van burgers met hun advocaten. De minister van Justitie deelde het standpunt van het CBP echter niet en heeft de aanbevelingen niet overgenomen.

Administratieve lastenverlichting

Het aantal verzoeken om kennisneming bij de politie door personen die willen weten of en hoe zij geregistreerd staan in politieregisters, was in voorgaande jaren aanzienlijk toegenomen. Het aantal verzoeken steeg van 1100 in 2000 tot 1850 in 2002. Het ging vooral om complexe en tijdrovende verzoeken van advocaten, die door een CIE worden behandeld. Een werkgroep van privacydeskundigen van de politie, het Openbaar Ministerie en het CBP kwam met een plan voor de stroomlijning van de behandeling van de verzoeken. Hiermee zal ook uitholling van het recht op kennisneming worden voorkomen.

Belangrijk in het kader van de administratieve lastenverlichting zijn ook de modelreglementen voor de politieregisters. In 2002 keurde het CBP 40 modelreglementen voor de permanente registers goed. In 2003 kwam het Modelreglement Tijdelijk register tot stand. Het gebruik van modelreglementen vermindert direct de administratieve lasten bij politie en CBP en schept tegelijkertijd waarborgen.

Marktwerking in de zorg

De discussie over kostenbeheersing en kwaliteitsversterking in de zorg wordt gedragen door een consensus over de noodzaak van meer marktwerking via publiek-private samenwerking waarbij voor de zorgverzekeraars zich een zeer

Een medisch dossier bij het UWV

Je wacht op een herbeoordeling voor een WAO-uitkering, je medische dossier bij het UWV – het Uitvoeringsinstituut werknemersverzekeringen – blijkt zonder je toestemming aan een andere arts van een extern bedrijf te zijn gegeven en het raakt ook een paar keer 'kwijt'. Niemand heeft je iets verteld of gevraagd. De klacht die het CBP hierover ontving, maakt twee dingen nog weer eens duidelijk. Overheid of bedrijfsleven kunnen alleen rekenen op vertrouwen als burgers goed geïnformeerd worden en dat vertrouwen is ook nodig om complexe maatschappelijke organisaties goed te laten draaien.

De verzekeringsartsen bij het UWV hadden met grote achterstanden te kampen zodat het onmogelijk was de schriftelijke herbeoordeling van alle dossiers uit te laten voeren door medewerkers van het UWV. Daarom werden verzekeringsartsen en arbeidsdeskundigen ingehuurd bij een bedrijf. Medische dossiers werden daarvoor ook op en neer gestuurd naar verschillende locaties in het land. Het is dan niet vreemd te denken dat je medische herbeoordeling zomaar is uitbesteed. De zaak lag echter toch anders.

Het UWV mag kerntaken – zoals het beoordelen van medische dossiers – immers niet uitbesteden aan private uitvoerders. Het UWV had daarom extra mensen ingehuurd bij een bedrijf waarmee ook een overeenkomst werd gesloten over de van toepassing zijnde geheimhoudingsplicht, het werken volgens kwaliteitsnormen en de naleving van het privacyreglement van het UWV. De ingehuurde deskundigen deden hun werk dus onder leiding en onder de voorwaarden van het UWV alsof zij medewerkers van het UWV waren.

prominente rol begint af te tekenen. De verzekeraars stellen echter dat zij zonder maximaal inzicht in de feitelijke, individuele zorg deze rol niet kunnen vervullen. Dit bleek in de discussie over de introductie van de Diagnose Behandeling Combinatie (DBC).

De DBC-systematiek is ontwikkeld voor de bekostiging van specialistische medische zorg en moet leiden tot een marktconforme prijsontwikkeling op basis van onderhandelingen tussen zorginstellingen en zorgverzekeraars. Een DBC is een combinatie van codes die gegevens bevatten over onder andere de zorgvraag, de diagnose en de behandeling van een patiënt. Op deze informatie is het medisch beroepsgeheim van toepassing. Zorgverleners dienen de DBC's te verstrekken aan zorgverzekeraars voor de declaratie van de verleende zorg.

Het CBP heeft zich sterk gemaakt voor het medisch beroepsgeheim en maatvoering bij de verstrekking van medische persoonsgegevens. Het CBP stond op het standpunt dat inzichtelijk moest worden gemaakt welke persoonsgegevens noodzakelijkerwijs door ziekenhuizen aan de zorgverzekeraars zouden moeten worden verstrekt. Als duidelijk is welke gegevensverwerkingen noodzakelijk zijn voor de diverse, gerechtvaardigde doeleinden, zou de juridische verankering van het nieuwe bekostigingssysteem daarop kunnen aansluiten.
De uitwerking van het noodzakelijkheidcriterium heeft geresulteerd in een toetsingskader. Dit biedt vijf criteria aan de hand waarvan bepaald wordt of een DBC al dan niet gedeclareerd zal worden met alle bijbehorende informatie over de diagnose.

De DBC-systematiek zal vanaf 1 januari 2005 gefaseerd ingevoerd worden. In een gezamenlijke brief hebben de minister van VWS en het CBP de betrokken partijen (zoals Zorgverzekeraars Nederland en koepelorganisaties) gevraagd de werkwijze voor de invoering van het stelsel onder de aandacht van hun leden te brengen.

De zieke werknemer

Al enkele jaren wordt getracht de instroom van zieke werknemers in de WAO te beperken. Dit heeft geleid tot maatregelen voor een actiever ziekteverzuimbeleid, strengere reïntegratieverplichtingen voor werknemer en werkgever en

Deze constructie – de gezagsverhouding en de overeenkomst – zorgde ervoor dat de verantwoordelijkheid voor het gebruik van de medische en andere persoonsgegevens in de uitkeringsdossiers bij UWV bleef, waar deze ook hoort. Hoe het werk door de verantwoordelijke georganiseerd wordt, is dan in principe een interne kwestie.
Maar was er dan geen toestemming nodig van de betrokkene voor de overdracht van het dossier aan een andere arts? Volgens de kwaliteitsrichtlijnen van UWV kan de verzekeringsarts alleen medische dossiers van andere verzekeringsartsen gebruiken voor zover hij hen opvolgt, voor hen waarneemt, of een bezwaarschrift behandelt. In dit geval kon naar het oordeel van het CBP gesproken worden van waarneming. De verzekeringsarts kon de schriftelijke beoordeling van het dossier immers niet zelf uitvoeren. Het vragen van toestemming aan de betrokkene was naar het oordeel van het CBP daarom ook niet verplicht. Het UWV had echter wel moeten zeggen dat voor heronderzoek het dossier aan een andere verzekeringsarts zou worden overgedragen. In dit geval werd immers afgeweken van wat de betrokkene redelijkerwijs had kunnen verwachten, namelijk een herbeoordeling door een arts die in dienst is bij de door de wet aangewezen instantie. Goede informatie had de betrokkene in staat gesteld hiertegen eventueel bezwaar te maken.
Het CBP kwam tot de conclusie dat het UWV heeft gehandeld in strijd met de Wet bescherming persoonsgegevens voor wat betreft de informatieplicht en de zorgvuldige omgang met het dossier. Het UWV hoefde echter geen toestemming aan de betrokkene te vragen voor de gang van zaken. Het UWV heeft ook maatregelen getroffen om het vervoer van de dossiers te verbeteren ●

Doelen 2004

In 2004 zullen met name de volgende resultaten worden nagestreefd:

- **Zieke werknemer**
  Het onderzoek naar de belangrijkste gegevensstromen omtrent de zieke werknemer en de daarbij behorende privacyregels zal in 2004 resulteren in de publicatie van een naslagwerk met vuistregels voor de praktijk. Het naslagwerk zal intensief onder de aandacht worden gebracht van de diverse bij reïntegratie van de zieke werknemer betrokken partijen.

- **Politieregisters**
  Het in 2003 gestarte onderzoek naar de registers van de Criminele Inlichtingeneenheden bij acht regiokorpsen zal in 2004 worden afgerond. De algemene bevindingen van het onderzoek zullen worden gepubliceerd.

- **Onderzoek tapkamers**
  Het CBP zal in 2004 een onderzoek instellen naar de privacy-aspecten van de gegevensverwerking in de tapkamers van de politie, dit in vervolg op het *Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie* uit 2003.

- **Cameratoezicht**
  De resultaten van het in 2003 gepubliceerde onderzoek *Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten* zullen in 2004 benut worden voor een studie over de privacyaspecten van cameratoezicht op de openbare ruimte waarin vuistregels gegeven zullen worden voor de praktijk.

- **Burgerservicenummer**
  Het CBP zal een bijdrage leveren aan het realiseren van de Nationale Vertrouwensfunctie, een organisatie die tot taak krijgt de burger inzicht te geven in alle gegevensstromen op basis van het burgerservicenummer. Het CBP zal in 2004 in de gelegenheid worden gesteld te beginnen met het toetsen van bestaande en nieuwe gegevensverwerkingen en zich voor te bereiden op een toekomstige ombudsfunctie.

- **Certificering**
  Het met NOREA en NIVRA uitgewerkte systeem van privacy-certificering dient in 2004 in de praktijk te worden gebracht, aanvankelijk in de vorm van proefcertificeringen, naderhand als marktproduct. Het CBP zal bijdragen aan de beoordeling van de proefcertificeringen.

- **Invoering DBC-systematiek**
  Op het gebied van de zorg zal het CBP nauw betrokken blijven bij de ontwikkeling en invoering van de financierings-systematiek op basis van de Diagnose Behandeling Combinatie.

- **Landelijke registraties in de zorg**
  In 2003 heeft het CBP een oriënterend onderzoek afgerond naar vijf landelijke registraties in de zorg. Het CBP zal de resultaten van het onderzoek in 2004 gebruiken voor de formulering van normen inzake landelijke registraties en het daarbij passende handhavingsbeleid.

- **Onderzoek privacybeleving**
  Het CBP zal een eerste onderzoek laten uitvoeren naar aspecten van privacybewustzijn en privacybehoeften bij de Nederlandse burger. Dergelijke onderzoeken zijn in verscheidene Europese landen reeds uitgevoerd. De resultaten zullen gebruikt worden bij het maken van strategische keuzes en de verdere invulling van het beleid van de toezichthouder.

- **Beleidsregels en tweedelijnspositie**
  Het CBP zal beleidsregels publiceren voor het in behandeling nemen van zaken en de publiciteit daaromheen. Ter uitvoering van het tweedelijnsbeleid zal het CBP sector-, branche-, koepel- en beroepsorganisaties benaderen om de mogelijkheden te onderzoeken van informatie-uitwisseling en taakverdeling bij voorlichting en klachtbehandeling.

- **Organisatieontwikkeling**
  In 2004 zal de afdeling Onderzoek operationeel moeten worden waarbij veel aandacht besteed zal worden aan differentiatie van onderzoeksvormen en de ontwikkeling van risico-analyse als instrument voor beleidsvorming. De afdeling speelt een belangrijke rol bij het voorgenomen onderzoek privacybeleving en is verantwoordelijk voor de meldingenanalyse 2004.

- **CBP-website**
  In 2004 zal het CBP zijn website vernieuwen met het oog op een betere voorlichting aan betrokkenen en verantwoordelijken. Het materiaal op de website zal meer vraaggericht ontsloten worden. Hiermee wordt ook een vermindering beoogd van de stroom van voorlichtingsverzoeken die het CBP telefonisch, per e-mail en per post jaarlijks bereiken.

Nevenfuncties van rechters

De burger heeft een groot belang bij een onafhankelijke en transparante rechterlijke macht. Informatie over nevenfuncties van rechters is daarom openbaar. Maar ook rechters hebben recht op privacy. Welke waarborgen kunnen worden getroffen om beide belangen in evenwicht te brengen? In 2003 heeft het CBP geadviseerd over de Wet nevenbetrekkingen rechterlijke ambtenaren evenals over de ermee samenhangende wijziging van de Wet rechtspositie rechterlijke ambtenaren.
Volgens het wetsvoorstel zou voortaan een nevenfunctie niet alleen gemeld moeten worden, maar zou ook worden beoordeeld of de nevenfunctie wel gewenst is. Gekeken wordt dan naar de goede vervulling van het ambt van rechter, diens onpartijdigheid en onafhankelijkheid of het vertrouwen daarin. Daarom moet ook de naam van het bedrijf of de instantie worden gemeld, het aantal uren per maand, de plaats en het moment van aanvang en beëindiging van de betrekking en of deze (on)bezoldigd is en de hoogte van de eventuele bezoldiging per jaar. Het wetsvoorstel regelt verder de (elektronische) openbaarmaking van deze gegevens. Deze aanscherping van de regeling past natuurlijk in de toegenomen aandacht voor de integriteit van ambtenaren en openbare ambtsdragers.
De onpartijdigheid en onafhankelijkheid van de rechterlijke macht vormen één van de essentiële verworvenheden van onze rechtsstaat. De inbreuk op de persoonlijke levenssfeer van rechterlijke ambtenaren was in de voorgestelde vorm dan ook te rechtvaardigen in het licht van de eisen die het Europese verdrag voor de rechten van de mens daaraan stelt. De openbaarmaking van al deze gegevens in een openbaar register was naar het oordeel van het CBP een minder uitgemaakte kwestie. De omvang en de verdiensten uit een nevenbetrekking kunnen van belang zijn voor de beoordeling van de verenigbaarheid van de nevenbetrekking met het rechtersambt. Vermelding van alle gegevens over de nevenbetrekking op een voor iedereen toegankelijke internetsite is echter voor deze beoordeling niet noodzakelijk. Dit kan door rechterlijke ambtenaren op goede gronden als een te vergaande inbreuk op hun persoonlijke levenssfeer worden ervaren. Het CBP adviseerde de volledige openbaarmaking te heroverwegen. In het openbaar register kan volstaan worden met het vermelden van de nevenfuncties ●

een langere verplichting voor de werkgever tot doorbetaling van het loon. Verder hebben ook andere organisaties en bedrijven een rol in het stelsel gekregen. Al deze partijen hebben een toenemende behoefte aan informatie over de zieke werknemer die direct raakt aan diens privacy.

Gezien de complexiteit van de regelgeving is het CBP in 2002 een onderzoek gestart naar de belangrijkste gegevensstromen omtrent de zieke werknemer en de daarbij behorende privacyregels. Eind 2003 kon het afgerond worden. Andermaal bleek hoe belangrijk het is dat de wetgever zorgt voor duidelijke regelgeving juist ook bij publiek-private samenwerking. Meer nog dan overheidsinstanties hebben bedrijven een belang bij duidelijkheid over wat wel en wat niet kan, zowel om redenen van bedrijfsvoering als omwille van reputatie en aansprakelijkheid.

Certificering van gegevensverwerkingen

In verschillende landen wordt gezocht naar manieren om concurrentie en marktwerking te benutten voor privacybescherming. Een van de mogelijkheden om in de markt zichtbaar te maken dat bedrijven en organisaties zich inspannen voor een zorgvuldige omgang met persoonsgegevens, is een privacycertificaat. Een aantal beroepsorganisaties heeft samen met het CBP een systeem ontwikkeld voor de private auditing van verwerkingen van persoonsgegevens. Het beoogde privacycertificaat kan worden toegekend aan een specifieke, rechtmatige verwerking van persoonsgegevens. Het certificaat is dus niet voor de organisatie in haar geheel. Het CBP zal in eerste instantie een tweetal accreditatie-instellingen benoemen, te weten NOREA en NIVRA voor het accrediteren van privacyauditors. In 2004 zal het systeem praktisch vorm krijgen.

Gedragscodes voor bedrijven

Bij de bescherming van persoonsgegevens is nadrukkelijk ruimte gecreëerd voor zelfregulering, onder meer door gedragscodes die zijn goedgekeurd door de toezichthouder. Gedragscodes zijn belangrijk, omdat de specifieke uitwerking van privacynormen voor een sector of beroep duidelijkheid schept voor de praktijk. Het CBP was betrokken bij het tot stand komen van gedragscodes voor financiële instellingen, de gerechtsdeurwaarders en de eerste Europese gedragscode voor direct marketing.

De begin 2004 goedgekeurde Privacygedragscode sector particuliere onderzoeksbureaus is opgesteld door de Vereniging van Particuliere Beveiligingsbureaus (VPB) en bindt de bij de VPB aangesloten bureaus. De particuliere recherche is een sterk groeiende sector waarvoor weinig geregeld was. De minister van Justitie is voornemens, in het kader van de vergunningverlening aan deze bureaus, de naleving van de gedragscode verplicht te stellen voor alle particuliere recherchebureaus. De minister van Justitie en het CBP hebben een overeenkomst gesloten om het toezicht op de branche af te stemmen.

Ook de Gedragscode inzake het verwerken van persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus (NVH) kon worden goedgekeurd. Juist in deze sector moest het CBP in de afgelopen jaren constateren dat er op grote schaal onzorgvuldig werd omgegaan met de bescherming van persoonsgegevens. Het CBP zal de gedragscode van de NVH hanteren als richtsnoer bij het toezicht op alle handelsinformatiebureaus.

Dwangsom voor handelsinformatiebureau X

In 2003 publiceerde het CBP de resultaten van het onderzoek naar handelsinformatiebureau X. De conclusie was dat het bureau onrechtmatig, onbehoorlijk en onzorgvuldig persoonsgegevens had verwerkt voor het maken van rapportages met verhaalsinformatie. Bij het Openbaar Ministerie werd aangifte

Pet past ons allemaal

Op 31 december 2003 werd het EU-project PISA succesvol afgesloten. In het project is beoogd aan te tonen dat persoonsgegevens ook met technologie beschermd kunnen worden door omzetting van wetgeving in computercode. Daarbij is gekozen voor een techniek waarbij software agents informatie uitwisselen in een internetomgeving in opdracht van hun eigenaar. Het gaat om software die zelfstandig beslissingen moet kunnen nemen. Opdrachten aan agents kunnen liggen in de sfeer van het boeken van de snelste reis of het reserveren van een restauranttafel, maar ook van het opvragen van belastinggegevens of medische informatie. Het kunnen vertrouwen op de technologie is in dergelijke gevallen noodzakelijk voor de acceptatie door het publiek, de overheid en het bedrijfsleven.

PISA staat voor Privacy Incorporated Software Agents en begon met een samenwerking tussen TNO-FEL en de Registratiekamer, de voorganger van het CBP, in 1999. In 2001 werd het een formeel project van de Europese Unie waarin naast TNO-FEL en het CBP ook TNO-TPD, de TU Delft, de National Research Council Canada, Sentient Machine Research, GlobalSign, Zeroknowledge en Finsa Consulting/Italsoft deelnamen.

Het CBP heeft de afgelopen jaren aan PISA bijgedragen, onder meer door de basisbegrippen van PET (Privacy-Enhancing Technologies) verder te verfijnen, door het ontwikkelen van een methodiek voor de omzetting van concepten uit de Europese Privacyrichtlijn 95/46 EG naar een metataal die gebruikt kan worden om computercode te schrijven en door hoofdstukken van de definitieve rapportage voor zijn rekening te nemen. Het CBP heeft in 2003 het eindrapport, Handbook of Privacy and Privacy-Enhancing Technologies, uitgegeven en zal in 2004 de finale privacyaudit uitvoeren. De materialen zijn beschikbaar via de website van het CBP.

PISA wordt afgesloten met de bottom line: "Privacy by design is achievable in even the most complex of applications" ●

gedaan van een vermoeden van een aantal strafbare feiten. Het opsporingsonderzoek heeft inmiddels geleid tot vervolging en berechting van enkele bij het bedrijf betrokkenen.

Het CBP had geconstateerd dat uit allerlei bestanden – waaronder die bij de Belastingdienst, uitkeringsinstanties en woningcorporaties – persoonsgegevens door het bureau onrechtmatig verkregen werden. Het CBP heeft daarom een groot aantal van deze instanties, bedrijven en beroepsorganisaties nader geïnformeerd over de bevindingen in het onderzoek, opdat zij passende maatregelen konden nemen. Een aantal van hen heeft daartoe relevante delen van het bewijsmateriaal ontvangen.

In mei 2003 legde het CBP bureau X een last onder dwangsom op. De last richtte zich op de naleving van twee punten waarop overtredingen van de WBP zijn geconstateerd: bureau X dient zich te onthouden van het verwerken van persoonsgegevens die onder geheimhoudingsverplichtingen vallen of waarvoor een verwerkingsverbod geldt en het bureau moet de betrokkene over wie persoonsgegevens worden verzameld, daarover inlichten.

Goede informatie voor de klant

Bedrijven hebben in beginsel ruime mogelijkheden om persoonsgegevens te verwerken voor marketingdoeleinden. Belangrijke voorwaarde voor een rechtmatige verwerking is goede informatie aan de klanten om wier gegevens het gaat. Transparantie is ook essentieel voor het vertrouwen van de klant. Dat bleek opnieuw in twee kwesties: het geheime nummer beleid van de KPN en de inrichting van een centrale database voor klantgegevens binnen de ING Groep.

ING Bank, Postbank en RVS – onderdelen van de ING Groep – hadden in 2002 een brief aan hun cliënten geschreven over het plan hun gegevens voor marketingdoeleinden voortaan ook in één centraal systeem vast te leggen. De geboden informatie gaf cliënten echter onvoldoende mogelijkheden hun rechten uit te oefenen. Na een onderzoek kwam het CBP tot de conclusie dat de bedrijven in deze onrechtmatig gehandeld hadden. Door de weinig specifieke wijze waarop de betrokkenen in de brief waren geïnformeerd over de gegevensverstrekking, was de verstrekking niet verenigbaar met het doel waarvoor de gegevens waren verzameld. De ING Groep had de cliënten van de diverse onderdelen beter moeten informeren om hun gegevens op centraal niveau verder te mogen verwerken. De klanten van ING Bank, Postbank en RVS hebben vervolgens aanvullende informatie gekregen.

Het CBP en de OPTA publiceerden medio 2003 het onderzoeksrapport over het beleid van Koninklijke KPN N.V. (KPN) omtrent nummers met beperkte bekendheid, algemeen bekend als ‘geheime nummers’. KPN bleek haar beleid halverwege de jaren ‘90 te hebben gewijzigd en stelt sinds geruime tijd de adresgegevens van abonnees met een geheim nummer voor direct marketing doeleinden aan derden ter beschikking zonder dat zij haar abonnees daarover expliciet heeft geïnformeerd. Het CBP verzocht KPN haar klanten actief te informeren over het beleid rond geheime nummers. Teleurstellend is dat de kwestie zich begin 2004 nog voortsleept, terwijl het in de kern gaat om een wettelijke plicht van het bedrijf om klanten te informeren over hun wettelijke rechten.

Beleid van de toezichthouder

De minister van Justitie, mr. J.P.H. Donner, zei bij de opening van het congres 'Programmatisch handhaven' op 15 mei 2003: "Handhaven van regels is de essentie van overheidsbestuur. Niet de regel, maar het resultaat – de naleving of uitvoering – is bepalend voor het functioneren van de samenleving. De werking van de regelgeving is daarom afhankelijk van de naleving."

Van regelgeving naar naleving

Het CBP onderschrijft de opvatting van de minister van Justitie over het belang van handhaving. In 2003 heeft het CBP de eerste boetes wegens het niet nakomen van de meldingsplicht door verantwoordelijken bij overheid en bedrijfsleven opgelegd (het gaat hierbij om de wettelijke bepaling die voorschrijft dat verwerkingen van persoonsgegevens dienen te worden bekendgemaakt aan de toezichthouder, tenzij hiervoor een vrijstelling geldt). Ook heeft het CBP voor het eerst gebruik gemaakt van zijn bevoegdheid tot het uitoefenen van bestuursdwang. Een intensief onderzoek dat het CBP heeft ingesteld bij een handelsinformatiebureau, leidde tot aangifte door het CBP wegens het plegen van strafbare feiten. Het Openbaar Ministerie is tot vervolging overgegaan. Deze acties passen in de verschuiving in de taakuitoefening naar een sterker accent op handhaving, die met de inwerkingtreding van de Wet bescherming persoonsgegevens in 2001 in gang is gezet.

De minister riep tijdens het congres toezichthouders, inspecties en handhavers op om slimme ideeën te ontwikkelen voor een efficiëntere handhaving. Vanuit een zelfde inspiratie heeft het CBP zijn eerdere strategie van het viersporenbeleid, de versterking van de tweedelijnspositie en meer aandacht voor handhaving bevestigd gezien en uitgebreid met een grotere diversiteit aan onderzoeksvormen.

Het CBP is van mening dat het hiermee een zeer efficiënte en slagvaardige wijze van toezichthouden heeft gerealiseerd. Met name met het oog op onderzoek en handhaving zal een uitbreiding van de formatie nodig zijn. De argumenten hiervoor zijn aangegeven in het rapport 'Organisatie Viersporenbeleid'. Gezien de maatschappelijke agenda – vormgeving van het veiligheidsbeleid in nationaal en internationaal verband, noodzakelijke versterking van de informatietechnologie in de gezondheidszorg, een nieuw stelsel van sociale zekerheid (nieuwe arbeidsongeschiktheidsverzekering, Zorgverzekeringswet 2006, Wet Werk en Bijstand) met een prominente plaats voor uitvoering door marktpartijen – is een intensieve inzet van de expertise van het CBP noodzakelijk.

Sinds begin 2002 is 'privacy' in de media meer en meer gebruikt als trefwoord en etiket voor overbodige bureaucratie, voor belemmerende regelgeving, voor gezeur 'met de rug naar de samenleving'. Politici en bestuurders van 'falende' overheden en instellingen konden en kunnen zonder dat verder lastige vragen worden gesteld, verwijzen naar 'de privacy' als obstakel voor effectief optreden. Symptomatisch waren in dit opzicht de uitlatingen in de pers over sofinummerfraude (UWV), falende bemoeizorg (rapport hulpverlening 'Roermond') en veiligheid en drugsoverlast (veiligheidsplan Rotterdam) waarin 'de privacy-regelgeving' zonder enige grond maar met groot publicitair effect in de landelijke media als probleem werd aangewezen. In de discussie over het nieuwe veiligheidsbeleid is van 'privacybescherming' herhaaldelijk een karikatuur gemaakt.

