Het CBP in 2012

COLLEGE BESCHERMING PERSOONSGEGEVENS

Iedereen heeft recht op een zorgvuldige omgang met zijn of haar persoonsgegevens. Door de toenemende digitalisering en globalisering groeit het aantal gegevensverwerkingen onophoudelijk. In dit licht is het des te belangrijker dat overheden en bedrijven persoonsgegevens slechts in overeenstemming met de wet verzamelen en gebruiken.

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. In voorkomende aangelegenheden werkt het CBP samen met andere toezichthouders, zowel op nationaal als internationaal niveau.

INHOUD

VOORWOORD

Bescherming van persoonsgegevens staat steeds vaker volop in de schijnwerpers. "Paspop bespiedt klant" (Spits); "Vertrouwelijke informatie op straat door lek randapparatuur" (Trouw); "Gemeenten slordig met privégegevens" (NRC)"; "Albert Heijn weet meer van ons dan de burgemeester" (Volkskrant), zijn een paar voorbeelden van de talloze koppen uit kranten van 2012.

Burgers zijn zich veelal onvoldoende bewust van de mogelijke gevolgen die het verzamelen en gebruiken van persoonsgegevens met zich brengen. Maar de schok – ook bij hen die zeggen niets te verbergen te hebben – is des te groter als blijkt dat in vertrouwen verstrekte gegevens op straat komen te liggen, dan wel dat zij zonder dat daarvoor een reden is, niet meer onbespied door het leven kunnen gaan.

De reactie van overheid en bedrijfsleven is op onderdelen hoopgevend. Zo gaan in het bedrijfsleven stemmen op om privacy als 'unique selling point' in te zetten. Ook het regeerakkoord kent een hogere prioriteit toe aan de verbetering van de bescherming van persoonsgegevens: op onrechtmatige verzameling en verwerking van persoonsgegevens komt een forse boete te staan.

Op Europees niveau is in 2012 eveneens een belangrijke stap gezet naar het bij de tijd brengen van de gegevensbescherming in de Europese Unie. In januari van dat jaar presenteerde de Europese Commissie (EC) een voorstel voor nieuwe wetgeving met als doel versterking, verbetering en versimpeling van de bescherming van persoonsgegevens. De discussie in het Europees Parlement (EP) en de Raad van Ministers (de Raad) en die tussen de EC, het EP en de Raad over de voorstellen voor nieuwe bindende wetgeving zijn op het moment van dit schrijven in volle gang.

Die discussie is op onderdelen echter ook zorgwekkend, daar waar sommige deelnemers aan het debat pleiten voor aanzienlijke verlaging van het huidige niveau van de bescherming van persoonsgegevens.

Zo circuleren in het EP voorstellen tot versmalling van de definitie van persoonsgegevens en bepleiten sommigen dat toestemming als grond voor gegevensverwerking stilzwijgend gegeven moet kunnen worden. Bovendien ligt een van de pijlers onder de bescherming van persoonsgegevens onder vuur, te weten doelbinding, het principe dat verder gebruik van persoonsgegevens verenigbaar moet zijn met het oorspronkelijke doel van de verzameling en verwerking.

Ook uit de kring van de Raad zijn zorgwekkende geluiden te horen, in het bijzonder daar waar gepleit wordt voor het inbouwen van grotere flexibiliteit voor de overheid bij de toepassing van de bepalingen van de voorgestelde EU-verordening.

Natuurlijk: voor politie en justitie gelden andere normen dan voor het bedrijfsleven. In het geval van een redelijke verdenking van strafbare handelingen hebben justitie en politie – binnen de aan de geweldsmonopolist gestelde wettelijke grenzen – nu juist de plicht om te grasduinen in persoonsgegevens! Reden waarom er voor justitie en politie een voorstel ligt voor een aparte EU-richtlijn. Maar de overheid is meer dan politie en justitie alleen, bijvoorbeeld op vele andere in de relatie tussen de overheid en burgers zo bepalende terreinen: belasting, sociale zekerheid, jeugdbeleid, onderwijs, verkeer en waterstaat et cetera.

Nu is in de conceptverordening voor de overheid met recht een aantal afwijkende bepalingen opgenomen ten opzichte van het bedrijfsleven. Maar in de onderhandelingen over de conceptverordening gaan, zoals gezegd, enkele lidstaten – waaronder Nederland – een stap verder en bepleiten een nog grotere flexibiliteit voor de publieke sector dan waarin thans reeds is voorzien. Het CBP, samen met de andere privacytoezichthouders in de EU, is kritisch over dat pleidooi, in hoofdzaak om drie redenen.

Ten eerste is de overheid vermoedelijk op afstand de grootste verzamelaar van persoonsgegevens, waarbij burgers daarenboven veelal op grond van wettelijke bepalingen verplicht zijn die gegevens aan de overheid te verschaffen. Noblesse oblige; en dus dient de overheid zich bij uitstek aan de voor de bescherming van persoonsgegevens essentiële randvoorwaarden te houden.

Vervolgens ligt, aangemoedigd door technologische ontwikkelingen in combinatie met de wens om taken van de overheid efficiënter en klantgerichter te vervullen, het gevaar van 'function creep' op de loer. De digitale hooiberg die door de genoemde ontwikkelingen toch al dreigt te ontstaan, nodigt al snel uit om in strijd met onder meer het principe van doelbinding allerlei koppelingen tussen de onderscheiden databases tot stand te brengen. Het voornemen van de regering om allerlei taken van het Rijk naar gemeenten over te hevelen zal deze tendens bijna zeker verder versterken. Voor de burger (en mogelijk ook voor de overheid) is het vervolgens nauwelijks inzichtelijk meer welke gegevens zich waar en waarom over hem bevinden. Daarmee dreigt ook een andere essentiële doelstelling van de bescherming van persoonsgegevens – die van transparantie – 'flexibel' achter de horizon te verdwijnen.

Ten slotte is in de EU bepaald dat bescherming van persoonsgegevens een grondrecht is. Grondrechten zien in eerste instantie – zeker in historisch perspectief – op de verhouding tussen overheid en burger. Het inbouwen van grotere flexibiliteit voor de publieke sector bij de toepassing van de bepalingen in de verordening zou tot de curieuze situatie kunnen leiden dat het grondrecht op bescherming van persoonsgegevens alleen onverkort van toepassing wordt op de verhouding tussen burger en bedrijfsleven.

De discussie en besluitvorming over de in 2012 ingediende conceptprivacyverordening van de EU zal in het komende jaar in een stroomversnelling raken. Alle belangen die daarbij een rol spelen zullen afgewogen moeten worden. In de uiteindelijke wetstekst zal met recht en rede de vertaalslag gevonden moeten worden van het grondrecht op de bescherming van persoonsgegevens, waaraan zowel de overheid als het bedrijfsleven zich hebben te houden.

Jacob Kohnstamm
Voorzitter College bescherming persoonsgegevens

INLEIDING

Profilering, adequate bescherming van medische gegevens en beveiliging van persoonsgegevens vormden in 2012 voor het CBP belangrijke speerpunten. Het CBP heeft daarbij in het bijzonder gelet op de wijze waarop bedrijven en organisaties mensen informeren over gegevensverwerkingen en hiervoor – voor zover dit wettelijk is voorgeschreven – toestemming vragen.

Veel mensen hebben geen zicht op de aard en de gevolgen van het (her)gebruik van hun persoonsgegevens, dat onder invloed van de groeiende technologische mogelijkheden enorm toeneemt. Het CBP richtte zich in het afgelopen jaar daarom vooral op het blootleggen van voor burgers veelal onbekende gegevensverwerkingen. Van de rechtsgronden waarop persoonsgegevens verzameld en verwerkt mogen worden, is die van toestemming in die situatie vaak de zwakste schakel. Daarom bestudeerde het CBP in veel van zijn onderzoeken of aan de vereisten van een rechtsgeldige toestemming was voldaan.

