



2005

in vogelvlucht

In de afgelopen jaren heeft de bescherming van de persoonlijke levenssfeer in de publieke opinie haar vanzelfsprekendheid verloren. Zorgen om terrorisme, onveiligheid en maatschappelijke misstanden bij burgers, bestuurders, politici en beleidsmakers hebben ertoe geleid dat de regels voor de bescherming van persoonsgegevens in het publieke debat als zondebok of als obstakel worden afgedaan. Behalve het politiek-maatschappelijke klimaat is ook het toezichtsdomein aan ingrijpende veranderingen onderhevig.

Het CBP heeft zich daarom in 2005 nadrukkelijk de vraag gesteld wat de essentie was en is van hetgeen met de WBP beschermd dient te worden en langs welke weg een en ander gerealiseerd dient te worden. In veranderende tijden kan minder vertrouwd worden op de zeggingskracht van de wet en zal meer gebruik moeten worden gemaakt van de visies en bevindingen van anderen. Het CBP prijst zich gelukkig dat het in 2005 bij deze reflexie – ook in het kader van de aanstaande evaluatie van de Wet bescherming persoonsgegevens – een beroep kon doen op de bereidheid van vele gesprekspartners – academici, experts uit het veld, bedrijven en maatschappelijke organisaties – om mee te denken.

Controle op de naleving is wat de wetgever bij uitstek van de toezichthouder vraagt. Effectief toezicht op de naleving van en zondig handhaving van de regels voor de omgang met persoonsgegevens is noodzakelijk. Onvoldoende mensen en middelen zijn echter beschikbaar om deze opdracht naar de volle omvang te kunnen verwezenlijken. Het CBP heeft in de afgelopen periode in allerlei kwesties zijn aandeel niet of slechts beperkt kunnen nemen. De maatschappelijk en politiek gewenste beleidsverschuiving naar meer onderzoek en handhaving kon slechts ten dele gerealiseerd worden. Het CBP heeft alle zeilen moeten bijzetten om althans op enkele grote dossiers te doen wat gezien de inherente risico's voor de bescherming van de persoonlijke levenssfeer gedaan moest worden.

Zorgstelsel

De stelselwijziging in de zorg gaf het CBP reden tot intensieve bemoeienis. Na de advisering in 2004 over de Zorgverzekeringswet (Zvw), heeft het CBP in 2005 veel aandacht besteed aan de uitwerking van de stelselwijziging. Met de minister van Volksgezondheid, Welzijn en Sport (VWS) zijn afspraken gemaakt over hoe de tekortkomingen in de Zorgverzekeringswet met betrekking tot de verwerking van persoonsgegevens zoveel mogelijk opgelost konden worden. Daartoe is onder meer artikel 87 Zvw in nauw overleg met het CBP uitgewerkt in een ministeriële regeling, de Regeling Zorgverzekering. Verder is afgesproken dat de 'prestatiebeschrijvingen' die voor een belangrijk deel de inhoud van de informatiestroom tussen zorgverleners en zorgverkeeraars vormen, in overleg met het CBP door de Zorgautoriteit zullen worden vastgesteld. De prestatiebeschrijvingen geven op detailniveau aan welke persoonsgegevens dienen te worden verstrekt ten behoeve van de declaratie van verleende zorg.

Risicoverevening

Met de minister van VWS is verder overeengekomen dat voor risicoverevening geen persoonsgegevens gebruikt zullen worden. Volstaan kan worden met gepseudonimiseerde gegevens, dat wil zeggen dat de gegevens gekoppeld worden aan een unieke maar anonieme code. Het CBP adviseerde ook een aantal randvoorwaarden vast te leggen in de ministeriële regeling ter uitwerking van artikel 35 Zvw, dat betrekking heeft op de verwerking van persoonsgegevens ten behoeve van de risicoverevening. Voor de overgangssituatie naar het stelsel onder de Zvw waren tijdelijk (uitsluitend voor de ex-ante berekening 2006) wel persoonsgegevens noodzakelijk. Het tijdelijke karakter van deze verwerking is vastgelegd evenals een maximale bewaartermijn voor de benodigde gegevens.

Resultaten 2005

IN HET VORIGE JAARVERSLAG IS AANGEKONDIGD DAT IN 2005 ZOU WORDEN GESTREEFD NAAR DE VOLGENDE RESULTATEN (HET JAARPLAN 2005 IS GETEMPORISEERD TOT MEDIO 2006):

• **Veiligheid en privacy**

In 2004 heeft het CBP geadviseerd over het concept wetsvoorstel ter verruiming van de mogelijkheden ter opsporing van terroristische misdrijven. Dit advies is op veel punten niet gevolgd. In 2005 heeft het CBP zijn advies onder de aandacht gebracht van de vaste commissie voor Justitie van de Tweede Kamer. Op verzoek van de Tweede Kamer heeft het CBP de opzet van de Contra-terrorisme-infobox (CT-infobox) geanalyseerd.

Verder heeft het CBP in samenwerking met de ministeries van BZK en Justitie de hoogleraren prof.mr. H.R.B.M. Kummeling en prof.mr.dr. E.R. Muller gevraagd onderzoek te doen naar de balans tussen veiligheid en privacy. In 2006 wordt het eindrapport verwacht.

• **Bijzondere politieregisters**

In het kader van het structurele toezicht op de bijzondere politieregisters, heeft het CBP in het najaar van 2005 onderzoek gedaan bij twee bijzondere opsporingsdiensten. De resultaten hiervan zullen in 2006 beschikbaar komen.

• **Risicoselectie**

In 2005 is een expertmeeting georganiseerd over risicoselectie. In 2006 zal hierover worden gepubliceerd.

• **Internet en privacy**

In 2005 heeft een expertmeeting plaatsgevonden over internet en de bescherming van persoonsgegevens. In 2006 zal een verkenning op dit terrein worden gepubliceerd.

• **Informatieplicht**

De voorlichting over de informatieplicht is versterkt. Verder zijn in 2005 enkele onderzoeken naar de naleving van de informatieplicht gestart die in 2006 zullen worden gepubliceerd.