De zaak Lindqvist

Eind 2003 deed het Europese Hof van Justitie uitspraak in de prejudiciële zaak Lindqvist. De zaak heeft betrekking op de toepasselijkheid van de Europese Privacyrichtlijn 95/46/EG op internetsites. Ook voor Nederland heeft deze uitspraak gevolgen. Het betekent dat de Wet bescherming persoonsgegevens nu ook in hoogste instantie in principe van toepassing is verklaard op webpublicaties in Nederland.

Mevrouw Lindqvist, een Zweedse, had op een internetcursus geleerd om een website op te zetten. Zij paste het geleerde toe op haar werk als vrijwilligster in haar lokale kerkgemeente, om zo de leden van de gemeente te informeren over de activiteiten. Daarbij ging zij niet voorbij aan de persoonlijke omstandigheden van haar collega's. Zij gaf medische informatie zoals het feit dat iemand zijn voet had bezeerd. De Zweedse privacy-toezichthouder verklaarde de nationale implementatie van de Privacyrichtlijn van toepassing en deelde mevrouw Lindqvist een boete uit wegens niet-melden, het vermelden van bijzondere, namelijk medische, gegevens en doorgifte naar derde landen buiten de EU zonder vergunning.

De Zweedse Hoge Raad vroeg in het hoger beroep het Europese Hof of de gestelde feiten in strijd waren met de Privacyrichtlijn. Het Hof verklaarde deze van toepassing op de website. De webpublicaties van mevrouw Lindqvist vallen naar het oordeel van het Hof niet onder de vrijstelling voor persoonlijk gebruik gezien het openbare karakter van de website. Aan de andere kant vond het Hof het begrip internationale doorgifte niet van toepassing. De Europese toezichthouders en ook het CBP zullen de grenzen van het arrest moeten verkennen om deze principiële uitspraak op de veelvormige praktijk van publicatie van persoonsgegevens op websites toe te passen ●

Geheime nummers op de rekening gespecificeerd?

Veel mensen hebben een zogeheten 'geheim nummer', een telefoonnummer dat niet op te vragen is bij informatiediensten en niet in telefoongidsen vermeld wordt. Mensen willen een geheim nummer omdat zij bijvoorbeeld als arts, leraar, politieman of hulpverlener privé en werk goed gescheiden willen houden of omdat zij last hebben van oud-echtelieden, telefoonterreur of stalkers. Aanbieders van telefoniediensten, of 'operators', geven hun klanten dan ook de mogelijkheid hun nummer te laten 'afschermen'.
Bij het factureren van geleverde belminuten en andere telecommunicatiediensten verwerken operators gegevens van personen naar wie gebeld is. Deze kunnen heel goed abonnee zijn bij een andere operator met wie afspraken zijn gemaakt over afscherming van het nummer. Op de telefoonrekening zijn in de specificatie – op schrift of via internet – van de gesprekskosten de gebelde nummers terug te vinden. Als het gaat om een geheim nummer zou er 'afgeschermd' moeten staan. Om dit te bereiken hebben sommige operators onderling afspraken gemaakt en zijn er technische voorzieningen om de afscherming te realiseren. Uit klachten bij het CBP bleek dat deze afscherming niet altijd goed gaat. Diverse houders van een geheim nummer maakten er bezwaar tegen dat hun nummer op de gespecificeerde nota van anderen was opgenomen. Het is immers niet gezegd dat de factuur alleen onder ogen komt van degene die het nummer toch al kent.
Wie is er nu verantwoordelijk voor een goede afscherming van geheime nummers? In de klachtzaken bleek dat de eigen operator, met wie de afspraken over de geheimhouding waren gemaakt, zich niet verantwoordelijk voelde voor afscherming op een factuur van een andere telefonieaanbieder. De opsteller van de factuur voelde zich niet verantwoordelijk voor het afschermen van het geheime nummer omdat de afspraken over de geheimhouding niet met hem waren gemaakt.
Het CBP heeft in deze kwestie uitspraken gedaan. Voor de verwerking van persoonsgegevens – in dit geval telefoonnummers – is een grondslag nodig. Wanneer de ene telefonieaanbieder aan een andere een abonneenummer doorgeeft, kan dat op grond van belang dat het bedrijf daarbij heeft. Doorgifte kan nodig zijn voor het leveren van diensten en de kosten van telecommunicatie moeten in rekening worden gebracht en onderling verrekend kunnen worden. De ontvanger van het nummer heeft daarmee nog geen vrijbrief om het nummer op nota's te vermelden. Hij dient rekening te houden met het privacybelang dat de gebelde kan hebben bij afscherming. Een operator moet er dus op toezien dat geheime nummers afgeschermd blijven, ook als ze verwerkt worden door andere operators. De onderlinge overeenkomsten scheppen een verantwoordelijkheid voor het daadwerkelijk afschermen van de geheime nummers die een operator ontvangt.
De operator die het geheime nummer aanbiedt, moet de abonnee goed informeren over wat er met zijn geheime nummer gebeurt en welke afspraken over afscherming met anderen zijn gemaakt, zodat ook duidelijk is wie de verantwoordelijke is.
De onduidelijkheid over wie verantwoordelijk is, is inmiddels verholpen – en daarmee hopelijk ook de klachten die hiermee samenhingen – door de inwerkingtreding van het Besluit afscherming nummers notaspecificatie. Hierin staan regels voor de hele sector inzake het afschermen van telefoonnummers, juist met het oog op de bescherming van de persoonlijke levenssfeer ●

In zijn brief aan het kabinet van 30 juni 2003 heeft het CBP betoogd dat een goede inbedding van het privacybelang in de besluitvorming en de ontwikkeling van nieuwe wetgeving juist problemen bij de implementatie en de uitvoering kan voorkomen. Bewindslieden reageerden hierop in positieve zin. Bij belangrijke (wetgevings)projecten is het CBP ook in staat gesteld het privacybelang zijn terechte plaats te kunnen geven.

Verwachting van de samenleving

De samenleving mag verwachten dat het CBP wezenlijke normen en afgesproken regels handhaaft en zonodig stevig optreedt. Bedrijven die investeren in een integere omgang met persoonsgegevens, moeten kunnen rekenen op een *level playing field*. Burgers hebben niet de middelen om alleen de risico's van fraude met of misbruik van hun gegevens te dragen. Een behoorlijke, zorgvuldige en rechtmatige omgang met persoonsgegevens borgt het onderlinge vertrouwen in het maatschappelijk verkeer.

Ook de integriteit van en het vertrouwen in de overheid zijn direct gebaat bij de wijze waarop zij met de gegevens van haar burgers omgaat. De normen voor het gebruik van persoonsgegevens behoren tot de grondslagen van de democratische rechtsorde. Als spelregels zijn zij uiterst bruikbaar voor een evenwichtige afweging van belangen bij het aanpakken van maatschappelijke problemen.

Het CBP wordt inmiddels zowel nationaal als internationaal gezien als toezichthouder waarmee rekening moet worden gehouden en die waar nodig zijn tanden laat zien. In deze positie schuilt echter ook een risico. De omgeving verwacht doortastend én zorgvuldig optreden van het CBP, omdat er grote belangen op het spel kunnen staan voor organisaties waar het CBP eisen stelt aan de naleving van de bescherming van persoongegevens. De kwaliteit van het optreden dient bij voortduring op een adequaat niveau te zijn en te blijven.

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 is in 2003 geactualiseerd voor de periode van 2003–2007. De hoofdlijnen van het beleid, die in het jaarverslag over 2001 nader zijn uiteengezet, zijn:

- een geïntegreerde 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 het uitvoeren van onderzoeknaar de naleving van de WBP en het waar nodig opleggen van sancties.

In 2003 zijn de beleidsregels voorbereid die het CBP zal hanteren voor de wijze van uitoefening van zijn meest voorkomende taken en bevoegdheden. In 2004 zullen deze worden gepubliceerd.

Toezichtstrategie

In het algemeen blijft de toezichtstrategie van het CBP berusten op het zogenaamde viersporenbeleid met aandacht voor zowel bewustwording, de praktijkgerichte uitwerking van wettelijke normen en de mogelijkheden van technologie, als voor het daadwerkelijk handhaven van de normen. De accentuering van de handhaving in 2003 komt voort uit de geleidelijke accentverschuiving naar het spoor van de handhaving. Aan het betrekken van een tweedelijnspositie ligt het uitgangspunt ten grondslag verantwoordelijkheden daar te laten waar zij horen en te stimuleren dat overheden, bedrijven en andere organisaties daaraan ook zelf actief invulling geven. In die zin geeft het CBP de voorkeur aan een tweedelijnspositie, aan een rol als metatoezichthouder op een stelsel van gegevensbescherming waarin ook andere partijen een actief aandeel nemen. Vanuit deze tweedelijnspositie kan het CBP zich bij voorrang richten op de taken waarvoor het speciaal is toegerust.

Voor individuele burgers en andere belanghebbenden houdt dit in dat het CBP permanent investeert in het beschikbaar stellen en ontsluiten van informatie waarmee zij in staat worden gesteld om zoveel mogelijk voor hun eigen belangen op te komen. De website van het CBP neemt hierbij een centrale

plaats in. De toegankelijkheid van deze site zal in 2004 in haar vorm en inhoud worden vergroot. Ook blijft het CBP investeren in contacten met eerstelijns-organisaties die belanghebbenden ter zijde kunnen staan of anderszins kunnen ondersteunen. Daar staat tegenover dat het CBP selectiever zal moeten zijn bij het in behandeling nemen van individuele klachten en verzoeken om voor-lichting of bemiddeling. De criteria voor die noodzakelijke selectie zullen in de in 2004 vast te stellen en te publiceren beleidsregels worden bekend gemaakt. Rechtstreekse contacten met individuele burgers – via het front office of anderszins – blijven evenwel van belang. Een systematische analyse van deze contacten zal worden gebruikt om relevante thema's op het spoor te komen en knelpunten te achterhalen.

Tot de speciale taken behoort de afstemming van beleid en standpunten met de andere privacytoezichthouders in de Europese Unie. De noodzaak van deze samenwerking groeit. Vraagstukken rond veiligheid en politiesamenwerking, gegevensverkeer met landen buiten de Europese Unie, het gebruik van DNA en andere biometrische gegevens, telecommunicatietechnologie en internet vragen om een internationale aanpak. De toepasselijkheid van privacywetgeving op websites en internetverkeer in het algemeen is vastgesteld door het Europees Hof van Justitie in het Lindqvist-arrest. Internationaal opererende organisaties, zoals Europol, vragen in de komende jaren meer aandacht van de toezicht-houder om de kwaliteit en zorgvuldigheid op deze voor de samenleving zo essentiële terreinen te borgen (zie ook pagina 62-63).

Mijn Zaken, dus niet alle zaken

'Niet meer dan noodzakelijk' of 'proportionaliteit' is een belangrijke norm voor de omgang met persoons-gegevens. Organisaties of personen die voor een bepaald doel toegang krijgen tot gegevens van indi-viduen, mogen daarbij niet meer gegevens ontvangen dan noodzakelijk. Dit was de inzet van een discussie in 2002 en 2003 tussen de Raad voor de Rechtspraak en het CBP over het informatiesysteem 'Mijn Zaken'. Dit infor-matiesysteem voorziet in de publicatie van de rol van de gerechten op een beveiligde website voor de advocatuur. De rol is het register van de bij een rechtbank lopende zaken. De rol laat zien wanneer een zaak behandeld wordt en geeft aan wat voor een soort zaak het is, wie eiser en gedaagde zijn, wie de procureurs en welke han-deling van de rechtbank aan de orde is (de zogenaamde status, bijvoorbeeld een rolbeschikking of een vonnis).

Mijn Zaken is een internetservice voor advocaten. Advocaten(kantoren) kunnen daarmee de actuele rol van de rechtbank via internet raadplegen. Aangezien het systeem landelijk zou worden ingevoerd, zouden de rol-gegevens van alle rechtbanken voor alle kantoren beschikbaar komen. Per kantoor kan een overzicht wor-den gekregen van alle lopende zaken – van het eigen kantoor maar ook van andere kantoren – bij een recht-bank op een bepaalde datum.

Het project is belangrijk voor de rechterlijke organisatie als stap in de verdere modernisering en informatisering van de rechtspraak. In de toekomst zul-len stukken digitaal worden aangeleverd en op den duur ook in geheel digitale dossiers worden opgenomen. Gezien de wettelijke verantwoordelijkheid van de gerechten voor een goede bedrijfsvoering is de ont-

Onderzoeksstrategie

De primaire taak van het CBP is het toezicht op de naleving van – en zo nodig de handhaving van – de wettelijke normen voor de verwerking van persoonsgegevens. De nieuwe onderzoeksstrategie en de nieuwe taken rond de rechtsbescherming hangen daarmee nauw samen. Risico's voor misbruik en fraude met persoonsgegevens in de samenleving dienen te worden opgespoord door sectoranalyses en waar nodig repressief onderzoek bij verantwoordelijken. Dit onderzoek kan plaatshebben op verschillende niveaus: onderzoek naar de risico's in de samenleving, sectorspecifiek onderzoek en het onderzoek bij een verantwoordelijke. De verschillende niveaus van onderzoek zijn essentieel voor een zorgvuldig en niet vooringenomen gebruik van de handhavingsbevoegdheden.

In dit verband is van belang dat het CBP werkt aan een systematiek voor analyse van de risico's voor schending van de privacywetgeving in bepaalde sectoren. In 2003 heeft het CBP een eerste onderzoek laten verrichten naar de naleving van de informatieverplichting van verantwoordelijken aan hun klanten/cliënten. Uit het onderzoek is een beeld naar voren gekomen van de risicogebieden in de verschillende branches. Op deze wijze kan een verantwoorde onderbouwing plaatsvinden van de keuzes die het CBP bij het uitoefenen van zijn toezichthoudende taak maakt.

Organisatie

Het CBP heeft sinds 2001 een sterke ontwikkeling doorgemaakt, waarbij zijn visie op de rol als toezichthouder in het publieke domein uitgangspunt is. Hoewel het domein waar persoongegevens worden verwerkt – met risico's voor

wikkeling van nieuwe systemen zoals Mijn Zaken dus zeker gerechtvaardigd inclusief de verwerking van persoonsgegevens die eruit voortvloeit.
Het is ook alleszins te rechtvaardigen dat de rechtbanken advocaten toegang geven tot gegevens betreffende hun zaken. Advocaten kunnen hun beroep of bedrijf niet goed uitoefenen indien zij geen mogelijkheid zouden hebben de daarvoor noodzakelijke persoonsgegevens te verwerken.
Strijdig met de Wet bescherming persoonsgegevens was het project echter waar het toegang gaf tot de gehele roladministratie van de rechtbanken. Het systeem Mijn Zaken zou kantoren en advocaten slechts toegang moeten geven tot de eigen zaken. Juist bij de inrichting van informatiesystemen kunnen en moeten privacynormen worden meegenomen.

'Mijn Zaken' wordt nu zo aangepast dat een advocaat alleen de rol van zijn eigen arrondissement kan raadplegen en niet van andere arrondissementen. Deze situatie komt overeen met de huidige, waarin advocatenkantoren binnen hun arrondissement toegang hebben tot de integrale papieren rol.

Voor zaken die op naam staan van een procureur in een ander arrondissement, wordt een nieuwe voorziening getroffen. Slechts met behulp van een extra gegeven (bijvoorbeeld het zaaknummer te verkrijgen via de procureur) zal het kantoor de noodzakelijke rolinformatie uit een ander arrondissement kunnen raadplegen ●

Efficiëntie, maar niet buiten de patient om

Huisartsen en assistentes hebben hun handen al meer dan vol aan hun patiënten en dan komt er nog de bedrijfsvoering bij. Administratie gaat al gauw ten koste van tijd voor zorg. De verwerking van nota's bijvoorbeeld is arbeidsintensief. Huisartsenpraktijken en organisaties voor huisartsendiensten sluiten overeenkomsten met zorgverzekeraars om ook nota's van particuliere patiënten direct aan de verzekeraar te sturen. In de praktijk is gebleken dat dit daadwerkelijk bijdraagt aan de efficiëntie in de huisartsenzorg. Een huisartsenpost had daarom met een aantal verzekeraars afspraken gemaakt om de nota's van particulier verzekerden rechtstreeks in te kunnen dienen. De huisartsenpost controleerde in het informatiesysteem van de verzekeraar of de patiënt inderdaad verzekerd was. Als de huisartsenpost niet alle gegevens bleek te hebben voor het maken van een factuur, werden deze meestal even (elektronisch) opgevraagd bij de verzekeraar, bij het naastgelegen ziekenhuis of bij de huisarts. De nota's gingen vervolgens naar de zorgverzekeraar. Voor één patiënt was dit reden om te klagen. Hij gaf er de voorkeur aan zelf de nota te ontvangen. Het CBP gaf hem gelijk.

Sinds de oprichting van de huisartsenpost enkele jaren geleden had geen enkele particulier verzekerde patiënt bezwaar gemaakt tegen rechtstreekse verzending van de factuur naar de verzekeraar of tegen het opvragen van gegevens. De huisartsenpost vond daarom dat de toestemming van de patiënt mocht worden verondersteld. Grotere efficiëntie was bovendien in het belang van de patiënt zelf. Een afweging tegen het privacybelang van de patiënt moest in het voordeel van de huisartsenpost uitvallen.

De huisartsenpost gaf toe dat nota's evengoed aan het privé-adres van verzekerden kunnen worden gestuurd zoals voorheen. Ontbrekende gegevens hadden bij de verzekerde zelf opgevraagd kunnen worden. Hoe men in het geval van de klager aan de ontbrekende gegevens gekomen was, kon niet meer achterhaald worden.

Patiënten waren evenmin in het algemeen geïnformeerd over het opvragen van gegevens bij derden. Voor controle op het al dan niet verzekerd zijn was dit overigens wel gerechtvaardigd. De huisartsenpost erkende dit gemis en zegde toe zijn patiënten hierover te zullen informeren via de regionale kranten.

Het direct naar de verzekeraar versturen van nota's is zonder ondubbelzinnige toestemming van de betrokkene echter niet toegestaan. De nota's bevatten bovendien ook (extra beschermde) medische persoonsgegevens. Het is zeker een efficiënte werkwijze, maar het is niet noodzakelijk en dus niet rechtmatig om de betrokkenen hierbij te passeren.

De toestemming van de betrokkene voor het versturen van de rekeningen aan zijn zorgverzekeraar hoeft slechts eenmalig gevraagd te worden. Dit kan via een standaardformulier dat de betrokkene invult bij zijn (eerste) bezoek aan de huisartsenpost. Duidelijk moet zijn dat hij de rekeningen ook gewoon zelf kan krijgen. Op basis van informatie kan de patiënt dan kiezen. Patiënten zullen zelf ook voor grotere efficiëntie kiezen als zij vertrouwen hebben in de manier waarop met hun persoonsgegevens wordt omgegaan ●

het niet naleven van de WBP – sterk blijft groeien, zal de toezichthouder niet navenant mee groeien. Het CBP heeft gekozen voor een strategie, waarbij de inzet van het CBP bij één verantwoordelijke een zo groot mogelijk effect in de hele sector kan bereiken.

De nieuwe bevoegdheden van het CBP op het terrein van de handhaving en de daarmee samenhangende rechtsbescherming maken een beperkte groei (55 fte's in 2002 naar 75 fte in 2005) van het CBP noodzakelijk. Daartoe heeft het CBP op basis van het rapport 'Organisatie Viersporenbeleid' van KPMG Consulting een plan ontwikkeld waarbij voorzien is in een beperkte groei in de periode van 2003 tot 2006. In deze periode is naast de bestaande beleidsafdeling, de afdeling communicatie en de in 2003 gestarte afdeling interventie, bezwaar en beroep, ook de oprichting van een separate afdeling onderzoek voorzien per 1 januari 2004.

activiteiten

Openbaar bestuur

Het recht op privacybescherming is een grondrecht, maar daarmee nog geen absoluut recht. Tot dit recht behoort de zorgvuldige omgang met persooonsgegevens. Het hierin gelegen belang zal steeds afgewogen moeten worden tegen andere belangen. In de publieke sector vindt deze belangenafweging in laatste instantie plaats in het parlement en vertaalt zich doorgaans in waarborgen voor de burger bij het verzamelen en gebruiken van zijn persoonsgegevens. Burgers kunnen zich vaak in een dergelijke afweging vinden. In beide schalen van de balans liggen immers authentieke belangen. Een democratische belangenafweging dient te resulteren in een zorgvuldige en systematische omgang met persoonsgegevens van burgers door de overheid.

Van de overheid mag worden verwacht dat zij voor de burger transparant maakt welk gebruik zij voor welke overheidstaken van hun persoonsgegevens maakt. Hierbij is eenmalige aanlevering van gegevens, zoals verwoord in het rapport 'De andere overheid' een goed uitgangspunt. Anderzijds dienen ook binnen de overheid grenzen van de onderlinge uitwisseling van gegevens te worden gehandhaafd dan wel gesteld: de gegevens uit de zorg- en onderwijssector verdienen een aparte behandeling.

Privacy van meet af aan

Bij het aantreden van het nieuwe kabinet heeft het CBP aandacht gevraagd voor een zorgvuldige omgang met persoonsgegevens. Op tal van punten – zorg, veiligheid, fraudebestrijding en elektronische overheidsdienstverlening – raakt het kabinetsbeleid immers aan een zorgvuldige en behoorlijke verwerking van persoonsgegevens. Als privacybescherming veronachtzaamd wordt, ontstaan aanzienlijke risico's voor de houdbaarheid in rechte van beleidsinitiatieven en overheidsoptreden. Grotere speelruimte voor succes wordt gewonnen door van meet af aan privacybescherming mee te nemen bij het ontwerp van maatregelen en informatiesystemen.

Het CBP kan hier ook actief aan bijdragen. Het CBP dient immers om advies te worden gevraagd over voorstellen voor wet- en regelgeving die in belangrijke mate betrekking heeft op de verwerking van persoonsgegevens. In overleg tussen de betrokken departementen en het CBP zijn in 2003 betere voorwaarden geschapen voor de adequate invulling van deze verplichting.

Identificatieplicht

In januari 2003 adviseerde het CBP het wetsvoorstel voor een uitgebreide identificatieplicht niet in te dienen. Het wetsvoorstel beoogde invoering van een algemene identificatieplicht voor alle burgers vanaf 12 jaar. Zij zouden zich overal en altijd moeten kunnen identificeren tegenover politie en andere toezichthouders. De conclusie van het CBP was dat de wetgever schromelijk tekort schoot in de noodzakelijke onderbouwing van deze verplichting in het algemeen alsook in de rechtvaardiging ervan voor zover de verplichting als een inbreuk op de eerbiediging van de persoonlijke levenssfeer moet worden beoordeeld. Bovendien kreeg de politie een bevoegdheid om te specifiek te controleren of burgers konden voldoen aan de identificatieplicht. Deze bevoegdheid zou naar het oordeel van het CBP slechts controleerbaar zijn indien veel meer gegevens worden opgeslagen over het gedrag van onverdachte burgers.

Op een aantal punten heeft de minister van Justitie in het uiteindelijke wetsvoorstel het advies gevolgd. Belangrijk is dat er na drie jaar een evaluatie komt, met name gericht op de leeftijdsgrens en op een eventuele aanscherping van criteria voor bevoegdheidsverlening aan de politie en toezichthouders. Verder worden geen stelselmatige controles mogelijk gemaakt, alleen controles die noodzakelijk zijn met het oog op een goede taakuitoefening. Wanneer een proces-verbaal wordt opgemaakt wegens het niet kunnen voldoen aan de identificatieplicht, moet de politie daarin aangeven wat de identiteitscontrole noodzakelijk maakte. De leeftijdsgrens is opgetrokken van 12 naar 14 jaar.

In de toelichting werd uitgebreid ingegaan op de toetsing aan het Europese Verdrag voor de rechten van de mens en de fundamentele vrijheden. Volgens vaste jurisprudentie van het Europese Hof voor de rechten van de mens dient de beperking op het recht op eerbiediging van de persoonlijke levenssfeer te worden gerechtvaardigd door een zwaarwegend maatschappelijk belang. Het wetsvoorstel is inmiddels door de Tweede Kamer aangenomen.

Burgerservicenummer en authenticatie

In 2003 werd vervolg gegeven aan het advies Persoonsnummerbeleid in het kader van identiteitsmanagement van de zogenaamde Tafel Van Thijn over het inrichten van een overkoepelende informatie-infrastructuur voor de overheid. Onder leiding van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties werd in 2003 een plan voor de invoering ontwikkeld. Het CBP was hierbij zowel op stuurgroep- als op werkgroepniveau intensief betrokken en heeft vooral een bijdrage geleverd aan de nadere invulling van de Nationale Vertrouwensfunctie.

Om de burger inzicht te geven in het nieuwe burgerservicenummer (BSN) komt er een 'landkaart' die een begrijpelijk overzicht van alle gegevensstromen op basis van dit nummer zal geven. Belangrijk is ook dat de burger vertrouwen heeft in de elektronische overheid. Het CBP zal daarom in de gelegenheid worden gesteld bestaande en nieuwe gegevensverwerkingen te toetsen en in de toekomst een ombudsfunctie te vervullen. Ook de organisatie van het delen van kennis over de verwerking van persoonsgegevens door de elektronische overheid zal bij het CBP belegd worden. Bij de implementatie van het BSN vanaf 2004 wordt het CBP intensief betrokken.

Verder heeft het CBP zich breder met identiteitskwesties bezig-gehouden onder andere met de Nationale Authenticatievoorziening (NAV). In het elektronische contact tussen burger en overheid is het noodzakelijk dat steeds zeker is wie met wie te maken heeft. De NAV moet ervoor zorgen dat bij het contact tussen burgers en overheid online vastgesteld wordt dat partijen zijn wie ze voorgeven te zijn. De NAV is een concreet gevolg van het manifest Innovatie in uitvoering waarin een aantal belangrijke instanties die zeer veel persoonsgegevens verwerken, waaronder de Belastingdienst, het Uitkeringsinstituut Werknemersverzekeringen en de Informatie Beheer Groep, zich verplichten om de elektronische overheid snel te realiseren. Het CBP heeft zijn steun voor het initiatief betuigd, maar heeft erop gewezen dat de verdeling van verantwoordelijkheden en bevoegdheden rondom de NAV goed geregeld moet worden.

