



Het CBP in 2009





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

Het College bescherming persoonsgegevens (CBP) houdt toezicht op de naleving van de wettelijke regels die zien op de bescherming van persoonsgegevens, zo nodig met behulp van sancties.

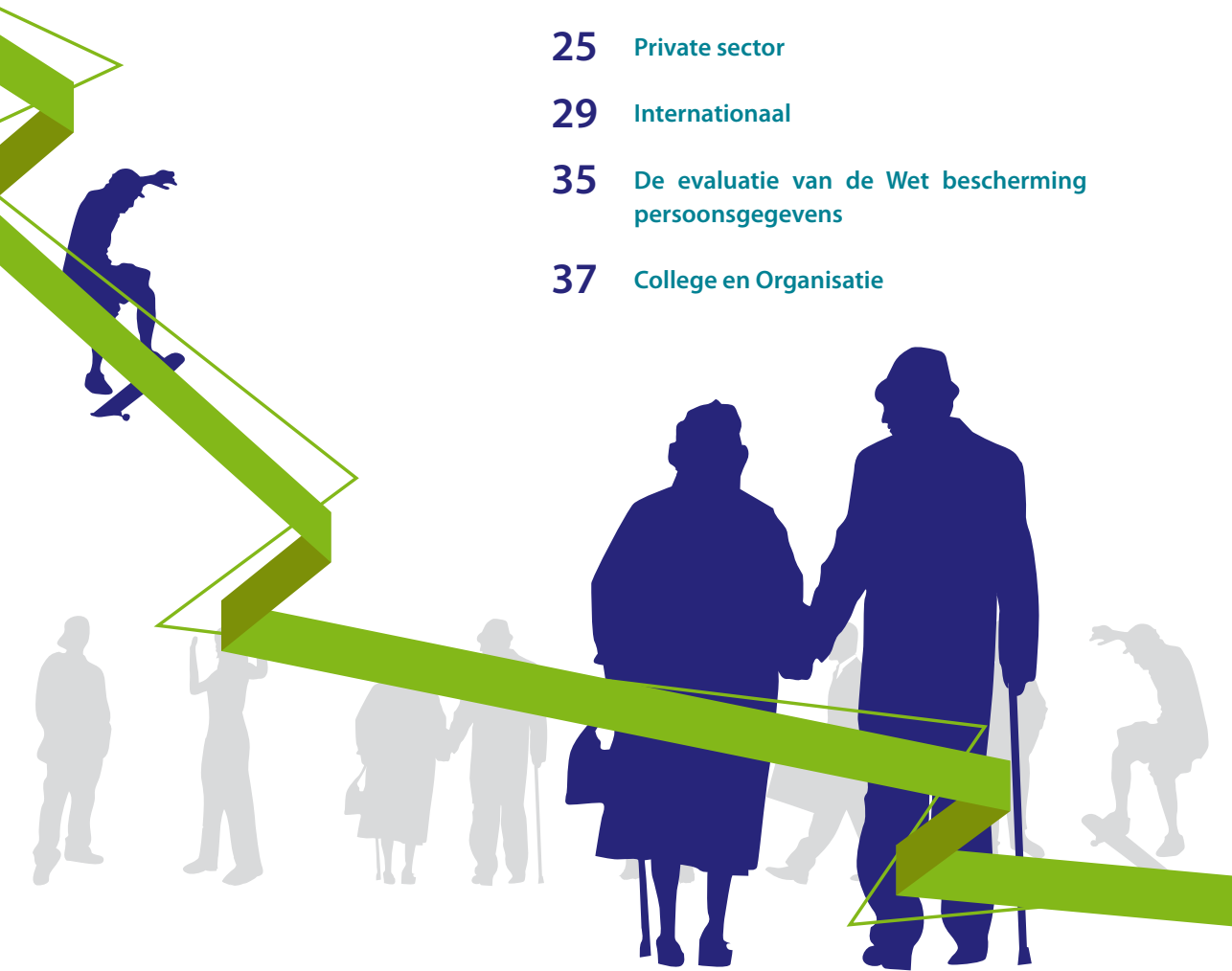
Daarnaast adviseert het CBP de regering over voorgenomen wetgeving die betrekking heeft op de verwerking van persoonsgegevens.

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



Inhoud

- 2 Voorwoord
- 4 Inleiding
- 7 Internet en Telecom
- 11 Financiële gegevens
- 13 Medische gegevens
- 17 Jongeren
- 21 Politie en Justitie
- 25 Private sector
- 29 Internationaal
- 35 De evaluatie van de Wet bescherming
persoonsgegevens
- 37 College en Organisatie



Voorwoord

De grenzeloze mogelijkheden van de technologie bieden individu en samenleving ongekende voordelen waarover niemand kortgeleden nog durfde te dromen. Internet, mobiele telefonie, RFID, sociale netwerksites, biometrie en *cloud computing* hebben bijvoorbeeld ingrijpende verbetering en verandering tot gevolg in ieders leven en in organisatie en dienstverlening van markt en overheid.

Een van de vaak onontkoombaar geachte gevolgen van die veranderingen is gelegen in het feit dat wij allen bij ons doen en laten digitale sporen achterlaten. Opgeteld bij de inmiddels eveneens grenzeloze mogelijkheden tot opslag, koppeling en verwerking van allerhande gegevens, ontstaat daarom een kafkaeske situatie: het zicht ontbreekt op wat er met onze gegevens gebeurt, bij wie deze terechtkomen, hoe en waar welke profielen van ons gemaakt worden en welke – mogelijk bepalende – invloed dat alles heeft op rechtmatige individuele keuzen en ontplooiingsmogelijkheden.

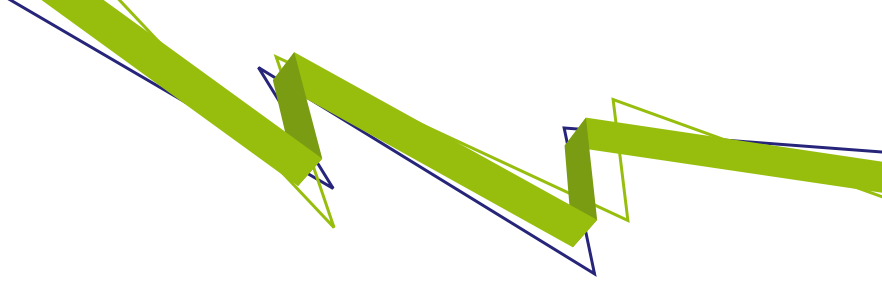
Er zijn ten minste drie belangrijke mogelijkheden om op deze ontwikkelingen te reageren.

De eerste is om diezelfde technologische ontwikkelingen te gebruiken om de kans op inbreuk op de persoonlijke levenssfeer zo klein mogelijk te maken, in het jargon *privacy by design* genaamd. Het maakt bijvoorbeeld een cruciaal verschil of een kastje in de auto ten behoeve van de kilometerheffing continu via de ether locatiegegevens doorseint aan een centrale database, dan wel dat dat kastje zo wordt

ontwikkeld dat alle gegevens in de auto blijven en de automobilist de zeggenschap houdt over het vrijgeven van die gegevens.

Natuurlijk zullen bedrijven en overheden altijd knappe koppen willen inzetten voor de ontwikkeling van nieuwe, snelle, efficiënte en winstgevende producten en diensten. Het is echter ook in het belang van het uiteindelijke succes van veel van die producten en diensten om de knapste koppen de opdracht te geven deze producten zó te ontwikkelen dat ze geen of veel minder inbreuk maken op de persoonlijke levenssfeer.

Te vaak hebben zij die zich storten op nieuwe technologische ontwikkelingen waarbij persoonsgegevens worden verwerkt een bijna blinde vlek voor het feit dat die technologie tevens ingezet kan worden om reeds bij het ontwerp van een nieuw product of dienst te voorzien in waarborgen om persoonsgegevens te beschermen en te beveiligen. Het zou goed zijn als de na 9 juni 2010 te vormen nieuwe regering wegen gaat bewandelen om de inzet van *privacy by design* te bevorderen of te verplichten.



Een tweede mogelijkheid om Kafka enigszins buiten de deur te houden is gelegen in het geven van informatie aan burgers over de vraag wie welke gegevens over hen waar en waarom opslaat en verwerkt. Om hun rechten op het gebied van bescherming van persoonsgegevens te kunnen uitoefenen is het onontbeerlijk dat burgers over deze informatie beschikken, zodat zij niet onverhoeds geconfronteerd worden met (bijzondere) gegevens die in een totaal andere context werden opgeslagen en verwerkt.

Ten slotte hebben burgers ook recht en belang te weten of de bestanden waarin hun persoonsgegevens worden verwerkt, adequaat zijn beveiligd tegen onrechtmatig inzien alsmede tegen diefstal, verlies en misbruik. Patiënten die een ziekenhuis bezoeken moeten er bijvoorbeeld van op aan kunnen dat hun medische gegevens daar in veilige handen zijn. Zo moet een adequate risicoanalyse zijn uitgevoerd ten behoeve van de informatiebeveiliging. Als die beveiliging in private of publieke secto-

ren tekortschiet, kan dit leiden tot grote ongelukken, tot identiteitsfraude of tot datalekken, reden waarom de meldplicht voor datalekken voor alle sectoren in de samenleving dient te gelden.

Bescherming van persoonsgegevens is niet alleen een grondrecht gericht op het individu. Uiteindelijk dient de bescherming van persoonsgegevens een belangrijk collectief belang in een democratische samenleving: elkaar kunnen vertrouwen. De klant moet het bedrijfsleven kunnen vertrouwen en de burger de overheid. In dat licht bezien zijn *privacy by design*, grotere transparantie over wie wat en waarom met onze persoonsgegevens doet en adequate beveiliging van die gegevens het alfa en omega om kafkaëske vervreemding tegen te gaan.

J. Kohnstamm
Voorzitter

Inleiding

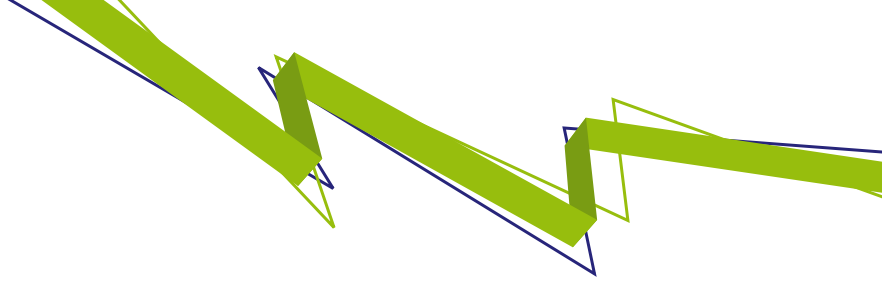
Het CBP heeft ervoor gekozen als toezichthouder de prioriteit bij handhaving te leggen in de overtuiging zo de meest effectieve bijdrage te kunnen leveren aan de bevordering van de naleving van de Wet bescherming persoonsgegevens (Wbp). Bij het vaststellen van prioriteiten voor 2009 is gebruik gemaakt van een risicoanalyse van verwerkingen van persoonsgegevens in verschillende sectoren van de samenleving. Het CBP selecteerde vervolgens zaken waarbij sprake is van aanwijzingen van ernstige overtredingen van de wet, die structureel van aard zijn, veel burgers raken en waarbij het CBP met zijn bevoegdheden kan optreden. Het CBP hield tevens een open oog voor actuele gebeurtenissen gedurende het jaar. De onderzoeken en interventies van het CBP leidden niet alleen bij individuele verantwoordelijken tot resultaat, maar bleken ook uitstralende werking te hebben.