• **Meldingsplichtonderzoek**

In 2005 zijn de jaarlijkse meldingsplichtonderzoeken voorbereid maar uiteindelijk niet uitgevoerd. Temporisering van het jaarplan leidde tot uitstel van de start van de onderzoeken. Na de uitspraak van de Raad van State (uitspraak van 21 september 2005, 200504372/1: geen grondslag voor boete voor het niet melden van verwerkingen gestart voor 1 september 2001) is de reeks meldingsplichtonderzoeken voor 2005 uiteindelijk afgelast. De WBP wordt op dit punt in 2006 gerepareerd.

• **Administratieve lasten**

In aansluiting op eind 2004 gedane voorstellen heeft het CBP verschillende malen overleg gevoerd met het ministerie van Justitie en het VNO/NCW, onder meer over verruiming van de vrijstelling van de meldingsplicht. Het is uiteindelijk aan de minister van Justitie om de Tweede Kamer voorstellen te doen. Dit is in 2005 niet gebeurd.

• **Binding Corporate Rules**

Het CBP heeft actief bijgedragen aan een vereenvoudiging van de regels voor de doorgifte van persoonsgegevens naar verantwoordelijken buiten de Europese Unie. De Artikel 29-werkgroep heeft in 2005 Europese afspraken gemaakt over een uniforme procedure voor het aanvragen van vergunningen en over een gecoördineerde afhandeling van vergunningaanvragen gebaseerd op zogenaamde binding corporate rules (BCR's).

• **Samenwerkingsverbanden**

Het CBP heeft in 2005 in diverse gevallen bijgedragen aan de verheldering van de regels voor de noodzakelijke uitwisseling van persoonsgegevens in samenwerkingsverbanden. In april 2005 heeft het CBP een symposium over dit onderwerp georganiseerd. Speciale bijeenkomsten gericht op toezichthouders zijn niet georganiseerd.

• **Toezicht en toezichthouders**

Met de Commissie gelijke behandeling, de Nationale ombudsman en het Studie- en informatiecentrum mensenrechten heeft het CBP in 2005 een advies aan de regering uitgebracht over de wenselijkheid van de oprichting van een nationaal mensenrechteninstituut. Met OPTA en IWI zijn in 2005 samenwerkingsovereenkomsten gesloten. Het aantal functionarissen voor de gegevensbescherming is in 2005 licht gegroeid.

• **Zorg en zekerheid**

In 2005 is veel aandacht besteed aan de Zorgverzekeringswet en alle veranderingen die deze met zich meebracht en aan de plannen voor invoering van het burgerservicenummer in de zorg. Verder is een verkennend onderzoek bij verzekeraars uitgevoerd naar gegevensstromen bij reïntegratie en de uitwisseling van medische gegevens tussen concernonderdelen. De publicatie van een normatief kader voor de sociale diensten zal worden uitgebracht in 2006.

• **Burgerservicenummer**

Het CBP heeft in 2004 al geadviseerd over het Wetsvoorstel algemene bepalingen burgerservicenummer. In het wetsvoorstel zoals in 2005 bij de Tweede Kamer ingediend, is onvoldoende rekening gehouden met de bezwaren van het CBP. Het CBP heeft bij de Tweede Kamer zijn zorgen hierover geuit. De voorgenomen voorbereiding op de taken die het CBP zou krijgen in het kader van de Nationale ombudsfunctie, was door uitstel van de inwerkingstreding van de wet nog niet aan de orde.

• **Evaluatie Wet bescherming persoonsgegevens**

Het CBP heeft zich op verschillende manieren voorbereid op de evaluatie van de Wet bescherming persoonsgegevens die is voorzien voor 2006 (artikel 80 Wbp). Onder andere door een aantal bijeenkomsten met experts uit het veld en overleg met het ministerie van Justitie.

Addendum Zorgverzekeraars bij gedragscode

Het Addendum Zorgverzekeraars, opgesteld door Zorgverzekeraars Nederland (ZN), bevat gedragsregels voor de omgang met persoonsgegevens door ziekte- kostenverzekeraars en is een aanvulling op de reeds bestaande Gedragscode Verwerking Persoonsgegevens Financiële Instellingen. Het addendum bevat onder meer regels met betrekking tot de omgang met declaratiegegevens en het uitvoeren van materiële controle op de declaraties.

Intensief overleg tussen ZN, het ministerie van VWS, de artsenfederatie KNMG en de Nederlandse Patiënten Consumenten Federatie (NPCF) en het CBP heeft eind 2005 geleid tot overeenstemming over de inhoud van dit addendum. In april 2006 is de goedkeurende verklaring van het CBP ex artikel 25 WBP voor het Addendum gegeven.

Diagnose behandeling combinatie en DBC-informatiesysteem

De afspraak met het ministerie van VWS en Zorgverzekeraars Nederland om de Diagnose Behandeling Combinaties (DBC's) minder gedetailleerd en zo minder privacygevoelig te maken, bleek in 2005 helaas niet meer op de agenda te staan. Dit betekent dat vanaf 2006 DBC's met gedetailleerde informatie die onder het medisch beroepsgeheim valt, door zorgverleners in ziekenhuizen aan zorgverzekeraars zullen worden verstrekt. Het ministerie heeft het CBP de toezegging gedaan om de komende jaren tot een vereenvoudiging van de DBC-systematiek te komen.

Met de minister van VWS zijn afspraken gemaakt over de inzet van Privacy Enhancing Technologies (PET) bij het gebruik van gegevens in het DBC-informatiesysteem (DIS). Het DIS is een grote databank, een landelijk knooppunt voor het ontvangen, verwerken en verstrekken van gegevens die worden aangeleverd door ziekenhuizen en medisch specialisten. Door deze technische oplossing in te zetten kan de identiteit van de individuen achter de gegevens onbekend blijven. Dit neemt niet weg dat het DIS wat betreft omvang, dekking en inhoud een van de meest risicovolle verwerkingen in Nederland zal zijn.

Geestelijke gezondheidszorg

Per 2007 zal een groot deel van de geestelijke gezondheidszorg (GGZ) worden vergoed via de Zorgverzekeringswet (Zvw). Nu valt de GGZ nog onder de Algemene wet bijzondere ziektekosten (AWBZ). De bedoeling is om de 'op genezing gerichte' geestelijke gezondheidszorg onder de Zvw te brengen. Per 2007 zullen daarom ook DBC's worden ingevoerd in de GGZ. In overleg met de beroepsgroep heeft het CBP in 2005 nadrukkelijk aandacht gevraagd voor het belang van de bescherming van persoonsgegevens op dit terrein.