Gemeenten

De gemeente is voor de burger een belangrijke overheid waarmee hij veel te maken heeft. Gemeenten verwerken daarom ook veel persoonsgegevens van burgers: in de Gemeentelijke basisadministratie (GBA), bij de sociale dienst, in het kader van vergunningverlening of bij het toezicht op de openbare orde. Door ontwikkeling in de taken en het bestuur van de gemeente neemt de verantwoordelijkheid voor de bescherming van persoonsgegevens ook toe. Wijziging in de sociale wetgeving heeft de gemeente meer invloed en verantwoordelijkheid gegeven bij het verlenen van bijstand. De aanstaande wijziging van de Gemeentewet zal bij gemeenteraad en burgemeester meer bevoegdheden en verantwoordelijkheden leggen voor het invoeren van cameratoezicht op de openbare ruimte. In veel gemeenten worden samenwerkingsverbanden tussen allerlei instanties en organisaties in het leven geroepen om maatschappelijke problemen aan te pakken. Hierbij wisselen organisaties met sterk verschillende taken en doelen vaak persoonsgegevens uit. De zich aftekenende verdere politisering van het bestuur van de gemeente door de dualisering – en in de toekomst wellicht de gekozen burgermeester – zal deze ontwikkeling vermoedelijk versterken; bestuurders zullen meer armslag willen.

Het is daarom van groot belang dat gemeenten hun informatiehuishouding op orde hebben, ook ten behoeve van de bescherming van de persoonsgegevens van hun ingezetenen.

Positief is het toenemend aantal functionarissen voor de gegevensbescherming (FG's) bij gemeenten. Wel bleek een grote variatie in kennis, kunde en arbeidsomstandigheden van FG's op de contactdag die in 2003 georganiseerd werd in samenwerking met de gemeente Arnhem.

De aanpassing van de beheersregelingen voor de GBA aan de Europese Privacyrichtlijn bleek in 2003 helaas nog sterk achtergebleven. Het gaat om reglementen die onder meer bepalen aan wie door de gemeenteorganisatie gegevens van burgers verstrekt mogen worden. Gemeenten hebben op grond van de Wet GBA de plicht deze regelingen bij het CBP te melden. Het was er in veel gevallen nog niet van gekomen en in april 2003 heeft het CBP de gemeenten opgeroepen hiervan werk te maken.

Melding door gemeenten

In 2003 heeft het CBP de eerste 13.000 meldingen van verwerkingen van persoonsgegevens onder de Wet bescherming persoonsgegevens (WBP) geanalyseerd. Onder meer bij gemeenten bleef het aantal meldingen sterk achter bij de verwachtingen; zeker 60 gemeenten bleken de meldingsplicht consequent te negeren. In een steekproef heeft het CBP vervolgens bij een aantal gemeenten gecontroleerd of zij voldaan hadden aan de meldingsplicht. In december 2003 is aan een eerste gemeente een boete opgelegd voor het niet nakomen van de meldingsplicht.

Gemeenten die hun verwerkingen van persoonsgegevens reeds gemeld hadden bij het CBP, is gevraagd of zij de procesbeschrijving 'Heimelijke waarneming door sociale diensten' konden onderschrijven. De sociale diensten verwerken veel privacygevoelige gegevens, zoals gegevens over het arbeidsverleden, sociale omstandigheden en financiële gegevens, ter uitvoering van de Algemene bijstandswet, nu de Wet Werk en Bijstand. In het kader van fraudebestrijding worden deze gegevens soms verkregen zonder dat de betreffende persoon hierover wordt geïnformeerd (heimelijke waarnemingen). Dergelijke gegevensverwerkingen vormen een bijzonder risico voor de persoonlijke levenssfeer van de betrokkenen en zijn daarom onderworpen aan een zogenaamd vooraf-gaand onderzoek door het CBP.

De procesbeschrijving is opgesteld door Stimulansz (de dienstverlenende organisatie voor sociale diensten) in afstemming met vertegenwoordigers van het Landelijk Contact Sociaal Rechercheurs en rechercheurs van enkele gemeenten. In januari 2003 keurde het CBP de procesbeschrijving goed en in augustus hadden al meer dan 100 gemeenten te kennen gegeven op de beschreven manier te werken. De procesbeschrijving kan als leidraad dienen bij de melding van gegevensverwerkingen door een sociale dienst. Indien deze aangeeft de werkwijze van de procesbeschrijving te zullen volgen, kan het CBP het voorafgaand onderzoek direct afronden. In samenwerking kon dus worden gezorgd voor administratieve lastenverlichting én privacywaarborgen bij fraudebestrijding.

Samenwerkingsverbanden

In veel gemeenten wordt gezocht naar een samenhangende aanpak van maatschappelijke problemen. Nauwere samenwerking tussen allerlei organisaties is daarvoor nodig. De samenwerking is doorgaans gericht op het aanpakken van een bepaalde groep – bijvoorbeeld drugsverslaafden – of van een bepaald gebied, bijvoorbeeld een wijk met veel problemen. Er zijn veel initiatieven tot samenwerking en het CBP ontving met regelmaat verzoeken om advisering over de privacyaspecten van het samenwerken. Bij samenwerkingsverbanden zijn meestal gemeente en politie betrokken maar ook (geestelijke) gezondheidszorg, maatschappelijke opvang, jongerenwerk of scholen en woningcorporaties. In 2003 heeft het CBP onder meer overleg gevoerd met de gemeente Rotterdam over het project Persoonsgebonden aanpak (zie p. 32). In veel andere gevallen heeft het CBP zich moeten beperken tot meer algemeen advies. In 2004 zal meer sturingsinformatie beschikbaar worden gesteld.

De WBP biedt zeker mogelijkheden voor het delen van persoonsgegevens door samenwerkende organisaties. Belangrijk is de gewenste gegevensstromen precies in kaart te brengen en deze vervolgens te toetsen aan de taken en bevoegdheden van de verantwoordelijken en aan de Wet bescherming persoonsgegevens en andere relevante wettelijke regels, bijvoorbeeld voor het medisch beroepsgeheim. In ieder geval mogen niet meer dan de noodzakelijke gegevens worden verstrekt.

Cameratoezicht door gemeenten

Het CBP heeft in 2003 een onderzoek laten verrichten bij alle Nederlandse gemeenten naar de inzet van cameratoezicht. Doel van het onderzoek Cameratoezicht in de openbare ruimte was een overzicht te verkrijgen van de wijze waarop cameratoezicht in de praktijk functioneert en hoe met de privacyaspecten van cameratoezicht in de verschillende gemeenten wordt omgegaan. Gemeenteraad en burgemeester zullen immers volgens het wijzigingsvoorstel van de Gemeentewet duidelijke bevoegdheden krijgen om cameratoezicht in de openbare ruimte in te richten als instrument van gemeentelijk veiligheidsbeleid.

Uit het onderzoek bleek dat één op de vijf gemeenten camera's inzet voor openbare orde, toezicht en veiligheid. Meer dan de helft van de gemeenten met cameratoezicht heeft echter de effectiviteit ervan niet geëvalueerd. Dit kan rechtstreeks raken aan de rechtmatigheid van het voortduren van het toezicht.

Ruim de helft van de gemeenten benut het cameratoezicht in het kader van samenwerking met andere instanties en organisaties. Meestal gaat het om samenwerking met de politie bij opsporing, maar ook samenwerking met bedrijven en andere organisaties komt regelmatig voor. De kaders waarbinnen dit gebeurt, zijn echter vaak niet duidelijk.

Naar aanleiding van het onderzoek is een aantal gemeenten aangesproken op de meldingsplicht. Het CBP heeft ook een beperkt aantal gemeenten benaderd voor een verdere bestudering van de praktijk. De uitkomsten van het onderzoek zal het CBP benutten voor een studie waarin het normenkader voor cameratoezicht wordt geactualiseerd en waar nodig aangescherpt met het oog op de nieuwe bepalingen in de Gemeentewet. Het resultaat daarvan wordt in 2004 gepubliceerd. Het CBP ziet gericht en selectief gebruik van cameratoezicht als een aanvaardbare aanvulling op een breder pakket van maatregelen. Het CBP is wel van mening dat maathouden noodzakelijk is, evenals een regelmatige evaluatie van de effectiviteit van het cameratoezicht ■

Politie en Justitie

In de discussie over veiligheid ontbrak ook in 2003 de balans. De roep om nog meer bevoegdheden hield aan en privacybescherming werd bij herhaling als obstakel voor de politie, als belemmering voor betere resultaten aangewezen. Toonaangevende politiemensen leken te miskennen dat de politie nu al kan beschikken over zeer veel bronnen van informatie over burgers. Vaak is dat informatie die met ingrijpende methoden verworven is. Privacybescherming verplicht de politie daarmee op verantwoorde en controleerbare wijze om te gaan.

Privacybescherming is een grondrecht van de democratische rechtstaat die de politie haar bevoegdheden verleent. Het dienen van deze rechtsstaat in woord en daad is een plicht. De typering van het recht op privacy als 'schuilplaats voor het kwaad' door de korpschef van groningen was ver over de schreef.

Toezicht op politie

Het CBP onderkent dat de politie een grote en legitieme informatiebehoefte heeft, waaraan moeilijk inhoudelijke beperkingen opgelegd kunnen worden. Zeer veel verschillende soorten informatie kunnen immers relevant zijn voor opsporing en bestrijding van criminaliteit. De politie krijgt daarom ook bij wet toegang tot steeds meer bronnen van informatie over personen. Naar het oordeel van het CBP is dan wel een contragewicht nodig. Niet alleen dient informatie gericht en selectief verzameld en gebruikt te worden maar er dient ook toezicht op de informatiehuishouding van de politie te zijn, onder andere in de vorm van periodieke en onafhankelijke controles achteraf. In 2003 heeft het CBP hiervoor op diverse momenten gepleit.

Advocaten afgeluisterd

In een onderzoek naar het afluisteren en registreren van gesprekken van burgers met hun advocaten moest het CBP constateren dat het beroepsgeheim van advocaten onvoldoende gerespecteerd werd. Het stelselmatig opnemen, registreren, uitwerken en kennisnemen van deze vertrouwelijke communicatie door de politie en het Openbaar Ministerie (OM) is strijdig met de bij wet en verdrag erkende bijzondere positie van beroepsgeheimhouders. Het is daarmee ook in strijd met de Wet politieregisters en de Wet bescherming persoonsgegevens. Politie en justitie waren doorgeschoten bij het afluisteren en registreren van gesprekken van burgers met hun advocaten.

Het CBP was het onderzoek in 2002 begonnen op verzoek van de Nederlandse Vereniging van Strafrechtadvocaten en enkele advocaten. In zijn rapport vroeg het CBP om meer technische en organisatorische maatregelen om de vertrouwelijkheid van de gesprekken te waarborgen. Ook dient het OM te zorgen voor een duidelijke norm voor de vernietiging van onverhoopt toch geregistreerde gesprekken. Van advocaten mag verwacht worden dat zij bij het begin van een gesprek duidelijk aangeven dat zij dat voeren in hun hoedanigheid als rechtshulpverlener. De minister van Justitie deelde het standpunt van het CBP niet en heeft de aanbevelingen niet overgenomen. In 2004 zal het CBP naar de naleving van de technische en organisatorische maatregelen een onderzoek instellen.

Criminele inlichtingeneenheden

In 2003 is het CBP begonnen met een eerste serie onderzoeken bij de criminele inlichtingeneenheden (CIE's) van acht politiekorpen in aanvulling op de door de politie georganiseerde zelfevaluatie en onafhankelijke review van 2002. CIE's voeren een aantal bijzondere registers: het register zware criminaliteit, het voorlopig register en het informantenregister. De inhoud van de dossiers wordt afgeschermd voor anderen, zelfs de rechter. De registers bevatten ook opsporingsinformatie over niet-verdachte personen. Onafhankelijk, extern toezicht is daarom van wezenlijk belang. Alleen het CBP kan als externe toezichthouder kennisnemen van de inhoud van de dossiers. Het CBP doet dit soms in het kader van bemiddeling en advisering bij inzage- en correctiegeschillen, maar bij deze serie onderzoeken gaat het om steekproefsgewijze doorlichting van de praktijk. In de geselecteerde dossiers werd onderzocht in hoeverre de regels voor de informatieverwerking daadwerkelijk waren gevolgd. In 2004 zullen de onderzoeken worden afgerond en zal een rapport over de algemene bevindingen worden gepubliceerd.

Ook bijzondere opsporingsdiensten kunnen toegerust worden met een CIE. In het kader van de oprichting van een CIE bij de Fiscale Inlichtingen- en Opsporingsdienst en de Economische Controledienst (FIOD-ECD)/Belastingdienst heeft het CBP geadviseerd over het instellingsbesluit en de beheersvoorschriften. De beheersvoorschriften die gelden voor de criminele inlichtingeneenheden bij de politie en Koninklijke Marechaussee, kunnen van overeenkomstige toepassing worden verklaard op bepaalde registers van bijzondere opsporingsdiensten.

In zijn advies heeft het CBP erop gewezen dat is voorgeschreven dat de betreffende beheersvoorschriften moeten overeenkomen met de organisatieregels zoals die volgens de Regeling CIE gelden voor de politiële criminele inlichtingen eenheden. Meer in het algemeen adviseerde het CBP aansluiting te zoeken bij de regelingen voor de CIE's op het gebied van inzagerecht, modelreglementen, opleidingseisen en de periodieke audit.

Verder heeft het CBP aangedrongen op een duidelijke regeling voor het beheer van de registers, goede beveiliging van de gebruikte systemen en een duidelijke regeling van de verantwoordelijkheden daarvoor.

Ruimere bevoegdheden politie

De algemene maatschappelijke discussie over een veiliger samenleving blies wind in de zeilen van het streven naar uitbreiding van de politiebevoegdheden. In deze discussie bleef de vraag naar de effectiviteit van de bevoegdheden en de politieorganisatie vaak achterwege. Ook uit het onderzoek van het CBP naar Cameratoezicht op de openbare ruimte van 2003 dat veelal onder regie van de politie wordt uitgevoerd, bleek een gebrek aan aandacht bij de verantwoordelijke bestuurders voor de evaluatie van de effectiviteit van het cameratoezicht. Een geïntegreerde, landelijke politiële informatiehuishouding en uniforme werkwijze bleven nog uit ondanks de vele aanzetten en initiatieven.

In 2003 heeft het CBP de onderbouwing en uitwerking van een algemene identificatieplicht voor alle burgers gekritiseerd. Inmiddels is het wetsontwerp in gewijzigde vorm ingediend en aanvaard door het parlement. Hierbij heeft de politie conform het standpunt van het CBP niet de bevoegdheid tot stelselmatige controle gekregen. Het pleidooi van de Raad van Hoofdcommissarissen voor een dergelijke bevoegdheid miskende de gevolgen ervan, onder meer dat gegevens over het gedrag van onverdachte burgers zouden moeten worden opgeslagen om te kunnen nagaan of de politie de bevoegdheid rechtmatig gebruikt.

Het CBP kon zich op hoofdlijnen vinden in de voorgenomen uitbreiding van de bevoegdheid van justitie en politie om persoonsgegevens op te vragen bij bedrijven, organisaties en beroepsbeoefenaren als dat voor de opsporing noodzakelijk is. Het wetsvoorstel Bevoegdheden vorderen gegevens dat in 2004 is ingediend, is gebaseerd op de voorstellen van de commissie Mevis (2001) en schept vooral duidelijkheid voor het bedrijfsleven. De aanzienlijke verruiming van bevoegdheden vergt wel dat voldoende structurele waarborgen worden aangebracht. Het CBP betoogde in elk geval de noodzaak van systematische controle achteraf. De minister van Justitie heeft dit ook toegezegd in het kabinetsstandpunt over de voorstellen van de commissie Mevis. Het CBP heeft aangedrongen op een spoedige invoering van deze periodieke audits op alle politieregisters.

Justitiële gegevens

Het CBP heeft lang gepleit voor een wettelijke regeling voor verstrekkingen van persoonsgegevens door het Openbaar Ministerie (OM). Het CBP adviseerde daarom positief over de hoofdlijnen van het concept-wetsvoorstel Justitiële en strafvorderlijke gegevens. Het CBP vroeg echter nadrukkelijk bijzondere aandacht voor de rechtsbescherming van betrokkenen van wie strafvorderlijke informatie wordt verstrekt.

Voor de regelmatig voorkomende verstrekkingen en verstrekkingen op basis van convenanten kan worden volstaan met de voorgestelde vorm van rechtsbescherming aangevuld met voorlichting op ruime schaal. Voor de meer geïndividualiseerde verstrekkingen – veelal aan (toekomstige) werkgevers – is een zwaarder niveau van rechtsbescherming noodzakelijk. Het OM zou betrokkene voorafgaand aan de verstrekking verplicht kunnen horen, waarna deze eventueel op basis van de Algemene wet bestuursrecht in actie kan komen. Een ruimer verstrekkingenregime maakt ook een goede controle op de betreffende gegevensverwerkingen noodzakelijk in de vorm van audits uitgevoerd door onafhankelijke deskundigen. Het wetsvoorstel is inmiddels in behandeling bij de Tweede Kamer.

Politiegegevens voor luchtvaartmaatschappijen

Om de stroom drugskoeriers uit de Nederlandse Antillen, Aruba en Suriname in te dammen werd voorgesteld persoonsgegevens van aangehouden drugskoeriers geregistreerd op zwarte lijsten te verstrekken aan luchtvaartmaatschappijen die rechtstreeks vliegen op deze gebieden. Deze maatschappijen zouden zo de eerder aangehouden drugskoeriers een volgend ticket naar de Nederlandse Antillen, Aruba en Suriname gedurende drie jaar kunnen weigeren.

Een dergelijke verstrekking van strafrechtelijke gegevens afkomstig uit politieregisters kan echter niet zomaar. De minister van Justitie stelde voor de Koninklijke Marechaussee een machtiging te verlenen voor deze verstrekking. Het CBP heeft in zijn advies hiermee ingestemd onder aanbeveling van extra waarborgen, waaronder een klachtenprocedure voor de betrokkene. In vervolg op dit advies oordeelde het CBP in 2004 dat voor doorgifte van de zwarte lijsten van drugskoeriers met een vervoersverbod aan luchtvaartmaatschappijen buiten de EU geen vergunning nodig is. Het CBP beschouwt de doorgifte van de zwarte lijst als een wezenlijk onderdeel van de vervoersovereenkomst van de luchtvaartmaatschappijen met de betrokkenen.

Persoonsgebonden aanpak

Eind 2002 bestreed het CBP de opvatting van het stadsbestuur van Rotterdam dat aanpassing van de privacywetgeving nodig was voor een veilige stad. Het CBP betoogde dat integendeel een tijdige aandacht voor privacybescherming in positieve zin bijdraagt aan de oplossing van belangrijke sociale problemen. In vervolg hierop heeft het CBP in 2003 overleg gevoerd met de partijen die betrokken zijn bij de diverse projecten voor de zogenaamde Persoonsgebonden aanpak (PGA) die voortkomen uit de Alijda-projecten. Deze projecten voor bestrijden van drugshandel, drugspanden en drugsgebruik dateren al van 1998. Kenmerkend voor de aanpak is dat verschillende instanties nauw samenwerken en daarbij ook persoonsgegevens uitwisselen.

Rotterdam streeft naar een integrale aanpak door diverse instanties van een groep van circa 700 drugsverslaafden die voor overlast zorgen of crimineel gedrag vertonen en doorgaans ook medische zorg en sociale hulp mijden. Het doel van de PGA is het terugdringen van de overlast in het publieke domein en het verbeteren van de gezondheidssituatie en het levensperspectief van deze personen. Aan dit samenwerkingsverband nemen onder meer deel de politie, de hulpverlening en de reclassering. Van de betrokken verslaafden worden gegevens uitgewisseld over hun contacten met zowel de politie als de hulpverlening uitgewisseld. De gedeelde informatie wordt opgeslagen in een basisdossier. Op basis van het dossier wordt vervolgens besloten tot een bepaalde aanpak, de zogenaamde zorg-, drang-, of dwangtrajecten.

De discussie binnen het samenwerkingsverband en met het CBP spitste zich toe op de grenzen die het beroepsgeheim van de zorgverleners stelt. Het CBP heeft in het overleg gewezen op essentiële uitgangspunten voor samenwerking. Zorgverleners dienen vast te houden aan de wettelijke plicht te handelen in het belang van de cliënt. Indien het naar hun professionele oordeel in het belang van de cliënt is dat zij informatie delen met andere instanties, is dat in principe mogelijk. De cliënt dient hiervan volledig op de hoogte te worden gebracht. Het uitwisselen van de informatie dient ook te passen in het gemeenschappelijk overeengekomen doel van het samenwerkingsverband. Dit doel mag niet op gespannen voet staan met de taak van de deelnemende organisaties of met de wettelijke grenzen die voor de organisatie gelden. In de loop van 2003 hebben de betrokken partijen de regels voor de informatie-uitwisseling uitgewerkt en kon het Informatiesysteem PGA gemeld worden bij het CBP.

Stroomlijning inzageverzoeken

Het aantal verzoeken om kennisneming bij de politie door personen die willen weten of en hoe zij geregistreerd staan in politieregisters, was in voorgaande jaren aanzienlijk toegenomen. Het aantal verzoeken steeg van 1100 in 2000 tot 1850 in 2002. Het ging vooral om complexe en tijdrovende verzoeken van advocaten, die door een CIE worden behandeld. Gevolg was ook dat het CBP fors meer verzoeken om bemiddeling ontving.

In zijn jaarverslag 2001 spreekt het CBP al over *fishing expeditions* van advocaten die over het doel van het inzagerecht heen schieten. Wanneer politie en justitie genoodzaakt worden in een te vroeg stadium informatie prijs te geven, doorkruist dat de opsporing of schaadt het de belangen van derden. Op verzoek van de politie en het OM werd door de Raad van Advies voor de CIE een werkgroep ingesteld waarin privacydeskundigen vanuit het politieveld, OM en het CBP deelnamen. In januari 2003 heeft de werkgroep Stroomlijning inzagerecht het rapport met een plan voor een andere en efficiëntere werkwijze uitgebracht. Hiermee wordt ook uitholling van het recht op kennisneming voorkomen.

Modelreglement Tijdelijk register goedgekeurd

Het CBP gaf in 2003 een verklaring van overeenstemming af voor het Modelreglement Tijdelijk register. De politie werkt voor het uitoefenen van de politietaak met verschillende politieregisters. Hierop zijn de Wet politieregisters en het Besluit politieregisters van toepassing. Er zijn permanente registers (bijvoorbeeld het Arrestantenregister of het register Jeugd en zedenzaken) waarvoor een reglement moet worden gemaakt. In 2002 keurde het CBP 40 modelreglementen voor dit type register goed. Daarnaast zijn er zeer veel tijdelijke registers die worden bijgehouden voor één specifiek politieonderzoek (bijvoorbeeld naar een moord of inbraak).

Kenmerkend voor een tijdelijk register is dat er, onder bepaalde voorwaarden, ook langer dan 4 maanden informatie over niet-verdachte personen in opgeslagen kan worden, voor het geval dit in een later stadium van het onderzoek van pas kan komen. Wanneer een tijdelijk register gereglementeerd werd, was daarvoor een procedure bij het CBP noodzakelijk. Ook voor deze registers kan nu een modelreglement worden gehanteerd onder vermelding van het specifieke doel van het onderzoek. Het gebruik van modelreglementen schept niet alleen waarborgen maar vermindert ook direct de administratieve lasten bij politie en CBP. In 2003 is door de politiekorpsen op aandringen van het CBP gestart met het op orde krijgen van de informatiehuishouding met betrekking tot deze tijdelijke registers ■

Arbeid en sociale zekerheid

In de sector arbeid en sociale zekerheid worden rond inkomen, uitkering en verzekering kolossale gegevensstromen gegenereerd door talloze instanties en bedrijven. Het terrein is voortdurend in beweging door nieuwe wetgeving. Het streven naar de inrichting van een overkoepelende elektronische informatie-infrastructuur voor de overheid met basisregistraties voor de kerngegevens komt daar nog bij. Ook in 2003 investeerde het CBP daarom stevig in advisering rond nieuwe wetgeving. Bescherming van de persoonlijke levenssfeer en rechtmatig gebruik van persoonsgegevens dienen immers van meet af aan te worden mee-genomen bij de inrichting van maatschappelijke instituties. Juist gericht op de praktijk was het in 2003 voltooide onderzoek naar de toepasselijke regelgeving voor gegevensuitwisseling omtrent de zieke werknemer. In 2004 zal de studie 'De zieke werknemer en privacy' worden gepubliceerd.

Wet werk en bijstand

In december 2002 heeft het CBP geadviseerd over een nieuwe bijstandswet, inmiddels de Wet werk en bijstand (WWB) geheten. De wet is op 1 januari 2004 in werking getreden. De kern van de wet is dat gemeenten meer (financiële) verantwoordelijkheid krijgen voor de bijstandsverlening. Het college van Burgemeester en Wethouders (B&W) is verantwoordelijk voor het beleid en de uitvoering ervan, de gemeenteraad ziet hierop toe. 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 een doelmatiger uitvoering van de bijstand waarbij onder andere de reïntegratie van bijstandsgerechtigden versneld wordt.