Het CBP had voor 2009 een aantal thematische 'leidraden' vastgesteld – informatieplicht en transparantie en verstrekking van persoonsgegevens aan derden – die terug te zien zijn in meerdere onderzoeken. Zo concludeerde het CBP na onderzoek bij internetbedrijf Advance dat het bedrijf de wet heeft overtreden door via internetplatforms gevoelige gegevens van mensen te verzamelen en vervolgens hun geprofileerde persoonsgegevens aan derden te verkopen zonder de betrokkenen hierover duidelijk en volledig te informeren. Circa 2,2 miljoen mensen namen op dat moment deel aan de internettests van Advance. Advance bood hen de mogelijkheid op internet een test in te vullen om bijvoorbeeld 'je echte leeftijd' te achterhalen. Uit het onderzoek bleek dat Advance onder meer medische gegevens heeft verzameld en verwerkt, terwijl hiervoor in beginsel een wettelijk verbod geldt. Advance had de betrokkenen niet volgens de wettelijke eisen geïnfor-

meerd over het gebruik van hun gegevens.

Het CBP constateerde na onderzoek bij twee lopende regionale elektronische patiëntendossiers (REPD's) dat de Wbp werd overtreden. Ten aanzien van beide REPD's is een handhavingprocedure gestart. Deze procedure leidde ertoe dat één van de twee REPD's een einde heeft gemaakt aan de geconstateerde onrechtmatigheden, onder meer door alsnog alle patiënten persoonlijk te informeren over de opname van hun gegevens in het REPD.

Na onderzoeken van het CBP en de Inspectie voor de Gezondheidszorg (IGZ) in 2007 en 2008 was gebleken dat geen van de twintig onderzochte ziekenhuizen voldeed aan de norm voor informatiebeveiliging. Het CBP legde in 2009 vier ziekenhuizen die hun zaken nog steeds niet op orde hadden een last onder dwangsom op.



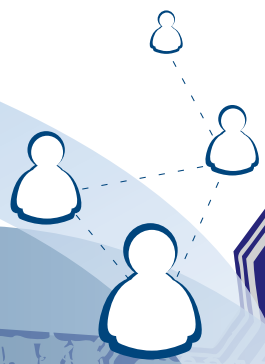
Het CBP stelde in 2009 richtsnoeren op inzake automatische kentekenherkenning (ANPR) door de politie. Het CBP zet daarin uiteen welke uitleg van de wettelijke normen het als toezicht-houder hanteert bij de uitoefening van zijn bevoegdheden. Later in het jaar deed het CBP bij een tweetal politiekorpsen onderzoek naar de toepassing van ANPR en concludeerde dat de korpsen Rotterdam-Rijnmond en IJsselland willens en wetens in strijd met de Wet politiegegevens (Wpg) handelden door *no-hits* 120 respectievelijk 10 dagen te verwerken. Een *no-hit* betekent dat een gescand kenteken niet voorkomt in het vergelijkingsbestand en dat dit kenteken dus niet wordt gezocht door de politie. Deze kentekens moeten direct worden vernietigd. In reactie op de publicatie van de definitieve onderzoeksbevindingen hebben beide korpsen begin 2010 laten weten de onrechtmatigheden te beëindigen.

Onderzoek naar de werkwijze van een aantal arbodiensten leidde tot de conclusie dat ten minste een arbodienst – Tredin – stelselmatig in strijd met de wet handelde door medische gegevens van zieke werknemers te verstrekken aan hun werkgevers terwijl deze gegevens onder het medisch beroepsgeheim vallen. Het CBP heeft deze arbodienst in 2009 een last onder dwangsom opgelegd. De arbodienst heeft de overtredingen vervolgens binnen de gestelde begunstigingstermijn beëindigd.

Onderzoek naar drie andere arbodiensten is voortgezet.

Na de introductie van het instrument ‘zienswijze’ in 2008 stelde het CBP in 2009 op verzoek van de Stichting Landelijk Informatiesysteem Schulden (LIS) zijn eerste zienswijze op, die werd gevolgd door een tweede naar aanleiding van een nieuw ontwerp van het LIS. Beide ontwerpen bleken na een toets van het CBP niet aan de eisen van de wet te voldoen. Ten aanzien van het tweede ontwerp concludeerde het CBP dat het ontwerp het oorspronkelijke doel – het registreren van achterstallige schulden ter voorkoming van problematische schulden – ver te buiten ging. Dit kan tot gevolg hebben dat een substantiële groep mensen wordt geregistreerd die niet in het register thuishoort, maar wel wordt geconfronteerd met de negatieve gevolgen van het te boek staan als problematisch schuldenaar.

Deze publicatie behandelt een selectie van onderzoeken en wetgevingsadviezen van het CBP in 2009. Een uitgebreid Jaarverslag is gepubliceerd op onze site www.cbppweb.nl. Op deze site en op de site www.mijnprivacy.nl is tevens meer informatie te vinden over de activiteiten van het College bescherming persoonsgegevens.



Internet en Telecom


Als persoonsgegevens eenmaal op internet zijn gepubliceerd, door zoekmachines zijn geïndexeerd en door internetarchieven vastgelegd, zijn deze gegevens 24 uur per dag voor de hele wereld toegankelijk. Ze zijn hierdoor gemakkelijk te hergebruiken met alle risico's, zoals identiteitsfraude, van dien. De gevolgen van internetpublicaties op het privé- en professionele leven van personen kunnen dus zeer groot zijn. Het CBP ontvangt veel klachten en signalen over de publicatie van persoonsgegevens op internet. Door op te treden tegen websitehouders die op structurele wijze de Wbp overtreden, beoogt het CBP de alertheid te vergroten van zowel de verantwoordelijken als van de betrokkenen.

Internetbedrijf verstrekt gevoelige gegevens aan derden

Het CBP concludeerde na onderzoek bij internetbedrijf Advance dat het bedrijf de wet heeft overtreden door via internetplatforms gevoelige gegevens – zoals medische en financiële gegevens – van mensen te verzamelen en vervolgens hun geprofileerde persoonsgegevens aan derden te verkopen zonder de betrokkenen hierover duidelijk en volledig te informeren. Circa 2,2 miljoen mensen namen op dat moment deel aan de internettests van Advance. Advance bood de mogelijkheid op internet een test in te vullen om bijvoorbeeld 'je echte leeftijd' te achterhalen. Uit het onderzoek bleek onder meer dat Advance medische gegevens heeft verzameld en verwerkt, terwijl hiervoor in beginsel een wettelijk verbod geldt. Advance heeft de betrokkenen van het gebruik van hun gegevens niet volgens de wettelijke eisen geïnformeerd.

Internetsite www.beoordeelmijnleraar.nl

In 2009 heeft het CBP naar aanleiding van klachten van leraren onderzoek ingesteld naar de website www.beoordeelmijnleraar.nl. Op de site werden de naam, werkplek en beoordelingen over leraren vastgelegd die vervolgens 24 uur per dag voor de hele wereld toegankelijk waren. Deze werkwijze had zeer negatieve gevolgen voor de persoonlijke levenssfeer van leraren, temeer omdat de beoordelingen hoog scoorden in internetzoekmachines. Het CBP heeft naar aanleiding van klachten onderzoek gedaan naar de rechtmatigheid van de publicatie van persoonsgegevens van leraren via deze site. Na ontvangst van de voorlopige onderzoeksbevindingen heeft de websitehouder de site aangepast. De toegang tot de namen en andere persoonsgegevens van leraren is sindsdien beperkt tot personen die tot de school van de leraar behoren. Bezoekers van de site moeten zich laten registreren om de



persoonsgegevens te kunnen bekijken en de site is afgeschermd van zoekmachines. Het CBP concludeerde dat de eerder geconstateerde onrechtmatigheden zijn weggenomen.

Sociale netwerksites en andere op jongeren gerichte sites

Sociale netwerksites trekken vooral jongeren. Die zijn zich niet steeds voldoende bewust van de risico's van publicatie van hun persoonsgegevens op het internet. Zij kunnen zich hier ook lang niet altijd van bewust zijn aangezien veel websitehouders onvoldoende informatie bieden over de wijze waarop zij met persoonsgegevens omgaan. Profielpagina's worden ook doorzocht door anderen en door zoekmachines en persoonsgegevens kunnen onrechtmatig worden gebruikt door derden met het risico van onder meer identiteitsfraude. Het CBP heeft in 2009 veel aandacht besteed aan de rechten van deelnemers aan sites die zich vooral op jongeren richten. Er zijn in dit kader twee onderzoeken uitgevoerd.

Het eerste onderzoek betreft *www.zikle.nl*, een sociale netwerksite voornamelijk gericht op jongeren. Het CBP stelde vast dat de websitehouder deelnemers aan het netwerk onvoldoende informatie gaf over de doeleinden van het verzamelen en verwerken van de persoonsgegevens en te weinig beveiligingsmaatregelen nam om de risico's van publicatie van deze ge-

gevens op internet te beperken. Het CBP heeft hem onder meer gesommeerd de profielpagina's standaard af te schermen voor anderen en voor zoekmachines totdat een lid expliciet een keuze over de mate van afscherming heeft gemaakt. Hierna beëindigde de websitehouder de geconstateerde onrechtmatigheden.

De websitehouder van een andere site, *www.jiggy.nl*, gebruikte een spelletje, Coco Banana, om bezoekers van de site te bewegen e-mailadressen van derden op te geven in ruil voor extra speelbeurten. Die derden hadden hiervan geen weet en kregen ongevraagd e-mails toegezonden. Zolang mensen niet weten dat bedrijven hun persoonsgegevens gebruiken, kunnen zij bepaalde rechten ook niet uitoefenen, zoals het recht om verwijdering of correctie van hun gegevens te vragen. Het CBP heeft deze praktijk onderzocht en concludeerde dat deze in strijd is met de Wbp. Naar aanleiding van de onderzoeksbevindingen heeft de websitehouder het spel *off line* gehaald.

Meldplicht datalekken

Als de beveiliging van persoonsgegevens en bestanden tekortschiet en persoonsgegevens (soms letterlijk) op straat komen te liggen, moet dat bekend worden gemaakt. In de herziene Europese e-Privacy Richtlijn is een meldplicht opgenomen voor datalekken. Het CBP is voor-

stander van het invoeren van een meldplicht die van toepassing is op zowel de private als op de publieke sector. In een aantal omringende landen is dat al gebeurd. Voor het CBP is de meldplicht datalekken geen doel op zich maar een middel om verantwoordelijken aan te sporen aan de beveiligingsvereisten van de Wbp te voldoen en om het toezicht op de beveiliging te versterken.