Wet gebruik burgerservicenummer in de zorg

Het huidige sofinummer zal onder de naam burgerservicenummer (BSN) vanaf de inwerkingtreding van de Wet algemene bepalingen burgerservicenummer worden gebruikt door en voor alle communicatie met de (semi-)overheid. De Wet gebruik BSN in de zorg bepaalt dat zorgaanbieders, ziektekostenverzekeraars en indicatieorganen het BSN zullen moeten gebruiken in hun onderlinge communicatie over patiënten. Het BSN zal in de toekomst ook worden gebruikt om het Elektronisch Medicatiedossier en het Elektronisch Patiëntendossier mogelijk te maken. Het CBP was zeer kritisch over dit conceptwetsvoorstel. De invoering van een dergelijk uniek identificerend nummer brengt grote risico's met zich mee, risico's die in ieder geval beperkt moeten worden. Het wetsvoorstel dat uiteindelijk aan de Tweede Kamer is voorgelegd, schiet op dit punt te kort.

Terrorisme en veiligheid

Vanwege de toename van plannen en maatregelen op Europees niveau voor veiligheid en criminaliteits- en terrorismebestrijding, zal de uitwisseling van gegevens van verdachte en onverdachte personen tussen de lidstaten van de EU steeds groter worden. Daarom neemt ook het belang toe van een geharmoniseerd en adequaat raamwerk voor de bescherming van persoonsgegevens voor de internationale uitwisseling van gegevens op het terrein van justitie en binnenlandse zaken, de zogenaamde derde pijler van de Europese Unie.

Toezichthouder voor de derde pijler

De voorjaarsconferentie van Europese privacytoezichthouders in Krakow in april 2005 betuigde zijn instemming met het plan van de Europese Commissie om een nieuw juridisch kader voor gegevensbescherming in de derde pijler te ontwikkelen. Het hoge beschermingsniveau van de algemene privacyrichtlijn 95/46/EG zou daarbij het uitgangspunt moeten zijn. Tevens werd gepleit voor een onafhankelijk toezicht- en adviesorgaan, waarin de privacytoezichthouders zouden samenwerken. Nu het Constitutioneel Verdrag niet is aangenomen, blijft de pijlerstructuur van de Europese Unie voorlopig bestaan. Daarom is naast de Artikel 29-werkgroep voor de eerste pijler ook voor de derde pijler een dergelijk orgaan noodzakelijk. In de loop van het 2005 hebben de Europese privacytoezichthouders een gedetailleerder advies opgesteld, dat begin 2006 aangeboden is aan de Europese Raad en de Europese Commissie.

Den Haag-programma

Het zogenaamde Den Haag-programma, een meerjarig programma vastgesteld onder het Nederlandse voorzitterschap van de Europese Unie in de tweede helft van 2004, bevat voorstellen met het oog op de strijd tegen terrorisme en grensoverschrijdende criminaliteit, zowel op het terrein van de derde pijler, justitie en binnenlandse zaken, als de eerste pijler van de EU, de interne markt.

De belangrijkste voorstellen in 2005 behelsden het kaderbesluit gegevensbescherming in de derde pijler, de verdere ontwikkeling van bestaande Europese informatiesystemen, het zorgen voor betere interoperabiliteit en synergie tussen Europese databanken, introductie van biometrie in paspoorten en de centrale opslag van onder andere visuminformatie. Daarnaast kwam de richtlijn tot stand met de bewaarplicht voor verkeersgegevens van telecommunicatie.

Verstrekkend was het voorstel voor een kaderbesluit over het principe van de beschikbaarheid van politiegegevens op grond waarvan meer gegevens van politie en justitie tussen lidstaten uitgewisseld kunnen worden. Handhavingsinformatie die beschikbaar is in één lidstaat zou zo direct beschikbaar worden voor de andere lidstaten. De Europese privacytoezichthouders hebben in 2005 in Wroclaw verklaard dat het principe van beschikbaarheid van handhavingsinformatie alleen zou mogen worden ingevoerd indien er ook een geharmoniseerd en adequaat kader voor gegevensbescherming in de gehele EU is.

Bevoegdheden opsporing terroristische misdrijven

In 2004 heeft het CBP geadviseerd over het conceptwetsvoorstel ter verruiming van de mogelijkheden ter opsporing van terroristische misdrijven. Dit advies is op veel punten niet gevolgd. In 2005 heeft het CBP zijn kritiek daarom onder de aandacht gebracht van de vaste commissie voor Justitie van de Tweede Kamer.

Het wetsvoorstel beoogt de politie in staat te stellen alle mogelijke aanwijzingen voor terrorisme te onderzoeken. Naar het oordeel van het CBP is dat de exclusieve taak van de AIVD, omdat de AIVD bij uitstek is toegerust voor die taak en omdat het

inlichtingenwerk van de AIVD sterk is afgeschermd. Als de politie dergelijke vergaande bevoegdheden al moet krijgen, zal ook voorzien moeten worden in passende waarborgen. Het wetsvoorstel schiet daarin tekort omdat de klassieke strafvorderlijke waarborgen als transparantie en rechterlijke controle vanuit het oogpunt van gegevensbescherming niet effectief zijn. Aan de mogelijk negatieve effecten van het voorstel voor de maatschappelijke positie van onschuldige burgers is vrijwel geheel voorbijgegaan. Het CBP heeft daarom geadviseerd een apart, sterk afgeschermd, eigen regime te creëren voor de verwerking van 'zachte' inlichtingen door de politie.

Contraterrorisme-Infobox

In 2005 heeft het CBP op verzoek van de Tweede Kamer de opzet van de Contraterrorisme-Infobox (CT Infobox) geanalyseerd. Deze CT Infobox beoogt praktische uitvoering te geven aan bestaande wettelijke mogelijkheden tot uitwisseling van gegevens over terrorisme. Een eerste analyse door het CBP heeft geleid tot verduidelijking door de minister. Nadere analyse hiervan liet zien dat in ieder geval de deelname van de IND niet conform de wet is. Ook dient de grens tussen inlichtingenwerk en opsporing te worden gerespecteerd. Het kan legitiem zijn die grens te overschrijden, maar daarbij dient duidelijk gemarkeerd te blijven waar het inlichtingenwerk overgaat in de opsporing en vervolging van strafbare feiten. Bovendien moet voorzien zijn in effectief toezicht.