Een selectie uit de activiteiten van het CBP in 2012:

Profilering en marketing

Uit publieke uitingen bleek dat Albert Heijn van plan was persoonlijke analyses van klanten te maken op basis van hun aankoopgedrag om hun vervolgens gepersonaliseerde aanbiedingen te doen. Het CBP concludeerde na onderzoek dat de door Albert Heijn gevraagde toestemming niet voldeed aan de eisen die aan geldige toestemming worden gesteld. Uit een ander onderzoek van het CBP kwam naar voren dat NS het reisgedrag van OV-chipkaarthouders gedetailleerd vastlegde en deze gegevens vervolgens gebruikte voor marketingdoeleinden zonder de daarvoor benodigde toestemming van de reizigers.

Medische gegevens

Bij de onrust die ontstond rond het filmen van patiënten op de spoedeisende hulp van het VU medisch centrum speelde het toestemmingsvereiste een belangrijke rol. Het CBP concludeerde dat producent Eyeworks geen rechtsgeldige toestemming had verkregen voor het maken van deze opnamen, aangezien de patiënten niet vooraf en op basis van gedegen informatie ondubbelzinnig en uitdrukkelijk toestemming hadden gegeven. Van een rechtsgeldige toestemming kon ook overigens gegeven de concrete situatie geen sprake zijn geweest: de patiënten bevonden zich in een buitengewoon afhankelijke positie, namelijk op de spoedeisende hulp met een dringende hulpvraag.

In een ander onderzoek stelde het CBP vast dat Bureau Jeugdzorg Noord-Brabant psychologische testresultaten van werknemers verzamelde zonder rechtsgeldige toestemming. Van vrijelijk gegeven toestemming van de werknemers was geen sprake: als zij weigerden mee te werken aan een assessment, riskeerden de werknemers op staande voet te worden ontslagen.

Het CBP onderzocht in 2012 de interne toegang tot patiëntendossiers bij meerdere zorginstellingen. Bij in ieder geval een daarvan bleken onvoldoende beveiligingsmaatregelen te zijn getroffen om ervoor te zorgen dat uitsluitend bevoegde ziekenhuismedewerkers toegang konden krijgen tot de elektronische patiëntendossiers.

Beveiliging

De beveiliging van persoonsgegevens was een belangrijk thema voor het CBP in 2012. Het besteedde daarom veel aandacht aan het onderzoeken van (mogelijke) datalekken. Bij de onderzochte datalekken werd betrokkenen bijvoorbeeld vaak gevraagd op een webfor-

mulier persoonsgegevens in te vullen, die vervolgens onbeveiligd via het internet werden verstuurd. Het beveiligingsaspect speelde ook een grote rol bij een onderzoek naar WhatsApp, een populaire app voor smartphones waarmee berichten, foto's en video's kunnen worden verstuurd. De beveiliging van de app was op verschillende punten onder de maat, onder meer doordat WhatsApp de berichten via de app op onversleutelde wijze verstuurde. Hierdoor konden derden de inhoud daarvan in leesbare vorm onderscheppen, zonder dat de oorspronkelijke 'whatsapper' daar weet van had. Naar aanleiding van het onderzoek heeft WhatsApp terstond maatregelen genomen om het berichtenverkeer te versleutelen.

Het CBP constateerde in dit onderzoek tevens dat gebruikers van WhatsApp verplicht zijn toegang te geven tot het volledige adresboek op hun telefoon. Dit heeft tot gevolg dat het bedrijf álle telefoonnummers uit die adresboeken verzamelt, ook de nummers van contacten die geen WhatsApp gebruiken. Gebruikers kunnen er niet voor kiezen om alleen de nummers door te geven van contacten met wie zij ook echt willen whatsappen. Hierdoor hebben dus niet alleen de WhatsApp-gebruikers geen zeggenschap over welke gegevens zij willen delen, maar geldt dit zelfs voor mensen die de app niet gebruiken.

Internationale samenwerking

Op internationaal gebied richtte het CBP zich in 2012 op het versterken van de effectiviteit van het toezicht op de bescherming van persoonsgegevens door samen te werken met buitenlandse collega-toezichthouders. Bij mondiaal opererende verantwoordelijken horen mondiaal samenwerkende toezichthouders. Het genoemde onderzoek naar WhatsApp heeft het CBP dan ook samen met de Canadese privacytoezichthouder verricht. Samen met zijn Europese collega-toezichthouders deed het CBP onderzoek naar de nieuwe privacyvoorwaarden van Google. De nieuwe voorwaarden bleken op verschillende punten strijdig met de Europese regelgeving, onder meer omdat Google geen toestemming vroeg voor het koppelen van bepaalde persoonsgegevens.

Deze publicatie behandelt een selectie van onderzoeken en wetgevingsadviezen van het CBP in 2012. Een uitgebreid jaarverslag is gepubliceerd op **www.cbpweb.nl**. Op deze website en op **www.mijnprivacy.nl**, de publiekssite van het CBP, is tevens meer informatie te vinden over de werkzaamheden van het CBP.

GEZONDHEIDSZORG

Medische gegevens zijn gevoelige persoonsgegevens, waarmee organisaties uiterst zorgvuldig dienen om te gaan. Mensen moeten erop kunnen vertrouwen dat medische gegevens niet in verkeerde handen terechtkomen, zoals die van hun werkgever of onbevoegde ziekenhuismedewerkers. Adequate beveiliging van medische gegevens is daarom van cruciaal belang, evenals het vragen van toestemming om medische gegevens te verwerken.

Doorstart landelijk elektronisch patiëntendossier

Het CBP beoordeelde eind 2011/begin 2012 de plannen van de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) voor de private doorstart van het landelijk elektronisch patiëntendossier (EPD). De Eerste Kamer had in het voorjaar van 2011 het wetsvoorstel tot invoering van het landelijk EPD verworpen. Hierdoor is geen wettelijke basis tot stand gekomen voor de landelijke uitwisseling van medische gegevens. Daaropvolgend hebben verschillende organisaties in de gezondheidszorg gezamenlijk onderzocht of en in welke vorm het landelijk EPD op private basis alsnog doorgang zou kunnen vinden. Zij ontwikkelden hiervoor het zogeheten doorstartmodel.

Het CBP concludeerde dat dit model in theorie geen bijzondere risico's bevat voor overtreding van de Wet bescherming persoonsgegevens. Het doorstartmodel gaat uit van toestemming van patiënten als basis voor de verwerking van hun medische gegevens. Het CBP heeft er overigens op gewezen dat deze conclusie alleen geldt voor de beoordeling van het doorstartmodel en niets zegt over de wijze waarop daarmee in de praktijk wordt omgesprongen.

Eind oktober 2012 ontving het CBP informatie

van de VZVZ over de in 2012 geboekte voortgang bij het alsnog verkrijgen van toestemming van patiënten die al in het systeem waren opgenomen. Het CBP eiste van VZVZ dat – conform de in het doorstartmodel aangegeven planning – per 1 januari 2013 het systeem geschoond zou worden van gegevens van patiënten die vóór deze datum geen toestemming hadden verleend voor opname in het systeem. VZVZ liet hierop weten tot een dergelijke opschoning over te gaan.

Filmen op spoedeisende hulp ziekenhuis

De televisieopnamen die producent Eyeworks maakte op de spoedeisende hulp van het VU medisch centrum (VUmc) waren in strijd met de wet. Dit concludeerde het CBP na onderzoek dat het deed vanwege de onrust die was ontstaan rond het filmen van patiënten in dit ziekenhuis.