Bewaarplicht telecomgegevens

Toezicht op het zorgvuldig bewaren en het tijdig vernietigen van de gegevens is van groot belang voor de bescherming van de persoonlijke levenssfeer. De nieuwe Wet bewaarplicht telecommunicatiegegevens is op 1 september 2009 in werking getreden. Op 15 september 2009 hebben het Agentschap Telecom (AT) en het CBP een overeenkomst gesloten om samen te werken bij het toezicht op de naleving van de wet. Het eerste onderzoek waarin is samengewerkt levert voor het AT een nulmeting op als startpunt voor toezicht op de naleving van de wet. Voor het CBP is het een onderdeel van gecoördineerd onderzoek door de Europese privacytoezichthouders.



Financiële gegevens

Of het nu gaat om informatie over iemands actuele financiële positie of over zijn pensioenaanspraken, het verzamelen, opslaan en gebruiken van dit soort gevoelige gegevens dient aan strikte zorgvuldigheidseisen te voldoen.

Landelijk Informatiesysteem Schulden


De Stichting Landelijk Informatiesysteem Schulden i.o. (LIS) diende in 2009 een tweede ontwerp van een schuldenregistratiesysteem in bij het CBP. Het CBP heeft het ontwerp vervolgens aan de Wbp getoetst en geconcludeerd dat dit ontwerp niet aan de eisen van de wet voldoet. Het LIS had in 2008 al een eerste ontwerp ingediend voor een vergelijkbaar systeem ten aanzien waarvan het CBP ook had geconcludeerd dat het niet aan de wet voldeed. Ten aanzien van het tweede ontwerp, dat ten opzichte van het vorige enigszins is aangepast, concludeert het CBP dat het het oorspronkelijke doel – het registreren van achterstallige schulden ter voorkoming van problematische schulden – ver te buiten gaat. Voorts zijn de regels inzake het soort schuld dat wordt opgenomen en de toetreding van bedrijven en organisaties die het register mogen inzien onvoldoende objectief. Dit kan tot gevolg hebben dat een substantiële groep mensen wordt geregistreerd die niet in het register thuishoort, maar wel wordt geconfronteerd met de negatieve gevolgen van het te boek staan als problematisch schuldenaar. Dat verdraagt zich niet met de eisen van de wet.

De minister van Financiën heeft in de Tweede Kamer een drietal alternatieven geschetst voor een schuldenregistratiesysteem. Het ministerie onderzoekt deze alternatieven op haalbaarheid.

Bank geeft persoonsgegevens door aan derden

Ieder die een rekening opent bij een bank moet erop kunnen vertrouwen dat de bank dat feit niet aan andere partijen doorgeeft en zeker niet met de adresgegevens erbij, ook al is dat voor een charitatief doel.

Naar aanleiding van een klacht heeft het CBP onderzoek gedaan naar een dergelijke derdenverstrekking van persoonsgegevens door ASN Bank n.v. De klager stelde dat zijn minderjarige dochters een wervende brief met acceptgirokaart hadden gekregen van de Stichting Cordaid Kinderstem. Toen de betrokkene daarover een klacht indiende bij Cordaid, bleek dat deze stichting de adressen had gekregen van ASN, omdat op naam van de dochters een Jeugdspaarrekening was geopend. Uit het onderzoek is gebleken dat de bank in strijd met de Wbp gegevens van rekeninghouders heeft



verstrekt aan Cordaid en aan de Waddenvereniging. Na ontvangst van de onderzoeksbevindingen van het CBP heeft de bank haar werkwijze aangepast.

Het pensioenregister

Het pensioenregister maakt uitwisseling mogelijk van pensioengegevens tussen pensioenuitvoerders/Sociale Verzekeringsbank (svb) en burgers. Dit gebeurt via een pensioenportaal waarop iedere burger via zijn burgerservicenummer zijn opgebouwde pensioenaanspraken kan inzien. In eerste instantie gaat het alleen om aanspraken op ouderdomspensioen, later worden er mogelijk aanspraken op grond van andere (volks)verzekeringen aan toegevoegd. De minister van Sociale Zaken en Werkgelegenheid heeft het CBP in 2009 gevraagd te adviseren over het wetsvoorstel dat de invoering van het pensioenregister beoogde.

Het CBP erkent het grote belang van het pensioenregister voor betrokkenen. Het heeft er wel op gewezen dat het beschikbaar zijn van

financiële gegevens van (het overgrote deel van) de Nederlandse bevolking via het pensioenregister een enorme aantrekkingskracht zal uitoefenen op andere partijen. Daarom acht het CBP het van groot belang dat reeds in het beginstadium zeer zorgvuldig wordt omgegaan met de inrichting (waaronder beveiliging) van het pensioenregister en dat expliciet wordt afgebakend in formele wetgeving wat de doeleinden van de verwerking van persoonsgegevens door middel van het pensioenregister zijn. Het advies is overgenomen.

In de wet is nu expliciet bepaald wat het doel is van het pensioenregister en is zeker gesteld dat alleen de betrokkenen zelf het overzicht van hun pensioenaanspraken kunnen inzien. De memorie van toelichting is gewijzigd met het oog op zorgvuldige inrichting en beveiliging van het pensioenregister. Tevens is voorzien in een grote publiekscampagne om betrokkenen te informeren over het pensioenregister. Daarnaast is geregeld hoe de pensioenuitvoerders en de svb het toezicht zullen inrichten op de instelling die het pensioenregister ontwikkelt en beheert.

Medische gegevens

Registraties van medische gegevens, vooral het Elektronisch patiëntendossier, hebben in 2009 de gemoeders weer beziggehouden. Wie krijgen toegang tot patiëntgegevens? Worden deze afdoende beveiligd? Wat mag de bedrijfsarts wel en niet doorgeven aan de werkgever van een zieke werknemer?

Geen toegang tot EPD voor zorgverzekeraars

Het Elektronisch patiëntendossier (EPD) is opgezet als een systeem waarmee hulpverleners voor hulpverleningsdoeleinden toegang kunnen krijgen tot gegevens over de patiënten die zij behandelen. Toegang voor anderen dan hulpverleners en voor andere doeleinden verdraagt zich noch met de opzet van dat systeem noch met de juridische legitimatie daarvoor.

Begin 2009 is in de Tweede Kamer het wetsvoorstel dat het EPD regelt behandeld. In het wetsvoorstel is op belangrijke punten rekening gehouden met het kritisch advies dat het CBP erover in 2007 had uitgebracht. In de Tweede Kamer is het voorstel van wet op het EPD geamendeerd. Daarbij is een aantal bepalingen toegevoegd waarin nog eens expliciet de toegang voor bedrijfsartsen, keuringsartsen en zorgverzekeraars wordt uitgesloten. In die bepalingen zijn echter ook uitzonderingsgronden opgenomen in verband waarmee wel toegang tot het EPD mogelijk moet zijn. In het aan het CBP voorgelegde voorstel tot wijziging van het Besluit BSN in de zorg zijn die uitzonderings-

mogelijkheden voor zorgverzekeraars verder uitgewerkt. Het CBP heeft in zijn advies over het conceptbesluit de minister van Volksgezondheid, Welzijn en Sport geadviseerd de uitzonderingsmogelijkheden op het verbod op toegang tot het EPD voor verzekeraars te schrappen. De minister heeft inmiddels aangegeven dat hij het advies van het CBP overneemt en de Tweede Kamer een voorstel tot wijziging van de wet zal voorleggen.

Regionale elektronische patiëntendossiers

In de eerste helft van 2009 heeft het CBP onderzoek gedaan bij twee regionale elektronische patiëntendossiers (REPD's). Het CBP constateerde dat de onderzochte samenwerkingsverbanden de Wbp overtraden. Dit was zorgwekkend omdat het gaat om uitwisseling van per definitie gevoelige gegevens. Mensen moeten worden geïnformeerd over de opname van hun gegevens in een REPD en erop kunnen vertrouwen dat alleen een behandelend arts toegang heeft tot hun medische gegevens. Samenwerkingsverbanden dienen voldoende maatregelen te nemen om dit te garanderen. Ten aanzien van beide REPD's is



naar aanleiding van de onderzoeksbevindingen een handhavingsprocedure gestart. Op basis van een vervolgens gehouden hoorzitting heeft het CBP geconstateerd dat deze procedure bij een van de twee REPD's ertoe heeft geleid dat er een einde is gemaakt aan de geconstateerde onrechtmatigheden. Alle patiënten zijn inmiddels persoonlijk geïnformeerd en er is voldoende aannemelijk gemaakt dat de toegangsbeveiliging inmiddels adequaat is geregeld en dat er voldoende controle is op de rechtmatige toegang tot patiëntendossiers.

Informatiebeveiliging ziekenhuizen

Patiënten in ziekenhuizen moeten ervan uit kunnen gaan dat zorgvuldig en veilig met hun medische gegevens wordt omgegaan. In 2007 en 2008 hebben het CBP en de Inspectie voor de Gezondheidszorg bij twintig ziekenhuizen onderzoek gedaan naar de beveiliging van de gegevens van hun patiënten. Geen van de ziekenhuizen bleek te voldoen aan de norm voor informatiebeveiliging. Vier ziekenhuizen die in 2009 nog steeds hun zaken niet op orde hadden en daarmee in strijd handelden met de Wbp heeft het CBP in juni een last onder dwangsom opgelegd. Vooral het ontbreken van kennis over waar men welke risico's loopt op het gebied van informatiebeveiliging rekent het CBP de ziekenhuizen aan. Dit kan namelijk ernstige gevolgen hebben voor de kwaliteit van de zorg en de privacy van patiënten. De zieken-


huizen is onder meer opgedragen een risicoanalyse informatiebeveiliging te maken, een functieprofiel op te stellen voor een informatiebeveiligingsfunctionaris, een informatiebeveiligingsfunctionaris aan te stellen en een portefeuillehouder informatiebeveiliging aan te wijzen binnen de Raad van Bestuur.

Verstrekking van medische gegevens door arbodiensten aan werkgevers

Onderzoek naar de werkwijze van een aantal arbodiensten leidde tot de conclusie dat ten minste één arbodienst – Tredin – stelselmatig in strijd met de wet handelde door medische gegevens van zieke werknemers te verstrekken aan hun werkgevers terwijl deze gegevens onder het medisch beroepsgeheim vallen. Het CBP heeft deze arbodienst in 2009 een last onder dwangsom opgelegd. De arbodienst heeft de overtredingen vervolgens binnen de gestelde begunstigingstermijn beëindigd.