Wetsvoorstel bevoegdheden vorderen gegevens

Op 1 januari 2006 is na een jaren durend voortraject de Wet bevoegdheden vorderen gegevens in werking getreden. Het wetsvoorstel is gebaseerd op de voorstellen van de Commissie strafvorderlijke gegevensvergaring (Commissie Mevis). De wet maakt het voor justitie en politie mogelijk om persoonsgegevens op te vragen bij maatschappelijke instellingen en bedrijven als dat voor de opsporing noodzakelijk is. Begin 2005 heeft de vaste commissie voor Justitie van de Eerste Kamer het CBP uitgenodigd voor een gesprek in het kader van de voorbereiding van de behandeling van het Wetsvoorstel bevoegdheden vorderen gegevens. Het CBP heeft gepleit voor twee structurele waarborgen: de mogelijkheid van een voorafgaande toetsing van een vordering door de rechter en een systematische en regelmatige controle op de verwerking van gegevens in de politieregisters.

Bewaarplicht verkeersgegevens

Het CBP heeft zich in 2005 met kracht verzet tegen de introductie van een algemene bewaarplicht voor de zogenaamde verkeersgegevens van telecommunicatie. Nut noch noodzaak van een dergelijke massale, preventieve opslag van telecommunicatiegegevens van alle 450 miljoen Europese burgers waren aangetoond. Specifieke waarborgen ontbraken. Zowel op nationaal als op Europees niveau was er breed gedragen politieke kritiek op het voornemen van de Europese ministers van Justitie en Binnenlandse Zaken de bewaarplicht in een kaderbesluit te regelen. Dit politieke verzet kaliede in de loop van het jaar af.

CIOT

Aanbieders van vaste en mobiele telefonie – en op termijn ook aanbieders van internet – zijn verplicht een supertelefoongids beschikbaar te houden voor raadpleging door politie, justitie en de inlichtingendiensten. Het Centraal Informatiepunt Opsporing Telecommunicatie (CIOT) in Zoetermeer valt onder het ministerie van Justitie en fungeert als doorgeefluik tussen telefoniesector en de autoriteiten. Veel telecoaanbieders laten hun bestand ook beheren door het CIOT. Op aandrang van het CBP werd een bewerkersovereenkomst serieus ter hand genomen in onderhandelingen tussen telecommunicatieaanbieders en CIOT. Ook is een auditovereenkomst tot stand gebracht.

Periodiek zal nu daadwerkelijk gecontroleerd worden of politie en justitie uitsluitend gegevens verkrijgen die op rechtmatige wijze zijn gevorderd. Beide overeenkomsten waren in januari 2006 gereed voor ondertekening door overheid en telecombedrijven.

Fraudebestrijding

Zwarte lijsten

Waarschuwinglijsten als middel ter bestrijding van fraude en criminaliteit bleven in 2005 populair. Bij de beoordeling van de rechtmatigheid van een dergelijke lijst laat het CBP zwaar meewegen of het voorstel van de verantwoordelijke voldoende waarborgen biedt voor een zorgvuldige gegevensverwerking. Deze waarborgen vloeien voort uit de afweging van het belang van de organisatie en het privacybelang van de betrokkene. De Kamers van Koophandel hebben in 2005 een waarschuwinglijst ter beoordeling voorgelegd die bedoeld is om fraude door advertentieverkoop, loterijen en ongevraagde leveringen te signaleren. De omvang van de fraude via spooknota's en acquisitiefraude brachten het Steunpunt Acquisitiefraude (SAF) er toe een waarschuwinglijst in het leven te roepen. Het SAF verzamelt gegevens en geeft meldingen op het gebied van

Biometrie in het paspoort

Paspoorten moeten veilig zijn en betrouwbare identificatie van reizigers mogelijk maken. Wat ligt er dan meer voor de hand dan het paspoort te voorzien van unieke lichaamskenmerken van de drager? Biometrische kenmerken – een digitale gezichtsfoto en vingerafdrukken – kunnen het paspoort veilig maken, zo is de gedachte. Nadat er in EU-verband afspraken zijn gemaakt over het opslaan van biometrische gegevens op reisdocumenten, zijn er in 2005 bovendien weer voorstellen gepresenteerd voor nationale centrale opslag van dergelijke gegevens.

De technologische aspecten van het op grote schaal toepassen van biometrie worden echter nauwelijks besproken. Bij het verzamelen en gebruiken van biometrische gegevens bestaan altijd foutmarges. Dat wil zeggen dat het technische systeem aan de hand van het biometrisch kenmerk op het paspoort ten onrechte besluit dat document en reiziger niet of juist wel bij elkaar horen. De grootte van de fout is afhankelijk van de soort biometrie en van de kenmerken van de groep personen om wie het gaat. Wanneer het gaat om controle op vele miljoenen reizigers, leidt een foutmarge van enkele procenten al tot zeer veel probleemgevallen.

Bij invoering van biometrie op het paspoort zal dit probleem zich direct doen gelden. Het gaat dus niet alleen om principiële of langetermijnkwesties. Nu geclaimd wordt dat de landelijke inzet van biometrie om zwaarwichtige redenen nodig is, dreigen er ernstige effecten voor burgers die niet voldoen aan de door machines gestelde eisen, hetzij door tekortkomingen in de omgang met biometrische gegevens, hetzij vanwege de foutmarges die eigen zijn aan biometrie.

De privacyaspecten van het grootschalige gebruik van biometrische gegevens zijn in 2004 naar voren gebracht in adviezen van de Artikel 29-werkgroep over de ontwikkeling van visumsystemen waarin ook sprake is van een gecentraliseerde opslag van biometrische gegevens. In 2005 heeft de Artikel 29-werkgroep advies uitgebracht over de implementatie van de Europese verordening om paspoorten te voorzien van vingerafdrukken. De werkgroep herhaalde haar bezwaar tegen de invoering van vingerafdrukken en tegen een eventuele Europese centrale database met de paspoortgegevens. Verder werd gewaarschuwd voor de veiligheidsrisico's bij invoering van biometrie op een RFID-chip ●

vermoedelijke acquisitiefraude en van verzenders van spooknota's door aan opsporings- en vervolgingsinstanties. Het Centraal Bureau Levensmiddelenhandel (CBL) wilde voor deelnemende organisaties een winkelwaarschuwingsregister beheren. Hiermee zou moeten worden voorkomen dat deelnemende winkels eveneens de dupe worden van criminele incidenten die al bij andere deelnemers zijn voorgevallen.