Eyeworks had de medische gegevens – opnamen op een afdeling spoedeisende hulp vallen hieronder – wettelijk gezien alleen mogen verwerken als de patiënten hiervoor vooraf en op basis van gedegen informatie ondubbelzinnig en uitdrukkelijk toestemming hadden gegeven. Eyeworks bleek in sommige gevallen achteraf om toestemming te hebben gevraagd. Daarnaast oordeelde het CBP dat de verstrekte informatie te summier was. Van een rechtsgeldige toestemming kon ook overigens gegeven de concrete situatie geen sprake zijn geweest: de patiënten bevonden zich in een buitengewoon afhankelijke positie, namelijk op de spoedeisende hulp met een dringende hulpvraag.

VUmc en Eyeworks zagen af van verdere uitzending van de gemaakte opnamen en het verkregen beeldmateriaal is vernietigd.

Medische gegevens zieke werknemers

Het verzuimbedrijf VerzuimReductie heeft zijn werkwijze aangepast na onderzoek van het CBP naar de verwerking van medische gegevens. Verzuimbedrijven houden zich in opdracht van werkgevers bezig met verzuimpreventie en re-integratie van zieke werknemers.

Werkgevers, of in hun opdracht werkende verzuimbedrijven, mogen voor de verzuimbegeleiding van zieke werknemers een beperkt aantal noodzakelijke medische persoonsgegevens verwerken, zoals de verwachte duur van het verzuim en de mate waarin een werknemer arbeidsongeschikt is. VerzuimReductie bleek echter aanzienlijk meer medische gegevens op te vragen, waaronder de oorzaak van het verzuim. Bovendien bleek dat de verzamelde medische informatie vaak ook toegankelijk was voor de werkgevers.

VerzuimReductie heeft alle onrechtmatig verzamelde medische gegevens in de lopende en afgesloten dossiers vernietigd. Werknemers zijn hierover geïnformeerd en hebben de tijd gekregen om de over hen verwerkte informatie op te vragen vóór de gegevens zijn vernietigd. Met het treffen van deze maatregelen zijn de geconstateerde overtredingen van de Wet bescherming persoonsgegevens beëindigd.

Onderzoek bij arbodienst en werkgever

Naast het onderzoek bij VerzuimReductie heeft het CBP in 2012 nog twee onderzoeken gedaan naar de verwerking van medische gegevens van zieke werknemers. De onderzoeken vonden plaats bij een arbodienst en bij een werkgever.

In beide (los van elkaar staande) gevallen constateerde het CBP dat werkgevers de beschikking hadden over medische gegevens van hun werknemers. Het ging daarbij om medische informatie die niet noodzakelijk was voor de re-integratie of begeleiding bij ziekte of arbeidsongeschiktheid. Voorbeelden hiervan

zijn aard en oorzaak van de ziekte, medicijngebruik en behandelingen.

Zowel de onderzochte werkgever als de arbodienst hebben hun werkwijze en de vragenlijsten voor werknemers aangepast. Ook hebben zij verklaard dat alle onrechtmatig verzamelde medische gegevens zijn vernietigd.

Psychologische testresultaten werknemers

Bureau Jeugdzorg Noord-Brabant (BJZ NB) verzamelde in strijd met de wet psychologische testresultaten van werknemers. Dit kwam naar voren uit onderzoek van het CBP.

Alle werknemers van BJZ NB waren sinds 2011 verplicht mee te werken aan een assessment voor personeelsbeoordeling en -ontwikkeling. Voor de verwerking van de testresultaten was geen wettelijke grondslag, omdat van vrijelijk daarvoor gegeven toestemming van de werknemers geen sprake was. Werknemers die weigerden mee te werken, riskeerden namelijk ontslag op staande voet. Eventueel wel verleende toestemming was daarom niet rechtsgeldig. Daarnaast oordeelde het CBP dat het verplicht laten afnemen van een assessment door alle medewerkers niet noodzakelijk is voor een goede bedrijfsvoering, waaronder valt het vergroten van de professionaliteit van de medewerkers. Deze kan namelijk ook op andere wijze worden vergroot, bijvoorbeeld door het volgen van vakgerichte opleidingen of andere cursussen.

Het door BJZ NB verplichte assessment bestond uit psychologische testen. Een deel van de testresultaten, de functiegerelateerde competenties, was behalve door de betreffende medewerker ook in te zien door de leidinggevende. De gegevens die bij de testen werden verzameld zijn gevoelig van aard. Zij zeggen iets over de psychische gesteldheid, vaardigheden en beperkingen van betrokkenen en kunnen zwaarwegende consequenties hebben voor de opstelling van de werkgever ten opzichte van de werknemer. BJZ NB heeft in reactie op het onderzoek aangegeven de testresultaten niet langer te gebruiken en deze te hebben vernietigd.

Doorbreken medisch beroepsgeheim

In december 2012 bracht het CBP een kritisch advies uit over een voorstel tot doorbreking van het medisch beroepsgeheim om van behandelend artsen bestaande medische gegevens te kunnen vorderen als verdachten weigeren aan tbs-onderzoek mee te werken. Deze gegevens worden vervolgens gebruikt om een mogelijke psychische stoornis te bepalen bij deze verdachten.

Het CBP constateerde dat de voorgestelde regeling – een wettelijke verplichting om het medisch beroepsgeheim te doorbreken – raakt aan de kern van de bescherming van de persoonlijke levenssfeer in de gezondheidszorg. Ook merkte het CBP op dat de regeling een trendbreuk inhoudt ten opzichte van de gangbare benadering en jurisprudentie in Nederland betreffende het medisch beroepsgeheim en dat daarvoor een overtuigende motivering ontbreekt.

Het doel van de voorgestelde regeling is bescherming van de maatschappij tegen de mogelijke veiligheidsrisico's die weigerachtige verdachten opleveren. Het CBP mist echter een beschouwing over alternatieve mogelijkheden om die risico's te verminderen. Verder treft de voorgestelde doorbreking van het medisch beroepsgeheim niet alleen de betreffende verdachten maar ook een grote groep (potentiële) patiënten met psychische en/of psychiatrische problemen, die mogelijk nalaten hulp te zoeken uit vrees voor doorbreking van het medisch beroepsgeheim.

In januari 2013 werd bekend dat de regering ook op andere gebieden tot regelingen wil

komen waardoor het medisch beroepsgeheim (wettelijk) doorbroken kan worden. Het CBP blijft mogelijke aantasting van het medisch beroepsgeheim ten principale aan de orde stellen.

Interne toegang patiëntendossiers

Het Ruwaard van Putten Ziekenhuis heeft onvoldoende beveiligingsmaatregelen getroffen om ervoor te zorgen dat uitsluitend daartoe bevoegde ziekenhuismedewerkers toegang hebben tot de elektronische patiëntendossiers. Dit concludeerde het CBP na onderzoek. Alleen medewerkers die rechtstreeks betrokken zijn bij de behandeling van patiënten mogen toegang hebben tot hun medische gegevens. Anderen mogen slechts (delen van) patiëntendossiers raadplegen als dit noodzakelijk is voor de uitoefening van hun functie.

Op basis van diverse signalen startte het CBP in 2012 een onderzoek naar de interne toegang tot patiëntendossiers bij meerdere instellingen voor gezondheidszorg, waaronder het Ruwaard van Putten Ziekenhuis. In 2013 volgen de onderzoeksresultaten over de andere zorginstellingen.

Elektronische gegevensuitwisseling in de zorg

In april 2012 adviseerde het CBP op verzoek van de minister van Volksgezondheid, Welzijn en Sport (VWS) over het wetsvoorstel elektronische gegevensuitwisseling in de zorg. Dit voorstel beoogt de patiënt meer rechten te bieden bij elektronische dossiervorming en gegevensuitwisseling door zorgaanbieders. Daarnaast komt er een algemene maatregel van bestuur (AMvB) waarin de beveiligingseisen worden geregeld.