Uitbesteding verwerking patiëntgegevens

Het internet biedt mogelijkheden om ICT-diensten op afstand aan te bieden. De aanbidders van zulke diensten worden doorgaans Application Service Providers (ASP's) genoemd. Veel zorgverleners maken inmiddels gebruik van deze diensten, waarbij extern opgeslagen patiëntgegevens via internet worden benaderd. Het CBP heeft de minister van Volksgezond-



heid, Welzijn en Sport aandacht gevraagd voor de risico's die de aldus gegroeide praktijk meebrengt en voor de juridische vragen die hierbij rijzen.

De uitbesteding van de verwerking van gegevens waarop het medisch beroepsgeheim van toepassing is – zonder dat voor zover bekend de patiënt daarvoor om toestemming wordt gevraagd – heeft een hoge vlucht genomen. De praktijk is niet normvast en de mate

waarin bij uitbesteding aandacht wordt geschonken aan de bescherming van persoonsgegevens loopt zodanig uiteen, dat naar het oordeel van het CBP nadere regulering – zelfregulering of wetgeving – geboden is. Er zullen stevige waarborgen moeten worden geboden voor een veilige en discrete verwerking bij de dienstverlener. Uitbesteding mag er nooit toe leiden dat op ongerechtvaardigde wijze gegevens aan personen of instellingen buiten de gezondheidszorg worden gebracht.

Jongeren

Jongeren vormen een kwetsbare groep. Zeer zorgvuldige omgang met hun gegevens is van groot belang om te voorkomen dat zij met een stigmatiserend etiket opgroeien. Van even groot belang is het jongeren bewust te maken van de risico's die zij kunnen lopen door op internet onzorgvuldig om te gaan met persoonsgegevens. Voor het onderwerp 'jongeren en internet' wordt verwezen naar het hoofdstuk 'Internet en Telecom'.

Verwijsindex risicjongeren

In het vorige jaarverslag van het CBP is uitvoerig ingegaan op de kritiek van zowel het CBP als de Raad van State op het wetsvoorstel voor een landelijk verwijssysteem voor hulpverlening aan 'probleemjongeren'. Het wetsvoorstel is in juli 2009 door de Tweede Kamer aanvaard en op 2 februari 2010 door de Eerste Kamer.

De minister van Jeugd en Gezin heeft het CBP in september 2009 advies gevraagd over het ontwerpbesluit dat de uitvoering regelt van de Verwijsindex risicjongeren. Daarin worden instanties aangewezen waar functionarissen werken die als bevoegde kunnen worden aangewezen om een jeugdige aan de verwijssysteem te melden. Daarnaast worden in het ontwerpbesluit eisen vastgesteld voor de meldingsbevoegde personen en instanties en voor de veilige aansluiting van signaleringssystemen op de verwijssysteem.

Het CBP constateerde in zijn advies dat het

aantal in het ontwerpbesluit aangewezen instanties en functionarissen dusdanig groot is dat artsen en andere meldingsbevoegden niet de vereiste beoordeling kunnen maken of met de melding de schade aan het kind zal worden voorkomen of beperkt. Het CBP heeft voorts kanttekeningen geplaatst bij het melden door de doelgroepencoördinator en gewezen op het risico dat meldingsbevoegden etniciteit gaan registreren in hun eigen administratie zonder dat hiervoor een wettelijke basis is. Het CBP heeft de minister geadviseerd het ontwerpbesluit en de nota van toelichting op onderdelen aan te passen om niet in strijd te komen met de Wbp.

Bij een melding aan de Verwijsindex risicjongeren worden op voorhand ongericht persoonsgegevens verstrekt aan een potentieel groot aantal organisaties afkomstig uit verschillende domeinen. Hierdoor kan bijvoorbeeld een arts die in het belang van het kind overweegt het medisch beroepsgeheim te doorbreken, niet de vereiste beoordeling maken of met de melding de schade aan het kind zal kunnen



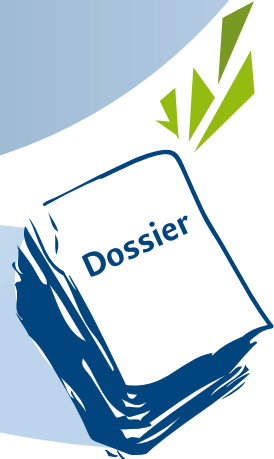
8




5

10

4





worden voorkomen of beperkt. Hij weet namelijk bij het melden niet aan welke instanties en/of functionarissen de persoonsgegevens via de verwijzindex worden verstrekt.

In het ontwerpbesluit is in reactie op een motie van de Tweede Kamer de mogelijkheid opgenomen van melding aan de verwijzindex door bij de jeugd betrokken 'doelgroepen-coördinatoren'. Uit de nota van toelichting leidt het CBP af dat hiermee wordt voldaan aan het in de motie opgenomen verzoek te bevorderen dat de Antillianencoördinator bevoegd wordt om jeugdigen aan de verwijzindex te melden. Hoewel in de nota is aangegeven dat ook andere bij de jeugd betrokken doelgroepen-coördinatoren kunnen melden, vraagt het CBP zich af om hoeveel en welke doelgroepen-coördinatoren het gaat. Uit de nota blijkt dat in de melding niet wordt opgenomen met welke doelgroep de coördinator zich bezighoudt. Indien echter in de praktijk alleen zal worden gemeld door de Antillianencoördinator, zal uit een dergelijke melding toch kunnen worden afgeleid dat het om een Antilliaanse jeugdige gaat. Hierdoor zal strijd ontstaan met het in de Wbp neergelegde verbod op het verwerken van persoonsgegevens betreffende iemands ras.

Een ander probleem geldt de melding door Bureau Jeugdzorg op initiatief van de politie. Een dergelijke getrapte melding zal herkenbaar zijn als politiemelding, waardoor de jongere

met de politie wordt geassocieerd, terwijl de politie niet een voor melding aangewezen instantie is. Het CBP oordeelt dat het noemen van de politie in een melding van Bureau Jeugdzorg niet noodzakelijk is voor de afstemming van de hulpverlening en daarom in strijd is met de Wbp.

Wat betreft de meldingsbevoegden merkt het CBP op dat door de vaag geformuleerde meldcriteria moeilijk kan worden vastgesteld aan welke kennisvereisten een meldingsbevoegde moet voldoen om te mogen melden. Als voorbeeld kan genoemd worden het na de behandeling in de Tweede Kamer in het wetsvoorstel neergelegde criterium op grond waarvan een meldingsbevoegde een jongere aan de verwijzindex kan melden indien hij een redelijk vermoeden heeft dat de jeugdige daadwerkelijk in zijn ontwikkeling wordt bedreigd omdat hij of zij blootstaat aan risico's die in bepaalde etnische groepen onevenredig vaak voorkomen. Door de ruime formulering van dit toegevoegde criterium is niet duidelijk of bijvoorbeeld een huisarts of een schooldirecteur voldoende kennis en ervaring heeft om een jeugdige op grond van deze bepaling te mogen melden. Het CBP wijst er tevens op dat dit toegevoegde meldcriterium geen wettelijke basis biedt voor het vastleggen van etniciteit van jeugdigen in de eigen administratie van meldingsbevoegden. Meldingsbevoegden dienen hiervan op de hoogte te worden gesteld.



Onderwijskundige rapporten

Basisscholen zijn verplicht een onderwijskundig rapport op te stellen over leerlingen die de school verlaten om naar een vervolgopleiding te gaan en de ouders van de leerlingen hierover te informeren. De juiste naleving van de informatieplicht stelt ouders van een leerling in staat om te volgen welke gegevens van de leerling worden verwerkt en op welke wijze.

In 2009 heeft het CBP bij twintig basisscholen onderzocht of deze de informatieplicht naleefden bij het verstrekken van onderwijskundige rapporten aan scholen in het voortgezet onderwijs. Uit het onderzoek is gebleken dat meer dan de helft van de onderzochte scholen in hun leerlingdossiers niet heeft bijgehouden of aan de informatieplicht is voldaan.

Richtsnoeren

Ter verduidelijking en concretisering van de wettelijke norm met betrekking tot de informatieplicht in de Wbp heeft het CBP voor basisscholen richtsnoeren opgesteld aan de hand waarvan zij actief invulling kunnen geven aan de informatieplicht.

Basisscholen dienen de ouders actief op individueel niveau te informeren over het onderwijskundig rapport dat betrekking heeft op hun kind. Dat de ouders zijn geïnformeerd, dient duidelijk te blijken uit het leerlingdossier. Dit kan bijvoorbeeld door in het leerlingdossier een kopie op te nemen van de brief die de school aan de ouders heeft gestuurd, of een verslag van het gesprek dat hierover tussen school en ouders heeft plaatsgevonden.

Bescherming persoonsgegevens van kinderen

De Artikel 29-werkgroep van Europese Privacytoezichthouders heeft op 11 februari 2009 een Opinie aangenomen die algemene aanbevelingen doet voor de bescherming van persoonsgegevens van en door kinderen, in het bijzonder gericht op scholen. Het doel van het document is een analyse te geven van de algemene beginselen met betrekking tot de bescherming van de persoonsgegevens van kinderen en om een handleiding te verschaffen aan degenen die op dit terrein werkzaam zijn. De Opinie moet gelezen worden in de context van het bredere initiatief van de Europese Commissie om te komen tot een strategie van de Europese Unie met betrekking tot de rechten van kinderen.

Politie en Justitie

Technologische ontwikkelingen maken het voor de overheid in toenemende mate mogelijk grote hoeveelheden gegevens van al haar onderdanen te verzamelen en te verwerken. De noodzaak en effectiviteit van al deze verzamelingen dient keer op keer te worden aangetoond en wettelijk te worden onderbouwd. Dat geldt temeer als het gaat om politiebesteden.

Automatische kentekenherkenning

Automatische kentekenherkenning (ANPR) mag voor de uitvoering van de dagelijkse politietaak onder voorwaarden worden toegepast. Alleen de *hits* (dat zijn de kentekens die in de automatische vergelijking leiden tot een *match* met een kenteken in het vergelijkingsbestand) mogen worden bewaard. Een *no-hit* betekent dat een gescand kenteken niet voorkomt in het vergelijkingsbestand en dat dit kenteken dus niet wordt gezocht in het kader van de ANPR-actie. Deze kentekens moeten direct worden vernietigd. Als dit niet gebeurt, komt iedere automobilist die over een traject rijdt waar de politie automatische kentekenherkenning toepast als potentiële verdachte in de politiebesteden terecht. Dit is in strijd met de wet en een onrechtmatige inbreuk op de persoonlijke levenssfeer.

Richtsnoeren

Het CBP publiceerde na consultatie van organisaties en personen die bij de toepassing van automatische nummerplaatherkenning betrokken zijn op 14 juli 2009 de definitieve versie van zijn Richtsnoeren ANPR. Het CBP zet

daarin uiteen welke uitleg van de wettelijke normen het als toezichthouder hanteert bij de uitoefening van zijn bevoegdheden.