Koppeling van bestanden bij fraudebestrijding

De grotere belangstelling voor uitkeringsfraude bij gemeenten weerspiegelt het gewijzigde maatschappelijke klimaat rond uitkeringen en vloeit direct voort uit het financiële belang dat gemeenten hebben bij een effectieve controle op de uitvoering van de Wet werk en bijstand. Medio 2005 heeft de staatssecretaris de gemeenten geïnformeerd over de mogelijkheden om bestanden te koppelen voor fraudebestrijding.

Om recht te doen aan het belang van een effectieve fraudebestrijding en aan het belang van de bescherming van de persoonlijke levenssfeer van uitkeringsgerechtigden heeft het CBP in het najaar van 2005 de notitie *Fraudebestrijding door bestandskoppeling* aan de staatssecretaris van Sociale Zaken en Werkgelegenheid gestuurd.

Controle via ontsluiting en koppeling van bestanden betekent veelal dat persoonsgegevens gebruikt worden voor een ander doel dan waarvoor de burger mocht verwachten dat de gegevens gebruikt zouden worden. Al te gemakkelijke koppeling van bestanden met gegevens van grote groepen onverdachte burgers acht het CBP buiten verhouding en onwenselijk. Uitgangspunt voor fraudebestrijding door bestandsontsluiting en -koppeling moet zijn dat de controlemogelijkheden ten aanzien van een individuele uitkeringsgerechtigde mogen toenemen naarmate er een sterker vermoeden van fraude aanwezig is, een methodiek die vergelijkbaar is met die van de Belastingdienst. In december 2005 informeerde de staatssecretaris de Tweede Kamer over de elektronische ontsluiting van een aantal bestanden voor de gemeenten. De staatssecretaris heeft daarbij de visie van het CBP op bestandsontsluiting en -koppeling een "helder kader voor besluitvorming" door gemeenten genoemd.

Informatie-infrastructuur

De informatie-infrastructuur van de overheid ondergaat een ingrijpende verbouwing die de komende twee jaar zijn beslag zal krijgen. Zorgelijk is dat een overkoepelende visie op het persoonsinformatiebeleid ontbreekt. Een kamerdebat over het totale persoonsinformatiebeleid heeft hierdoor nog niet kunnen plaatsvinden.

Burgerservicenummer

In 2005 is het Wetsvoorstel algemene bepalingen burgerservicenummer (Wabb) ingediend bij de Tweede Kamer. Het wetsvoorstel introduceert het gebruik van het burgerservicenummer (BSN) als algemeen persoonsnummer door de overheid. Het wetsvoorstel gaat in op het genereren, distribueren, toekennen en beheren van de nummers. Het voorstel voorziet echter niet in een regeling die ertoe bijdraagt dat in de praktijk zorgvuldig met het BSN wordt omgegaan. Het CBP wees hier al op in zijn advies over het wetsvoorstel uit 2004.

Aangezien in het wetsvoorstel naar het oordeel van het CBP onvoldoende met dit bezwaar rekening gehouden was, heeft het CBP in oktober 2005 bij de Tweede Kamer zijn zorgen hierover geuit. Het CBP waarschuwt dat het voorstel voor de Wet algemene bepalingen burgerservicenummer ernstig tekortschiet als het gaat om de beperking van de risico's verbonden aan invoering en gebruik van een dergelijk nummer. De fracties in de Tweede Kamer hebben over de punten die door het CBP naar voren zijn gebracht,

Doelen 2006

IN 2006 ZULLEN MET NAME DE VOLGENDE RESULTATEN WORDEN

NAGESTREEFD:

- **Zorgverzekeraars in heel Europa onderzocht**

Het CBP is in 2005 een van de initiatiefnemers geweest voor het uitvoeren van een gezamenlijke handhavingsactie door alle EU-privacytoezichthouders. In 2006 zullen gezamenlijk afgestemde handhavingsonderzoeken worden uitgevoerd bij zorgverzekeraars. De uitkomsten van de onderzoeken zullen worden gebundeld in een gezamenlijk uit te brengen rapport.

- **Informatiebeveiliging van ziekenhuizen**

In 2005 is veel publiciteit geweest over de informatiebeveiliging in ziekenhuizen. De Inspectie voor de Gezondheidszorg (IGZ) heeft in 2003 het onderzoek 'ICT in ziekenhuizen' uitgevoerd. In 2006 zullen het CBP en de IGZ in vervolg hierop gezamenlijk een onderzoek uitvoeren naar de informatiebeveiliging in ziekenhuizen.

- **Elektronisch Kinddossier**

Het voornemen bestaat om per 1 januari 2007 het elektronisch kinddossier in de jeugdgezondheidszorg in te voeren. Dit legt vanaf (voor) de geboorte de ontwikkeling van een kind en de kenmerken uit zijn omgeving vast. Het kinddossier zal worden gekoppeld aan het toekomstige burgerservicenummer. Het CBP zal in 2006 deze ontwikkeling intensief volgen en zo nodig adviseren.

- **Interventieteams voor fraudebestrijding**

Er is een landelijk dekkend netwerk van interventieteams dat in heel Nederland zwart werk, illegale arbeid, sociale zekerheidsfraude en fiscale fraude aanpakt. In deze teams werken gemeenten, Belastingdienst, Sociale Verzekeringsbank, Arbeidsinspectie, Uitvoeringsinstituut Werknemersverzekeringen en het Openbaar Ministerie samen. In 2006 zal het CBP onderzoek doen naar het naleven van de informatieplicht evenals naar de rechtmatigheid van het informatiedelen en het gebruik van politie-informatie door interventieteams.