Het CBP drong erop aan om in de aangekondigde AMvB te verwijzen naar de specifiek voor de zorg ontwikkelde beveiligingsnormen NEN 7510-7513 en daarnaast aandacht te schenken aan de beveiligingsaspecten van elektronische inzage. Het wetsvoorstel zelf dient naar het oordeel van het CBP erin te voorzien dat het onderscheid helder blijft tussen gegevens die de zorgverlener noteert en de aanvullingen van de patiënt hierop.

Het definitieve wetsvoorstel is op 4 januari 2013 ingediend bij de Tweede Kamer. Hierin is rekening gehouden met het advies van het CBP. Verder is aangegeven dat bij het opstellen van de AMvB de opmerking van het CBP over de NEN-normen zal worden meegenomen. Ook onderschrijft de minister van VWS het standpunt van het CBP dat deze AMvB uiterlijk tegelijkertijd met het wetsvoorstel in werking moet treden.

HANDEL & DIENSTEN

Persoonsgegevens zijn goud waard. Hoe meer bedrijven weten over hun klanten, hoe meer zij kunnen verdienen. Ze kunnen dan namelijk gericht(er) adverteren of gegevens doorverkopen aan andere bedrijven. Consumenten hebben echter ook rechten. Zo moeten bedrijven consumenten laten weten wat zij precies van plan zijn met hun persoonsgegevens en hiervoor in beginsel toestemming vragen.

Privacybeleid 'Mijn Bonus' van Albert Heijn

Albert Heijn heeft het privacybeleid van het nieuwe voordeelprogramma 'Mijn Bonus' aangepast na onderzoek van het CBP. Hiermee beëindigde Albert Heijn de door het CBP geconstateerde overtredingen van de Wet bescherming persoonsgegevens (Wbp).

Begin 2012 kondigde Albert Heijn aan een nieuw programma in te voeren met persoonlijke aanbiedingen voor bonuskaarthouders. Bij 'Mijn Bonus' gaat het om aanbiedingen voor producten waarvan Albert Heijn op basis van bonuskaartgegevens weet dat de klant die regelmatig koopt. Daarnaast zouden klanten aanbiedingen ontvangen voor producten waarvan Albert Heijn verwacht dat die goed aansluiten bij hun wensen.

Om persoonlijke analyses van klanten te maken op basis van hun aankoopgedrag en vervolgens gepersonaliseerde aanbiedingen te doen, heeft Albert Heijn op grond van de Wbp ondubbelzinnige toestemming nodig van de klanten. Het CBP concludeerde dat de door Albert Heijn gevraagde toestemming niet voldeed aan de eisen die aan geldige toestemming worden gesteld. Zo moet de klant onder meer goed worden geïnformeerd om de toestemming rechtsgeldig te laten zijn. Albert Heijn schortte hierop het 'Mijn Bonus'-programma op tot klanten hernieuwde toestemming zouden hebben gegeven.

Het CBP stelde daarnaast vast dat Albert Heijn over adresgegevens kan beschikken van houders van een anonieme bonuskaart, bijvoorbeeld als de klant NAW-gegevens opgeeft bij bestellingen in de webwinkel. Hierdoor verliest deze persoon zijn anonieme status. Albert Heijn heeft hierop het privacy- en cookiebeleid aangepast en op de website gepubliceerd en aangegeven in welke gevallen houders van de anonieme bonuskaart hun anonieme status verliezen.

Gebruik reisgegevens OV-chipkaart door NS

Na onderzoek van het CBP wijzigde NS het gebruik van persoonsgegevens van OV-chipkaarthouders voor marketingdoeleinden. Hiermee beëindigde NS de door het CBP geconstateerde overtredingen van de Wet bescherming persoonsgegevens (Wbp).

Uit het onderzoek bleek dat NS een gedetailleerd beeld van het reisgedrag van OV-chipkaarthouders vastlegde. NS gebruikte deze reisgegevens voor marketingdoeleinden zonder hiervoor de vereiste toestemming van de reizigers te hebben verkregen. Daarmee leefde het vervoerbedrijf de eerder door het CBP op grond van de Wbp geformuleerde voorwaarden waaronder OV-bedrijven reisgegevens mogen verwerken voor marketingdoeleinden niet na. Dit terwijl NS in 2008 uitdrukkelijk had toegezegd zich aan deze voorwaarden te zullen houden.

Ook kwam uit het onderzoek naar voren dat NS persoonsgegevens van anonieme OV-chipkaarthouders verzamelde. Het bedrijf gebruikte voor direct marketing namelijk de e-mailadressen van anonieme OV-chipkaarthouders die hun saldo via de website van NS activeerden.

Invordering dwangsommen vervoerbedrijven

Het CBP vorderde in het voorjaar van 2012 dwangsommen in bij respectievelijk NS en het Rotterdamse vervoerbedrijf RET. Eerder had het CBP aan NS, RET, het Amsterdamse vervoerbedrijf GVB en kaartuitgever TLS een last onder dwangsom opgelegd voor het in strijd met de wet bewaren van reisgegevens van studenten die reizen met de studenten-OV-chipkaart.

Het CBP vorderde bij NS een dwangsom in van 125.000 euro en bij RET van 120.000 euro. De bedrijven hadden tot eind 2011 de tijd gekregen om de maximale bewaartermijn van 24 maanden in te voeren en de reisgegevens na afloop van deze bewaartermijn te vernietigen of afdoende te anonimiseren. Beide bedrijven verklaarden de reisgegevens te anonimiseren, maar het CBP constateerde dat het toch mogelijk was om reizigers te identificeren en hun reisgedrag langere tijd te volgen. Zowel NS als RET hebben hierop alsnog alle reisgegevens ouder dan 24 maanden vernietigd. Bovendien hebben beide vervoerbedrijven de verschuldigde dwangsom betaald. Wel is RET in bezwaar gegaan tegen de invorderingsbeschikking.

Het CBP had NS een tweede last onder dwangsom opgelegd voor het niet adequaat informeren van studenten over het in- en uitchecken met de studenten-OV-chipkaart. Het CBP concludeerde dat NS de studenten binnen de gestelde termijn alsnog goed heeft geïnformeerd, onder meer via een paginagrote advertentie in twee landelijke dagbladen en informatie op alle stations.

GVB heeft bezwaar en beroep ingesteld tegen de last onder dwangsom. De beroepsprocedure bij de rechtbank loopt nog. TLS heeft de last onder dwangsom volledig nageleefd en daardoor geen dwangsommen verbeurd.

‘Kopietje paspoort’ in de private sector

Bedrijven en organisaties kopiëren steeds vaker het identiteitsbewijs van bijvoorbeeld klanten en relaties. Dit verschijnsel staat ook wel bekend als ‘kopietje paspoort’. In juli 2012 publiceerde het CBP richtsnoeren voor het kopiëren/scannen van identiteitsdocumenten en het overnemen van persoonsgegevens hiervan. Een kopie maken van een paspoort, rijbewijs of identiteitskaart is op grond van de Wet bescherming persoonsgegevens slechts in uitzonderlijke gevallen toegestaan. Bedrijven en organisaties in de private sector kunnen in de meeste gevallen voor legitimatie volstaan met de vraag aan klanten om hun paspoort of ander identiteitsdocument te tonen.

Het op grote schaal kopiëren of scannen van identiteitsdocumenten kan risico’s opleveren voor de persoonlijke levenssfeer. Denk aan identiteitsfraude, waarvan iemand jarenlang financiële en maatschappelijke schade kan ondervinden. De richtsnoeren zijn opgesteld om de wettelijke regels te verduidelijken en bevatten ter illustratie veelvoorkomende situaties waarbij om een identiteitsbewijs wordt gevraagd, zoals bij hotels en sportscholen. Ook is op Mijnprivacy.nl, de publiekswebsite van het CBP, een speciaal dossier ‘Kopie identiteitsbewijs’ geplaatst met antwoorden op veelgestelde vragen.