Het CBP heeft zich in 2002 en in 2003 meerdere malen uitgesproken over de inrichting van het toezicht op de WWB. Met de staatssecretaris van Sociale Zaken en Werkgelegenheid zijn hierover standpunten uitgewisseld en de behandeling van het wetsvoorstel door de Tweede en Eerste Kamer in 2003 is nauwlettend gevolgd. Verscheidene keren is met de Inspectie Werk en Inkomen (IWI) hierover gesproken. Het CBP komt tot de conclusie dat ondanks dit alles onduidelijkheid is blijven bestaan over het toezicht van IWI op de uitvoering van de WWB door gemeenten.

Toezicht op uitvoering WWB

Het CBP heeft de Vaste Kamercommissie van zowel de Tweede als de Eerste Kamer erop gewezen dat het toezicht op de verwerking van persoonsgegevens door gemeenten onvoldoende gerealiseerd dreigt te worden. Er is een kloof tussen de formele regeling dat het IWI toeziet op de rechtmatigheid van de uitvoering (inclusief de verwerking van persoonsgegevens) en de praktische uitwerking. Deze kloof is niet gedicht bij de parlementaire behandeling. Het gevolg hiervan is dat het IWI niet de nodige informatie ontvangt om toe te kunnen zien op de gegevensverwerking door gemeenten bij de uitvoering van de WWB en de wet Structuur Uitvoeringsorganisatie Werk en Inkomen (wet SUWI).

De verantwoordelijkheid voor het toezicht op de uitvoering van WWB is vooral bij de gemeenteraad gelegd. Het IWI zal toezicht houden op de werking van het systeem van sturing, beheersing en verantwoording bij gemeenten. In geval van ernstige tekortkomingen in de rechtmatigheid van de uitvoering kan de minister bijsturen. Tot de rechtmatigheidvereisten van de WWB behoren echter ook de bepalingen met welke instanties en personen gegevens mogen worden uitgewisseld, de daarbij behorende geheimhoudingsplicht en de doelbinding van de gegevensverstrekking door gemeenten aan andere in de wet genoemde instanties. Het IWI dient ook de rechtmatigheid van de uitvoering van deze bepalingen vast te stellen. Het IWI houdt verder toezicht op de rechtmatigheid, doelmatigheid en doeltreffendheid van de samenwerking tussen de gemeenten en de SUWI-partijen. Onderdeel hiervan is de gegevensuitwisseling tussen partijen via Suwi-net.

Om toezicht op deze gegevensuitwisseling mogelijk te maken zullen de gemeenten naar het oordeel van het CBP zich dienen te verantwoorden aan het IWI over de verwerking van persoonsgegevens. Het IWI zal dit toezicht kunnen uitoefenen op basis van de Verslagen van Uitvoering. De gemeenten zijn echter niet verplicht zich via dat verslag te verantwoorden over de juiste naleving van de bepalingen over gegevensuitwisseling, noch inzake de WWB noch inzake Suwinet.

Het CBP maakt zich over dit gebrek aan verantwoordingsplicht zorgen. Het zal voor IWI op deze manier niet mogelijk zijn om structureel toe te zien op de gemeenten voor deze aspecten van de WWB. Deze uitwerking van het toezicht is voor wat betreft de verwerking van (persoons)gegevens overigens niet in overeenstemming met het standpunt van de staatssecretaris tijdens de parlementaire behandeling.

Ook het toezicht op de beveiliging van Suwinet schiet in de uitwerking ernstig tekort. IWI zal geen toezicht kunnen houden op de beveiliging van de gegevensuitwisseling via Suwinet tegen inbreuken op de beschikbaarheid, de integriteit en de vertrouwelijkheid. De gemeenten zijn uitgezonderd van de verantwoordingsplicht die geldt voor andere SUWI-partners. De enige verplichting is om aan te geven of er een beveiligingsplan aanwezig is. Het CBP is van oordeel dat dat onvoldoende is en stelt voor dat gemeenten als partij met een verantwoordingsplicht in de Regeling SUWI worden opgenomen.

Reïntegratie

Het CBP adviseerde tevens over het eerste onderdeel van het conceptbesluit tot wijziging van het Besluit Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI). Voorgesteld werd om reïntegratiebedrijven en arbodienst te verplichten om het Uitvoeringsinstituut Werknemersverzekeringen (UWV) of het college van Burgemeester en Wethouders van de betrokken gemeente op verzoek én uit eigen beweging op de hoogte te brengen van een gegrond vermoeden dat iemand van wie de inschakeling in de arbeid wordt bevorderd, onvoldoende hieraan meewerkt.

Het CBP heeft in afgelopen jaren verscheidene malen verzocht om heldere regels te stellen voor overdracht van persoonsgegevens in het kader van reïntegratie. De voorgestelde wijziging van het Besluit SUWI draagt daar toe bij. De grondslag voor de verwerking bleef echter onduidelijk. Dat heeft ook consequenties voor de toepasselijkheid van het recht van de betrokkene op verzet tegen deze teruglevering van gegevens op grond van bijzondere persoonlijke omstandigheden. Juist bij reïntegratie kan dit een voor de betrokkene essentieel recht zijn. De teruglevering van gegevens aan de publieke opdrachtgevers dient overigens wel binnen de grenzen van het medisch beroepsgeheim te blijven. Bovendien dient telkens getoetst te worden of de verstrekking noodzakelijk is in het kader van de reïntegratie. Het tekstvoorstel was op dit punt te ruim geformuleerd.

Polisadministratie

Het CBP adviseerde over de Wet financiering sociale verzekeringen. Deze heeft als doel de heffing en inning van premies te concentreren bij de Belastingsdienst. Deze zal dan zorgen voor de heffing en de inning van de premies van zowel volksverzekeringen als de werknemersverzekeringen. Werkgevers doen dan aangifte van de loonbelasting en alle premies sociale verzekeringen en dragen op basis daarvan premies af. Deze aangifte bevat alle relevante gegevens van werknemers die van belang zijn voor zowel de loonbelasting en de premieheffing als het toekennen van een uitkering.

De fiscale database voor loongegevens (FI-base) zal worden gecombineerd met de verzekerdenadministratie van het UWV tot de polisadministratie. De polisadministratie zal uitgroeien tot een registratie van alle nominatieve loongegevens, loon- en dienstverbanden en uitkeringsverhoudingen voor werknemersverzekeringen, premies en loonheffing. De gegevensset van de polisadministratie zal zodanig wordt gedefinieerd dat hergebruik van de geregistreerde gegevens door andere bestuursorganen optimaal mogelijk is.

Het CBP steunde en steunt een verbetering van de gegevenshuishouding van de overheid maar had moeite met de globale regeling van de uitwisseling van gegevens door diverse bestuursorganen. De regering beoogt ook andere bestuursorganen de UWV-gegevens uit de polisadministratie te laten hergebruiken, wanneer dit de administratieve lasten van burgers en bedrijven vermindert of fraudebestrijding door en dienstverlening van de overheid bevordert. Gedacht wordt om deze gegevens beschikbaar te maken voor het CBS en uitvoerders van verplichte ziektekostenverzekeringen.

Stroomlijning van basisgegevens dient echter niet uit te monden in ongebreideld verkeer van persoonsgegevens binnen de overheid. Voor grote gegevensstromen is een specifieke en duidelijke wettelijke regeling geboden, met aandacht voor onder meer de maatschappelijke noodzaak, rol- en taakverdelingen, het feitelijke gegevensverkeer en transparantie (zie in dit verband ook de opmerkingen over de toekomstige ombudsfunctie van het CBP bij de invoering van het Burgerservicenummer op p. 27). De voorgestelde regeling schoot op een aantal van deze punten tekort. In de toelichting ontbrak dan ook een uiteenzetting over hoe de voorstellen zich verhouden tot de Wet bescherming persoonsgegevens. Privacyregels dragen echter bij tot het succes van de toekomstige elektronische informatie-infrastructuur van de overheid indien zij van begin af aan bij het ontwerp van de regelingen en systemen worden meegenomen.

De zieke werknemer

Al enkele jaren wordt getracht de instroom van zieke werknemers in de WAO te beperken. Dit heeft geleid tot maatregelen voor een actiever ziekteverzuimbeleid, strengere reïntegratieverplichtingen voor werknemer en werkgever en een langere verplichting voor de werkgever tot doorbetaling van het loon. Hierdoor is de behoefte bij de werkgever aan informatie over de zieke werknemer voor onder andere controle, reïntegratie en herverzekering toegenomen. Daarnaast hebben ook andere partijen een toenemende behoefte aan informatie over de zieke werknemer. Arbodienst, reïntegratiebedrijf, UWV of de verzuimverzekeraar hebben informatie nodig voor controle, begeleiding of reïntegratie en het uitbetalen van uitkeringen of verzekeringsclaims. Deze toenemende behoefte aan informatie over de zieke werknemer raakt direct aan de privacy van de zieke werknemer. Het is veelal informatie over de gezondheid van een werknemer die in een kwetsbare positie zit. Bij het CBP en zijn voorganger de Registratiekamer kwamen op dit gebied altijd al veel vragen binnen. Het is al met al van groot belang dat alle partijen geïnformeerd zijn over de geldende privacyregels.

Gezien de complexiteit van de totale regelgeving is het CBP in 2002 een onderzoek gestart naar de belangrijkste gegevensstromen omtrent de zieke werknemer en de daarbij behorende privacyregels. Het onderzoek omvatte het gehele proces van sollicitatie, het verzuimbeleid, ziekmelding, en reïntegratie tot herstel dan wel overgang naar de WAO. Eind 2003 kon het onderzoek afgerond worden. Voor het onderzoek zijn ook interviews gehouden met betrokken partijen. Voor de praktijk zijn vuistregels opgesteld waarover in januari 2004 vertegenwoordigers van de betrokken partijen zijn geconsulteerd. Het onderzoek heeft geresulteerd in een studie. De studie is vooral bedoeld als naslagwerk op de huidige regelgeving maar inventariseert ook de knelpunten.

Het is aan de betrokken partijen om de vuistregels in de eigen organisatie toe te passen. De concrete invulling is maatwerk. Werkgevers zullen in overleg met de ondernemingsraad deze invulling tot stand moeten brengen. Het CBP rekent erop dat de vuistregels spoedig worden ingebed in de praktijk en ook bruikbaar zullen blijken bij de behandeling van geschillen rond de zieke werknemer door de rechter.

Uit het onderzoek bleek andermaal hoe belangrijk het is dat de wetgever zorgt voor duidelijke regelgeving juist ook bij publiek-private samenwerking. Meer nog dan overheidsinstanties hebben bedrijven een belang bij duidelijkheid over wat wel en wat niet kan, zowel om redenen van bedrijfsvoering als omwille van hun reputatie en aansprakelijkheid.

Zwarte lijst frauderende werknemers

De Raad Nederlandse Detailhandel (RND) had het voornemen een waarschuwingslijst op te stellen van werknemers die ontslagen zijn wegens fraude en waartegen aangifte is gedaan, om zo potentiële werkgevers in de sector te kunnen informeren over het arbeidsverleden van de sollicitant. Het CBP toetste in 2003 vooraf de rechtmatigheid van de gegevensverwerking aan de normen van de Wet bescherming persoonsgegevens in het kader van een voorafgaand onderzoek.

Bedrijven en bedrijfstakken kunnen een gerechtvaardigd belang hebben bij het gebruik van een waarschuwingslijst. Een waarschuwingslijst, vaak zwarte lijst genoemd, maakt inbreuk op de persoonlijke levenssfeer en andere rechten en vrijheden van de betrokkene. Het aanleggen van een waarschuwingslijst is pas te rechtvaardigen wanneer schade een zodanige omvang heeft bereikt dat het noodzakelijk is het recht van bescherming van de persoonlijke levenssfeer en andere rechten en vrijheden van betrokkene deels te beperken. De verantwoordelijke moet er hierbij voor zorgen dat een zorgvuldige omgang met het systeem gegarandeerd is en de rechten van betrokkenen beschermd worden. Dit geldt des te meer als het recht op arbeid in een passende werkomgeving op het spel staat.

Op basis van het voorstel van de RND oordeelde het CBP dat de zwarte lijst van frauderende werknemers niet aan de eisen voldeed. De noodzakelijke waarborgen voor een zorgvuldige verwerking van persoonsgegevens en de bescherming van de rechten van de betrokkenen waren niet getroffen. De voorgestelde waarschuwingslijst was daarom in de gepresenteerde vorm onrechtmatig.

Het CBP vond onder meer dat onvoldoende gedegen en overtuigend was onderbouwd waarom een bedrijfstakbrede waarschuwingslijst noodzakelijk is en waarom niet volstaan kan worden met de bestaande mogelijkheden van screening. Om te voorkomen dat de waarschuwingslijst in de praktijk gaat uitwerken als een 'beroepsverbod' in de sector, is het noodzakelijk dat een zorgvuldige werkwijze in een protocol wordt vastgelegd. Dat was onvoldoende gedaan. Het doel van de waarschuwingslijst was te ruim genomen en niet gericht op bepaalde functies. De criteria voor opname in het systeem hielden onvoldoende rekening met de ernst van de misdragingen. Het CBP is van oordeel dat alleen werknemers die zeer ernstige (strafbare) feiten hebben gepleegd, in aanmerking komen voor plaatsing op een waarschuwingslijst voor de hele bedrijfstak. De RND zal in 2004 met een nieuw voorstel komen en dit ter beoordeling aan het CBP voorleggen ■

Zorg en welzijn

De discussie over kostenbeheersing en kwaliteitsversterking in de zorg wordt gedragen door een consensus over de noodzaak van meer marktwerking en meer informatisering. Naar marktwerking wordt gezocht via publiek-private samenwerking waarbij voor de zorgverzekeraars zich een zeer prominente rol begint af te tekenen. De verzekeraars stellen echter dat zij zonder maximaal inzicht in de feitelijke zorg deze rol niet kunnen vervullen.

Duidelijk bleek dit in de discussie rond de introductie van de Diagnose Behandeling Combinatie (DBC). De verzekeraars streefden naar een massale verstrekking van gedetailleerde, individuele behandelingsgegevens. Het CBP heeft zich in 2003 daartegen verzet en zich sterk gemaakt voor de bescherming van het medisch beroepsgeheim en het in acht nemen van maatvoering bij de verstrekking van medische persoonsgegevens.

Onrechtmatige verstrekking door verzekeraars

Ook met het oog op een breed vertrouwen in noodzakelijke verwerkingen van gezondheidsgegevens, dient de verwerking van deze gegevens zorgvuldig en volgens de gelden normen te geschieden. Het CBP behandelde in 2003 een klacht over onrechtmatige verstrekking van gezondheidsgegevens van een verzekerde door twee zorgverzekeraars aan derden. De zorgverzekeraars hadden informatie over tandartsnota's verstrekt aan de rechtsbijstandverzekeraar van zijn tegenpartij in een civiele procedure. Het CBP stelde de klager in het gelijk en beide zorgverzekeraars erkenden dat de – telefonische – verstrekking van de gegevens onzorgvuldig was geweest.

Alle gegevens over de geestelijke of lichamelijke gezondheid van een persoon zijn gegevens betreffende iemands gezondheid. Deze gegevens zijn bijzondere persoonsgegevens in de zin de Wet bescherming persoonsgegevens (WBP). Het verwerken van deze gegevens is in beginsel verboden. De verstrekking was niet noodzakelijk voor de beoordeling van het te verzekeren risico, noch voor de uitvoering van de verzekeringsovereenkomst. Op artikel 23 van de WBP (de verwerking is noodzakelijk voor vaststelling, uitoefening of verdediging van een recht in rechte) kon alleen een beroep gedaan worden als er een rechtmatige grondslag voor de verwerking zou zijn.

Aangezien van toestemming van de betrokkene geen sprake was, kwam in dit geval alleen het gerechtvaardigd belang van de rechtsbijstandsverzekeraar in aanmerking als grondslag. Dit impliceert een motiveringsplicht voor de verantwoordelijke: noodzakelijkheid, evenredigheid en doelmatigheid van de verstrekking moeten worden afgewogen. Bij het 'verder verwerken' van de gegevens mag de verstrekking bovendien alleen plaatsvinden ten behoeve van doeleinden die verenigbaar zijn met het doel waarvoor de gegevens oorspronkelijk werden verwerkt. Betrokkenen dienen in de regel vooraf in de gelegenheid te worden gesteld bezwaar te maken tegen een dergelijke verstrekking. Indien de betrokkene bezwaar maakt, dient dit bezwaar in de afweging van de verantwoordelijke betrokken te worden.

De verzekeringsmaatschappijen hadden voor de verstrekking geen toestemming gevraagd aan de klager noch een belangenafweging gemaakt. Evenmin hadden zij hem tevoren in de gelegenheid gesteld zich uit te spreken zodat hij zijn belangen naar voren had kunnen brengen. Het ontbrak de verzekeraars dus aan een rechtmatige grondslag voor deze verwerking.

Controlebevoegdheid zorgverzekeraar

Een zorgverzekeraar bleek apothekers de verplichting op te leggen per kwartaal een geautomatiseerde rapportage per verzekerde te verstrekken over het individuele verbruik van diabetes-testmateriaal. Het CBP stelde een onderzoek in naar aanleiding van een klacht van een apotheker en stelde hem in het gelijk.

De zorgverzekeraar wilde de gegevens per individuele gebruiker om te controleren of de verstrekking van hulpmiddelen doelmatig was. Het CBP onderkent de bevoegdheid van de zorgverzekeraar tot controle, maar oordeelde dat de manier waarop daaraan invulling werd gegeven, onrechtmatig was. De zorgverzekeraar is verplicht om bij het uitoefenen van zijn controletaak rekening te houden met zowel de bescherming van de persoonlijke levenssfeer en als met het medisch beroepsgeheim.

Structurele verstrekking van gegevens over het individuele gebruik van diabetes-testmateriaal door de apotheker aan de verzekeraar oordeelde het CBP onrechtmatig op grond van de WBP. Controle kan steekproefsgewijs en op geaggregeerd niveau plaatsvinden; individuele patiëntengegevens zijn daarvoor in beginsel niet noodzakelijk. Alleen bij concrete twijfel aan de juistheid van de declaratie en de verstrekking van medicijnen en andere middelen kan het gerechtvaardigd zijn dat de verzekeraar een nader onderzoek instelt. Het op voorhand verzamelen van alle verbruiksgegevens op individueel patiëntenniveau is niet geoorloofd.

Fraudebestrijding zorgverzekeringswetten

Het CBP adviseerde positief over een aantal aspecten van het wetsvoorstel fraudebestrijding zorgverzekeringswetten, waaronder het scheppen van een identificatieplicht en het benutten van het sofinummer.

Het voorstel was om een identificatieplicht op te nemen in de Algemene Wet Bijzondere Ziektekosten (AWBZ) en de Ziekenfondswet (Zfw). Het CBP was het daarmee niet oneens. Het inroepen van zorg ten laste van de sociale ziektekostenverzekeringswetten is een geldige reden om van de burger identificatie te eisen. Een identificatieverplichting bij zorgverlening kan overigens onaanvaardbare consequenties hebben wanneer er zonder een identiteitsbewijs geen toegang is tot noodzakelijke – zij het mogelijk niet steeds spoedeisende – gezondheidszorg. Het CBP vroeg wel zich af of de noodzakelijke toegang tot zorg voldoende gegarandeerd zou blijven.

Ook het gebruik van het sofinummer in de administratie van de ziektekostenverzekeraars dient vooral controle en fraudebestrijding. Het CBP kwam tot de conclusie dat de invoering van het sofinummer voldoende was onderbouwd, niet onverenigbaar is met de doeleinden waarvoor het nummer is ingericht en aansluit bij het bestaande wettelijke stelsel voor het gebruik ervan.

Diagnose behandeling combinatie

Binnen de zorgsector is de Diagnose Behandeling Combinatie (DBC)-systematiek ontwikkeld voor de bekostiging van specialistische medische zorg. DBCs zijn combinaties van codes die gegevens bevatten over onder andere de zorgvraag, de diagnose en de behandeling van een patiënt. Deze gegevens dienen door een zorgverlener verstrekt te worden aan een zorgverzekeraar voor declaratie van de verleende zorg. Dit nieuwe bekostigingssysteem moet leiden tot een marktconforme prijsontwikkeling op basis van onderhandelingen tussen zorginstellingen en zorgverzekeraars.

Een DBC bevat gedetailleerde (medische) informatie over een patiënt. Er zijn tienduizenden mogelijke DBCs. De informatie hiervoor komt uit de behandeling voort en op deze informatie is het medisch beroepsgeheim van toepassing. Zowel de WBP als het medisch beroepsgeheim stellen strikte beperkingen aan de gegevensuitwisseling tussen hulpverleners, ziekenhuizen en zorgverzekeraars. Alleen gegevens die noodzakelijk zijn voor uitvoering van de wettelijk omschreven doeleinden mogen worden verstrekt (noodzakelijkheidsvereiste).

Op 26 februari 2003 heeft het CBP de nota over de invoering van de DBC-systematiek van de minister van Volksgezondheid, Welzijn en Sport (VWS) besproken met in het bijzonder het ministerie van VWS en Zorgverzekeraars Nederland. Het CBP stond op het standpunt dat inzichtelijk moest worden gemaakt welke per-

soonsgegevens – zo deze al verwerkt mochten worden – noodzakelijkerwijs door ziekenhuizen aan de zorgverzekeraars zouden moeten worden verstrekt om de verschillende doelen te bereiken die met de invoering van de DBC-systematiek worden nagestreefd.

Managementinformatie bijvoorbeeld kan met niet tot personen herleidbare gegevens worden gerealiseerd en voor de betaling van zorg door de verzekeraars kan met een beperkte set persoonsgegevens worden volstaan. Het noodzakelijkheidsvereiste is de kern van de zaak. Als duidelijk is welke gegevensverwerkingen noodzakelijk zijn voor de diverse, gerechtvaardigde doeleinden, kan de juridische verankering van het nieuwe bekostigingssysteem daarop aansluiten. In afwachting van deze uitwerking bestond voor de invoering van het DBC-systeem geen toereikende juridische grondslag.

Op 26 juni 2003 zag het CBP aanleiding te waarschuwen voor het gevaar van schending van het medisch beroepsgeheim door invoering van de DBC-systematiek. Het CBP stelde ook de artsenorganisatie Koninklijke Nederlandse Maatschappij tot bevordering der Geneeskunst (KNMG) op de hoogte van zijn standpunt. De DBC-systematiek zou leiden tot een gegevensstroom van patiëntgegevens die verder zou gaan dan noodzakelijk was voor de afhandeling van declaraties, onder andere door het verstrekken van diagnose-informatie.

In november 2003 heeft de minister van VWS het CBP om advies gevraagd over de wettelijke grondslag voor de DBC-systematiek. In het advies op het wetsvoorstel Wijziging Ziekenfondswet en de Algemene Wet Bijzondere Ziektekosten stemde het CBP in met de voorgestelde wettelijke grondslagen, mits deze worden uitgewerkt in onderliggende regelingen. Wel dient evaluatie van het systeem op den duur te leiden tot minder gedetailleerde informatieverstrekking door zorgverleners aan zorgverzekeraars. De privacygevoeligheid van het DBC-stelsel zal daarmee afnemen.

De uitwerking van het noodzakelijkheidsvereiste heeft geleid tot een toetsingskader voor de DBC-systematiek. Het CBP adviseerde de minister van VWS dit onder te brengen in een ministeriële regeling. Het toetsingskader biedt vijf criteria aan de hand waarvan bepaald wordt of een DBC al dan niet gedeclareerd zal worden met alle bijbehorende informatie over de diagnose. Deze toetsing dient ervoor te zorgen dat alleen noodzakelijke informatie wordt verstrekt.

De DBC-systematiek zal vanaf 1 januari 2005 gefaseerd ingevoerd worden. In een gezamenlijke brief hebben de minister van VWS en het CBP de betrokken partijen (zoals Zorgverzekeraars Nederland en koepelorganisaties) gevraagd de werkwijze voor de invoering van het stelsel onder de aandacht van hun leden te brengen.

De werkwijze voor de invoering gaat uit van verdeling van de ziekenhuisproductie in een segment A met vaste prijzen en een segment B met prijzen waarover onderhandeld wordt. Het toetsingskader dient als basis voor de informatieverstrekking door ziekenhuizen aan verzekeraars voor segment A, ongeveer 90 % van de behandelingen in de ziekenhuizen. Voor behandelingen in segment B worden de DBC's volledig gespecificeerd verstrekt. Toepassing van het toetsingskader op dit segment liet onvoldoende mogelijkheden voor controle op de juistheid van de declaraties. Voor het moment is dit alleen aanvaardbaar omdat het om een klein aantal DBC's gaat, 300 op een totaal van enkele tienduizenden.

Voor uitbreiding van het segment met vrije prijzen zijn ingrijpender maatregelen voorgesteld. De medische informatie in een DBC zal 'grover' moeten worden. Dat zal leiden tot vermindering van het aantal DBC's en tot minder gedetailleerde informatie per DBC. Ook zullen de DBC's in homogenere groepen – qua kosten en in medisch opzicht – moeten worden ondergebracht, zodat de prijsonderhandelingen voor de zorgverzekeraars eenvoudiger worden. Eventueel zal een zogenaamde trusted third party (TTP) worden opgericht. Deze TTP zou enerzijds kunnen zorgen voor het groeperen van declaraties en anderzijds voor het aanleveren van geanonimiseerde beleidsgegevens aan de verzekeraar.

Verder worden aanvullende maatregelen getroffen. Zo zullen verzekeraars in 2004 de Gedragscode Verwerking persoonsgegevens financiële instellingen (banken en verzekeraars) uitbreiden met specifieke gedragsregels met betrekking tot de zorgverzekeraars. Tussen het CBP en Zorgverzekeraars Nederland vindt reeds overleg plaats over de mogelijkheden voor controle en fraudebestrijding.

Eisenbesluit lichaamsmateriaal

Het CBP adviseerde ook over het concept van het Eisenbesluit lichaamsmateriaal, dat het Besluit kwaliteitseisen orgaanbanken zal vervangen. Het besluit is gebaseerd op de Wet veiligheid en kwaliteit lichaamsmateriaal en de Wet op de orgaandonatie. Het heeft tot doel de overdracht van besmettelijke ziekten te reduceren en de ontvanger van lichaamsmateriaal tegen kwalitatief slechte producten te beschermen.