- **Fraudebestrijding in de sociale zekerheid**

Om fraude in de sociale zekerheid te bestrijden worden veel voorstellen gedaan die allemaal in meer of mindere mate een inbreuk maken op de persoonlijke levenssfeer van mensen die een uitkering ontvangen. Gemeenten vragen toegang tot steeds meer bestanden van uiteenlopende organisaties. Het CBP zal in 2006 een expertmeeting organiseren over een duidelijker systematiek bij het bestrijden van deze fraude. Uitkeringsgerechtigden dienen niet meer 'verdacht' te zijn dan andere burgers. Verder zal in 2006 de naleving van de informatieplicht door sociale recherche worden onderzocht.

- **Administratieve lasten en privacy: Binding Corporate Rules**

In 2006 zal het CBP de vergunningaanvragen behandelen en coördineren van enkele grote multinationals volgens de nieuwe uniforme procedure voor het aanvragen van vergunningen voor doorgifte van persoonsgegevens naar landen buiten de Europese Unie en voor de gecoördineerde Europese afhandeling hiervan.

- **De plicht om burgers te informeren**

Eind 2005 is door TNS/NIPO in vijf branches een onderzoek uitgevoerd naar de naleving van de informatieplicht op grond van de WBP en een onderzoek naar de naleving van de informatieplicht zoals burgers die ervaren. De resultaten zullen begin 2006 gepubliceerd worden. In 2006 zal het onderzoek leiden tot actie in de verschillende branches gericht op bekendheid met en naleving van de informatieplicht.

- **Internetpublicaties en privacy**

Het internet confronteert gebruikers met vragen over hun privacy en de veiligheid van hun persoonsgegevens. Internet stelt het CBP voor vragen over zijn bevoegdheid als toezichthouder en de mogelijkheid van effectief toezicht op internet. In 2006 zal het CBP hierover een symposium organiseren en daarnaast een eerste position paper en enkele informatiebladen publiceren.

- **RFID en privacy**

Radio Frequency Identification is een technologie waarmee allerhande voorwerpen voorzien kunnen worden van kleine, uitleesbare zogenaamde tags (minuscule radiochips). Wat de chip aan informatie geeft over het voorwerp en wat de opvraager van de informatie vervolgens met de gegevens kan en mag doen raakt ook de bescherming van persoonsgegevens. In 2006 zal hiervan een publieke consultatieronde worden gehouden uitmondend in een extern rapport.

- **Biometrie in reisdocumenten**

In 2006 wordt uitbreiding verwacht in het gebruik van biometrie in reisdocumenten. Het CBP zal een expertmeeting organiseren over de vraag naar nut, noodzaak en eventuele nadelen van grootschalige gecentraliseerde opslag van biometrische gegevens.

- **Burgerservicenummer (BSN)**

De invoering van het burgerservicenummer en het gebruik van dit nummer in de zorg is uitgesteld. In vervolg op zijn brieven naar de Tweede Kamer over dit onderwerp van oktober 2005 en januari 2006 zal het CBP de invoering blijven volgen en waar nodig de ministers en/of de Kamers adviseren.

- **Veiligheid en privacy**

In samenwerking met de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie heeft het CBP prof.mr. H.R.B.M. Kummeling en prof.mr.dr. E.R. Muller gevraagd onderzoek te doen naar een goede balans tussen 'veiligheid' en 'privacy'. Het CBP zal in het voorjaar van 2006 hierover een congres organiseren.



Verpakkingsmanagement, augustus 2005

Het CBP acht het van groot belang voor de burger, de bescherming van diens persoonsgegevens en de maatschappelijke aanvaardbaarheid van de invoering van het burgerservicenummer, dat duidelijk wettelijk geregeld wordt: a) onder welke voorwaarden het BSN gebruikt mag worden; b) welke overheidsinstanties (en eventueel bedrijven) gebruik mogen maken van het BSN; c) dat vastgestelde vergissingen en fouten aan de burger gemeld worden; d) dat er een effectieve ombudsfunctie voor de burger komt; en e) dat er eisen worden gesteld aan de ICT-beveiliging van bestanden, die gebruik maken van het BSN.

Stroomlijning basisgegevens

In het programma stroomlijning basisgegevens dat medio 2004 een herstart heeft gekregen, wordt de ontwikkeling van voorlopig zes basisregistraties (personen, gebouwen, adressen, Kadaster, topografie en bedrijven) beoogd. Daarnaast bestaat het voornemen om ook de zogenaamde polisadministratie (de administratie van de werknemersverzekeringen), het kentekenregister en de inkomensadministratie van de Belastingdienst aan te wijzen als basisadministraties. Kerngegevens in deze basisregistraties zullen verplicht door de overheid worden gebruikt en mogen niet meer worden opgevraagd van de burger of het bedrijf, het zogenaamde beginsel van eenmalige gegevensverstrekking en verplicht hergebruik. De invoering van het BSN en het daarbij behorende stelsel staat hiermee in nauwe relatie.

In 2005 heeft het CBP over drie wetsvoorstellen van dit programma geadviseerd, namelijk het Wetsvoorstel register van ondernemingen en instellingen (vervanging van de huidige Handelsregisterwet), het Wetsvoorstel basisregistratie kadaster en geografie

OV-chipkaart

In het openbaar vervoer zal de OV-chipkaart worden geïntroduceerd, één kaart voor het gehele openbaar vervoer.

Op de kaart kan een saldo in euro's worden geladen, maar ook een enkele reis, retour of abonnement. De op afstand uitleesbare kaart met het formaat van een bankpas is voorzien van een chip. De kaart moet het reizen gemakkelijker maken, zwartrijden tegengaan en de weg openen voor nieuwe diensten voor reizigers. Omdat de kaart bovendien dient als 'toegangssleutel' tot stations, kan de introductie ervan bijdragen aan het terugdringen van overlast op persons en in trein, tram, bus en metro.

Een mooie vinding, handig voor iedereen? Zeker, maar wel met een paar privacykanten om goed over na te denken.

Het CBP heeft zich in 2005 uitgebreid laten informeren over de werking van het OV-chipkaartsysteem. Met de NS en TransLink Systems BV (TLS), de belangrijkste betrokken partijen, werd regelmatig overleg gevoerd over de effecten die gebruik van de kaart kan hebben voor de persoonlijke levenssfeer. In de gesprekken met de NS, TLS en ook in de twee bijeenkomsten die het CBP heeft belegd met de openbaarvervoerbedrijven, het ministerie van Verkeer en Waterstaat en organisaties zoals de Consumentenbond, de ANWB en ROVER zijn de zienswijzen van de diverse deel-

nemers uitgebreid aan bod gekomen. Besproken is onder meer hoe techniek, bedrijfsvoering en privacyaspecten met elkaar te verenigen zijn.