Zie voor de richtsnoeren kopie paspoort:
www.cbpweb.nl/12/1

INTERNET & TELECOM

Technologische ontwikkelingen volgen elkaar in razendsnel tempo op. Met behulp van die innovatieve technologie worden buitengewoon handige communicatiemiddelen gemaakt en kan dienstverlening aanzienlijk worden verbeterd. Daaraan zijn echter ook nadelen verbonden, doordat mensen steeds nauwkeuriger te volgen zijn en bijvoorbeeld te achterhalen is waar zij zich op elk moment van de dag en nacht bevinden. Ook kunnen de gevolgen groot zijn als persoonsgegevens op straat komen te liggen door een datalek. Adequate beveiliging van gegevens is daarom van het grootste belang.

WhatsApp

Na gezamenlijk onderzoek van het CBP en de Canadese collega-toezichthouder heeft WhatsApp, een populaire app voor smartphones waarmee berichten, foto's en video's kunnen worden verstuurd, een aantal van de geconstateerde privacyovertredingen beëindigd.

De beveiliging van de app was op verschillende punten onder de maat. Zo bleek tijdens het onderzoek dat WhatsApp de berichten via de app op onversleutelde wijze verstuurde. Hierdoor konden derden de inhoud daarvan in leesbare vorm onderscheppen, zonder dat de oorspronkelijke 'whatsapper' daar weet van had. Naar aanleiding van het onderzoek heeft WhatsApp terstond maatregelen genomen om het berichtenverkeer te versleutelen.

Zie voor meer informatie over het onderzoek naar WhatsApp: **www.cbpweb.nl/12/2**

Een andere geconstateerde overtreding is dat gebruikers van WhatsApp verplicht zijn toegang te geven tot het volledige adresboek op hun telefoon. Het bedrijf verzamelt vervolgens álle telefoonnummers uit die adresboeken, ook de nummers van contacten die geen WhatsApp gebruiken. Gebruikers kunnen er niet voor kiezen om alleen de nummers door te geven van contacten met wie zij ook echt willen whatsappen. Hierdoor hebben dus niet alleen de WhatsApp-gebruikers geen zeggenschap over welke gegevens zij willen delen, maar geldt dit zelfs voor mensen die de app niet gebruiken. Alleen de iPhone met het besturingssysteem iOS 6 biedt de mogelijkheid om per app de toegang tot het adresboek uit of aan te zetten.

Nu de onderzoeksfase is afgesloten, geven de twee privacytoezichthouders los van elkaar een vervolg aan de bevindingen. In Nederland bekijkt het CBP in hoeverre de geconstateerde overtredingen voortduren. Afhankelijk van de uitkomst van dat onderzoek beslist het CBP of het handhavende maatregelen zal nemen.

Datalekken

Het CBP besteedde in 2012 gerichte aandacht aan het onderzoeken van (mogelijke) datalekken. In dat jaar ontving het CBP gemiddeld 32 signalen per maand over de manier waarop bedrijven en organisaties in de praktijk met de beveiliging van persoonsgegevens omgaan. Het CBP beoordeelde of bij deze gevallen sprake was van een concreet vermoeden van een datalek of van een tekortkoming in de beveiliging die tot datalekken kan leiden. Daarnaast volgde het CBP nauwlettend berichtgeving in de media om eventuele datalekken op het spoor te komen.

Uiteindelijk startte het CBP op basis van prioriteitstelling 25 onderzoeken. Het CBP bekeek hierbij onder meer of de oorzaak van een datalek te achterhalen was en welke maatregelen het bedrijf of de organisatie inmiddels had genomen om herhaling te voorkomen. In 2012 zijn 21 onderzoeken afgerond. Bij de onderzochte datalekken werd betrokkenen bijvoorbeeld vaak gevraagd op een webformulier persoonsgegevens in te vullen die vervolgens onbeveiligd via het internet werden verstuurd. Soms ging het hierbij om bijzondere (medische) persoonsgegevens, bijvoorbeeld als iemand online een afspraak met een zorgverlener maakte. Andere categorieën onderzochte datalekken betroffen onder meer:

- gebrek aan een werkend alarmsysteem, waardoor (eerdere) hackpogingen onopgemerkt bleven;
- e-waste, waarbij persoonsgegevens bij anderen terechtkwamen na reparatie van apparaten als telefoons en laptops;
- systemen waarvan de toegang onvoldoende beveiligd was, bijvoorbeeld omdat was nagelaten de rechten van mapjes op een webserver te beperken, waardoor toegang tot bijvoorbeeld cv's mogelijk was.

Meldplicht datalekken

Het CBP adviseerde in mei 2012 over een wetsvoorstel dat bedrijven en organisaties verplicht een datalek zo snel mogelijk te melden bij het CBP. Doen zij dit niet, dan kan het CBP volgens dit wetsvoorstel een boete van maximaal 200.000 euro opleggen. Het CBP staat positief tegenover de meldplicht datalekken en de bijbehorende boetebevoegdheid, onder meer omdat deze bedrijven en organisaties stimuleren om al in de ontwerpfase van diensten en producten goed na te denken over de beveiliging.

Richtsnoeren beveiliging persoonsgegevens

In 2012 stelde het CBP richtsnoeren op voor de beveiliging van persoonsgegevens, die begin 2013 zijn gepubliceerd. De richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens de beveiligingsnormen uit de Wet bescherming persoonsgegevens (Wbp) toepast. De richtsnoeren vormen de verbindende schakel tussen het juridisch domein, met daarbinnen de eisen uit de Wbp, en het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig zijn om daadwerkelijk aan die eisen te voldoen. De richtsnoeren zijn zowel van toepassing op de publieke als de private sector.

De persoonsgegevens van de gemiddelde Nederlander komen in honderden tot duizenden bestanden voor. Mensen moeten erop kunnen vertrouwen dat hun gegevens voldoende worden beveiligd. Onvoldoende beveiliging kan leiden tot verlies en diefstal van persoonsgegevens en vervolgens tot misbruik van deze gegevens, bijvoorbeeld voor identiteitsfraude. Bedrijven en organisaties die persoonsgegevens verwerken moeten deze volgens de Wbp beveiligen en hiervoor passende technische en organisatorische maatregelen nemen. De maatregelen dienen er mede op gericht te zijn onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Zie voor de richtsnoeren beveiliging van persoonsgegevens:
www.cbpweb.nl/12/3

Zienswijze over cloud computing

Het CBP gaf in september 2012 in een zienswijze antwoord op drie vragen van SURFmarket over de bescherming van persoonsgegevens bij cloud computing. Dit is een verzamelnaam voor technologieën en diensten die gericht zijn op het gebruik van IT-applicaties, rekenkracht en opslag op afstand via internet. Het CBP heeft de vragen in algemene zin beantwoord, om daarmee een zo groot mogelijke groep van aanbieders van clouddiensten en hun afnemers duidelijkheid te bieden over de door SURFmarket opgeworpen privacykwesties rondom cloud computing.

De zienswijze van het CBP gaat over in Nederland gevestigde bedrijven of organisaties die gebruikmaken van de cloudcomputingdiensten (onder meer e-mail, agendabeheer, groepsdiscussies en relatiebeheer) van een leverancier die gevestigd is in de Verenigde Staten. In de zienswijze benadrukt het CBP dat een belangrijk uitgangspunt is dat Nederlandse bedrijven of organisaties die clouddiensten afnemen bij een Amerikaanse aanbieder eindverantwoordelijk zijn voor de naleving van de Wet bescherming persoonsgegevens. Bij het sluiten van een overeenkomst voor clouddienstverlening moeten bedrijven of organisaties zich er dan ook van vergewissen dat de toepasselijke wettelijke regels zijn afgedekt. Zo nodig moeten zij aanvullende afspraken opnemen in de overeenkomst met de Amerikaanse aanbieder van de clouddiensten. Dat geldt in ieder geval voor de beveiliging van de in de cloud verwerkte persoonsgegevens.