In de toelichting op wet- en regelgeving blijft nog al eens de relatie met de regels voor zorgvuldige en rechtmatige verwerking van persoonsgegevens onbesproken. Het CBP adviseerde de minister van VWS om aan de grondslagen en de voorwaarden voor verwerking van persoonsgegevens uitdrukkelijk aandacht te besteden in de nota van toelichting, te meer daar het gegevens omtrent de gezondheid betreft. De verwerking daarvan is immers aan strikte regels gebonden. Een nadere uitwerking was gewenst van onder andere de beveiliging, het inzagerecht van de betrokkene en de vraag welke partijen welke (noodzakelijke) gegevens mogen verwerken. Evenmin was duidelijk of ook erfelijkheidsgegevens verwerkt zullen worden.

Landelijke registraties

Zorginstellingen zijn ook informatiefabrieken, die zeer veel persoonsgegevens produceren. Daarnaast is het aantal landelijke registraties van medische gegevens groeiende. Deze registraties dienen uiteenlopende doelen. Vaak gaat het om wetenschappelijk onderzoek of om informatie ter vergelijking voor bepaalde hulpverleners beschikbaar te maken. Op deze registraties was al geruime tijd weinig zicht.

In 2003 heeft het CBP een oriënterend onderzoek afgerond naar landelijke registraties in de zorg. Na een globale inventarisatie zijn vijf registraties uitgekozen voor onderzoek. Eerst werden schriftelijk vragen aan de verantwoordelijke organisaties gesteld over onder meer het soort gegevens, de omvang van de registratie, en hoe de gegevens verkregen, gebruikt en beveiligd werden. Daarna werden interviews en feitelijke controles gehouden, in een aantal gevallen ook bij een bewerker van de gegevens. De resultaten van het onderzoek zijn gerapporteerd aan de verantwoordelijken. Het CBP zal de resultaten van het onderzoek gebruiken voor de formulering van beleid inzake landelijke registraties in de zorg in 2004 ■

Handel en diensten

De wetgever heeft bij de bescherming van persoonsgegevens een duidelijke plaats ingeruimd voor zelfregulering, onder meer door uitdrukkelijk ruimte te laten voor gedragscodes die worden opgesteld door de desbetreffende sector en worden goedgekeurd door de toezichthouder. Doorgaans wordt het CBP nauw betrokken bij het tot stand komen van de gedragscode. Gedragscodes zijn belangrijk, omdat zij het bewustzijn van de normen voor de bescherming van persoonsgegevens vergroten en duidelijkheid scheppen voor de praktijk. De instelling van goed toegankelijke, onafhankelijke geschillencommissies versterken de werking van gedragscodes. De specifieke uitwerking van privacynormen voor bepaalde sectoren of beroepen schept ook voor het handhaven van de normen door de toezichthouder een helder kader.

Gedragscode financiële instellingen

In januari 2003 kon de belangrijke Gedragscode verwerking persoonsgegevens financiële instellingen worden goedgekeurd. De doorzichtigheid van het gebruik van persoonsgegevens in de financiële sector is hierdoor voor consumenten vergroot. Belangrijkste aandachtspunt binnen de gedragscode is de doelbinding: 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. Zo worden financiële instellingen bijvoorbeeld vaak benaderd – ook door handelsinformatiebureaus – met verzoeken om informatie over de kredietwaardigheid van hun cliënten. Dergelijke informatie mag door de financiële instelling echter niet worden verstrekt, omdat dat onverenigbaar is met het doel waarvoor de gegevens zijn verzameld. Alleen indien de cliënt expliciet toestemming heeft gegeven, mag de financiële instelling de gevraagde informatie verstrekken. Daarnaast gaat de gedragscode ook in op enkele bijzondere onderwerpen, zoals het gebruik van cameratoezicht en het opnemen van telefoongesprekken.

De gedragscode is de opvolger van de Privacy Gedragscode Banken uit 1995 en de Gedragscode Verwerking Persoonsgegevens Verzekeringsbedrijf van 1998. Gezien de toenemende verwevenheid tussen banken en verzekeraars en met het oog op de invoering van de WBP besloten de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars de beide gedragscodes samen te voegen.

Gedragscode handelsinformatiebureaus

In augustus 2003 kon ook de Gedragscode inzake het verwerken van persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus (NVH) worden voorzien van een goedkeurende verklaring. Het CBP is tevreden met de totstandkoming van een gedragscode in deze sector. De afgelopen jaren onderzochten het CBP en zijn voorganger, de Registratiekamer, meerdere handelsinformatiebureaus en concludeerden dat er op grote schaal onzorgvuldig werd omgegaan met de bescherming van persoonsgegevens.

De gedragscode van de NVH kan een belangrijke bijdrage leveren aan een zorgvuldiger omgang met persoonsgegevens binnen deze sector. In de gedragscode zijn bepalingen opgenomen die aangeven voor welke doeleinden persoonsgegevens verwerkt mogen worden en dat deze persoonsgegevens slechts uit een beperkt aantal bronnen mogen worden verkregen. Ook wordt er invulling gegeven aan de rechten van de betrokkenen en de verplichting van een handelsinformatiebureau om betrokkenen uit eigen beweging te informeren over de verwerking van hun persoonsgegevens. Het CBP zal de gedragscode van de NVH hanteren als richtsnoer voor het handelen van alle handelsinformatiebureaus.

Gedragscode particuliere recherche

De Privacygedragscode voor de particuliere onderzoeksbureaus werd in januari 2004 goedgekeurd. De gedragscode is opgesteld door de Vereniging van Particuliere Beveiligingsbureaus (VPB) en bindt de bij de VPB aangesloten bureaus. De minister van Justitie is echter voornemens in 2004 de naleving van de gedragscode verplicht te stellen voor alle particuliere recherchebureaus in het kader van de vergunningverlening aan deze bureaus.

De particuliere recherche is een sterk groeiende sector waarin vergaande methoden van particulier onderzoek worden toegepast, terwijl tegelijkertijd weinig geregeld was. De code beschrijft de praktijk van het particulier onderzoek en geeft daarbij normen voor onder andere heimelijke observatie, verborgen camera's, het afluisteren van telefoongesprekken en het onderscheppen van e-mail.

Bedrijven – de grote opdrachtgevers voor de particuliere recherche – en ook particulieren kunnen zich nu beter informeren over de mogelijkheden die zij hebben voor de bestrijding van onregelmatigheden.

De gedragscode geeft ook bescherming aan personen die onderzocht worden door particuliere recherchebureaus.Onderzochte personen moeten in enig stadium van het onderzoek worden geïnformeerd over de uitkomsten van het onderzoek. Zij kunnen ook klachten indienen tegen aangesloten recherchebureaus. De gedragscode voorziet in onafhankelijke geschillenbeslechting. De minister van Justitie en het CBP sloten begin 2004 een samenwerkingsovereenkomst om het toezicht op de branche af te stemmen.

Gedragscode gerechtsdeurwaarders

In februari 2004 heeft het CBP de Gedragscode gerechtsdeurwaarders ter bescherming persoonsgegevens van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders goedgekeurd. Gerechtsdeurwaarders kennen twee soorten werkzaamheden. De gerechtsdeurwaarder oefent een ambtelijke taak uit, zoals onder meer het uitbrengen van dagvaardingen. Daarnaast mag een gerechtsdeurwaarder ook niet-ambtelijke werkzaamheden verrichten, zoals het incasseren van geldvorderingen.

Omdat gerechtsdeurwaarders als openbaar ambtenaar vergaande wettelijke bevoegdheden hebben om informatie in te winnen, is het noodzakelijk dat zij informatie verkregen uit hoofde van deze bijzondere wettelijke bevoegdheden niet zonder meer gebruiken voor de niet-ambtelijke werkzaamheden. De gedragscode geeft daarom regels voor een zorgvuldige informatiehuishouding bij gerechtsdeurwaarders. Ook schrijft de gedragscode voor dat een gerechtsdeurwaarder ervoor moet zorgen dat duidelijk is in welke hoedanigheid hij optreedt, als openbaar ambtenaar of als commerciële dienstverlener.

Europese gedragscode direct marketing

In juli 2003 werd de eerste gedragscode onder de Europese Privacyrichtlijn goedgekeurd door de Artikel 29-werkgroep van Europese privacytoezichthouders, genoemd naar het desbetreffende artikel van deze richtlijn. Het gaat om de gedragscode van de Europese direct marketing brancheorganisatie FEDMA (Federation of European Direct Marketing).

Deze Europese gedragscode schept – als instrument voor best practice – niet alleen verplichtingen voor de bij de FEDMA aangesloten nationale brancheorganisaties, maar indirect ook voor de direct marketing dienstverleners en voor bedrijven en organisaties die zelf direct marketing activiteiten ontplooien.

Relatiebestand ING Groep

Bedrijven hebben in beginsel ruime mogelijkheden om persoonsgegevens te verwerken voor marketingdoeleinden. Belangrijke voorwaarde voor een rechtmatige verwerking is goede informatie aan de klanten om wier gegevens het gaat. Transparantie en goede informatie zijn ook essentieel voor het vertrouwen van de klant. Dat bleek opnieuw uit de kwestie van de geheime nummers bij KPN (zie p. 43-44) en uit de klachten die binnenkwamen naar aanleiding van een ontwikkeling binnen de ING Groep.

ING Bank, Postbank en RVS – van de ING Groep – hadden in 2002 een brief aan hun cliënten geschreven over het plan hun gegevens voor marketingdoeleinden voortaan ook in één centraal systeem vast te leggen. De geboden informatie gaf cliënten echter onvoldoende mogelijkheden hun rechten uit te oefenen. Naar aanleiding van klachten en berichten in de pers werd een onderzoek ingesteld. In maart 2003 kwam het CBP tot de conclusie dat de bedrijven in deze onrechtmatig gehandeld hadden.

De ING Groep had de cliënten van de diverse onderdelen beter moeten informeren om hun gegevens op centraal niveau verder te mogen verwerken. De cliënt kon niet – bijvoorbeeld bij het openen van een rekening bij de Postbank – vermoeden dat hij steeds als klant van de gehele ING groep zou worden beschouwd. De spanning tussen de toenemende integratie van de interne bedrijfsvoering en het hanteren van verschillende merknamen was hier deels debet aan. Door de weinig specifieke wijze waarop de betrokkenen in de brief waren geïnformeerd over de gegevensverstrekking, was de verstrekking niet verenigbaar met het doel waarvoor de gegevens waren verzameld.

De ING Groep heeft de cliënten van ING Bank, Postbank en RVS in december 2003 aanvullend geïnformeerd over de aanleg van het centrale klantenbestand. De ING Groep gaf met dit voorstel gevolg aan de uitspraak van het CBP.

Dwangsom voor handelsinformatiebureau X

In april 2003 publiceerde het CBP de resultaten van het in juli 2002 gestarte onderzoek naar de wijze waarop handelsinformatiebureau X omging met persoonsgegevens. Het CBP kwam in zijn rapport op basis van de ter plaatse verzamelde gegevens tot de conclusie dat het bureau onrechtmatig, onbehoorlijk en onzorgvuldig persoonsgegevens had verwerkt voor het maken van rapportages met verhaalsinformatie. Bureau X handelde structureel in strijd met een groot aantal specifieke bepalingen van de WBP.

Uit het onderzoeksmateriaal bleek dat het bureau gegevens verwerkte die onder de geheimhoudingsverplichtingen van medewerkers van diverse instanties vielen. Bij het Openbaar Ministerie werd aangifte gedaan van een vermoeden van een aantal strafbare feiten. Het hierop gestarte opsporingsonderzoek heeft inmiddels geleid tot strafrechtelijke veroordeling van een belangrijke sleutelfiguur en vervolging van directie, personeelsleden en het bureau. Het CBP had geconstateerd dat uit allerlei instanties – waaronder de Belastingdienst, uitkeringsinstanties, Kamers van Koophandel, de Rijksdienst voor het Wegverkeer en woningcorporaties – onrechtmatig persoonsgegevens aan het bureau verstrekt werden. Het CBP heeft daarom ook een groot aantal van deze instanties, bedrijven en beroepsorganisaties nader geïnformeerd over de bevindingen in het onderzoek opdat zij passende maatregelen konden nemen. Een aantal van hen heeft daartoe relevante delen van het bewijsmateriaal ontvangen. Ook stelden diverse opdrachtgevers van bureau X vragen waarvan zij dienden te weten dat de antwoorden niet rechtmatig zonder toestemming van de betrokkenen konden worden verkregen. Veel opdrachtgevers van het bureau waren advocatenkantoren. De Nederlandse Orde van Advocaten heeft inmiddels aangekondigd stappen te zullen ondernemen om dit in de toekomst te voorkomen.

In mei 2003 legde het CBP bureau X een last onder dwangsom op. De last richtte zich op de naleving van twee punten waarop overtredingen van de WBP zijn geconstateerd: bureau X dient zich te onthouden van het verwerken van persoonsgegevens die onder geheimhoudingsverplichtingen vallen of waarvoor een verwerkingsverbod geldt en het bureau moet de betrokkene over wie persoonsgegevens worden verzameld inlichten.

Bureau X diende vervolgens een bezwaarschrift in. Bij besluit van 21 augustus 2003 is het bezwaarschrift ongegrond verklaard en de last onder dwangsom gehandhaafd. Het bureau tekende beroep aan bij de bestuursrechter te Den Haag en startte tevens een rechtszaak om de last onder dwangsom te laten schorsen. In maart 2004 heeft de rechter in beide zaken uitspraak gedaan en bureau X in het ongelijk gesteld. Naar het oordeel van de rechter heeft het CBP terecht gesteld dat het bureau structureel in strijd met de privacywetgeving handelde.

In beide rechtszaken speelde de formulering van de last onder dwangsom een belangrijke rol. Bureau X stelde dat de last zo algemeen geformuleerd was dat deze in strijd zou zijn met de rechtszekerheid. De rechter was echter van mening dat zowel uit de toelichting van het CBP in zijn beslissing op het bezwaarschrift als uit de Gedragscode inzake het verwerken van persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus duidelijk genoeg bleek hoe bureau X geacht werd om te gaan met de verwerking van persoonsgegevens en in welke gevallen het een dwangsom verbeurt. De naleving van de last zal in 2004 door het CBP worden gecontroleerd.

Zwarte lijsten

Zwarte lijsten als hulpmiddel bij de bestrijding van fraude en criminaliteit bleven in 2003 in de belangstelling. Het CBP verwees bij verzoeken om informatie veelal naar de regels voor het aanleggen van waarschuwingslijsten die samen met praktijkinformatie op de CBP-website gepubliceerd zijn in het dossier Zwarte Lijsten. In enkele zaken werd een rechtmatigheidsoordeel uitgesproken. De waarschuwingslijst van frauderende werknemers van de Raad Nederlandse Detailhandel werd afgekeurd. De waarschuwingslijst van Koninklijk Horeca Nederland (KHN) van 'eetpiraten' en andere fraudeurs werd in eerste instantie afgekeurd, maar kon naderhand in gewijzigde vorm rechtmatig worden bevonden.

KHN had een interne waarschuwingsdienst in gebruik genomen als middel ter bestrijding van fraude en misbruik door klanten of leveranciers. Deze dienst maakte gebruik van een zwarte lijst. Een eerdere vorm van de zwarte lijst in het kader van de Waarschuwingsdienst werd in februari 2003 door het CBP onrechtmatig verklaard na een voorafgaand onderzoek. KHN maakte vervolgens bewaar tegen deze onrechtmatigheidsverklaring. Tijdens overleg in het kader van deze procedure bleek dat de waarschuwingslijst aangepast kon worden. Naar aanleiding van de nieuwe melding en het nieuwe protocol kwam het CBP in juli 2003 tot het oordeel dat de waarschuwingslijst in de aangepaste vorm rechtmatig was ■

Telecommunicatie

De complexiteit van de in elkaar grijpende Europese en nationale wet- en regelgeving op het gebied van de telecommunicatie maakte dat wetgevingsadvisering en het volgen van de normatieve ontwikkelingen prioriteit hield. Daarnaast is het CBP in 2003 gestart met het consulteren van de telecomsector om te komen tot verheldering van de normen voor de praktijk als opmaat tot daadwerkelijke handhaving. Ook in de telecommunicatiesector zal het CBP overgaan tot meer handhaving.

KPN-beleid geheime nummers

Medio 2002 hebben het CBP en de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), mede naar aanleiding van klachten, een onderzoek ingesteld naar het beleid van Koninklijke KPN N.V. (KPN) omtrent nummers met beperkte bekendheid, algemeen bekend als 'geheime nummers'. De toezichthouders wilden weten hoe abonnees geïnformeerd werden over dit beleid en hoe het bedrijf vorm gaf aan de rechten van de abonnee op geheimhouding. Onderzocht werd ook het verstrekken aan derden van de adresgegevens behorende bij geheime nummers voor reclamedoeleinden.

Het onderzoeksrapport is medio 2003 gepubliceerd. De voornaamste constatering was dat KPN haar beleid halverwege de jaren '90 heeft gewijzigd en sinds geruime tijd de adresgegevens van abonnees met een geheim nummer voor direct marketing doeleinden aan derden ter beschikking stelt zonder dat zij haar abonnees daarover expliciet heeft geïnformeerd.

PTT Telecom (verder: KPN) had begin jaren '90 als beleid dat adresgegevens behorende bij geheime nummers niet aan derden werden verstrekt voor direct marketing. KPN droeg dit beleid ook actief uit in haar externe communicatie. Abonnees werd onomwonden verteld dat de adresgegevens behorend bij geheime nummers niet aan derden zouden worden verstrekt. Abonnees mochten dus verwachten dat hun gegevens inderdaad 'geheim' zouden blijven. Deze verwachting is grotendeels door KPN zelf opgeroepen en bestendigd.

De voorlichting van KPN na de beleidswijziging is veel minder duidelijk. In plaats van 'geheim nummer' wordt meestal de term

'nummer met beperkte bekendheid' gebruikt, die de meeste abonnees minder zegt. Ook wordt in plaats van 'adresgegevens' doorgaans eenvoudig 'gegevens' gebruikt. Bovendien is voorlichting over het gebruik van de adresgegevens niet altijd te vinden bij de overige informatie over geheime nummers.

Het CBP concludeerde dat KPN de beleidswijziging onvoldoende aan abonnees met een geheim nummer heeft gecommuniceerd, en dat zij informatie over geheime nummers sindsdien op een ondoorzichtige manier verschaft.Het CBP verzocht KPN binnen vier weken te laten weten hoe en wanneer zij klanten actief zou informeren over het beleid rond geheime nummers. KPN vroeg vervolgens meer tijd om de gevraagde informatie aan het CBP voor te leggen en kreeg ruimte tot 1 december 2003. Teleurstellend is dat de kwestie zich begin 2004 nog voortsleept, terwijl het in de kern gaat om een wettelijke plicht van het bedrijf om klanten actief te informeren over hun wettelijke rechten.

Afscherming nummers op telefoonnota's

Het CBP adviseerde over het ontwerp-Besluit afscherming nummers notaspecificatie. Ook volgens de nieuwe Europese Richtlijn privacy en elektronische communicatie moeten lidstaten in hun wetgeving het recht op gespecificeerde rekeningen voor telecommunicatiediensten in evenwicht brengen met het recht op privacy van gebruikers. De verplichting hieraan praktisch inhoud te geven dateert overigens al van 1997 en het voorgestelde besluit zal nu in deze leemte voorzien.

Het vermelden van gebelde telefoonnummers op gespecificeerde rekeningen door telecommunicatiebedrijven blijkt in de praktijk vooral problemen op te leveren omdat de telefoonrekening inzicht geeft in het communicatiegedrag van werknemers of van medegebruikers van de aansluiting (zie ook p. 20).

Volgens het ontwerp-Besluit moeten voortaan alle telecommunicatiebedrijven bij notaspecificatie de mogelijkheid aanbieden tot afscherming. De abonnee kan voortaan zijn eigen telecommunicatiebedrijf daarop aanspreken. In de huidige situatie worden klagende abonnees nog wel eens van het kastje naar de muur gestuurd. Iedere operator moet nu de af te schermen nummers van de eigen abonnees kenbaar maken aan andere aanbieders met het oog op afscherming op nota's.

Het CBP kon zich vinden in deze aanpak. In sommige andere Europese landen is inmiddels ervaring opgedaan met een vergelijkbare oplossing en navraag bij Europese privacytoezichthouders leverde in het algemeen een positieve indruk op. De WBP werd overigens te weinig in aanmerking genomen. Ook op grond van deze wet kunnen klanten aanspraak maken op afscherming en hebben telecommunicatieaanbieders de plicht om klanten actief te informeren over de keuzemogelijkheden. Een en ander bleek ten onrechte niet uit de memorie van toelichting.

Nieuwe Telecommunicatiewet

Eind 2002 adviseerde het CBP over de nieuwe telecommunicatiewet (Tw), de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002, die in het najaar van 2003 door de Tweede Kamer werd aanvaard. Het gaat om de implementatie van een vijftal Europese richtlijnen waaronder ook de Richtlijn privacy en elektronische communicatie. Deze laatste richtlijn die ook van toepassing is op internet en andere nieuwe technologie, scherpt de informatieplicht voor telecommunicatieaanbieders aan en geeft regels inzake spam, cookies en spyware. In zijn advies vroeg het CBP aandacht voor een aantal algemene kwesties. Verder is een groot aantal opmerkingen gemaakt bij uiteenlopende onderdelen van hoofdstuk 11 en andere relevante bepalingen in het wetsvoorstel.

In het wetsvoorstel zoals dat aan de Tweede Kamer is aangeboden, zijn enkele onderdelen die vragen bij het CBP oproepen, geschrapt waaronder een bevoegdheid van de minister van Economische Zaken om vormen van elektronische dienstverlening te verbieden die niet aftapbaar waren. De minister van Economische Zaken zette in de memorie van toelichting uiteen dat voor hoofdstuk 11 Tw zowel de OPTA als het CBP bevoegd zijn om toezicht uit te oefenen. OPTA en CBP dienen te overleggen over de concrete uitoefening van hun bevoegdheid. Hierover vindt inmiddels overleg tussen de OPTA en het CBP plaats; beide toezichthouders streven naar samenwerking en een heldere taakverdeling.

Consultatie sector over nummeridentificatie

De complexiteit van de wet- en regelgeving in relatie tot de telecommunicatiepraktijk heeft het CBP doen besluiten meer aandacht te geven aan voorlichting binnen de sector. Het CBP onderkent daarbij de waarde van de kennis en ervaring van de telecommunicatiesector zelf voor een evenwichtige afweging van belangen bij de bescherming van persoonsgegevens. In het najaar van 2003 is het CBP daarom een eerste consultatieronde gestart over nummeridentificatie.

Het CBP had zich in 2003 eerst een beeld gevormd van het aanbod van nummeridentificatiediensten, de technische werking en de beschikbaarheid van informatie voor consumenten. Tussen de operators verschilde het aanbod niet veel, evenmin als de aangeboden blokkeringsmogelijkheden. Met de consultatie beoogt het CBP te komen tot invulling van de aspecten waarvoor het normenkader onvoldoende helder is. Alle telecommunicatieaanbieders zijn uitgenodigd schriftelijke hun visie te geven op een vijftiental kwesties. De resultaten van de consultatie zullen in 2004 worden gebruikt voor de formulering van het CBP-beleid gericht op de naleving van de privacyregels voor de telecommunicatiesector ■

Technologie en audit

Het CBP heeft steeds veel tijd geïnvesteerd in het volgen van ontwikkelingen in de technologie, niet alleen op het terrein van de informatie- en communicatie-technologie maar ook op het terrein van de genetica en biometrie. Ook in de samenwerkingsverbanden met Europese en andere privacytoezichthouders staan technologische ontwikkelingen hoog op de agenda. Daarnaast heeft het CBP ook zelf bijgedragen aan het ontwikkelen van technische concepten, met name dat van de Privacy-Enhancing Technologies (PET), technische middelen om de rechtmatige omgang met persoonsgegevens zeker te stellen. De deelname aan het Europese project PISA (Privacy Incorporated Software Agent) is daarvan het meest recente en laatste voorbeeld.

In de toekomst zal het CBP zich richten op technology watching, het volgen van de technologische ontwikkelingen met het oog op de kansen en bedreigingen voor de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Ook bij technologie wil en moet het CBP in de tweede lijn opereren. De gedachte dat technologie gebruikt kan worden om persoonsgegevens efficiënt te gebruiken én goed te beschermen zal met kracht worden uitgedragen onder het motto *Privacy by design*.

Implementatie van privacy

Het CBP brengt bedrijven en organisaties regelmatig advies uit over technische concepten en ontwikkelingen. In 2003 is met name tijd besteed aan het ontwikkelen van een set producten waardoor *technology consultants*, systeemarchitecten en verwante adviseurs het concept *Privacy by design* in hun adviezen en ontwerpen voor hun klanten mee kunnen nemen. Deze virtuele gereedschapskist wordt ontwikkeld in samenwerking met een internationaal adviesbureau op het gebied van technologie-implementatie. Naderhand zal het materiaal voor alle geïnteresseerde partijen vrijelijk beschikbaar zijn. Het CBP verwacht op deze wijze de implementatie van PET in concrete systemen te stimuleren.

Op het gebied van normontwikkeling heeft het CBP een bijdrage geleverd aan de ontwikkeling van formele normen voor gegevensbescherming binnen de zorg. Het NNI/NEN heeft in opdracht van het Ministerie van VWS gewerkt aan de ontwikkeling van een normenset, afgeleid van de internationale ISO norm 17799, de Code voor Informatiebeveiliging.

Ook via voordrachten en door deelname aan sectorale beurzen heeft het CBP in de sector informatiebeveiliging het *Privacy by design-concept* verder post doen vatten. Op een grote sectorbeurs heeft het CBP zelfs een miniseminar kunnen organiseren dat veel belangstellenden trok. Nimmer heeft het CBP op een beurs zo veel informatiemateriaal verstrekt. Ook voor de studie *Beveiliging van persoonsgegevens (2000)* is grote en voortdurende belangstelling gebleken.