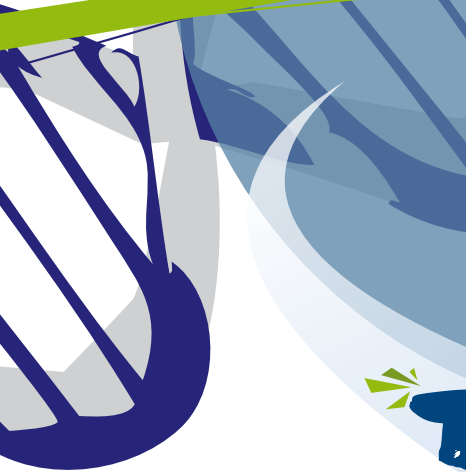
Onderzoek

Onderzoek van het CBP in de periode september 2009-januari 2010 heeft aangetoond dat de twee onderzochte regionale politiekorpsen, IJsselland en Rotterdam-Rijnmond, de gegevens van niet-gezochte kentekens, de zogeheten *no-hits*, 10 respectievelijk 120 dagen bewaren. Hiermee handelen zij in strijd met de Wet politiegegevens. De *no-hits* zijn voor het doel van de ANPR-actie niet noodzakelijk nu deze niet waren opgenomen in het vergelijkingsbestand. De *no-hits* kunnen evenmin verder worden verwerkt ten behoeve van gerichte onderzoeken. Voor verdergaande toepassing van ANPR ontbreekt vooralsnog een juridisch kader.

Het CBP heeft dan ook geconstateerd dat beide korpsen willens en wetens in strijd met de wet *no-hits* verwerken. In reactie op publicatie van de definitieve onderzoeksbevindingen hebben beide korpsen begin 2010 laten weten de onrechtmatigheden te beëindigen.



NL XX-00-00



Politie Infodesk

Politiegegevens zijn per definitie gevoelig van aard. Het is niet de bedoeling dat onbevoegden daarin kunnen neuzen. Het raadplegen van deze gegevens dient dan ook met de nodige zorgvuldigheidseisen te zijn omgeven.

Volgend op het algemene onderzoek in 2007/2008 naar het functioneren van de infodesks – loketten die op verzoek intern operationele informatie verstrekken – bij de regionale politiekorpsen, heeft het CBP in 2009 bij drie daarvan een vervolgonderzoek uitgevoerd. Het onderzoek heeft plaatsgevonden bij de politiekorpsen Brabant-Noord, Drenthe en Amsterdam-Amstelland en bij de desbetreffende verzorgingsgebieden van de Voorziening tot samenwerking Politie Nederland.

Tijdens het onderzoek is nagegaan of de korpsen voldoen aan het autorisatievereiste. Ook is onderzocht of zij de protocolplicht naleven, enerzijds ten aanzien van autorisaties en anderzijds ten aanzien van de mogelijkheid om aanwijzingen voor onbevoegd gebruik van politiegegevens door de infodesk door middel van een audit te controleren. Hoewel de uitkomsten per korps verschillen, zijn bij geen van de drie korpsen de autorisaties en de controle beide volledig op orde.

Daarnaast is onderzoek gedaan naar de wijze waarop de privacyfunctionarissen bij de drie onderzochte korpsen hun taak uitoefenen. Het CBP heeft geconstateerd dat zij hun advies- en/of controletaak niet overeenkomstig de wet uitoefenen. Bij het korps Amsterdam-


Amstelland was de privacyfunctionaris bovendien ten tijde van het onderzoek in strijd met de wet niet aangemeld bij het CBP. Tot slot wordt bij alle drie de korpsen door de privacyfunctionaris niet voldaan aan de verplichting een jaarverslag op te stellen.

Toegang inlichtingendiensten tot politie-informatie

Inlichtingen- en veiligheidsdiensten hebben de mogelijkheid om eigen informatie rechtstreeks geautomatiseerd te vergelijken met gegevens die zich bevinden in de bestanden van de politie. Het CBP heeft de minister van Justitie geadviseerd over een ontwerpbesluit dat deze zelfstandige bevraging regelt. Het CBP adviseert om in de nota van toelichting duidelijk te maken waarom het noodzakelijk is voor de inlichtingen- en veiligheidsdiensten om op grote schaal politiegegevens te kunnen bevragen. Ook dient in de toelichting voor elk van de categorieën gegevens nader te worden gemotiveerd waarom deze rechtstreeks moeten kunnen worden bevraagd en waarom de inlichtingen- en veiligheidsdiensten de gerelateerde informatie automatisch ter beschikking moeten krijgen. De politie verliest door de zelfstandige bevraging namelijk de controle over haar eigen gegevens. Het gevaar bestaat dat gegevens daardoor zonder de juiste context worden geïnterpreteerd.

Geautomatiseerde grenspassage

Steeds meer luchthavens ontwikkelen een systeem om reizigers geautomatiseerd de grens te kunnen laten passeren, bijvoorbeeld door



middel van een irisscan en een vingerafdruk. Om te voorkomen dat reizigers zich voor alle systemen apart moeten aanmelden, bestaan vergevorderde plannen om de systemen aan elkaar te koppelen. Als eerste proef is nu een koppeling gemaakt tussen het Nederlandse en het Amerikaanse systeem voor geautomatiseerde grenspassage.

Reizigers die willen deelnemen aan een dergelijk systeem moeten aantoonbaar van onbesproken gedrag zijn. De minister van Justitie zal hiertoe na achtergrondonderzoek een positieve of negatieve verklaring afgeven. Om deze verklaring ook te kunnen gebruiken voor buitenlandse grenspassagesystemen wordt het Besluit justitiële gegevens aangepast. Het CBP heeft de minister van Justitie geadviseerd om in de toelichting op het gewijzigde besluit duidelijk te maken welke uitgangspunten worden gehanteerd bij het achtergrondonderzoek dat moet leiden tot de verklaring van de minister.

Europese politie- en justitiesamenwerking

Eind 2008 zijn de Europese lidstaten het eens geworden over nieuwe regels over de verwerking van persoonsgegevens die tussen hen worden uitgewisseld ten behoeve van de opsporing en vervolging van strafbare feiten en het ten uitvoer leggen van straffen. Dit zogenoemde kaderbesluit derde pijler moet nu in de Nederlandse wetgeving worden opgenomen.

Hoewel de Nederlandse wetgeving op grote lijnen reeds met de besluiten in overeenstemming is, acht de regering aanvullingen op onderdelen van de Wet en Besluit politiegegevens en de Wet en Besluit justitiële en strafvorderlijke gegevens noodzakelijk. Het CBP heeft de minister van Justitie over de voorgestelde wijzigingen geadviseerd en heeft enkele aanpassingen voorgesteld.

Een van de voorgestelde aanpassingen betreft de door het kaderbesluit geïntroduceerde nieuwe adviestaak voor de nationale toezichthouders, onder meer voorafgaand aan het verwerken van gevoelige persoonsgegevens in een nieuwe databank of wanneer bij de verwerking van persoonsgegevens nieuwe technologieën worden ingezet. Het CBP zal bij de vormgeving van deze nieuwe adviestaak aansluiten bij het instrument van de zienswijze. Het verwacht daartoe een gemotiveerde adviesaanvraag.

In de artikelen die het inzagerecht betreffen wordt de mogelijkheid gecreëerd kennis te nemen van verstrekkingen die in een periode van drie jaar voorafgaand aan het inzageverzoek zijn gedaan. Het CBP acht deze termijn niet voldoende gemotiveerd en adviseert de memorie van toelichting op dit punt aan te passen. Voorts adviseert het CBP de regering nader te motiveren hoe het nationale toezicht op de informatieplicht dient te worden ingevuld.

Private sector

Hoe men er ook aan gewend lijkt te raken, cameratoezicht blijft een ingrijpend controlemiddel, waarover het CBP door de jaren heen vragen en signalen van burgers ontvangt. Inzet ervan moet zeer zorgvuldig worden gerechtvaardigd. Veel ophef veroorzaakte de introductie van de 'slimme energiemeter'. Is het voor het aankweken van milieubewust energieverbruik echt nodig dat de meterstanden bijna continu worden afgelezen, waardoor veel duidelijk wordt over het daagse reilen en zeilen achter de voordeur? Voor informatie over de werkzaamheden van het CBP in de private sector wordt tevens verwezen naar de hoofdstukken 'Internet en Telecom', 'Financiële gegevens' en 'Medische gegevens'.

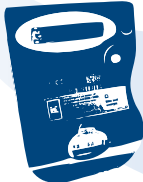
De 'slimme energiemeter'

Het wetsvoorstel tot wijziging van de Elektriciteitswet 1998 en de Gaswet is vooral bekend geworden omdat het voorziet in de invoering van op afstand uitleesbare energiemeters. Deze 'slimme energiemeters' kunnen een zeer nauwkeurig beeld geven van iemands huishouden en daarmee van zijn of haar aan- en afwezigheid en doen en laten. Om aan kritiek hierover van de Eerste Kamer tegemoet te komen, heeft de minister van Economische Zaken vorig jaar een novelle bij het wetsvoorstel ingediend. Het CBP heeft in 2009 twee keer geadviseerd over deze novelle. In eerste instantie voldeed de novelle op een aantal punten niet aan de vereisten van de Wbp. De belangrijkste kritiek betrof de informatieplicht. Over de op afstand uitleesbare energiemeters dienen consumenten op behoorlijke wijze keuzes te kunnen maken, ook als deze al geplaatst zijn. Zij moeten ook over voldoende informatie beschikken om waar nodig ondubbelzinnige toestemming te kunnen

geven voor het voortdurend of zeer frequent aflezen van hun energieverbruik. Naar aanleiding van dit advies is het wetsvoorstel aangepast.

Cameratoezicht op een bedrijventerrein

Rechtvaardigen de omvang van de criminaliteit, onveiligheid en overlast op een bedrijventerrein de inzet van cameratoezicht op dat bedrijventerrein? Kan men ook met minder ingrijpende middelen nagaan welke motorvoertuigen zich op het terrein bevinden voor, tijdens en vlak na een alarmmelding? Deze vragen stonden centraal bij het onderzoek van het CBP naar het cameratoezicht op een bedrijventerrein in Vianen. Het CBP constateerde dat er geen aanwijzingen zijn dat de Stichting Beveiliging Bedrijventerrein Vianen (SBBV) in strijd met de door het CBP getoetste vereisten van de Wbp handelt. Er is overleg gevoerd met de bewoners van bedrijfswoningen op het bedrijventerrein over de plaats waar de camera's zijn



Gedragscodes

Sectorale gedragscodes zijn een middel voor zelfregulering. Een organisatie (bijvoorbeeld een brancheorganisatie) kan het CBP verzoeken de eigen gedragscode te toetsen. In de samenleving wordt veel vertrouwen gesteld in gedragscodes. Het CBP is meestal bereid deze vorm van zelfregulering te ondersteunen. Het toetst de gedragscode zorgvuldig aan artikel 25 Wbp. Het gaat dan onder meer om de juiste uitwerking van de wet, een nauwkeurige omschrijving van de sector, de representativiteit van de organisatie die de gedragscode opstelt en de waarborgen voor onafhankelijkheid bij de beslechting van geschillen.