Begin 2006 publiceerde het CBP zijn standpunt inzake de voorgenomen implementatie van het OV-chipkaartsysteem. Bij de realisatie van het OV-chipkaartsysteem moet rekening gehouden worden met de eisen die door de WBP gesteld worden. In het plan zouden tot dan toe de gegevens over individuele gebruikers van een op naam gestelde OV-chipkaart en over hun reisgedrag ter beschikking komen van vervoerders, ook in gevallen waarin het gebruik van deze gegevens niet is toegestaan.

De bezwaren van het CBP spitsen zich toe op het gebruik van gedetailleerde, tot een persoon herleidbare reisgegevens voor onder meer marketingdoelen. Voor een dergelijk gebruik dienen de betrokken reizigers toestemming te geven. Het CBP realiseert zich dat nog niet alle beslissingen rond de inrichting van het OV chipkaartsysteem definitief zijn. Juist daarom wijst het tijdig op de noodzaak het systeem zó in te richten dat het functioneert in overeenstemming met de eisen van de privacywetgeving ●

(een vernieuwde Kadasterwet) en een wijziging van de Wet gemeentelijke basisadministratie persoonsgegevens. In deze wetsvoorstellen wordt het verplichte gebruik van bepaalde gegevens door de overheid voorgeschreven. Daarbij is nauw aangesloten bij het regime van de al bestaande regelgeving.

Informatiehuishouding politie

De huidige Wet politieregisters wordt integraal herzien. Het CBP heeft in 2004 de minister van Justitie geadviseerd over het conceptvoorstel Wet politiegegevens. Het CBP stemde in met de structuur voor de verwerking van politiegegevens binnen de politie maar kritiseerde het voorstel op onderdelen.

Eind 2005 heeft het CBP de vaste commissie voor Justitie van de Tweede Kamer geïnformeerd over zijn kritiek op het uiteindelijke wetsvoorstel omdat het advies op essentiële punten niet gevolgd is: a) gegevens worden niet voorzien van een code die de betrouwbaarheid (het onderscheid tussen zachte en harde informatie) en afbreukrisico aangeeft, b) er zijn onvoldoende waarborgen aangebracht tegen derdenverstrekkingen van gegevens met een geringe betrouwbaarheid, c) er zijn geen extra waarborgen geschapen bij gegevens over onverdachte personen en d) een te ruime verzameling van gegevens over onverdachte personen is mogelijk gemaakt. Verder is het noodzakelijk de auditverplichting voor de informatiehuishouding van de politie, waarin ook een verplichting tot zelfevaluatie is opgenomen, wettelijk te verankeren.

Schengen Informatiesysteem II

Het CBP was ook in 2005 voorzitter van de Gemeenschappelijke Controleautoriteit (GCA) Schengen. De belangrijkste ontwikkeling bleef de ontwikkeling van het Schengen Informatiesysteem (SIS) II. Het bestaande Schengen Informatiesysteem is ontoereikend voor uitbreiding naar de nieuwe lidstaten en kan geen biometrische gegevens bevatten. In vervolg op het advies over SIS II van 2004 adviseerde de GCA Schengen in oktober 2005 over het door de Europese Commissie voorgestelde juridische kader voor het nieuwe informatiesysteem. De GCA heeft enkele fundamentele bezwaren tegen de voorgestelde juridische grondslag. Het is niet duidelijk onder welke Europese juridische kaders SIS II zal komen te vallen en wie daarvoor bevoegd zal zijn. Het doel van de gegevensverwerking wordt onvoldoende specifiek gedefinieerd waardoor de rechtsgrondslag niet voldoet aan de grondbeginselen van gegevensbescherming. Verder is het toezicht door de nationale en de Europese toezichthouders onvoldoende geregeld. De rol van de Europese Commissie, de European Data Protection Supervisor (EDPS) en de nationale privacytoezichthouders blijven in het voorstel onduidelijk. Alle huidige taken van de GCA dienen opnieuw belegd te worden in de nieuwe toezichtstructuur.

Europees visuminformatiesysteem

De Artikel 29-werkgroep heeft in 2005 een opinie uitgebracht over het voorstel om een Europees visuminformatiesysteem (VIS) op te zetten dat de uitwisseling van visumgegevens mogelijk maakt tussen lidstaten die de binnengrenscontroles hebben afgeschaft. Geen enkel Europees systeem is qua omvang en capaciteit met het VIS vergelijkbaar. Er zullen persoonsgegevens, waaronder biometrische gegevens, van miljoenen mensen in een centrale gegevensbank worden opgeslagen en tussen staten worden uitgewisseld. Het voorstel maakt ruime toegang tot het VIS mogelijk voor brede doeleinden. De werkgroep heeft daarom geadviseerd het doel waarvoor gegevens worden verwerkt in het VIS nauwkeurig te omschrijven en te beperken tot wat nodig is om het gemeenschappelijke visumbeleid te verbeteren. De systematische toegang moet worden beperkt tot de autoriteiten die het visumbeleid uitvoeren. Het doel waarvoor de verschillende Europese systemen zijn ontwikkeld, mag niet uit het oog worden verloren. Het streven de interoperabiliteit tussen Europese databanken als het VIS, het SIS II en

Eurodac te verbeteren, mag er niet toe leiden dat autoriteiten toch toegang hebben tot gegevens die zij niet mogen gebruiken.

Onderzoek en toezicht

De naleving van de informatieplicht door overheden, bedrijven en andere organisaties heeft in 2005 bijzondere aandacht gekregen. De voorlichting hierover is versterkt en er zijn enkele onderzoeken naar de naleving van de informatieplicht gestart die in 2006 zullen worden gepubliceerd. De informatieplicht is een essentiële voorwaarde voor burgers om hun recht van inzage en correctie te kunnen uitoefenen ter behartiging van hun belangen. TNS-NIPO Consult heeft in opdracht van het CBP onderzoek gedaan naar de informatieplicht in drie sectoren: bij huisartsen, onderwijsinstellingen en woningbouwcorporaties. Ook is een representatieve enquête onder burgers gehouden naar hun opvattingen over de waarde van de informatieplicht en hun ervaringen met de manier waarop verantwoordelijken hen informeren over de verwerking van hun persoonsgegevens. Opnieuw bleek een tekort in het vertrouwen van burgers in de wijze waarop met hun gegevens wordt omgegaan.