PISA

De afronding van het project PISA in 2003 was voor het CBP een doorbraak en een afsluiting. Het was een afsluiting omdat het CBP, zoals in 2002 al werd aangekondigd, in de toekomst niet meer zo nadrukkelijk mede eindverantwoordelijk kan zijn voor dergelijke projecten. De toezichthoudende taak staat dat in de weg. PISA was ook de afronding van een project dat een technisch *proof of concept* moest leveren waarmee kon worden aangetoond dat abstracte en open normen uit de privacywet- en regelgeving technisch vertaald konden worden in werkende producten, die rechtmatig handelen afdwingen.

In 2003 leverde het CBP inhoudelijke bijdragen aan het definitieve PISA-handboek; daarnaast droeg het bij aan de redactie van het boek en aan de publicatie en de beschikbaarstelling hiervan ervan. In 2004 wordt het afgeronde project op instructie van de Europese Commissie door het CBP nog onderworpen aan een privacy audit.

Het volgen en beoordelen van technologie blijft in de visie van het CBP wel een integraal onderdeel van zijn taak, ook met het oog op voorlichting, advisering en de onderzoeken in het kader van de handhaving. Het CBP is in 2003 door verschillende internationale projecten gevraagd om een adviesrol te vervullen; voor enkele projecten heeft het CBP dit verzoek geaccepteerd. De Europese toezichthouders zullen naar verwacht hun krachten bundelen bij het aanpakken van vraagstukken van technologie en privacy.

Certificering

Tijdens het congres van NOREA, ISACA en VERA op 12 en 13 november 2003 kon bekend worden gemaakt dat het CBP samen met een aantal beroepsorganisaties een systeem heeft ontwikkeld voor de auditing van verwerkingen van persoonsgegevens, waarbij het voldoen aan wet- en regelgeving resulteert in de afgifte van een goedkeurende verklaring en certificaat. Een 'privacycertificaat' zal worden toegekend aan een specifieke, rechtmatige verwerking van persoonsgegevens door een organisatie.

Het CBP zal in eerste instantie een tweetal accreditatie-instellingen benoemen, te weten NOREA en NIVRA. Deze instellingen zijn bevoegd tot het accrediteren van auditors. Deze privacy-auditors zijn onderzoekers die verwerkingen van persoonsgegevens in organisaties zullen toetsen aan de geldende wet- en regelgeving. Wanneer een privacy-auditor tot een positief oordeel komt, mag deze de onderzochte verwerking voorzien van een certificaat. Het certificaat is dus niet voor de organisatie in haar geheel. Het certificaat verklaart dat de verwerking is getoetst aan het door het CBP erkende normenkader, maar is geen bewijs van goedkeuring door het CBP. Burgers en betrokkenen kunnen er het vertrouwen aan ontlenen dat persoonsgegevens rechtmatig verwerkt worden. Afronding in 2004.

Van audit naar onderzoek

De verschuiving van het accent binnen de taakopvatting van het CBP van bewustwording en normontwikkeling naar meer daadwerkelijk handhaving van de normen vraagt om de verdere professionele ontwikkeling van de onderzoekscapaciteit. In 2003 is daar een begin mee gemaakt en met ingang van 2004 is dit ook formeel in een onderzoeksafdeling ondergebracht. Voorheen is de auditing-expertise van het CBP vooral in een adviserende rol ingezet, onder meer bij de ontwikkeling van het PET-concept en bij de ontwikkeling van de auditinstrumenten die de Registratiekamer en aansluitend het CBP in een samenwerkingsverband met koepelorganisaties van auditors en marktpartijen heeft ontwikkeld. De *Quickscan*, de *WBP-Zelfevaluatie* en het *Raamwerk Privacy Audit* zijn nog steeds veelgevraagde producten, omdat organisaties zelf ermee kunnen nagaan hoe het met de bescherming van persoonsgegevens in hun organisatie is gesteld.

De auditing-capaciteit van het CBP is versterkt en begin 2004 formeel ondergebracht in een onderzoeksafdeling. De afdeling zal analyses maken van de risico's als gevolg van het niet naleven van privacyregels. Verder zullen verschillende typen onderzoek ontwikkeld worden: periodieke controles op de naleving van de meldingsverplichting, brede onderzoeken rond privacythema's, sectoranalyses en onderzoeken bij verantwoordelijken. De resultaten van de diverse onderzoeken zullen bijdragen aan de beleidsvorming en aan de handhaving.

In 2003 werden al enkele onderzoeken met dit oogmerk opgezet. De naleving van de meldingsplicht is geanalyseerd. De analyse werd gevolgd door systematisch onderzoek in de sectoren gemeentes, arbo-diensten, zorgverzekeraars en direct marketing-organisaties. In een aantal gevallen werd vervolgens onderzoek bij de verantwoordelijke gedaan. In 2003 is ook een extern bureau in de arm genomen voor een pilot-onderzoek naar de naleving van de informatieverplichting in de private sector ■

Internationaal

De door Amerikaanse en andere overheden verplicht gestelde verstrekking van passagiersgegevens door luchtvaartmaatschappijen ten behoeve van terrorisme-bestrijding en nationale veiligheid was de belangrijkste internationale privacy-kwestie van 2003.

Multinationale bedrijven toonden interesse voor het initiatief om te komen tot een effectiever regime voor internationale doorgiften van gegevens in de private sector; het gaat om het concept van gedragscodes voor bedrijven, de Binding Corporate Rules.

De Europese Privacyrichtlijn is in 2003 geëvalueerd. De voornaamste doelen van de richtlijn – vrij verkeer van persoonsgegevens én privacybescherming – zijn bereikt. Er is geen noodzaak de Privacyrichtlijn aan te passen. Wel zijn een meer geharmoniseerde toepassing ervan en afstemming door de toezichthouders gewenst.

Passagiersgegevens

In het kader van de bestrijding van terrorisme en het nationale veiligheidsbeleid verplichten de Verenigde Staten en andere overheden vliegtuigmaatschappijen passagiersgegevens te verstrekken vanuit hun reserveringssystemen. In 2003 heeft de Europese Commissie hierover intensief overleg gevoerd met de Amerikaanse autoriteiten. De Artikel 29-werkgroep, het op artikel 29 Richtlijn 95/46/EG gebaseerde onafhankelijke overleg- en adviesorgaan van Europese nationale toezichthouders, heeft gedurende deze onderhandelingen meerdere malen advies uitgebracht aan de Europese Commissie. Hierbij is geconcludeerd dat ondanks de geboekte vooruitgang in de onderhandelingen de voorgestelde regeling nog onvoldoende in lijn is met de Europese regelgeving. Over het beschermingsniveau voor passagiersgegevens in Australië heeft de werkgroep daarentegen wel positief geoordeeld.

Binding Corporate Rules

De Artikel 29-werkgroep heeft zich ingespannen om het regime voor internationaal gegevensverkeer binnen multinationals te vereenvoudigen. In juni 2003 heeft zij een document aangenomen dat internationale uitwisseling van persoonsgegevens binnen multinationals mogelijk maakt op basis van zogenaamde *Binding Corporate Rules,* interne gedragscodes van multinationals die bindend zijn voor het hele concern.

Nadat het CBP in de zomer een druk bezochte algemene expertmeeting had georganiseerd over internationale doorgiften, heeft het in het najaar een serie workshops gehouden met een groep Nederlandse multinationals om *Binding Corporate Rules* te ontwikkelen. Hierbij is onder andere een modelgedragscode ontwikkeld. Het CBP streeft ernaar dit proces in samenwerking met andere Europese privacytoezichthouders in 2004 af te ronden met het verlenen van de eerste vergunningen op grond van deze interne gedragscodes.

Europese Unie

In mei 2003 presenteerde de Europese Commissie haar evaluatierapport over de implementatie van de Privacyrichtlijn. Zij komt hierin tot de conclusie dat de richtlijn haar hoofddoel heeft bereikt, namelijk de opheffing van belemmeringen voor het vrije verkeer van persoonsgegevens tussen de lidstaten. Ook is het andere doel, het waarborgen van een hoog beschermingsniveau, verzekerd. Zij signaleert wel knelpunten, zoals het gebrek aan middelen voor rechtshandhaving en verschillen tussen de wetgeving van lidstaten, maar volgens de Commissie kunnen deze worden aangepakt zonder wijziging van de richtlijn. Hiertoe is een werkprogramma opgesteld waaraan de Artikel 29-werkgroep een actieve bijdrage levert. Zo onderzoekt zij onder andere mogelijkheden tot vereenvoudiging van de melding.

De Artikel 29-werkgroep heeft de eerste gedragscode onder de Europese Privacyrichtlijn goedgekeurd. Het gaat om de gedragscode van de Europese direct marketing brancheorganisatie van de Federation of European Direct Marketing (FEDMA), die verplichtingen schept voor alle bij FEDMA aangesloten organisaties, waaronder de Dutch Dialogue Marketing Association.

In 2002 is de nieuwe Richtlijn 2002/58/EG over privacy en elektronische communicatie tot stand gekomen. Deze richtlijn verbiedt het zenden van commerciële elektronische boodschappen zonder voorafgaande toestemming van de abonnee (“spamverbod”). De Artikel 29-werkgroep heeft in 2003 hierover een opinie opgesteld. Het CBP heeft bijgedragen aan overleg in zowel Europees verband als in het kader van de Organisatie voor Economische Samenwerking en Ontwikkeling om te komen tot internationale samenwerking bij de bestrijding van spam.

De eerste twee arresten van het Europese Hof van Justitie, ‘Österreichischer Rundfunk’ en ‘Lindqvist’, hebben de ruime werkingssfeer van de Europese privacyrichtlijn bevestigd. Tevens is door het Hof benadrukt dat deze richtlijn moet worden uitgelegd op basis van artikel 8 van het Europees Verdrag voor de rechten van de mens.

Schengen en Europol

Het CBP is met andere nationale toezichthouders vertegenwoordigd in gemeenschappelijke controleautoriteiten die toezien op de gegevensverwerking in Europese informatiesystemen. Het gaat om de Gemeenschappelijke Controleautoriteit (GCA) Schengen, het Gemeenschappelijke Controleorgaan (GCO) van Europol en de Gemeenschappelijke Controleautoriteit voor het Douane Informatiesysteem.

De GCA Schengen heeft tot taak toezicht te houden op het Schengen Informatie Systeem (SIS) en inspecteerde in dat kader het centrale informatiesysteem in Frankrijk. De bevindingen waren over het algemeen positief. Ook initieerde de GCA een gecoördineerd onderzoek door de nationale toezichthoudende autoriteiten naar de signalering van vreemdelingen in het SIS en werd een oordeel gegeven over de te hanteren bewaartermijnen voor persoonsgegevens in het SIS. Daarnaast werd advies uitgebracht over een tweede generatie SIS. In verband met de uitbreiding van de Europese Unie tot 25 lidstaten is een vernieuwing van het SIS noodzakelijk. Mogelijk worden meer soorten gegevens in het SIS opgenomen en zullen deze breder gebruikt worden.

Het GCO van Europol houdt toezicht op de gegevensverwerkingen bij Europol. Het CBP heeft deelgenomen aan de jaarlijkse controles bij Europol, waarbij de gegevensverwerkingen en de beveiliging daarvan worden geïnspecteerd. Het Comité van beroep van het GCO deed in september 2003 uitspraak in een geschil van een burger met Europol over inzage in de van hem verwerkte gegevens.

Het GCO heeft onder meer adviezen uitgebracht over de voorgenomen wijziging van de Europol-overeenkomst en ontwerp-overeenkomsten betreffende de uitwisseling van gegevens met derde landen. Na advies van het GCO is in februari 2003 een overeenkomst voor gegevensuitwisseling tussen Europol en de Verenigde Staten ondertekend. In voorbereiding op de uitbreiding van de EU met 10 nieuwe lidstaten zijn de vertegenwoordigers van die staten geïntroduceerd bij het GCO en Europol.

Samenwerking met andere toezichthouders

Samenwerking en informatie-uitwisseling vindt ook plaats tijdens de halfjaarlijkse workshops voor medewerkers van Europese toezichthouders, de *Complaints Workshop*. In deze op de dagelijkse praktijk van toezichthouders gerichte workshop heeft het CBP onder andere zijn ervaringen gedeeld betreffende handhaving. Het bijbehorende

besloten internetplatform biedt het CBP de mogelijkheid tot snelle en effectieve informatie-uitwisseling en samenwerking bij grensoverschrijdende zaken, en het geven van advies aan onder andere de vele nieuwe Europese collega's.

Tijdens de jaarlijkse Voorjaarsconferentie van Europese toezichthouders heeft het CBP de resultaten gepresenteerd van de in het kader van de *Complaints Workshop* gemaakte inventarisatie van het doorgiftebeleid van de deelnemende landen. Aan deze conferentie neemt een groeiend aantal Europese landen en toezichthoudende instanties deel. Het CBP heeft in 2003 tevens voorbereidingen getroffen voor de organisatie van de Voorjaarsconferentie van 2004, die in Nederland zal plaatsvinden.

De 25e Wereldconferentie in september 2003 in Sydney stond in het teken van privacy in de praktijk, voor burgers, overheid, en bedrijfsleven. De Australische toezichthouder benadrukte dat wereldwijd een cultuur moet worden gecreëerd waarin het respect voor privacy verankerd is, ook als het gaat om de bestrijding van terrorisme en criminaliteit. Een door de toezichthouders aangenomen resolutie pleit voor een internationaal verdrag dat voldoende waarborgen biedt voor de doorgifte van passagiersgegevens. Ook is in een resolutie het belang van compacte, heldere en uniforme informatievoorziening over de verwerking van persoonsgegevens aan betrokkenen benadrukt. Tevens presenteerde een aantal multinationals hoe privacy als 'succesfactor' was geïntegreerd in de bedrijfscultuur ■

Organisatie

Door de invoering van de WBP met nieuwe taken, bevoegdheden en gevolgen in het kader van de rechtsbescherming, is het CBP als organisatie sterk in verandering. Uitspraken van het CBP hebben grotere rechtsgevolgen voor verantwoordelijken en betrokkenen, waardoor de eisen ten aanzien van de juridische kwaliteit zijn aangescherpt.

Het CBP heeft in vervolg op het door KPMG Consulting uitgebrachte rapport 'Organisatie Viersporenbeleid' van 14 juni 2002 in de afgelopen periode gewerkt aan de inrichting van de nieuwe werkprocessen en de uitwerking van de organisatiestructuur. Inmiddels is het CBP gegroeid van 50 fte (in 2001) naar inmiddels 62 fte op 1 januari 2004. De beoogde afdeling Interventie, bezwaar en beroep is geïmplementeerd en sinds 1 januari 2004 is ook de afdeling Onderzoek van start gegaan. Het CBP zet hiermee in op een snelle, verdere professionalisering in het licht van de handhaving.

Voorheen waren medewerkers van de beleidsafdeling belast met alle taken, van wetgevingsadvies, verzoeken om voorlichting, bemiddeling, klachtbehandeling tot ambtshalve onderzoek binnen hun eigen beleidsterrein. Professionalisering van het onderzoek, zoals het uitvoeren van risicoanalyses, sectorgericht onderzoek en preventief en repressief gericht onderzoek bij verantwoordelijken, vraagt specifieke competenties. De afdeling onderzoek zal zich daarin specialiseren.

Een organisatie in verandering, waar vrijwel dagelijks de afweging moet worden gemaakt wat wel en wat niet wordt aangepakt, is vaak een uitdaging voor professionals, maar kan ook stress tot gevolg hebben. Het HRM-beleid is daarmee een kritische succesfactor: de kwaliteit van het CBP is immers in hoge mate afhankelijk van de kwaliteit van het personeel.

Formatieplan 2003

Het formatieplan 2003 'In beweging voor toezicht en handhaving' is na raadpleging van de ondernemingsraad vastgesteld. De functieprofielen zijn in 2003 voor een deel aangepast aan de nieuwe organisatie. In 2004 wordt verder gewerkt aan de actualisering van de overige functieprofielen.

De personele ontwikkeling en de uitbreiding met fte's is omwille van een zorgvuldige opbouw en aanpassing van de organisatie iets vertraagd. In 2003 is derhalve niet volledig gebruik gemaakt van de beschikbare financiële ruimte.

	2001		2002		2003	
	m	v	m	v	m	v
In dienst	5	8	6	9	5	6
Uit dienst	6	6	5	2	2	0
Bezetting einde jaar m / v	22	30	23	37	26	43
Bezetting einde jaar totaal	52		60		69	
Mobiliteit	23%		13%		13%	
In tijdelijke dienst	9		11		11	
Fulltime in dienst	43		49		41	
Gemiddelde bezetting (fte's)	49,6		49,6		58,9	
Bezetting einde jaar totaal (fte's)	50,7		54,3		61,6*	

FORMATIE 2001–2003

*Per 1 januari 2004 is het aantal fte's 62,6

	2001	2002	2003
	Fte's	Fte's	Fte's
Uitzendkrachten	00,49	1,25	0,6
Stagiaires	0,76	0,75	0,8

OVERZICHT MEDEWERKERS BUITEN FORMATIE 2001-2003

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.

Werkbelevingsonderzoek

De resultaten van het werkbelevingsonderzoek zijn in 2003 met het management, de ondernemingsraad en de medewerkers besproken. Als vervolg op het onderzoek is het plan van aanpak door de arbodienst getoetst en – na overleg met de ondernemingsraad – vastgesteld en in uitvoering genomen.

	2001	2002	2003
Totaal ziekteverzuim excl. zwangerschap	6,97%	6,27%	6,35%
Waarvan langdurig verzuim	3,78%	0	2,74%
Ouderschapsverlof	2	3	3
Verlof zwangerschap/bevalling	2	0	2
Kinderopvangplaatsen	2	4	4
Opleiding (euro's x 1000)	56	99	84
Opleiding in % t.o.v. personele budget	2,05 %	3,47%	2,53%

ZIEKTEVERZUIM EN OVERIGE PERSONELE INFORMATIE 2001–2003

Het ziekteverzuim is in 2003 iets toegenomen. Deze stijging is vooral toe te schrijven aan langdurig ziekteverzuim en was niet werkgerelateerd. In het Sociaal-Medisch-Team wordt periodiek afgestemd met de bedrijfsarts en de personeelsfunctionaris en zonodig gezocht naar passende oplossingen. Een aandachtspunt blijft de werkdrukbeleving van met name de professionals. Vanwege de grote mate van betrokkenheid bij de verschillende aandachtsgebieden en de noodzakelijke selectiviteit in de aanpak zal er aandacht moeten blijven voor het hanteerbaar houden van de werkdruk.

Bedrijfsvoering

Het CBP kan – gelet op de beperkte capaciteit – niet altijd voldoen aan de verwachtingen van de individuele verantwoordelijke of burger. Het CBP krijgt als gevolg daarvan ook steeds meer te maken met verzoeken om heroverweging, bezwaar- en beroepszaken. Het jaar 2003 kenmerkte zich dan ook als een jaar waarin het CBP de gekozen tweede-lijnsstrategie met een belangrijke plaats voor zelfregulering waar moest maken. Deze strategie is in het besturingsmodel van het CBP verankerd en wordt jaarlijks getoetst en geconcretiseerd in een voortschrijdend vijfjarenplan. Op basis van strategische verkenningen en de analyse van beschikbare informatie worden aan de hand van criteria prioriteiten vastgesteld en keuzes gemaakt voor de wijze waarop binnen een bepaalde sector de naleving van de WBP het meest effectief kan worden bevorderd.

Communicatie is een wezenlijke factor in de gehele cyclus van bewustwording naar normontwikkeling – ook in technisch opzicht – en handhaving. Een goed gerichte en weloverwogen informatievoorziening vergroot de effectiviteit van het toezicht door het CBP. Het CBP ziet communicatie als 'multiplier' voor de inspanningen van de organisatie.

Productie

De taken en bevoegdheden van het CBP leiden tot vraaggestuurde productie en daarnaast zelf geïnitieerde ambtshalve onderzoeken. De WBP heeft nieuwe taken aan het CBP opgedragen, met name in de sfeer van toezicht en handhaving. In 2003 heeft zich dat geuit in een sterke toename van het aantal voorafgaande onderzoeken en de ambtshalve onderzoeken. Het betreft hier onder meer 50 onderzoeken naar de meldingsplicht. Het CBP is steeds op zoek naar een balans in de verschillende taken. Het CBP is derhalve selectief bij het in behandeling nemen van individuele verzoeken om bemiddeling of klachtbehandeling. Vooral de vraag naar voorlichting neemt steeds toe. Het CBP gaat hier noodzakelijkerwijs selectiever mee om dan in het verleden. Getracht wordt vooral via de ontwikkeling van de website aan deze vraag tegemoet te komen.

	2000	2001	2002	2003
Wetgevingsadviezen	35	43	26	25
Gedragscodes	6	1	5	3
Reglement WPR (tot 1 sept 2001) en WpolR*	88	50	40	30
WBP-meldingen vanaf 1 sept 2001**	n.v.t.	591	7.863	13.083
Voorafgaand onderzoek	n.v.t.	12	190	257
Voorlichtingsverzoeken	910	1.204	686	725
Internationale zaken	10	13	33	46
Bijzondere gegevens	n.v.t.	0	0	1
Gegevensverkeer derde landen	n.v.t.	0	10	12
Bemiddeling en klachten	323	290	282	316
Ambtshalve onderzoek	17	24	11	73
Boete	n.v.t.	n.v.t.	0	1
Dwangsom	n.v.t.	n.v.t	0	1
Bestuursdwang	n.v.t.	n.v.t.	1	1
Beroep	n.v.t.	n.v.t.	1	2
Bezwaar	n.v.t.	0	4	2
Wet openbaarheid bestuur	0	0	19	0
Publieksvoorlichting (telefonisch spreekuur)	4.277	4.979	5.715	5.330
Vragen WBP-melding (telefonisch spreekuur)	n.v.t	0	2.500	2.070
Publieksvoorlichting (via e-mail)	n.v.t.	291	1.890	2.045
Klachten over het CBP	0	0	9	5

OVERZICHT VAN DE PRODUCTIE 2000 - 2003

* Door de invoering van modelreglementen, zal de toetsing van reglementen structureel verminderen, waardoor de uitvoeringslast voor de politieorganisaties afneemt.
** In de afgelopen jaren is er sprake van een opbouwfase met vooral nieuwe meldingen en een te verwaarlozen aantal wijzigingen en verwijderingen.

Melding van verwerkingen bij het CBP

Met de invoering van de WBP zijn verantwoordelijken verplicht bij verwerkingen van persoonsgegevens de WBP te implementeren. Verwerkingen van persoonsgegevens, voor zover deze niet zijn vrijgesteld van de meldingsverplichting dienen te worden gemeld bij het CBP. Voor het voldoen aan deze meldingsverplichting heeft het CBP drie mogelijkheden ontwikkeld, waardoor organisaties en bedrijven kunnen kiezen welke vorm het beste past bij de eigen bedrijfsvoering. Deze mogelijkheden zijn opgenomen in het Meldingsbesluit WBP (Stb. 2001,244).
De WBP biedt de verantwoordelijke ook de mogelijkheid om een eigen functio-

	2002	2003
Meldingen WBP in openbaar register	8.454	21.537
Functionarissen voor de gegevensbescherming	97	148
Aanpassingen GBA	208	350

MELDINGEN

Wijze van melden	2002	2003
Meldingsformulier	20%	23%
Meldingsprogramma op diskette	47%	30%
Elektronisch Meldingsprogramma via internet/email	33%	47%

MELDINGSBESLUIT WBP

naris voor de gegevensbescherming aan te stellen. In dat geval is er geen meldingsverplichting bij het CBP. Gemeenten dienen op grond van de WGBA expliciet aan te geven dat zij de gemeentelijke basisadministratie in overeenstemming hebben gebracht met de WBP.

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 hem ingediende schriftelijke klachten. Bijgevoegd overzicht geeft het aantal ingediende schriftelijke klachten weer met de wijze van afdoening.

Totaal aantal klachten in 2003	5
Klachten ongegrond verklaard	2
Klachten gegrond verklaard	2
Minnelijke regeling/geen oordeel/ingetrokken/andere wijze van afdoening/nog in behandeling	1

KLACHTEN OVER HET CBP 2003

GEEN VAN DE KLACHTEN HEEFT GELEID TOT EEN VERVOLGKLACHT BIJ DE NATIONALE OMBUDSMAN.

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.

Totaal aantal heroverwegingen in 2003	20
Klachten ongegrond verklaard	14
Klachten gegrond verklaard	6
Minnelijke regeling/geen oordeel/ingetrokken/andere wijze van afdoening/nog in behandeling	-

HEROVERWEGINGEN

Project certificering

Het project Certificering is het kopstuk op een langlopend traject waarbij het CBP streeft naar gestructureerde zelfregulering door het bieden van een uniform toetsingskader. Het CBP hecht sterk aan zelfregulering. Dit is een uitgangspunt van de WBP en leidt tot een betere verankering van het rechtsgoed. Door het benadrukken van de eigen verantwoordelijkheid bij overheid en bedrijfsleven vermindert voorts de druk op de toezichthouder. Bij het project wordt gestreefd naar een auditmethodiek waardoor het CBP zich op termijn kan beperken tot het metatoezicht op die auditmethodiek en handhavend toezicht houdt op grove schendingen van de WBP.

De verwachting is dat in de eerste helft van 2004 overeenstemming is bereikt over het proces van accreditatie en certificering. Met de oprichting van een onafhankelijke stichting en een Raad van Deskundigen zullen verantwoordelijken, als bedoeld in artikel 1 onder d van de WBP, de mogelijkheid worden geboden hun verwerkingen van persoonsgegevens te laten certificeren. Het CBP zal zitting nemen in de Raad van Deskundigen.