Over gedragscodes in 2009 zijn onder meer de volgende ontwikkelingen te melden: De Nederlandse Vereniging van Banken en het Verbond van Verzekeraars hebben het CBP verzocht een goedkeurende verklaring af te geven over de gewijzigde gedragscode Verwerking Persoonsgegevens Financiële Instellingen. Het CBP heeft in juli 2009 een ontwerpbesluit genomen en zal in de eerste helft van 2010 het definitieve besluit nemen de aangevraagde verklaring al dan niet te verlenen.

Op 21 oktober 2009 is de Privacygedragscode van de Vereniging van Particuliere Beveiligingsorganisaties goedgekeurd. De code geeft specifieke normen voor de diverse onderzoeksmethoden en -middelen, zoals heimelijke observatie, verborgen camera's, het onderscheppen van e-mail-verkeer en het afluisteren van telefoongesprekken.

opgehangen en de SBBV gaat zorgvuldig om met de opgeslagen camerabeelden. Wel heeft de SBBV het recht op inzage uit de wet verkeerd geïnterpreteerd door alleen in te gaan op verzoeken tot inzage van de Officier van Justitie en niet op verzoeken van individuele burgers. Door deze werkwijze handelde de SBBV in strijd met het inzagerecht, concludeerde het CBP. De SBBV heeft naar aanleiding van de voorlopige bevindingen aangegeven het inzagerecht voortaan in overeenstemming met de Wbp te verlenen.

Richtsnoeren

De camera's bij het bedrijventerrein filmen ook delen van de openbare ruimte en de met slagbomen afgesloten openbare wegen. De gemeente blijft voor dat gedeelte verantwoordelijk. In de onderzochte situatie heeft de gemeente door schriftelijke afspraken met de SBBV haar

verantwoordelijkheid voldoende gewaarborgd. De inzet van cameratoezicht in de openbare ruimte blijft echter veel vragen oproepen. Het CBP heeft daarom besloten hiervoor richtsnoeren op te stellen.

Binding Corporate Rules

Multinationals kunnen intern bindende gedragscodes, *Binding Corporate Rules* (BCR's), opstellen voor de doorgifte van persoonsgegevens aan landen buiten de Europese Unie. Met de BCR's is het mogelijk om de bescherming van persoonsgegevens binnen één organisatie met vestigingen buiten de Europese Unie te verzekeren. De BCR's kunnen worden ingepast in de bestaande werkprocessen en managementstructuren en zijn een flexibele oplossing voor doorgifte van persoonsgegevens binnen een multinational.

Een groeiend aantal Europese privacy-toezichthouders heeft afgesproken om tot wederzijdse erkenning over te gaan van elkaars beoordelingen van de BCR's. De afspraak houdt in dat andere privacytoezichthouders de analyse van de leidende toezichthouder – de *lead DPA* – overnemen van een BCR die moet worden goedgekeurd. Hiermee wordt de procedure voor goedkeuring van de BCR's voor bedrijven aanzienlijk versneld. Het CBP was aan het einde

van 2009 *lead DPA* voor vier BCR's. Dat houdt in dat het CBP in de zogeheten coördinatieprocedure het voortouw neemt bij het beoordelen en goedkeuren van de BCR's. In 2009 hebben verschillende buitenlandse *lead DPA's* het CBP in totaal vijf keer verzocht om deel te nemen aan deze procedure van wederzijdse erkenning van BCR's. Het CBP heeft deze verzoeken gehonoreerd.

Zwarte lijsten

Diverse bedrijfstakken worden regelmatig geconfronteerd met structurele of ernstige vormen van overlast en criminaliteit. Dit wordt strafrechtelijk aangepakt, maar bedrijven en brancheorganisaties werken daarnaast zelf in toenemende mate aan het verbeteren van de veiligheid van hun klanten, personeel en bedrijfsmiddelen. Een belangrijk middel hierbij vormen 'zwarte lijsten' of waarschuwingsregisters. Daarin kunnen gegevens over overlastplegers en criminelen worden geregistreerd en uitgewisseld met deelnemende bedrijven met het doel te voorkomen dat het overlastgevende of criminele gedrag opnieuw tot schade of slachtoffers leidt.

Omdat plaatsing op een zwarte lijst diep kan ingrijpen in de persoonlijke levenssfeer van een geregistreerde persoon, is de verantwoordelijke verplicht een zwarte lijst vooraf te melden bij het CBP, dus al bij het voornemen een zwarte lijst aan te leggen. Indien op de lijst strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag geplaatst worden met de bedoeling deze informatie uit te wisselen met anderen stelt het CBP doorgaans een zogeheten voorafgaand onderzoek in. Als het CBP voldoende transparante en effectieve waarborgen aantreft waardoor de belangen van zowel het bedrijfsleven als van de geregistreerde persoon op een zorgvuldige wijze worden afgewogen, geeft het CBP een rechtmatigheidsverklaring af. Het CBP heeft in 2009 een rechtmatigheidsverklaring afgegeven voor onder meer de volgende twee zwarte lijsten.

Het ELENA waarschuwingssysteem van de Bond van Autohandelaren en Garagehouders (BOVAG), afdeling Verhuurbedrijven registreert meldingen over strafbare feiten of onrechtmatige gedragingen van huurders en maakt deze toegankelijk voor deelnemende verhuurbedrijven. Malafide huurders kunnen daardoor voortijdig worden geïdentificeerd, zodat schade aan voertuigen en geweld jegens personeel en klanten van de bedrijven kan worden voorkomen.

Om spelverruwing en wangedrag in het amateurvoetbal een halt toe te roepen, heeft de Koninklijke Nederlandse Voetbalm Bond (KNVB) de Lijst Landelijk Voetbalverbod ingevoerd waarop spelers – na een tuchtrechtelijke veroordeling – worden geregistreerd en zo van de voetbalvelden geweerd worden. De lijst is een signaleringssysteem dat voorkomt dat geschorste, geroyeerde en/of uit het lidmaatschap ontzette spelers lid worden van een andere KNVB-voetbalvereniging en deze vereniging met hetzelfde ontoelaatbare gedrag confronteren.

Internationaal

De verwerking van persoonsgegevens houdt niet op bij de Nederlandse grens. In toenemende mate worden op internationaal en Europees niveau op grote schaal persoonsgegevens verwerkt voor uiteenlopende doelen. Om persoonsgegevens van betrokkenen ook buiten de grens een hoog beschermingsniveau te bieden, is effectief geharmoniseerd toezicht nodig. Afstemming van beleid en samenwerking met de andere privacytoezichthouders in de Europese Unie en de rest van de wereld is daarvoor van groot belang.

De toekomst van privacy

Moet de Europese privacyrichtlijn van 1995 worden herzien en zo ja, op welke punten? Deze vraag is in 2009 in diverse Europese fora uitvoerig aan de orde geweest. Als voorzitter van de voorbereidende werkgroep van de Artikel 29-werkgroep van Europese privacytoezichthouders (WP29) heeft het CBP een grote rol gespeeld in de gezamenlijke standpuntbepaling van WP29 en de Werkgroep Politie en Justitie [Working Party on Police and Justice (WPPJ)], die op 1 december 2009 naar buiten is gebracht. De Europese toezichthouders concluderen dat de basisbeginselen van de bescherming van persoonsgegevens nog steeds goed functioneren, ondanks globalisering en nieuwe technologieën. Een betere toepassing in de praktijk van de bestaande beginselen kan het niveau van de bescherming van persoonsgegevens wel ten goede komen. Dit betekent niet dat er geen wijzigingen in de wet- en regelgeving nodig zijn. Integendeel, het is opportuun om deze gelegenheid te gebruiken om:

- de toepassing van sommige hoofdregels en beginselen van de bescherming van persoonsgegevens (zoals toestemming en transparantie) te verduidelijken;
- het raamwerk te vernieuwen door aanvullende principes te introduceren (zoals *privacy by design* en *accountability*);
- de effectiviteit van het systeem te verbeteren door bepaalde regelingen in Richtlijn 95/46/EC te moderniseren, bijvoorbeeld door het beperken van administratieve lasten en
- de fundamentele beginselen van de bescherming van persoonsgegevens op te nemen in één overkoepelend juridisch raamwerk, dat eveneens van toepassing is op de samenwerking door politie en justitie bij strafrechtelijke aangelegenheden.

De toezichthouders leggen verder onder meer nadruk op het versterken van de rollen van de verschillende actoren. De betrokkene moet in staat worden gesteld een actievere rol te spelen bij de bescherming van zijn persoons-



gegevens. De toerekenbaarheid en aansprakelijkheid van de verantwoordelijke moet worden vergroot. De rol van de nationale toezichthouders moet sterker en duidelijker zijn, in lijn met de huidige koers van het CBP.

Bijzondere aandacht krijgen de uitdagingen voor de bescherming van persoonsgegevens op het terrein van politie en de handhaving van de orde. De laatste jaren heeft in deze sector een ingrijpende toename plaatsgevonden van de opslag en uitwisseling van persoonsgegevens. Deze mede door technologische ontwikkelingen gestimuleerde toename is het gevolg van een groeiende behoefte aan informatie om nieuwe bedreigingen op het gebied van terrorisme en de georganiseerde misdaad het hoofd te kunnen bieden. In dit licht bezien zijn de uitdagingen voor de bescherming van persoonsgegevens immens. Het nieuwe juridische raamwerk moet deze uitdagingen het hoofd bieden.

Internationale standaarden


Het fundamentele recht op bescherming van persoonsgegevens en de persoonlijke levenssfeer moet niet alleen in Nederland en in Europa, maar wereldwijd worden gegarandeerd. De Internationale Conferentie van Privacytoezichthouders heeft in november 2009 te Madrid, met steun van onder meer het CBP, een resolutie aangenomen waarmee het 'Joint Proposal for the Draft of International Standards for Privacy and Data Protection' is verwelkomd.

Het 'Joint Proposal' is gebaseerd op beginselen uit verschillende bestaande internationale instrumenten, richtlijnen en aanbevelingen waarover brede consensus bestaat in hun respectievelijke geografische, economische of juridische domein. Inhoudelijk sluit het voorstel aan op de hierboven besproken opinie van de WP29 over de Future of Privacy.

Trans-Atlantische relaties

De spanning tussen de Verenigde Staten en Europa over de overdracht en bescherming van persoonsgegevens neemt toe. Bekende dossiers zijn de overeenkomst tussen de VS en de EU over de overdracht van passagiersgegevens (PNR-overeenkomst) en de onderhandelingen over een akkoord voor de overdracht van financiële gegevens van Europeanen (SWIFT). Ook worden er in toenemende mate verzoeken gericht aan Nederlandse bedrijven om buiten de officiële (rechtshulp)kanalen om persoonsgegevens te verstrekken.