Particuliere recherche

In 2005 zijn twee onderzoeken gedaan bij particuliere recherchebureaus. Bij de beoordeling van de naleving van de WBP is ook de Privacygedragscode voor particuliere onderzoeksbureaus betrokken, die sinds 13 januari 2004 van kracht is. De minister van Justitie stelde per 1 juni 2004 het naleven van deze gedragscode voor alle particuliere recherchebureaus verplicht als voorwaarde voor een vergunning. Het CBP-onderzoek is het eerste sinds de regulering van de branche.

Eén onderzoek betrof de naleving van de informatieplicht. Hiervoor zijn in een steekproef dertig bureaus benaderd met een enquête om een beeld te krijgen van de mate en de wijze van naleving van de informatieplicht. Het tweede onderzoek bestond uit verdiepende onderzoeken ter plaatse bij een drietal recherchebureaus. Hierbij werden naast de naleving van de informatieplicht ook diverse andere aspecten van de WBP getoetst, zoals het naleven van de bewaartermijn voor gegevens. De resultaten zullen in 2006 worden gepubliceerd.

Onderzoek bij zorgverzekeraars

In het voorjaar van 2005 heeft het CBP een onderzoek uitgevoerd bij een drietal zorgverzekeraars. Het doel was om een beeld te krijgen van de verwerkingen van persoonsgegevens die bij zorgverzekeraars plaatsvinden en de eventuele problemen. Het onderzoek werd ook uitgevoerd met het oog op de beoordeling van het Addendum Zorgverzekeraars.

Het Europese werkprogramma ter verbetering van de implementatie van de Privacyrichtlijn heeft onder meer als doel het versterken van de handhaving. De Artikel 29-werkgroep heeft in 2005 besloten dat het eerste gemeenschappelijke onderzoek van de nationale toezichthouders zich zal richten op de zorgverzekeraars. Het doel van het onderzoek is na te gaan of en hoe in de verschillende landen de privacyregels in deze sector worden nageleefd. Het onderzoek zal in 2006 van start gaan.

Onderzoek bij reïntegratiebedrijven

Bij zes reïntegratiebedrijven heeft het CBP een verkennend onderzoek uitgevoerd naar de uitvoeringspraktijk bij reïntegratie van bijstandsgerechtigden en zieke werknemers. De onderzoeksrapporten zijn op 12 december 2005 aangeboden aan Borea, de Brancheorganisatie Reïntegratiebedrijven.

De conclusie van het onderzoek naar reïntegratie van bijstandsgerechtigden was dat de manier waarop reïntegratiebedrijven persoonsgegevens verwerken voor een groot deel bepaald wordt door de opdrachtgevers, de gemeenten. Gemeenten lijken als opdrachtgever meer gegevens in de rapportages over bijstandsgerechtigden te verlangen dan noodzakelijk is.

Het onderzoek naar reïntegratie van zieke werknemers bevestigde de verwachting dat reïntegratiebedrijven ook in de praktijk last hebben van een lacune in de wetgeving voor arbeid. Er is onvoldoende wettelijke basis om te rapporteren over de mogelijkheden van werkhervatting en de mate waarin zieke werknemers hieraan meewerken. Binnen de huidige regelgeving hebben reïntegratiebedrijven geen mogelijkheid medische gegevens rechtmatig te rapporteren aan werkgever of arbodienst.

Onderzoek vernietiging van getapte advocatengesprekken

In 2005 is onderzoek gedaan naar de naleving van de regels voor de vernietiging van opgenomen telefoongesprekken van advocaten met hun cliënten. Op grond van het Wetboek van Strafvordering moeten deze gesprekken, die vallen onder het beroepsgeheim van advocaten, vernietigd worden. Het CBP heeft steekproefsgewijs onderzocht of gesprekken die vernietigd moesten worden, ook daadwerkelijk vernietigd zijn. Dit onderzoek zal in 2006 worden afgerond en gepubliceerd.

Onderzoek bij Europol

Het CBP heeft in 2005 de verwerking van persoonsgegevens door de Dutch Desk van Europol onderzocht. Europol is de Europese politiedienst voor bestrijding van grensoverschrijdende zware, georganiseerde criminaliteit. Elke bij de Europol-overeenkomst aangesloten lidstaat beschikt over een nationaal contactpunt voor informatieuitwisseling met Europol en de andere aangesloten lidstaten. De Nederlandse afdeling, de Dutch Desk, is organisatorisch ondergebracht bij het Korps Landelijke Politiediensten (KLPD). Uit het onderzoek is een positief beeld naar voren gekomen van de wijze waarop de gegevensverwerking plaatsvindt.

Het CBP heeft in 2005 ook deelgenomen aan de jaarlijkse audit van de Europol-systemen door het Gemeenschappelijk Controleorgaan van Europol. Uit de jaarlijkse controles blijkt telkens weer het grote belang van een behoorlijke kwaliteit van de door de lidstaten aangeleverde gegevens. Bij de audit van 2005 is tevens het nieuw ontwikkelde Informatie Systeem van Europol aan een onderzoek onderworpen.

Uitwisseling politiegegevens met de Antillen

Snelle en zorgvuldige uitwisseling van politiegegevens tussen de Nederlandse Antillen en Nederland is belangrijk voor de bestrijding van criminaliteit. Om een dergelijke gegevensuitwisseling mogelijk te maken hebben de minister van Justitie, de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie van de Nederlandse Antillen het Protocol gegevensuitwisseling tussen de Nederlandse Antillen en Nederland opgesteld en ondertekend. Het CBP houdt toezicht op de uitwisseling van gegevens vanuit Nederland met de Antillen en het gebruikte systeem. Met de betrokken ministers is destijds de afspraak gemaakt dat het CBP ter plaatse zou vaststellen hoe de uitwisseling van gegevens verloopt en of het protocol wordt nageleefd. Dit onderzoek heeft in het najaar van 2005 plaatsgevonden en wordt in 2006 gepubliceerd.