De CBP-zienswijze is gebaseerd op de opinie over cloud computing van de Artikel 29-werkgroep van Europese privacytoezichthouders. Meer informatie over deze opinie is te vinden in het hoofdstuk ‘Internationaal’.

Overtredingen TomTom beëindigd

TomTom beëindigde in 2012 de eerder door het CBP geconstateerde overtredingen van de Wet bescherming persoonsgegevens. Eind 2011 concludeerde het CBP na onderzoek dat TomTom de wet overtrad bij de verwerking van zogeheten geolocatiegegevens: de plaats waar gebruikers van de navigatieapparatuur van het bedrijf zich bevinden. De aan de gebruikers van de verschillende soorten on- en offline apparaten en smartphone-app gevraagde toestemming voor verwerking van deze geolocatiegegevens en de bijbehorende informatie over wat TomTom met de gegevens doet, waren onvoldoende specifiek.

In het voorjaar van 2012 constateerde het CBP dat TomTom houders van bepaalde oudere versies van de offline apparaten nog steeds niet actief om toestemming vroeg. TomTom verklaarde dat deze laatste overtreding op een ontwerpfout in de software berustte. In juli controleerde het CBP de oudere apparaten nogmaals en stelde vast dat de geconstateerde overtreding was beëindigd.

OVERHEID

De overheid is een van de grootste verwerkers van persoonsgegevens. De gegevens worden met meerdere partijen gedeeld, hetgeen de dienstverlening ten goede kan komen maar waarbij ook voorzichtigheid geboden is. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens bij de overheid in goede handen zijn en dat de overheid gegevens die in vertrouwen voor een bepaald doel zijn verstrekt, niet zomaar voor een ander doel gebruikt.

Aanpak scheefwonen

'Scheefwoners' zijn huurders van wie het inkomen te hoog is in vergelijking met de huur van hun sociale huurwoning. Het kabinet wil het scheefwonen bestrijden en de doorstroming op de huurmarkt bevorderen door de huurprijsverhoging te koppelen aan het huishoudinkomen. In mei 2012 nam de Tweede Kamer een wetsvoorstel aan dat regelt dat huurders met een jaarinkomen van meer dan 43.000 euro een extra huurverhoging van maximaal 5% opgelegd wordt.

Onderzoek CBP

Vooruitlopend op de wettelijke regeling bleek de Belastingdienst al inkomensgegevens te hebben verstrekt aan een aantal verhuurders. In het voorjaar van 2012 ontving het CBP hierover veel signalen van huurders. Het CBP startte een onderzoek en concludeerde dat de verstrekking in strijd was met de Wet bescherming persoonsgegevens. Een van de oorzaken hiervan was dat de Belastingdienst ten onrechte een ontheffing was verleend van de wettelijke geheimhoudingsplicht. Ook de kortgedingrechter oordeelde in een zaak die door enkele huurders was aangespannen dat de verstrekking onrechtmatig was, waarop de Belastingdienst stopte met het verstrekken van de inkomensgegevens.

Advies CBP

In juli 2012 bracht het CBP vervolgens advies uit over een wetsvoorstel dat een extra huurprijsverhoging regelt voor de zogeheten middeninkomens: huishoudens met een (gezamenlijk) jaarinkomen tussen 33.000 euro en 43.000 euro. Voor deze huurders zou volgens het wetsvoorstel een maximale huurstijging van inflatie plus 1% gaan gelden. Hiermee werd uitvoering gegeven aan een van de afspraken uit het begrotingsakkoord. Het CBP uitte bezwaar tegen het wetsvoorstel, onder meer omdat dit niet aantoonde in welke mate de koppeling van de huurverhoging aan het huishoudinkomen het probleem zou kunnen oplossen. Ook werd onvoldoende onderbouwd dat voor het effectief aanpakken van scheefwonen niet kan worden volstaan met minder ingrijpende middelen.

Toezicht op kentekenregister

De Dienst Wegverkeer (RDW) heeft het toezicht op het kentekenregister verbeterd na onderzoek van het CBP. Tijdens het onderzoek constateerde het CBP in eerste instantie dat de RDW onvoldoende controleerde of gegevens uit het kentekenregister aan de juiste ontvangers en om de juiste redenen werden verstrekt. In de loop van het onderzoek bleek dat de RDW, mede ingegeven door het lopende onderzoek, alsnog de vereiste controles had uitgevoerd. Hierdoor was bij het sluiten van het onderzoek niet langer sprake van strijd met de verplichtingen op dit punt uit de Wet bescherming persoonsgegevens en de wegenverkeerswetgeving.

Het onderzoek was toegespitst op de wijze van controle door de RDW op de online verstrekking van gegevens uit het kentekenregister aan verzekeraars en gerechtsdeurwaarders. De RDW mag alleen gegevens aan deze partijen verstrekken voor in de wet opgesomde doeleinden. Vervolgens is de RDW wettelijk verplicht om te controleren of een instantie die gegevens opvraagt inderdaad een verzekeraar of gerechtsdeurwaarder is en of deze de gege-

vens daadwerkelijk gebruikt voor het doel waarvoor ze zijn verstrekt. Tijdens het onderzoek bleek dat de RDW onvoldoende invulling gaf aan de vereiste controles en daarmee niet genoeg maatregelen had getroffen om persoonsgegevens in het kentekenregister te beveiligen tegen misbruik.

Mens Centraal

Het CBP deed in 2012 onderzoek naar de verwerking van persoonsgegevens via het volgsysteem Mens Centraal. Dit is een ICT-applicatie waarmee gemeenten en hun ketenpartners, zoals Bureau Jeugdzorg en UWV-Werkbedrijf, kunnen samenwerken op het gebied van maatschappelijke dienstverlening en veiligheid. Mens Centraal maakt op basis van vastgelegde klantkenmerken persoonsgegevens toegankelijk uit aangesloten bronnen. De applicatie is gebaseerd op een concept waarbij dienstverleningsprocessen worden verbonden aan gebeurtenissen in het leven van een klant (life events). De gemeenten en hun partners leggen vast op basis van welke persoonskenmerken zij bepalen of ze tot dienstverlening overgaan.

Het CBP constateerde tijdens het onderzoek dat de doeleinden van de gegevensverwerking binnen Mens Centraal zeer ruim zijn geformuleerd, waardoor deze niet – zoals de Wet bescherming persoonsgegevens vereist – welbepaald en uitdrukkelijk zijn omschreven. Daarnaast is de verdeling van verantwoordelijkheden onduidelijk en is deze verdeling ook niet formeel schriftelijk vastgelegd. Het CBP heeft het Kennisinstituut Nederlandse Gemeenten (KING), de toenmalige beheerder van Mens Centraal, hierop aangesproken.

Registratie etniciteit risicojongeren

De Rotterdamse deelgemeente Charlois mag geen gegevens over de etniciteit van zogeheten risicojongeren registreren. De rechtbank van Rotterdam verklaarde het beroep dat Charlois had ingesteld tegen het CBP

ongegrond. Het CBP had de deelgemeente eerder een last onder dwangsom opgelegd. Deze sanctie volgde op onderzoek waarbij het CBP concludeerde dat Charlois in strijd met de wet handelde door structureel gegevens over etniciteit te verwerken voor een specifieke aanpak van risicojongeren, terwijl de deelgemeente niet kon aantonen dat deze aanpak geschikt is om de achterstand van de jongeren te verminderen of op te heffen.

Het registreren van etniciteit is op grond van de Wet bescherming persoonsgegevens verboden. Op dit verbod is in een beperkt aantal gevallen een uitzondering mogelijk. Charlois meende dat sprake was van een dergelijke uitzondering, omdat de registratie noodzakelijk zou zijn voor de verwezenlijking van voorkeursbeleid. Charlois voldeed echter naar het oordeel van de rechtbank, en eerder dat van het CBP, niet aan de voorwaarden om op deze wettelijke uitzonderingsmogelijkheid een beroep te kunnen doen. Zo heeft Charlois volgens de rechtbank niet aannemelijk gemaakt dat dit voorkeursbeleid in redelijkheid niet op een andere, voor de betrokken jongeren minder nadelige, wijze kan worden verwerkelijkt.