Profilering en samenwerking

In het huidige politieke en maatschappelijke klimaat staat de bescherming van de persoonlijke levenssfeer onder druk door de vraag naar veiligheid en naar daadkrachtige probleemoplossing door de overheid. Proactieve publiciteit en openbaarmaking rond het beleid, de taken, de onderzoeken en de standpunten van het CBP is in dat klimaat belangrijker dan ooit. Het CBP streeft daarom naar een effectieve profilering van het toezicht en naar samenwerking bij de voorlichting over privacykwesties met andere partijen, zoals brancheorganisaties, geschillencommissies en andere toezichthouders.

In 2003 zijn op dit gebied een aantal resultaten geboekt. Er is wat meer balans in de berichtgeving over privacy gebracht door het actief zoeken van de publiciteit en een intensivering van de berichtgeving over de activiteiten en standpunten van het CBP. Er is een inventarisatie gemaakt van organisaties in de eerste lijn en inmiddels zijn met een aantal van deze organisaties afspraken gemaakt over samenwerking bij het geven van voorlichting.

Gebruik website	2003
Gemiddeld aantal bezoekers per maand	39.270
Aantal abonnees elektronische nieuwsbrief per 31 december 2003	2.600
Aantal downloads van Achtergrondstudies en verkenningen	50.864
Aantal downloads van Auditinstrumenten (Raamwerk privacy audit, zelfevaluatie, quickscan)	51.660
Aantal downloads WBP-meldingsprogramma	11.214

WEBSITE

De website is in 2003 uitgebreid met materiaal terwijl de website in 2004 een nieuwe structuur en vormgeving zal krijgen. De website zal meer vraaggericht worden ingericht, ook met het oog op een vermindering van de voorlichtingslast voor het CBP. Op termijn zal ernaar gestreefd worden de website ook een grotere rol te geven in de ondersteuning van het primaire proces.

Openbaarmaking en publiciteit zijn onderdeel van het optreden van de toezichthouder; in 2003 is daarom geïnvesteerd in de procedurele en inhoudelijke kwaliteitsborging van externe communicatie en voorlichting.

Het CBP heeft vrijwel dagelijks contact met landelijke media. Sinds juni 2003 wordt het aantal perscontacten bijgehouden.

Ontwikkeling en herinrichting van de website

Medium	vanaf juni 2003
Algemeen Nederlands Persbureau	8
Landelijke dagbladen	34
Landelijke radio en televisie (journaal, actualiteitenrubrieken en consumentenprogramma's)	76
Relevante vakbladen	18
Gemeenschappelijke Pers Diensten	9

PERSCONTACTEN

De website is voor het CBP een belangrijk medium om als toezichthouder naar buiten te treden. In 2003 is het CBP begonnen met het monitoren van het gebruik. Sinds begin 2003 brengt het CBP elke 2 à 3 weken ook een nieuwsbrief per e-mail uit.

Informatiebeveiliging

In 2003 is door een extern onderzoeksbureau een audit uitgevoerd naar de opzet en het bestaan van de maatregelen en procedures ter waarborging van de exclusiviteit, integriteit, controleerbaarheid en continuïteit bij het CBP. Daarbij is vastgesteld dat het niveau van de informatiebeveiliging voor een groot deel voldoende beantwoordt aan de normen, met uitzondering van enkele, niet-materiële, onderdelen.

Naar aanleiding van bovenbedoelde bevindingen is in het najaar van 2003 een plan van aanpak opgesteld op grond waarvan in 2004 kan worden gezorgd dat het CBP volledig zal voldoen aan de eisen die in het VIR aan informatiebeveiliging worden gesteld.

Archivering

In 2003 zijn in het kader van het Project Invoering Verkorting Overbrengingstermijn (PIVOT) maatregelen genomen om de archivering in overeenstemming te brengen met de eisen die worden gesteld overeenkomstig de wettelijke bepalingen (Archiefwet 1995). Met medewerking van een extern bureau is een institutioneel onderzoek uitgevoerd, en zijn basisselectiecriteria en een ordeningsplan vastgesteld. De archieven worden thans overeenkomstig deze documenten ingericht. Voorts is het onderzoek, inclusief de bijbehorende documenten, aangeboden aan het Nationaal Archief, ter voorbereiding op de goedkeuringsprocedure door de Minister van OCW.

Automatisering

In 2003 is een nieuw netwerkbesturingssysteem geïmplementeerd en zijn de werkplekken voorzien van nieuwe software. Voor de behandeling van verzoeken per e-mail is een voor het ministerie van Justitie ontwikkeld pakket geïmplementeerd en verder ontwikkeld, waarmee de afhandeling van informatievragen wordt gestructureerd en gearchiveerd. Voor de interne informatievoorziening is een intranet ontwikkeld en geïmplementeerd.

Financieel

In 2002 heeft het CBP een organisatieontwikkeling ingezet om invulling te geven aan de nieuwe taken en (sanctionerende) bevoegdheden de daarmee samenhangende noodzakelijke waarborgen. 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 per 2003 structureel te verhogen met 1.2 miljoen euro (ten opzichte van 2001).

In 2001 en 2002 is geïnvesteerd in geautomatiseerde gegevensverwerking van de WBP- meldingen en het via internet te raadplegen openbaar register.

2003	2004	2005	2006	2007
5,014	4.950	4.968	4.941	4.866

BEGROTING (STAND PER 12 DECEMBER 2003, BEDRAGEN X 1000)

	2001	2002	2003
Personeel	2.693,6	2.853,4	3.319,9
Materieel*	1.225,8	1.762,1	1.255,8
Totaal	3.919,4	4.615,5	4.575,7

BUDGETUITGAVEN 2001 - 2003 (BEDRAGEN X 1000 EURO)

* De huurlasten zijn hierin niet opgenomen; het ministerie van Justitie stelt de huisvesting beschikbaar.

In 2003 zijn de materiële uitgaven beperkt tot de noodzakelijke kosten voor onderhoud en beheer. Het CBP heeft in 2003 niet volledig gebruik kunnen maken van de beschikbare middelen. De organisatie had de tijd nodig om de ontwikkelingen te implementeren. Inmiddels is per 1 januari 2004 met de start van de afdeling onderzoek de beoogde organisatiestructuur gerealiseerd. In 2004 zal de omvang van de afdelingen op sterkte worden gebracht.

Bezoldiging collegeleden

Bij Besluit rechtspositie leden College bescherming persoonsgegevens (Stb.2001,382) is de bezoldiging van de voorzitter van het College vastgesteld op het maximum van salarisschaal 18 van bijlage B van het Bezoldigingsbesluit Burgerlijke Rijksambtenaren 1984. Voor de overige leden geldt het maximum van schaal 17.

	Uitgaven (x 1.000 euro)
Personele kosten primair proces	2.404,0
Overhead (management, ondersteuning, bedrijfsvoering)	637,2
Extern ingehuurde expertise (onderzoek, certificering, archivering, beveiligingsaudit	278,7

PERSONELE KOSTEN

Personele kosten

De personele kosten zijn te verdelen in kosten voor het primaire proces, voor organisatieontwikkeling en voor de bedrijfsvoering. Voor een deel van de bedrijfsvoeringstaken (PIOFAH) maakt het CBP gebruik van de stafdienst van het Paleis van Justitie. Dit betreffen de P&O-taken, financiële administratie en facilitaire ondersteuning. Deze dienstverleningsovereenkomst is onderdeel van de materiële uitgaven.

Sectoren	Uitgaven (x 1000 euro)
Politie en Justitie	549
Arbeid & Sociale Zekerheid	342
Zorg & Welzijn	317
Openbaar bestuur	452
Telecommunicatie	333
Handel & Diensten	299
Internationale activiteiten	
Internationaal	113
Audits voor gemeenschappelijke controle-autoriteiten	20
Project PISA	90
Beleidsterrein technologie en onderzoek	
Technologie en Onderzoek	517
Project certificering	75
Beheer van meldingen en openbaar register	
Bestandsbeheer	376
Communicatie	
Communicatie	413
Frontoffice voor de sectoren	327
Interventie, bezwaar en beroep	
Sancties en Rechtsbescherming	353

KOSTEN PER BELEIDSTERREIN/SECTOR

Uitgaven per beleidsterrein /sector

De keuzes voor inzet van de personele kosten zijn gemaakt op basis van het beleidsplan en de daarbij vastgestelde doelstellingen voor het jaar 2003. De tabel kosten per beleidsterrein/sector biedt inzicht in hoe het CBP zijn inspanningen heeft verdeeld over de verschillende aandachtsgebieden.

Uitgaven internationale samenwerking

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

In het kader van de Raad van Europa neemt het CBP deel aan de werkzaamheden van de Adviescommissie (T-PD), bedoeld in artikel 18 van het Dataverdrag van Straatsburg, waarin ook niet-EU-lidstaten zijn vertegenwoordigd.

Het CBP neemt verder deel aan de jaarlijkse Internationale en Europese Conferenties van privacytoezichthouders en aan de werkzaamheden van diverse subgroepen, zoals de internationale werkgroep telecom en media (Berlijn Telecom groep), de Europese werkgroep Politie en de Europese Complaints

Internationaal overleg	2002	2003
Artikel 29-werkgroep (Richtlijn 95/46/EG)	67	55
Adviescommissie T-PD (artikel 18, Dataverdrag van Straatsburg	16	3
Berlijn-werkgroep	13	3
Europese Complaints workshop	3	33
Europese en mondiale Conferenties van privacytoezichthouders	27	97
Overig	53	50

OVERZICHT AANTAL REIS- EN VERGADERDAGEN INTERNATIONAAL OVERLEG*

* voorbereidingstijd en inhoudelijke inbreng is hier niet inbegrepen.

workshops, waarin de Europese toezichthouders in concrete kwesties zoeken naar best practices en onderlinge afstemming. In 2004 zal het CBP optreden als gastheer voor de jaarlijkse conferentie van Europese privacytoezichthouders.

Het Europese ontwikkelingsproject PISA (Privacy Incorporated Software Agents), dat in 2001 onder aansturing van TNO en het CBP gestart is, is in 2003 formeel afgesloten. Het project werd financieel gesteund door de Europese Unie (5de IST Raamwerk). Gedurende het project heeft het CBP in verschillende rollen zichtbare bijdragen geleverd aan de succesvolle afronding, uitmondend in een werkend prototype en het door het CBP uitgegegeven eindrapport. Het CBP heeft voorts, op verzoek van de Europese Commissie, de definitieve audit op het projectresultaat uitgevoerd.

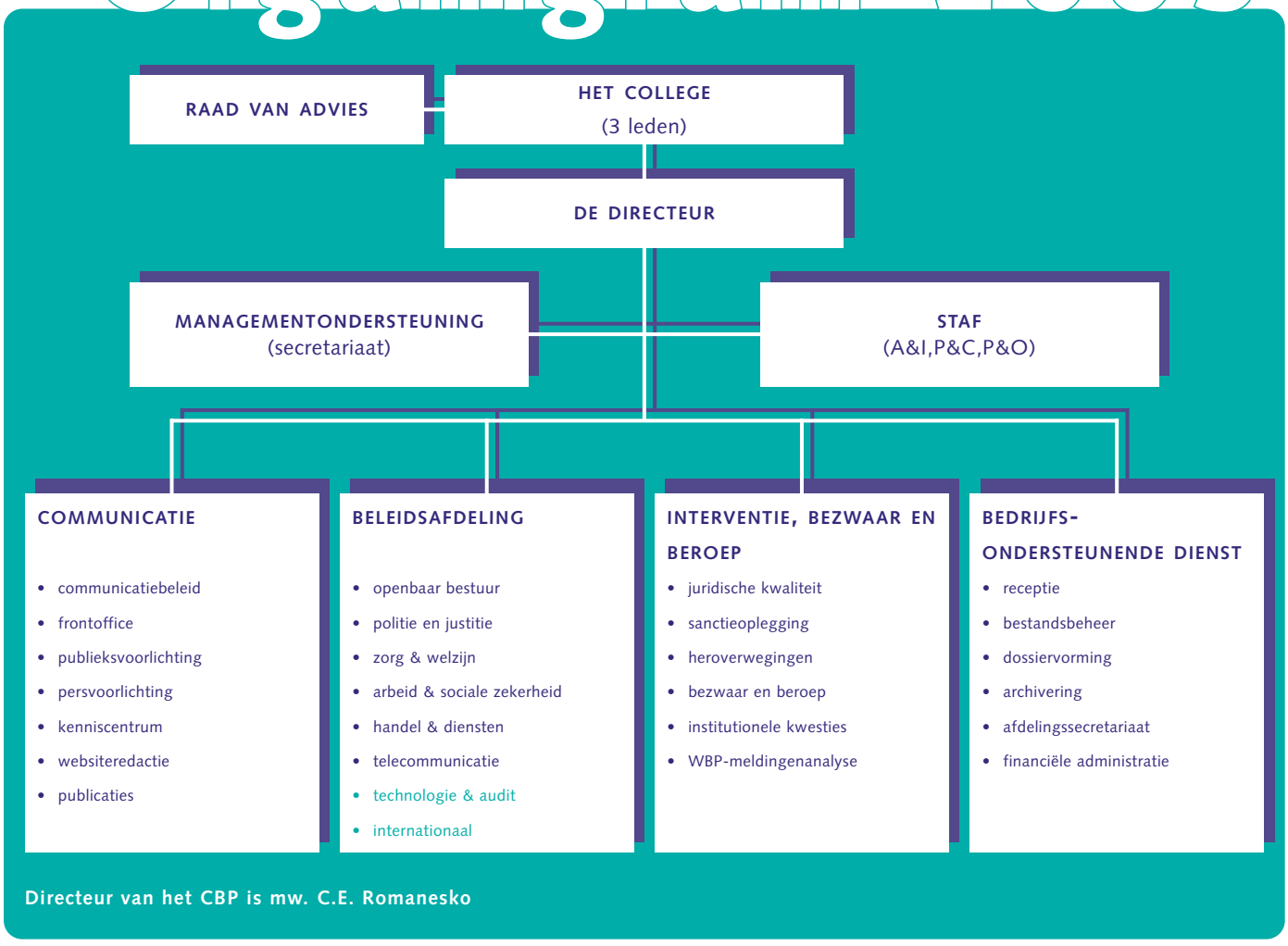
In de derde pijler van de EU maakt het CBP deel uit van de bij verdrag ingestelde gemeenschappelijke controleorganen (GCO) voor Schengen, Europol, Douane, Eurojust, Eurodac en Interpol, die allen beschikken over adviserende en controlerende bevoegdheden. Geschillen over de uitoefening van het recht op inzage en correctie bij Europol worden in hoogste instantie beslist door een Beroepscomité waarin het CBP ook is vertegenwoordigd. In 2004 treedt het CBP op als voorzitter van het GCA voor het Schengen informatiesysteem.

Gemeenschappelijke controleorganen	2002	2003
GCA Schengen	14	21
GCO Europol*	13	30
Beroepscomité		5
GCA Douane		2
GCO Eurojust *		3
GCA Eurodac	1	1
GCO Interpol	6	6

OVERZICHT AANTAL REIS- EN VERGADERDAGEN GCO (AFSTEMMING EN AUDITS)

* organisatie is in Nederland gevestigd.

Organigram 2003



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

bijlagen

wetgevingsadviezen

Besluit gemeentelijke basisadministratie persoonsgegevens
9 januari 2003

Besluit tot wijziging Besluit SUWI
21 januari 2003

Wetsvoorstel uitbreiding identificatieplicht
12 februari 2003

Wetsvoorstel toezicht trustkantoren
3 maart 2003

OM mag historische strafrechtelijke gegevens verstrekken aan samenwerkingsverbanden
3 maart 2003

Besluiten integere bedrijfsvoering financiële sector
27 maart 2003

Eisenbesluit lichaamsmateriaal
1 april 2003

Ministerie van Onderwijs: zijn IQ-gegevens bijzondere gegevens?
22 april 2003

Wetsvoorstel feitelijk arbeidsverleden
8 mei 2003

Besluit afscherming nummers notaspecificatie
28 mei 2003

Onderzoeksmethoden Belastingdienst
25 juni 2003

Aanpassing besluit Politieregisters
1 juli 2003

Instellingsbesluit CIE bij de FIOD-ECD
22 juli 2003

Nevenbetrekkingen van rechterlijke ambtenaren
29 juli 2003

Aanpassing van het Besluit kostenvergoeding rechten betrokkene WBP
25 augustus 2003

Wetsvoorstel fraudebestrijding zorgverzekeringswetten
25 augustus 2003

Wet financieringen sociale verzekeringen
1 september 2003

Besluit wijziging kentekenreglement
23 september 2003

Tijdelijk besluit tegemoetkoming buitengewone uitgaven
7 oktober 2003

Wet Justitiële strafrechtelijke gegevens
13 oktober 2003

Besluit gegevensverwerving CBS
15 oktober 2003

Besluit justitiële gegevens
3 november 2003

Wetsvoorstel toezicht accountantsorganisaties
3 november 2003

Wijziging Besluit Politieregisters
1 december 2003

Wijziging Besluit stralingbescherming
18 december 2003

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

Voor onderstaande is een verklaring van overeenstemming verleend onder de WBP.

Gedragscode Onderzoek & statistiek; geldig tot 24 februari 2009 (Stcrt. 2004, 36)

Gedragscode gerechtsdeurwaarders ter bescherming persoonsgegevens van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG); geldig tot 18 februari 2009 (Stcrt. 2004, 33)

Privacygedragscode sector particuliere onderzoeksbureaus van de Vereniging van Particuliere Beveiligingsorganisaties (VPB); geldig tot 13 januari 2009 (Stcrt. 2004, 7)

Gedragscode inzake het verwerken van persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus (NVH); geldig tot 19 augustus 2008 (Stcrt. 2003, 158)

Gedragscode Verwerking Persoongegevens Financiële Instellingen; geldig tot 4 februari 2008 (Stcrt. 2003, 7)

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).

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)
Tijdelijk register	(Stcrt. 2003, 131)
Vakantiecontrolekaarten	(Stcrt. 2002, 243)
Vandalismebestrijding	(Stcrt. 2002, 243)
Verdovende middelen	(Stcrt. 2002, 243)
Voorlopig register	(Stcrt. 2000, 198)
Zware criminaliteit	(Stcrt. 2000, 198)

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

bijlagen

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

17 December 2003 - **Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business assocations** (Document 11754/03, WP 84)

16 December 2003 - **Sixth 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 2001** (Document 12065/03)

12 December 2003 - **Opinion 7/2003 on the re-use of public sector information and the protection of personal data** (Document 10936/03, WP 83)

21 November 2003 - **Opinion 6/2003 on the level of protection of personal data in the Isle of Man** (Document 11580/03, WP 82)

1 August 2003 - **Working document on biometrics** (Document 10595/03, WP 80)

13 June 2003 - **Opinion 5/2003 on the level of protection of personal data in Guernsey** (Document 10595/03, WP 79)

13 June 2003 - **Level of Protection ensured in the United States for the Transfer of Passengers' Data, Opinion 4/2003 of the Art. 29 Working Party** (Document 11070/03, WP 78)

13 June 2003 - **European code of conduct of FEDMA for the use of personal data in direct marketing, Opinion 3/2003 of the Art. 29 Working Party** (Document 10066/03, WP 77)

13 June 2003 - **Opinion 2/2003 on the application of the data protection principles to the Whois directories** (Document 10972/03, WP 76)

3 June 2003 - **Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers** (Document 11639/03, WP 74)

8 May 2003 - **Working Document on E-Government** (Document 10593/03, WP 73)

29 March 2003 - **Work programme 2003 of the Art. 29 Data Protection Working Party** (Document 12054/03, WP 71)

29 January 2003 - **Opinion 1/2003 on the storage of traffic data for billing purposes** (Document 12054/03, WP 69)

29 January 2003 - **The Article 29 Working Party gives guidance regarding on-line authentication systems, Working Document** (Document 10054/03, WP 68)

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

onderzoeksrapporten 1996 - 2003

2003

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

Cameratoezicht in de openbare ruimte: Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten, november 2003.

KPN informeert abonnees met geheim nummer onvoldoende over direct marketing. Onderzoek naar beleid omtrent 'geheime' nummers; bevindingen, augustus 2003.

Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie, juli 2003.

Onrechtmatig, onbehoorlijk en onzorgvuldig. De verwerking van persoonsgegevens door een handelsinformatiebureau voor rapportage van verhaalsinformatie, april 2003.

1996 - 2002

- **Sociale diensten: bijstandsdossier en privacy,** februari 2002.
- **Privacy bij wetenschappelijk onderzoek en statistiek. Kader voor een gedragscode,** mei 2002.
- **Elektronische overheid en privacy,** december 2001.
- **Onrechtmatige handelswijze van een handelsinformatiebureau,** mei 2001.
- **Zorg voor gegevens bij indicatiestelling,** augustus 2000.
- **Politiegegevens beschermd,** juni 2000.
- **Verstrekken van gegevens door de Belastingdienst voor bijdrage thuiszorg,** april 2000.
- **Screening van politiepersoneel moet volgens de regels,** februari 2000.
- **Controle e-mailverkeer door werkgever,** december 1999.
- **Onderzoek naar handelsinformatiebureau Goderie van Groen,** november 1999.
- **Uitbesteden van taken Algemene bijstandswet,** september 1999.
- **Bijstanddossiers en bescherming persoonsgegevens,** juli 1999.
- **Verstrekken van gegevens door deurwaarders,** juni 1999.
- **Vastleggen en verstrekken van call detail records,** juni 1999.
- **Verzekeringsmaatschappij verplicht Arbo-dienst tot registratie en rapportage gegevens,** juni 1999.
- **Is Landelijk Alcohol en Drugs Informatiesysteem een persoonsregistratie?,** november 1999.
- **Doorzenden voorlichtingsrapport reclassering na toestemming,** december 1998.
- **Medicatiebewaking door centrale patiëntenregistratie,** oktober 1998.
- **Beroepscode psychologen,** juli 1998.
- **Reglementering en beveiliging persoonsregistraties door ministeries,** juli 1998.
- **Gegevens over honden en het verstrekken daarvan,** juli 1998.
- **Gegevens uit controle door de Rijksverkeersinspectie,** juni 1998.
- **Persoonsgebonden clubcard II,** mei 1998.
- **Persoonsgebonden clubcard,** februari 1998.
- **Meldpunt ongebruikelijke transacties,** juli 1997.
- **Videocamera's Wallen Amsterdam,** mei 1997.
- **In beeld gebracht. Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging,** januari 1997.
- **Als de telefoon wordt opgenomen. regels voor het registreren, meeluisteren en opnemen van telefoongesprekken van werknemers,** november 1996.

bijlagen

achtergrondstudies en verkenningen (1994 – 2003)

In de serie Achtergrondstudies en verkenningen zijn verschenen:

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

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, **Personeels-informatiesystemen - de Wet persoonsregistraties toegepast**. A&V 1; Registratiekamer, Rijswijk 1994 (niet meer beschikbaar)

brochures

Gedragscodes. Bescherming van persoonsgegevens door zelfregulering
oktober 2002

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

Derde landen. De doorgifte van persoonsgegevens naar landen buiten de Europese Unie/
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

Verstrekken van persoonsgegevens, mei 2004
Melden en vrijstellingen, april 2004
Verstrekken gegevens uit ledenadministratie, maart 2004
Inzagerecht, november 2003
Personeelsdossiers, juli 2003
Nummeridentificatie bij telefoonverkeer, mei 2003
Geadresseerde reclame, mei 2003
Klachtenbehandeling door het College bescherming persoonsgegevens (verantwoordelijke), april 2003
Opnemen telefoongesprekken op de werkplek, april 2003
Het melden van een gegevensverwerking, februari 2003
Uw gegevens bij de politie, januari 2003
Zwarte lijsten, november 2002
Cameratoezicht: richtlijnen en vuistregels voor verantwoordelijken in bedrijven en organisaties, augustus 2002
Cameratoezicht: rechten van de betrokkene, 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

bijlagen

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 (betrokkene), september 2001
Uw persoonsgegevens beveiligd, september 2001
Geadresseerde reclame, september 2001
Voorafgaand onderzoek, september 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.

publicaties in kranten, tijdschriften en vakbladen 2003

Artz, mw. S.M. en Lieon, mw. drs. S., **De transparante ambtenaar,** Privacy & Informatie nummer 5, oktober 2003, p. 213-215

Helden, mw. drs. W.J. van en Seumeren, mw .drs. N.M. van, **Vragen staat niet vrij! De verwerking van persoonsgegevens bij de uitvoering van de Algemene bijstandswet,** Rechtshulp, nummer 10 2003, p. 13-21

Heuver, mr. J.W., **Credit scoring en privacy,** Rechtshulp, nummer 10 2003, p. 55-61

Hustinx, mr. P.J., **Voorstel Algemene identificatieplicht ondoordacht,** NRC Handelsblad, 13 februari 2003, p. 1, 7

Hustinx, **mr. P.J., Dataprotection at crossroads, Digma, Zeitschrift für Datenrecht und Informationssicherheit,** 27 oktober 2003

Pol, mr. U. van de, **Hoofdcommissarissen lokken eigenrichting uit,** Algemeen Politieblad, 24 januari 2004, p. 7

Pol, mr. U. van de, **Aiming for effective co-regulation of data protection: policies and practices of the Dutch DPA** Council of Europe, 30 januari 2003

Pol, mr. U. van de, **Juridische grenzen,** NRC Handelsblad, 13 september 2003, p. 35

Pol, mr. U. van de en Wit, H. de, **Een grondrecht onder druk, Overmatig gebruik van inzagerecht aangepakt,** Recherche Magazine, november 2003, p. 28-29

Pol, mr. U. van de, **Privacy down under,** Privacy & Informatie, nummer 6 2003, p. 244-246

Wishaw RE, mr. R.W.A., **Vragen staat vrij?,** EDP-Auditor, jaargang 12, 2003, nummer 3, p. 22-30

Review of 2003

Although the right to protection of privacy is a constitutional right, this does not make it an absolute right. This right entails handling personal data with proper respect and caution. Vested in this are interests that will require constant balancing against other interests. In the public sector, this weighing up of interests is ultimately reviewed in parliament and is usually translated into guarantees for citizens with regard to collecting and using their personal data. Citizens usually have no objections to this assessment. Both sides of the balance are after all weighted by authentic interests. However, the rights of citizens in a democratic state of law are not served if government bodies deal with their personal data arbitrarily. A democratic balancing of interests should result in the careful, systematic government processing of citizens' personal data. The Dutch Data Protection Authority (DPA) is concerned about the erosion in public debate of the fundamental principle laid down in international treaties that the use of personal data and violation of personally privacy should be an actual necessity.