Het CBP heeft de afgelopen jaren vaak zorgen geuit over de wijze waarop overeenkomsten tot overdracht van persoonsgegevens tot stand komen en de wijze waarop officiële kanalen voor de overdracht van gegevens worden omzeild. Ook de onmogelijkheid voor Europese burgers en Europese privacytoezichthouders om het verdere gebruik van persoonsgegevens te controleren is verontrustend.



Ondanks de grote verschillen in de benadering van persoonsgegevens aan weerszijden van de oceaan, lijkt de bescherming van persoonsgegevens onder de regering-Obama van de vs hernieuwde aandacht te krijgen. Aangezien dit de kans op een constructieve dialoog tussen de EU en de vs vergroot, bracht CBP-voorzitter Jacob Kohnstamm in november 2009 een bezoek aan de vs om met de nieuwe Amerikaanse privacyfunctionarissen te bespreken in hoeverre de conflicten tussen de vs en de EU op dit terrein overbrugbaar zijn.

De gesprekken met overheidsfunctionarissen, non-gouvernementele organisaties en privacyactivisten hebben de bereidheid aangetoond van de Amerikaanse partners om een intensieve discussie aan te gaan met de EU over de voor- en nadelen van de privacyssystemen aan beide zijden van de oceaan.

Verdere activiteiten van de Artikel 29-werkgroep

Naast de herziening van de EU-privacyrichtlijn heeft de WP29 zich in 2009 met een reeks materiële dossiers beziggehouden. Daarvan zijn de sociale netwerksites en de bescherming van de privacy van kinderen hiervoor al aan de orde geweest. Overige onderwerpen waren onder meer:

Internationale anti-doping standaard

Hoewel doping in de sport dient te worden bestreden, is de privacystandaard van de internationale dopingautoriteit, de World Anti-Doping Agency (WADA) te rigoureuus en in strijd met privacywetgeving. De WP29 heeft WADA aanbevolen deze aan te passen. Voorafgaande aan controle op de 'whereabouts' van de sporters moet een risicoanalyse worden gemaakt, mag alleen de noodzakelijke informatie worden opgevraagd en mag de controle niet disproportioneel zijn. Publicatie van sancties op internet zou kunnen worden vervangen door maatregelen te kiezen die minder ingrijpend zijn voor de persoonlijke levenssfeer. Ook mag toestemming van de sporters geen wettelijke grondslag zijn voor de verwerking van hun persoonsgegevens. De toestemming is in dit kader namelijk niet vrijelijk gegeven, gezien de consequenties die zijn verbonden aan het weigeren van medewerking.

Pre trials

Verantwoordelijken die onder de Europese privacywetgeving vallen, kunnen een verzoek krijgen persoonsgegevens te verstrekken naar andere landen voor gebruik in een civiele procedure. De WP29 heeft een werkdocument met richtlijnen gepubliceerd voor de internationale doorgifte van persoonsgegevens bij zulke civiele (voor)procedures. Het werkdocument is onder andere van belang voor bedrijven die

betrokken raken bij procedures in de vs. Het beschrijft de verschillen in procesrecht en het verzamelen van bewijs in (voor)procedures tussen de *civil law* stelsels en *common law* stelsels. Het geeft vervolgens richtlijnen voor verantwoordelijken die proberen de eisen van de Europese privacyrichtlijn te verenigen met de procesrechtelijke eisen van buitenlandse rechtsstelsels. De richtlijnen hebben onder meer betrekking op bewaartermijnen, grondslagen voor de verwerking van persoonsgegevens, proportionaliteit, transparantie, beveiliging en het recht op inzage, verwijdering en correctie.

Meldplicht datalekken

De Europese privacytoezichthouders zijn voorstander van een brede meldplicht voor datalekken. In hun *Opinie over de herziening van de Europese e-privacyrichtlijn* pleiten zij voor invoering van een brede meldplicht bij verlies, diefstal of misbruik van persoonsgegevens. De meldplicht moet gelden voor iedereen die diensten levert op internet en niet alleen voor telefoon- en internetaanbieders. Datalekken die nadelige gevolgen kunnen hebben voor de privacy van betrokkenen moeten zowel gemeld worden aan de betrokkenen zelf als aan de nationale toezichthouder. Als de meldplicht niet wordt nageleefd, moet de toezichthouder bovendien een boete kunnen opleggen.

Geen online toegang DNA- en vingerafdrukken-databanken voor niet-EU-landen

Het sluiten van bilaterale overeenkomsten met landen buiten de EU over toegang tot Europese vingerafdruk- en DNA-databanken, vergt een gemeenschappelijke Europese aanpak. Zo kan worden voorkomen dat door een lappendeken van regels grote verschillen in beschermingsniveau ontstaan bij de uitwisseling van deze gevoelige gegevens. De Working Party on Police and Justice (WPPJ), een werkgroep van de Europese Conferentie van Data Protectie Toezichthouders, heeft lidstaten opgeroepen om – als besloten wordt een bilaterale overeenkomst aan te gaan – onder meer te zorgen dat geen online toegang wordt verleend tot vingerafdruk- en DNA-databanken, maar alleen indirecte toegang door tussenkomst van een nationaal contactpunt.

De overeenkomsten zouden volgens de WPPJ verder heldere en krachtige waarborgen voor de gegevensbescherming moeten bevatten. Bovendien moeten lidstaten voldoende informatie inwinnen over de relevante omstandigheden voor de gegevensbescherming in het derde land waarmee de overeenkomst wordt aangegaan. Tot slot is ook van groot belang dat volledige parlementaire controle plaatsvindt.

Opsporingsdiensten geen toegang tot Eurodac

De Europese Commissie heeft in september 2009 voorgesteld om opsporingsdiensten van de EU-lidstaten toegang te verschaffen tot Eurodac, de EU-brede database voor het vergelijken van vingerafdrukken van vreemdelingen. Lidstaten nemen in hun land vingerafdrukken af van asielzoekers en van in hun land illegaal verblijvende personen en vergelijken deze op basis van een *hit/no hitsysteem* met de in de Eurodac-database aanwezige gegevens. Op deze manier kan worden vastgesteld welke lidstaat verantwoordelijk is voor de afhandeling van een asielverzoek.

De WPPJ heeft ernstige kritiek geuit op het 'ongefundeerde voorstel' van de Europese Commissie. De database bevat persoonsgegevens van een groep zeer kwetsbare personen en het Eurodac-systeem is voor een heel ander doeleinde opgezet dan terrorismebestrijding. Bovendien zijn er volgens de werkgroep al genoeg andere databases en informatiebronnen beschikbaar voor opsporingsdiensten en heeft de Commissie niet aangetoond waarom toegang tot Eurodac echt nodig is in de strijd tegen terrorisme en grensoverschrijdende ernstige criminaliteit. Het voorstel van de Commissie is in strijd met fundamentele beginselen van gegevensbescherming, waaronder de proportionaliteit van de gegevensverwerking en respect voor de doelbinding. De WPPJ zal zich in 2010

dieper buigen over het voorstel van de Commissie. In de tussentijd doet de werkgroep een klemmend beroep op het Europees Parlement en de Raad om een fundamenteel debat te beginnen over dergelijke initiatieven, gezien de mogelijk verstreckende gevolgen ervan voor de fundamentele rechten van burgers.

Gemeenschappelijke toezichhoudende organen

Het CBP is toezichthouder op het nationale gedeelte van systemen ten behoeve van Europese politie- en justitiesamenwerking, bijvoorbeeld de nationale invoer van gegevens bij Europol. Daarnaast is het CBP vertegenwoordigd in verschillende gemeenschappelijke toezichhoudende organen. Deze adviseren over de bescherming van persoonsgegevens in de verschillende systemen, nemen gemeenschappelijke standpunten in en bereiden gemeenschappelijke inspecties en onderzoeken voor. In 2009 zijn onder de loep genomen: gegevensverwerking door Europol, signaleringen in het Schengen Informatie Systeem (SIS) in het kader van terrorismebestrijding, signaleringen van vermiste en op te sporen personen en signalering van getuigen of andere personen op verzoek van de bevoegde justitiële instanties op grond van de Schengen Uitvoeringsovereenkomst, het toezicht op het SIS en het functioneren van Eurodac.

De evaluatie van de Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens is op 1 september 2001 in werking getreden. In de daaropvolgende jaren hebben zich revolutionaire technologische ontwikkelingen voltrokken. Denk onder meer aan het toenemend gebruik van internet, biometrie, kilometerbeprijzing, de OV-chipkaart, datamining en profiling. Biedt de Wbp in dit kader nog voldoende bescherming aan burgers en is vermindering van de uit de wet voortvloeiende lasten voor verantwoordelijken mogelijk zonder voor betrokkenen het gewenste beschermingsniveau op onaanvaardbare wijze aan te tasten? Dit zijn kernvragen bij de lopende evaluatie van de wet.

In reactie op de evaluatierapporten van de Wbp van mei 2007 respectievelijk februari 2009, het rapport van de Commissie Brouwer-Korf van januari 2009 over veiligheid en persoonlijke levenssfeer en het kabinetsstandpunt van 3 november 2009 over deze rapporten, vraagt het CBP aandacht voor de volgende drie onderwerpen:

- 1 de positie van de burger
- 2 de positie van de verantwoordelijke en
- 3 de positie van de toezichthouder.

Positie van de burger

Burgers moeten op een eenvoudige en toegankelijke manier kennis kunnen nemen van het doel van de gegevensverwerking, de waarborgen die zijn genomen om onrechtmatig gebruik van hun gegevens tegen te gaan en de

wijze waarop zij hun rechten kunnen uitoefenen (transparantie). Dat betekent dat verantwoordelijken hieraan veelal op een andere wijze invulling moeten geven.

Daarnaast moet worden gezocht naar laagdrempelige klachtenregelingen omdat de gang naar de rechter voor velen lastig en kostbaar is. De toezichthouder is voor individuele klachtenbehandeling en bemiddeling niet (meer) de eerst aangewezen. Daarom moet aansluiting worden gezocht bij bestaande klachtloketten en/of moet worden overgegaan tot de instelling van sectorale klachteninstanties. Tevens moet worden bezien of het instellen van *class actions*, bijvoorbeeld met behulp van consumentenorganisaties, mogelijk wordt.

Positie van de verantwoordelijke

Er vindt een verschuiving plaats van *ex ante* toezicht naar *ex post* toezicht waarbij wellicht procedurele verplichtingen verdwijnen (zoals het melden van gegevensverwerkingen bij de toezichthouder en het zogeheten voorafgaand onderzoek). In het kabinetsstandpunt van 3 november 2009 zijn in dit kader te weinig verplichtingen voor de verantwoordelijke opgenomen om een zorgvuldige verwerking van persoonsgegevens te waarborgen, terwijl *compliance* niet te vrijblijvend mag zijn. Bedrijven en overheden hebben de verantwoordelijkheid zelf in *compliance* te investeren. De toezichthouder stimuleert dit door het bieden van instrumenten als richtsnoeren en zienswijzen en verbindt tegelijkertijd consequenties aan *non compliance*.