Charlois heeft inmiddels voldaan aan de last onder dwangsom door te stoppen met het verwerken van gegevens over de etniciteit van risicojongeren en de al geregistreerde gegevens te verwijderen.

Paspoort en identiteitskaart

Het CBP adviseerde in 2012 over een wijziging van de Paspoortwet. Dit wetsvoorstel regelt onder meer dat de geldigheidsduur van nationale paspoorten wordt verlengd van vijf naar tien jaar. Het CBP adviseerde om hierbij aandacht te besteden aan de (toekomstige) beveiliging van het paspoort. Hoe blijft, rekening houdend met de stand der techniek, de beveiliging gegarandeerd als een paspoort voortaan tien jaar geldig is?

Ook regelt het wetsvoorstel dat de Nederlandse identiteitskaart niet meer de status heeft van een formeel reisdocument. Dit betekent dat voor de identiteitskaart geen vingerafdrukken meer nodig zijn. Bij de overige reisdocumenten worden bij de aanvraag voortaan geen vier maar twee vingerafdrukken opgenomen, die op grond van Europese regelgeving verplicht zijn. Deze vingerafdrukken worden vervolgens niet meer opgeslagen in de reisdocumentenadministratie maar alleen in de chip van het reisdocument.

Het CBP heeft in het verleden al een aantal malen geadviseerd over wijzigingen van de Paspoortwet. Zo heeft het CBP in 2007 aangegeven dat het aanleggen van een (centrale of decentrale) reisdocumentenadministratie met biometrische gegevens ernstige en waarschijnlijk onnodige risico's oplevert voor de persoonlijke levenssfeer.

Flexibel cameratoezicht

De minister van Veiligheid en Justitie wil flexibel cameratoezicht invoeren voor handhaving van de openbare orde. In augustus 2012 vroeg de minister het CBP hierover om advies. Burgemeesters krijgen door het betreffende wetsvoorstel de mogelijkheid een gebied aan te wijzen waarbinnen niet alleen de huidige vaste camera's maar ook mobiele camera´s kunnen worden ingezet.

Bij flexibel cameratoezicht is heldere communicatie over de noodzaak hiervan van groot belang, stelt het CBP. Ook binnen een aangewezen gebied kunnen snel en eenvoudig verplaatsbare camera's ertoe leiden dat mensen zich sneller dan voorheen gevolgd voelen.

Het CBP heeft geen bezwaar tegen de inhoud van het wetsvoorstel. Het gaat niet over het invoeren van een nieuw instrument maar over het flexibiliseren van het huidige cameratoezicht. De privacyrisico's zijn grotendeels het-

zelfde als bij vast cameratoezicht. De nieuwe risico's zijn in het wetsvoorstel met een zogeheten privacy impact assessment adequaat in kaart gebracht, aldus het CBP.

Openbaarmaking WOZ-waarden

Het CBP adviseerde in mei 2012 over een wijziging van de Wet waardering onroerende zaken (Wet WOZ). De voorgestelde wijziging betreft het voor iedereen zichtbaar maken van de WOZ-waarden van woningen in combinatie met adresgegevens.

Als een van de argumenten voor algehele openbaarmaking wordt genoemd dat de actuele maatschappelijke opvattingen over de privacygevoeligheid van de WOZ-waarde niet meer dezelfde zouden zijn als in de tijd dat de Wet WOZ tot stand kwam. In de maatschappelijke beleving zou de WOZ-waarde nu meer als een objectief kenmerk van de woning worden beschouwd dan als een persoonsgegeven.

Vanwege deze verandering is in de gemaakte belangenafweging minder gewicht toegekend aan het belang van de individuele burger. Het CBP oordeelt dat deze afweging onvolledig is. Het is onduidelijk waaruit blijkt dat de maatschappelijke beleving ten opzichte van de WOZ-waarde is veranderd en het belang van de burger is in het wetsvoorstel niet of zeer marginaal meegewogen.

Het CBP heeft in het verleden reeds een aantal keren geadviseerd over wijzigingen van de Wet WOZ. Omdat de WOZ-waarde een gegeven is dat een rol speelt bij de vaststelling van een belastingschuld en daarmee als privacygevoelig geldt, is uitdrukkelijk beoogd dat openbaarheid geen regel mag zijn. De WOZ-waarde zegt iets over de individuele fiscale positie van een belanghebbende bij een onroerende zaak en is dus wel degelijk een persoonsgegeven.

Naar aanleiding van het CBP-advies is het wetsvoorstel aangepast. De noodzaak van de algehele openbaarmaking is nader gemotiveerd en de veranderde maatschappelijke beleving van de WOZ-waarde beter uiteengezet.

Invoering wietpas

Het CBP gaf in april 2012 advies over de invoering van de zogeheten wietpas. De minister van Veiligheid & Justitie was van plan om coffeeshops besloten clubs te maken. De toegang tot coffeeshops zou voorbehouden zijn aan inwoners van Nederland van achttien jaar en ouder. Voor toegang zou een lidmaatschap van de coffeeshop verplicht gesteld worden. Leden zouden een clubpas ontvangen, de wietpas. Het maximum aantal leden zou 2000 mogen zijn, te controleren aan de hand van een ledenlijst.

Het CBP adviseerde onder meer om de noodzaak van de ledenlijst toe te lichten. Uit de toelichting zou ook moeten blijken dat andere, minder ingrijpende methoden waren onderzocht om coffeeshops beter beheersbaar te maken. De minister nam dit CBP-advies over en gaf een toelichting op de noodzaak voor de wietpas.

Daarop werd de wietpas ingevoerd in het zuiden van Nederland. Per 1 januari 2013 zou de wietpas in heel Nederland worden ingevoerd, maar in het regeerakkoord van oktober 2012 werd aangekondigd dat de wietpas zou komen te vervallen. Met ingang van 19 november 2012 is de wietpas afgeschaft. Per 1 januari 2013 geldt nog wel het ingezetenencriterium, waardoor alleen Nederlanders in coffeeshops wiet mogen kopen.

POLITIE & JUSTITIE

Politie en justitie hebben persoonsgegevens nodig voor de opsporing en vervolging van strafbare feiten. Het gaat hierbij om gevoelige gegevens. De waarborgen voor het gebruik van justitiële- en politiegegevens moeten daarom zonder meer in orde zijn. Iedereen moet erop kunnen vertrouwen dat politie en justitie persoonsgegevens in overeenstemming met de wet verwerken en bijvoorbeeld voldoende beveiligingsmaatregelen nemen.

Opvragen telecomgegevens via CIOT

Na onderzoek van het CBP troffen het politiekorps Haaglanden, de Dienst Nationale Recherche (DNR) en het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) maatregelen om ervoor te zorgen dat de gegevensuitwisseling tussen opsporingsdiensten en telecommunicatieaanbieders overeenkomstig de toepasselijke wet- en regelgeving plaatsvindt.

In 2011 constateerde het CBP tijdens onderzoek dat bij het politiekorps Haaglanden en de DNR formele procedures ontbraken voor het toekennen en intrekken van autorisaties voor toegang tot het CIOT-informatiesysteem en dat niet alle autorisaties aan de opsporingsambtenaren en de CIOT-medewerkers rechtsgeldig waren verleend. Uit het onderzoek bleek bovendien dat de beveiliging van de telecomgegevens niet op orde was in geval van rechtstreekse opvragingen door opsporingsdiensten bij de telecommunicatieaanbieders, dus zonder tussenkomst van het CIOT. Het betreft gevoelige gegevens waarvoor zware beveiligingseisen gelden ter voorkoming van verlies of onrechtmatige verwerking van de gegevens door onbevoegden.