Privacy and security

Although the right to protection of privacy is a constitutional right, this does not make it an absolute right. This right entails handling personal data with proper respect and care. Vested in this are interests that will require constant balancing against other interests. In the public sector, this weighing up of interests is ultimately reviewed in parliament and is usually translated into guarantees for citizens with regard to collecting and using their personal data. Citizens usually have no objections to this assessment. Both sides of the balance are after all weighted by authentic interests. The interests of citizens in a democratic state of law are not served if government bodies deal with their personal data arbitrarily. A democratic balancing of interests should result in the careful, systematic government processing of citizens' personal data. The Dutch Data Protection Authority (DPA) is concerned about the erosion in public debate of the fundamental principle laid down in international treaties that the use of personal data and violation of personally privacy should be an actual necessity.

Necessity as guiding principle

The necessity principle is eroded when politicians, civil servants and policy makers no longer ask whether gathering, using and retaining citizens' data is necessary for a specific purpose. The fact that institutions dispose over considerable quantities of citizens' details does not automatically legitimize using these data for other purposes, nor retaining them for extended periods or sharing them with other organisations.

The criteria of necessity leave scope for the use of a basic set of citizens' data by various government bodies and related agencies. Also collaboration between institutions is very well possible, providing organisations continually monitor which exchange of information is required for the collaboration, and providing the citizen in question is properly notified. The distribution of duties between public-private bodies creates a more complex situation. The transfer or contracting out of social security components calls for paying close attention to the correct use of (generally highly specific) personal data by the market parties. Contracting out activities does not acquit the government from its responsibility for ensuring that personal data are treated with due care.

Monitoring, security and freedom

Public debate constantly resounds with the call for more monitoring measures. Objective weighing up and realistic assessment of the effect of proposed measures seem to cave in beneath the very real threat of terrorist attacks and the problem of serious forms of crime. The symbolism of the proposals often is, however, far greater than their efficiency. Increasingly far-reaching monitoring measures will however not necessarily result in increasing citizens' security, while the social burden for state and citizens is considerable. Paying too much attention to security will encroach upon the freedom of the citizen in the long term.

Reflecting on the purpose, necessity and scale of monitoring measures to be taken, is imperative. Measures could also be temporary; their scope can be limited to places or times where there is increased risk. Evaluating the measures should be standard practice, certainly in the case of radical monitoring means like surveillance cameras, preventive searching and identity checks. Well thought out measures, their proportional use and measuring their efficacy in combating terrorism and other forms of serious crime are part and parcel of a government that protects our constitutional rights.

Privacy from the outset

When the new cabinet was installed in 2003, the Dutch DPA asked that attention be paid to the issue of processing personal data with due care. On a number of points – health care, security, tackling fraud and electronic government services – cabinet policy does after all touch on the careful and lawful processing of personal data. If privacy protection is disregarded, the ability of policy initiatives and government action to stand up in court can be at considerable risk. There is greater scope for success by paying close attention to privacy protection from the outset, when designing measures and information systems.

Legislative proposals that largely relate to processing personal data should be submitted to the Dutch DPA for advice. In consultation with the ministries, better conditions for fulfilling this obligation were created in 2003.

Information infrastructure

Streamlining basic data should not end in the unbridled flow of personal data within the government. A specific and clear legislative rule is required to cover large data flows, with attention for such aspects as social necessity, distribution of tasks and roles, actual data traffic and transparency.

In 2003 the recommendations of the Persoonsnummerbeleid (Personal Identification Number Policy) of the Tafel van Thijn (the Van Thijn Committee) on setting up an umbrella information infrastructure for the government, was followed up. The Dutch DPA was intensively involved, both at steering group and working group level, in developing a plan for the introduction. Among other things, the Dutch DPA contributed to the proposals for a Nationale Vertrouwensfunctie (National Confidentiality Function), an organisation that will be charged with providing citizens with insight in all data flows on the basis of the burgerservicenummer (public service number). Citizens' confidence in the electronic state is essential. This is why the Dutch DPA will recieve the means to examine current and new data processing and fulfil the role of 'ombudsman' in this area in future.

Municipalities

For the citizen, the municipality is an important area of government with which he or

Results secured in 2003

IN THE PREVIOUS ANNUAL REPORT, IT WAS ANNOUNCED THAT IN 2003 OUR TARGETS WOULD BE AS FOLLOWS:

- **Advice on legislation**
  In accordance with Article 51, second paragraph of the Personal Data Protection Act (WBP), the Dutch Data Protection Authority (DPA) should be asked to provide advice with regard to legislative proposals and the drawing up of implementing regulations (AMvBs) with any degree of relevance to the processing of personal data. The Dutch DPA has asked nearly all the Ministries to pay heed to the obligation to request for advice and has managed to make agreements in order to adequately fulfil this requirement.

- **Data protection officers**
  By the end of 2003, another 51 officers charged with data protection had been reported to the Dutch DPA on the grounds of Articles 62-64 of the Personal Data Protection Act, bringing the total number to 148. The Dutch DPA helped to organise a contact day for data protection officers employed by municipal authorities and all officers have been allocated a contact person within the Dutch DPA. The working relationship between the supervisor and the data protection officers is still being developed.

- **Camera surveillance**
  In 2003, the Dutch DPA published the results of a survey on the operation of camera surveillance of public places in Dutch towns and cities and how the various municipal authorities treat the privacy aspects. The report was entitled *'Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten'* (Camera surveillance of public places. Investigation into the use of camera surveillance in all Dutch municipalities).

- **Sick employees**
  For many years, attempts have made to stem the flow of sick employees claiming disability benefit under the Disability Benefits Act (WAO). This has led to an increased need for information on sick employees, thereby directly affecting the privacy of said employees. In 2003, the Dutch DPA completed an investigation into the privacy aspects of the complex rules and regulations and the main flows of information regarding sick employees. Publication of this investigation has been delayed.

- **Police registers**
  Following up on previous activities concerning the registers of the Criminal Intelligence Service Units (CIEs), the Dutch DPA has started a random investigation of the practices of eight of these units. The selected dossiers were examined to determine the extent to which the regulations governing data processing were actually being observed. The investigation is due to be completed in 2004.

- **Telecommunication**
  The Dutch DPA has been looking into notification obligations within the telecommunications sector and has been providing advice with regard to the new Telecommunications Act. In late 2003, the Dutch DPA consulted the sector in writing on the issue of number identification with a view to clarifying the standards used in practical situations.

she will be greatly involved. As a result, municipalities process great quantities of citizens' personal data. Because of developments in the duties and administration of the municipality, responsibility for protecting personal data is increasing. Consequently, it is crucial that municipalities have their information systems well organised, also with a view to protecting the personal data of their citizens.

An analysis of the first 13,000 notifications of processing personal data under the Wet bescherming persoonsgegevens (Personal Data Protection Act) showed that the number of notifications from municipalities greatly lagged behind expectations; at least 60 municipalities appeared to consistently ignore their obligation to notify. In a random check the Dutch DPA then assessed a number of municipalities to see whether they had complied with the obligation to notify. In December 2003, the first municipality was penalised for failing to comply with this obligation.

Public camera surveillance

In 2003 the Dutch DPA commissioned a survey into the use of camera surveillance by municipalities. The goal of the survey *Cameratoezicht in de openbare ruimte* (camera surveillance of public places) was to gain an overview of the way in which CCTV surveillance functions in practice and how the various municipalities address the privacy aspects of camera surveillance. The survey showed that one in five municipalities de-

- **Certification**
  The results of a previous project entitled 'Auditaanpak' (Audit Approach) have been used as the basis for developing a privacy certification scheme. The aim of this scheme is to comply with the legislation on privacy by further advancing self-regulation. In 2003, the Dutch DPA, in partnership with the future accreditation institutions NOREA *(National Professional Association for IT Editors in the Netherlands)* and the NIVRA *(Royal Netherlands Institute of Registered Accountants)*, ensured that this scheme was almost ready to be put into operation.

- **Notification obligation**
  The obligation to notify the processing of personal data to the Dutch DPA contributes towards transparency and enables verification and supervision. In 2003, the Dutch DPA used the public register to carry out an analysis of notifications with a view to the enforcement of this obligation. More detailed investigations were eventually conducted into three sectors and the municipal authorities which led to the first administrative fines being imposed in late 2003.

- **Internet site**
  Access to the Dutch DPA web site has been improved. Amongst other things, theme dossiers and an e-mail newsletter have been introduced. The increasing size of the web site and the need to provide insight into policy regarding new Dutch DPA tasks meant that in 2003, a start was made on re-designing the Dutch DPA web site. The planned separate section for dealing with practical questions from data subjects has not been realised. This will now be included in the new design.

- **Organisational set-up**
  In order to ensure that the new tasks in the areas of supervision and enforcement are carried out satisfactorily, the Dutch DPA has made modifications to its organisational set-up. In line with this new organisational set-up, the Intervention, Objections and Appeals Department has been operating since 1 January 2003. The modernisation of the organisational structure was rounded off in 2003 by the instigation of the Investigations Department on 1 January 2004. In as far as this was possible, the job profiles accompanying these changes were realised in 2003.

ploys such surveillance as a means of furthering security, public order and supervision. Over half of the municipalities that make use of CCTV however, have not reviewed its effectiveness. Around half of the municipalities use camera surveillance in the context of cooperation between institutions and organisations. This generally involves cooperation with the police in tracking down criminals, although cooperating with companies and other organisations is also a regular occurrence. The frameworks within which this takes place, however, often seem unclear.

Rotterdam: a personal approach is possible

At the end of 2002, the Dutch DPA contested the view of Rotterdam city council that adjusting privacy legislation was necessary for a safe city. Following on from this, in 2003 the Dutch DPA consulted all the parties involved in the various projects for an integral approach to around 700 drug addicts causing public nuisance, committing crimes and also avoiding medical and welfare aid. The police, welfare bodies and the probation service all took part in this project. Data on the contacts of addicts with police and the welfare authorities was exchanged. The shared information is stored in a basic dossier. The specific approach to be adopted, consisting of various forms of voluntary and compulsory treatment programmes, is then determined on the basis of the dossier.

Discussions with the partners in the project focused on the limits circumscribed by care workers' professional confidentiality. In the consultations, the Dutch DPA pointed out that welfare workers should adhere to their statutory duty of acting in the client's best interests. If, in their professional opinion, sharing information on the client with other bodies is in the client's best interests, it is possible in principle. This approach prompted a wider debate on the scope of medical professional confidentiality under the direction of the Inspectie voor de Gezondheidszorg (Health Protection Inspectorate). In the course of 2003, the parties involved elaborated the rules governing information exchange and the Informatiesysteem PGA (PGA Information System) was notified to the Dutch DPA.

Insufficient supervision of the implementation of the WWB

The core of the new Wet werk en bijstand (WWB or Work and Income Act) determines that municipalities acquire more (financial) responsibility for social security. In 2002 and 2003 the Dutch DPA drew attention to the system of supervising the implementation of the WWB. There is a gap between the official rule that the *Inspectie Werk en Inkomen* (IWI or Work and Income Inspectorate) supervises the legitimacy of implementation (including processing data on individuals) and the practical detailing in which the IWI does not receive the information necessary for structurally exercising supervision. This gulf has not been bridged during the discussion of the bill in both Houses. As regards processing (personal) data, the elaboration of the supervision is not in line with the view of the Dutch deputy minister of Social Affairs and Employment expressed during the parliamentary discussion. The Dutch DPA is concerned about the municipalities' lack of a duty to give account.

Police and privacy

The contribution of a number of chiefs of police to the public debate on security was out of balance. Protection of privacy was repeatedly underlined as an obstacle to police work, a hindrance to achieving better results. Prominent police officers seemed to deny the fact that the police has recourse to an extremely diverse range of sources of infor-

mation about citizens. With this, privacy protection obligates the police to deal with data in a responsible, controllable manner. The Groningen chief of police's typification of the constitutional right to privacy as a 'refuge of evil' was way out of line.

The Dutch DPA acknowledges that the police have a considerable and legitimate need for information and agreed with the main points laid down in the planned expansion of the powers of the Ministry of Justice and police to request personal data from organisations and companies, if necessary to an investigation. The bill is based on proposals tabled by the Mevis committee (2001) and primarily creates clarity for the business sector. The Dutch DPA is of the opinion that a counterweight is required. Information should not only be gathered and used purposively and selectively but police information administration must be supervised by, among other things, periodical and independent retroactive checks. In the cabinet standpoint on the proposals of the Mevis committee, the Minister of Justice also promised to effectuate this. The Dutch DPA insisted on the speedy implementation of these periodical audits on all police registers.

Criminal Intelligence Service Units

In 2003 the Dutch DPA commenced an initial series of audits into the criminele inlichtingen eenheden (CIEs or Criminal Intelligence Service Units) of eight police forces supplementary to the self-evaluation and independent review organised by the police in 2002. CIEs maintain a number of exceptional registers that also contain investigative data on persons who are not suspected of criminal involvement. Independent, external supervision is therefore of essential importance. Only the Dutch DPA can, as an external supervisor, appraise itself of the content of the dossiers. This series of surveys involved carrying out spot checks to audit this practice. In the selected dossiers, the research assessed the degree to which the rules for processing information were actually followed. The audit round will be completed in 2004.

Lawyers tapped

The Dutch DPA investigation into listening in on and registering conversations between citizens and their lawyers showed that there was insufficient respect for lawyers' professional confidentiality. The systematic recording, registration, working out and examination of this confidential communication by the police and *Openbaar Ministerie* (OM or Public Prosecutors Office) is in conflict with the exceptional position of those who can claim professional confidentiality as acknowledged in legislation and treaties. Consequently it is also in conflict with the *Wet politieregisters* (Police Registers Act) and the *Wet bescherming persoonsgegevens* (Personal Data Protection Act). Police and justice had gone too far in listening into and recording conversations between citizens and their counsel. The Minister of Justice did not however share the Dutch DPA's views on this, and did not adopt the recommendations.

Reducing the administrative burden

The number of requests submitted to the police by individuals wishing to know if and how they are registered in police registers, showed a considerable upswing in previous years. The number of requests jumped from 1100 in 2000 to 1850 in 2002. They primarily concerned complex, labour-intensive requests from lawyers, which were dealt with by a CIE. A working group of privacy experts from the police, the OM and the Dutch DPA devised a plan to streamline handling the requests. This will also prevent the erosion of

the right of inspection.

In the context of reducing the administrative burden, the model regulations for police registers are also important. In 2002, the Dutch DPA approved 40 model regulations for the permanent registers. In 2003, the *Modelreglement Tijdelijk Register* (Temporary Register Model Regulation) came into force. The use of model regulations immediately reduces the administrative burden for police and the Dutch DPA and simultaneously creates safeguards.

Market mechanisms in the healthcare sector

The discussion on cost control and improving quality in the healthcare sector is supported by a consensus on the need for stimulating market forces through public-private cooperation while an extremely prominent role for the healthcare insurance companies is beginning to take shape. However, the insurance companies assert that they cannot fulfil this role without maximum insight in the actual, individual healthcare cases. This emerged in the discussion on the introduction of the *Diagnose Behandeling Combinatie* (DBC or Diagnosis-Treatment Combination).

The DBC system was developed to defray the costs of specialised medical care and should result in a price development that conforms to the market on the basis of negotiations between healthcare institutions and medical insurance companies. A DBC is a combination of codes that contain data on, among other things, the demand for healthcare, the diagnosis and the treatment of a patient. This information is covered by the code of professional medical confidentiality. Healthcare professionals are expected to provide the DBCs to insurance companies as an account of the care provided.

The Dutch DPA emphasized the importance of professional medical confidentiality and proportionality in furnishing personal medical data. The Dutch DPA insisted that there should be greater clarity surrounding the personal data that hospitals are required to provide to health insurance companies. Once the data processing necessarily required for various legitimate purposes has been clarified, the legal embedding of the new pay system could be tailored to match it. Working out this necessity requirement resulted in a checking framework. This offers five criteria which serve as a basis for determining whether a DBC can be declared or not, together with all corresponding data on the diagnosis.

The DBC system will be gradually introduced starting on 1 January 2005. In a joint letter, the Minister of Health, Welfare and Sport and the Dutch DPA asked the parties involved (such as *Zorgverzekeraars Nederland* and professional associations) to bring the method involved in introducing the system to the attention of their members.

Sick employees

For several years now, attempts have been made to limit the number of sick employees claiming disability benefits under the Wet op de Arbeidsongeschiktheidsverzekering (WAO or Disability Benefits Act). This led to measures for a more active sick leave policy, more stringent reintegration obligations for employee and employer and a longer obligation for employers to continue paying wages. Further, other organisations and companies have also become involved in the system. All these parties have an increasing need of information on the sick employee, which directly impinges on his or her privacy.

Given the complexity of the legislation, in 2002 the Dutch DPA launched a study of the most important data flows concerning sick employees and the corresponding privacy

regulations. The study was rounded off in 2003. Once more, the importance of clear legislation on public-private cooperation was undeniable. More than government bodies, companies have an interest in clarity on what is and is not permitted, both in terms of management and reputation and liability.

Certification of data processing

In various countries a search is being conducted into ways of utilising competition and market mechanisms for privacy protection. One of the options of making it clear in the market that companies and organisations endeavour to handle personal data with due respect and care, is a privacy certificate. Together with the Dutch DPA, a number of regulatory bodies have developed a system for the private auditing of processing personal data. The privacy certificate in mind can be allocated to a specific, legitimate processing of personal data. The certificate is thus not awarded to an organisation in its entirety. In the first instance, the Dutch DPA will appoint two accreditation bodies, the NOREA and the NIVRA for the accreditation of privacy auditors. The system will gain practical form in 2004.

Codes of conduct for the business sector

When protecting personal data, explicit scope has been created for self-regulation by, among other things, codes of conduct that have been approved by the supervisor. Codes of conduct are important because the specific working out of privacy norms for a sector or profession creates clarity for professional practice. The Dutch DPA was involved with the realisation of codes of conduct for financial institutions, the bailiffs and the first European code of conduct for direct marketing.

The Privacygedragscode sector particuliere onderzoeksbureaus (Privacy Code of Conduct for Private Investigation Agencies) approved at the beginning of 2004 was drafted by the *Vereniging van particuliere Beveiligingsbureaus* (VPB or Association of Private Security Agencies) and binds the agencies affiliated to the VPB. Private investigation is a sector experiencing exponential growth, and one in which little was regulated. In the context of licensing these agencies, the Minister of Justice is planning to obligate all private investigation firms to comply with this code of conduct. The Minister of Justice and the Dutch DPA have concluded an agreement to coordinate supervision of the branch.

The Code of Conduct for processing personal data of the *Nederlandse Vereniging van Handelsinformatiebureaus* (NVH or Netherlands Association of Business Information Agencies) was also approved. In this sector in particular, over the last few years, the Dutch DPA was forced to conclude that personal data protection was not properly observed on a large scale. The Dutch DPA will maintain the code of conduct of the NVH as a guideline in supervising all trade information bureaux.

Penalty for business information bureau X

In 2003, the Dutch DPA published the results of the investigation into business information agency X. The conclusion was that the bureau had processed personal data illegitimately, improperly and negligently when compiling reports of claim information. The Public Prosecutor was informed that the company was suspected of having committed a number of punishable offences. The criminal investigation has since resulted in the prosecution and trial of a number of individuals involved in the enterprise.

Targets for 2004

THE MAIN TARGETS FOR 2004 WILL BE AS FOLLOWS:

- **Sick employees**
  The investigation of the most important data flows with regard to sick employees and the relevant privacy regulations will result in a study being published in 2004 containing rules of thumb to be used in the practical situation. This study will be brought to the attention of the various parties involved in the reintegration of sick employees.

- **Police registers**
  The investigation that was started in 2003 into the registers kept by the Criminal Intelligence Service Units at eight regional police forces will be completed in 2004. The general findings of this investigation will be published.

- **Investigation of wiretapping rooms**
  In 2004, the Dutch Data Protection Authority (DPA) is to conduct an investigation into the privacy aspects of data processing in police wiretapping rooms, as a follow-up to the 2003 investigation into the safeguarding of confidential communication between lawyers during the interception of telecommunications *(Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie)*.

- **Camera surveillance**
  The results of the investigation published in 2003 entitled *Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten* (Camera surveillance of public places. Investigation into the use of camera surveillance in all Dutch municipalities) will be used in 2004 for a study of the privacy aspects of camera surveillance of public places, which will outline rules of thumb for practical situations.

- **Public service number**
  The Dutch DPA will make a contribution towards the realisation of the *Nationale Vertrouwensfunctie* (National Confidentiality Function), an organisation which has been given the task of providing citizens with insight into the various data flows on the basis of a *burgerservicenummer* (public service number). During 2004, the Dutch DPA will be given the chance to start assessing existing and new data processing methods and to prepare for a future watchdog function.

- **Certification**
  The scheme developed in collaboration with the NOREA *(National Professional Association for IT Editors in the Netherlands)* and the NIVRA *(Royal Netherlands Institute of Registered Accountants)* for privacy certification is due to be put into operation in 2004. It will initially take the form test certifications, but will later become a market product. The Dutch DPA will help to assess the process of test certification.

- **Introduction of DBC system**
  In the area of healthcare, the Dutch DPA will closely follow the development and introduction of the health care finance system based on the Diagnose Behandeling Combinatie (Diagnosis-Treatment Combination).

- **National registration systems in the healthcare sector**
  In 2003, the Dutch DPA completed an exploratory investigation into five national registration systems in the healthcare sector. In 2004, the Dutch DPA will use the results of this investigation to formulate standards for use in national registration systems and the related enforcement policy.

- **Investigation into perception of privacy**
  The Dutch DPA is to conduct an initial enquiry into aspects of Dutch citizens' perception of and need for privacy. Investigations of this kind have already been carried out in various other European countries. The findings will be used to help make strategic choices and to formulate the policy of the supervisory body.

- **Policy regulations and 2nd line position**
  The Dutch DPA is to publish policy regulations for dealing with cases and the publicity surrounding them. In order to attain a 2nd line position, the Dutch DPA will approach sector, branch, umbrella and professional organisations to explore the possibility of exchanging information and dividing the tasks involved in providing information and handling complaints.

- **Organisational development**
  The Investigations Department is to become operational in 2004, focusing on the differentiation of the various forms of investigation and the development of risk analysis as an instrument for devising policy. The department will play an important part in the planned investigation into the perception of privacy and is responsible for the analysis of notifications for 2004.

- **Dutch DPA web site**
  The Dutch DPA is to revamp its web site in 2004 with a view to providing better information to data controllers and data subjects. Publication of information material on the web site will be more geared towards FAQs. This should result in a reduction in the annual flow of requests the Dutch DPA receives for information by telephone, e-mail and in the post.

The Dutch DPA had concluded that the bureau had illegitimately gathered personal data from all kinds of sources – including the tax administration, social security and benefits agencies and housing cooperations. Subsequently the Dutch DPA informed a large number of these bodies, companies and professional associations of the findings of the investigations so that they were able to take suitable steps. To which purpose, a number of organisations received relevant sections of the material serving as evidence.

In May 2003, the Dutch DPA imposed an obligation on bureau X subject to a penalty in case of non-compliance. The sanction focused on compliance with two points on which breaches of the WBP had been concluded: bureau X must refrain from processing personal data covered by professional confidentiality or which are banned from being processed, and the bureau must inform the individuals on whom it has gathered personal data.

Properly informing clients

In principle, companies have considerable options for processing personal data for market purposes. A key condition for the legitimate processing of information, is to furnish clients whose data is involved, with good information. Transparency is also essential for maintaining customer confidence. This re-surfaced in two issues: the unlisted number policy of the Dutch telecom company KPN and the creation of a central database for client data at the ING Group.

The ING Bank, Postbank and RVS (all parts of the ING Group) had sent a letter to their clients in 2002 outlining the plan to store their data in a single central system in future, for marketing purposes. The information offered, however, gave clients insufficient chance to exercise their rights. After an investigation, the Dutch DPA arrived at the conclusion that the companies had acted wrongfully. Because of the lack of specific detail in the letter sent to the data subjects, i.e. the clients, on the provision of data, the data provision was not compatible with the purpose for which the data had been gathered. The ING Group should have given the clients of the various sections clearer information in order to be permitted to further process their data at central level. The clients of ING Bank, the Postbank and RVS subsequently received additional information.

In mid 2003, the Dutch DPA and the OPTA (Independent Post and Telecommunications Authority) published an investigative report on the policy of Koninklijke KPN N.V. (KPN) on so-called ‘secret numbers’ (unlisted numbers). In the mid-nineties, KPN seems to have altered its policy, and has for some time been passing on addresses of subscribers with unlisted numbers to third parties for direct marketing purposes, without having explicitly informed its subscribers to this effect. The Dutch DPA requested KPN to actively inform its clients on the secret numbers policy. It is disappointing that the issue dragged on into early 2004 despite that fact that it essentially concerns a company’s statutory obligation to inform clients of their statutory rights.

COLOFON

Jaarverslag 2003

College bescherming persoonsgegevens, Den Haag, mei 2004.

Met medewerking van:
J.H.M. Baart, J.W. Broekema, M.A.H. Fontein,
G.O. van de Klashorst, P. Krul,
U. van de Pol, C.E. Romanesko, B. den Uyl,
en de beleidsafdeling.

Eindredactie: G.O. van de Klashorst

Ontwerp: Proforma, strategie, ontwerp en management (Miriam Monster)
Vertaling: Medendorp Vertaaldienst B.V.
Druk: Deltahage B.V. (Den Haag)