Het CBP stelt in dit licht het volgende voor:

- actievere invulling van de transparantieverplichting, bijvoorbeeld via privacy-statements;
- verplichte melding van datalekken (zoals verlies, diefstal en misbruik van persoonsgegevens);
- toepassing van *privacy by design*, zowel in technologische als in organisatorische zin. Hierdoor wordt misbruik, oneigenlijk en onrechtmatig gebruik van persoons-

gegevens zoveel mogelijk voorkomen. Bij gegevensverwerkingen die een aanzienlijke inbreuk op de persoonlijke levenssfeer kunnen meebrengen kan de verantwoordelijke vooraf een *Privacy Impact Assessment (PIA)* uitvoeren.

Positie van de toezichthouder

Het CBP constateert dat de regering in haar brief van 3 november 2009 schreef dat het CBP adequate boete- en handhavingsbevoegdheden nodig heeft om een robuuste toezichthouder te zijn. De onafhankelijkheid en de rolvastheid van de toezichthouder zijn hierbij essentieel. Het CBP concentreert zich op handhaving van de wet. Dat betekent dat het zijn bevoegdheden met name inzet op die zaken waar sprake is van structurele overtreding van de Wbp die grote groepen mensen raakt en waar het CBP met zijn bevoegdheden kan optreden. Dat heeft onder meer tot gevolg dat de toezichthouder overheden en bedrijven wel instrumenten biedt als richtsnoeren en zienswijzen, maar niet meer optreedt als adviseur voor individuen, bedrijven en overheden. Er is geen plaats meer voor advisering op maat en er zal een verschuiving plaatsvinden naar controles *ex post* in plaats van *ex ante*. Wetgevingsadvisering blijft een kerntaak van het CBP.



College en Organisatie

Het CBP heeft ervoor gekozen als toezichthouder de prioriteit bij handhaving te leggen in de overtuiging zo de meest effectieve bijdrage te kunnen leveren aan de bevordering van de naleving van de Wet bescherming persoonsgegevens. De rol van adviseur van individuele bedrijven en overheden heeft het dan ook achter zich gelaten. Dit betekent geenszins dat het CBP bedrijven, overheden en burgers in de steek laat. Het CBP is zich terdege bewust van de noodzaak tot uitleg van de normen en het geven van algemene voorlichting. Naast informatie op de websites biedt het CBP in dit kader een aantal instrumenten, zoals richtsnoeren en zienswijzen. In richtsnoeren geeft het CBP op deelgebieden aan welke uitleg van wettelijke voorschriften het CBP in zijn handhavingspraktijk hanteert. Op verzoek kan het CBP een 'zienswijze' opstellen als sprake is van een nieuwe rechtsvraag en van een groot (potentieel) maatschappelijk en/of economisch belang.

Het CBP kan uit eigen beweging onderzoek instellen naar de naleving van de wet en maakt in toenemende mate gebruik van deze bevoegdheid. In 2009 zijn 108 controlerende onderzoeken gedaan naar de manier waarop in de praktijk persoonsgegevens worden verwerkt, beduidend meer dan in voorgaande jaren. Daarnaast zijn voorafgaande onderzoeken gedaan naar voorgenomen verwerkingen waaraan bijzondere risico's kleven, zoals het opstellen van zwarte lijsten.

Het CBP adviseert de regering over voorgenomen wetgeving die betrekking heeft op de verwerking van persoonsgegevens. Het aantal wetgevingsadviezen blijft de laatste jaren op hetzelfde niveau; in 2009 waren dat er achtendertig.

Het aantal telefoontjes en mails in 2009 met vragen en verzoeken om advies bedroeg 5964, een daling van circa 10% ten opzichte van het jaar daarvoor. Antwoorden op veelgestelde vragen zijn te vinden op de websites. Burgers kunnen via de site www.mijnprivacy.nl een signaal afgeven over het gebruik van hun persoonsgegevens in de praktijk. In 2009 ontving het CBP zo 1098 signalen.

Eind 2009 werkten 90 mensen bij het CBP (81,50 fte's, vier vacatures). Gemiddeld was de bezetting 77 fte's. Als gevolg van de opgelegde taakstelling zal in 2010 het totaal aantal fte's niet boven de 82 mogen komen.

College 2009



Mr. J. Kohnstamm
Voorzitter



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



Mw. mr. M.W. McLaggan
Collegelid

Directie



Drs. P.J.J. Frencken
Directeur



Raad van Advies

De Raad van Advies van het CBP bestaat uit deskundigen uit verschillende maatschappelijke sectoren. Eind 2009 telde de Raad dertien leden. De Raad komt tweemaal per jaar bijeen. De leden van de Raad van Advies zijn:

Mevrouw drs. T.A. Maas-de Brouwer

Voorzitter, lid Raad van Commissarissen van o.m. ABN-AMRO, oud-senator pvda

De heer R.J.G. Bandell

Oud-burgemeester van Dordrecht, oud-voorzitter Nederlands Genootschap van Burgemeesters

De heer drs. H.G.M. Blocks

Adviseur/bestuurder, oud-directeur Nederlandse Vereniging van Banken

De heer drs. H.W. Broeders

Lid directieteam Capgemini

Mevrouw H.C.J. van den Burg

Oud-lid Europees Parlement, lid Raad van Commissarissen ASML (vanaf augustus 2009)

De heer drs. B.R. Combée

Directeur Consumentenbond (vanaf augustus 2009)

De heer prof. mr. E.J. Dommering

Hoogleraar informatierecht Universiteit van Amsterdam

De heer prof. mr. dr. J.K.M. Gevers

Hoogleraar gezondheidsrecht Universiteit van Amsterdam

De heer mr. R.J. Manschot

Oud-hoofdofficier van Justitie, oud-vice-voorzitter Eurojust, bestuurslid Amnesty International Nederland

De heer drs. L. J.E. Smits

Directeur Het Expertise Centrum, directeur ROI Opleiding Coaching & Advies

De heer drs. G.M. de Vries

Collegelid Algemene Rekenkamer en oud-terrorismecoördinator voor de Europese Unie

De heer mr. A.A. Westerlaken

Lid Raad van Bestuur Erasmus MC

De heer drs. L.J. Wijngaarden

Beroepscommissaris, voorheen CEO Postbank en CEO Nationale Nederlanden (vanaf augustus 2009)

Afgetreden in 2009 zijn

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

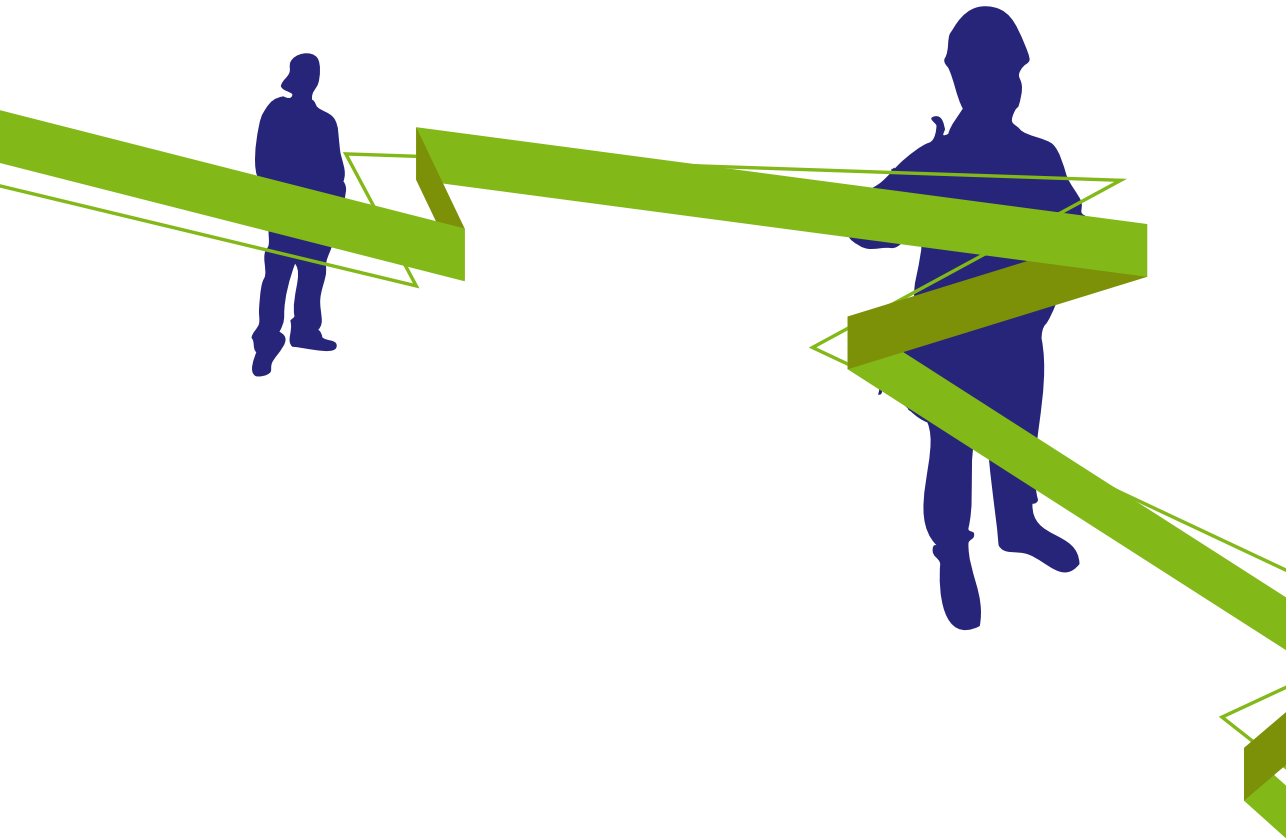
Hoogleraar sociaal recht aan de Radboud Universiteit Nijmegen en lid SER

De heer drs. F. Cohen

Oud-directeur van de Consumentenbond

De heer prof. dr. E.J. Fischer

Bijzonder hoogleraar bedrijfsgeschiedenis Universiteit van Amsterdam.



Colofon

Het CBP in 2009

©College bescherming persoonsgegevens, Den Haag, april 2010

ISBN/EAN: 978-90-74087-46-9

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

Ontwerp en illustraties: Proforma, ontwerpers en adiseurs, Janine Terlouw

Foto's: Mark Kohn

Druk: DeltaHage BV

Het CBP in 2009 behandelt een selectie van onderzoeken en wetgevingsadviezen van het CBP in 2009. Een uitgebreid Jaarverslag is gepubliceerd op de website www.cbpweb.nl.

Op deze site en op de site www.mijnprivacy.nl is tevens meer informatie te vinden over de activiteiten van het College bescherming persoonsgegevens.



COLLEGE BESCHERMING PERSOONSGEGEVENS

Juliana van Stolberglaan 4-10
2595 CL Den Haag

Postbus 93374
2509 AJ Den Haag

T 070 888 85 00
F 070 888 85 01
info@cbpweb.nl

www.cbpweb.nl
www.mijnprivacy.nl