In 2012 stelde het CBP vast dat het politiekorps Haaglanden en de DNR alsnog extra beveiligingsmaatregelen hebben genomen om de vertrouwelijkheid en de integriteit van de opgevraagde gegevens te waarborgen. De gegevensuitwisseling bij rechtstreekse opvragingen vindt nu plaats via een landelijk beveiligd netwerk. Ook hebben het politiekorps Haaglanden, de DNR en het CIOT ervoor gezorgd dat alleen bevoegden toegang hebben tot het systeem. Hierdoor is niet langer sprake van een overtreding van de Wet bescherming persoonsgegevens.

Bewaren politiegegevens bij Criminele Inlichtingeneenheden

Criminele Inlichtingeneenheden (CIE's) troffen onvoldoende maatregelen om de wettelijke eisen voor bewaartermijnen van politiegegevens na te leven. Dit concludeerde het CBP na onderzoek. Het CBP onderzocht de regionale politiekorpsen Flevoland en Brabant Zuid-Oost, de Koninklijke Marechaussee en de Inlichtingen en -Opsporingsdienst van de Inspectie Leefomgeving en Transport.

De CIE's verwerken politiegegevens om inzicht te krijgen in de betrokkenheid van personen bij ernstige en georganiseerde misdrijven. Voor de verwerking van deze gevoelige (politie)gegevens gelden strenge wettelijke eisen, mede omdat de informatie niet altijd betrouwbaar is terwijl de risico's en gevolgen van de verwerking voor de betreffende personen groot kunnen zijn.

De Wet politiegegevens bepaalt dan ook dat dergelijke gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn. Daarbij geldt dat uiterlijk vijf jaar nadat voor het laatst gegevens zijn toegevoegd, de gegevens moeten worden verwijderd. De wet eist bovendien een jaarlijkse toets om vast te stellen in hoeverre de gegevens nog noodzakelijk zijn voor het doel waarvoor ze werden verwerkt.

Uit het onderzoek bleek dat geen van de vier onderzochte partijen deze bij wet verplichte toets uitvoerde, dan wel niet concreet genoeg toetste of de opgenomen politiegegevens nog noodzakelijk zijn. Ook constateerde het CBP dat het verplichte interne toezicht door de privacyfunctionarissen op de naleving hiervan tekortschoot.

Plaatsen beelden van getuigen op internet

Het Openbaar Ministerie (OM) heeft aangegeven in beginsel geen beelden van getuigen meer te zullen publiceren op internet. Het OM deed deze toezegging nadat het CBP contact met het OM had opgenomen over deze kwestie, naar aanleiding van berichtgeving in de media in november 2012.

Het OM kan het publiek om hulp vragen bij het ophelderen van misdrijven. De regels hiervoor zijn vastgelegd in de Aanwijzing Opsporingsberichtgeving. Het gaat daarbij echter primair om het opsporen van verdachten, niet van getuigen.

Het CBP stelde dat het publiceren van beelden van (toevallige) getuigen aan hun persoonlijke levenssfeer raakt, terwijl zij op het plaatsen van de beelden geen invloed hebben. De risico's en nadelen van publicatie kunnen voor de getuige buitengewoon groot zijn. Dit dient zeer zwaar te wegen bij de zorgvuldige afweging die moet plaatsvinden tussen het algemeen (opsporings)belang en het belang van de getuige, aldus het CBP.

De huidige Aanwijzing opsporingsberichtgeving is tot 31 augustus 2013 geldig. Het CBP gaat ervan uit dat het OM in de nieuwe aanwijzing specifiek aandacht besteedt aan de bescherming van persoonsgegevens van getuigen van misdrijven.

INTERNATIONAAL

De verwerking van uw persoonsgegevens houdt niet op bij de Nederlandse grens. Om persoonsgegevens ook buiten Nederland te beschermen, is internationale samenwerking van groot belang. Het CBP stemt zijn beleid zo veel mogelijk af met buitenlandse privacytoezichthouders, werkt waar mogelijk samen aan concrete onderzoeken en wisselt kennis, ervaring en onderzoeksmethodes uit.

Europese samenwerking

Het zwaartepunt van de internationale werkzaamheden van het CBP ligt in Europa. De afgelopen jaren koos het CBP er steeds vaker voor om een Europese lijn aan te houden bij de uitvoering van nationale prioriteiten. Vice versa zijn nationale prioriteiten tot Europese prioriteiten gemaakt, door actieve deelname van het CBP aan de verschillende vergaderingen van Europese en internationale toezichthouders. Tot slot heeft het CBP in belangrijke mate bijgedragen aan de totstandkoming van gezamenlijke opinies en standpunten, vooral binnen de zogeheten Artikel 29-werkgroep.

Artikel 29-werkgroep

De Artikel 29-werkgroep ('Working Party 29', kortweg WP29) is een onafhankelijk, raadgevend orgaan dat bestaat uit vertegenwoordigers van de 27 nationale privacytoezichthouders in de Europese Unie en de Europese toezichthouder voor gegevensbescherming. Sinds 2010 is de voorzitter van het CBP tevens voorzitter van WP29. In 2012 is hij herkozen voor een tweede periode van twee jaar. WP29 speelt een belangrijke rol bij de totstandkoming van Europees beleid, Europese wetgeving en de ontwikkeling van Europese normen en gemeenschappelijke interpretaties.

Herziening Europese privacyrichtlijn

De internationale werkzaamheden van het CBP stonden in 2012 voor een groot deel in het teken van de herziening van het Europese wettelijke kader voor gegevensbescherming. Op 25 januari 2012 publiceerde de Europese Commissie de voorstellen voor de herziening van de Europese privacyrichtlijn. De voorstellen omvatten een algemene Europese privacyverordening, die de huidige privacyrichtlijn moet gaan vervangen, en daarnaast een nieuwe richtlijn voor gegevensverwerking door politie en justitie.

Verordening

Het CBP staat positief tegenover de conceptverordening. In het voorstel zijn veel van de wensen overgenomen die het CBP en WP29 de afgelopen jaren in het voorbereidingstraject van de herziening hebben geuit. De voorgestelde verordening versterkt de positie van burgers en bevordert dat bedrijven en organisaties die persoonsgegevens verwerken hun verantwoordelijkheid nemen. Verder krijgen de privacytoezichthouders een sterkere en onafhankelijkere positie en kunnen zij waar nodig boetes opleggen.

Richtlijn

Ondanks de uitdrukkelijke wens van het CBP en WP29 om één alomvattend wetgevend instrument te presenteren dat ook zou gelden voor politie en justitie, heeft de Europese Commissie voor twee verschillende instrumenten gekozen. Over de richtlijn is het CBP kritischer dan over de verordening. De ontwerprichtlijn kent namelijk een beschermingsniveau dat een stuk lager ligt dan dat van de verordening.

Uiteraard zijn persoonsgegevens belangrijk voor politie en justitie om hun taken goed te kunnen uitvoeren, maar goede gegevensbescherming is evenzeer in het belang van politie en justitie. De rechtshandhavingsautoriteiten moeten er immers van uit kunnen gaan dat de gegevens die zij verwerken accuraat en betrouwbaar zijn. De basisprincipes en -rechten zouden mede daarom in de richtlijn en de verordening gelijk moeten zijn, aldus het CBP.

Nieuwe privacyvoorwaarden Google

Onder aanvoering van de Franse toezichthouder CNIL is op verzoek van WP29 een gezamenlijk onderzoek ingesteld naar de nieuwe privacyvoorwaarden van Google, die op 1 maart 2012 in werking traden. Deze nieuwe voorwaarden bleken op verschillende punten strijdig met de Europese regelgeving. Uit het onderzoek kwam onder meer naar voren dat Google bepaalde persoonsgegevens van gebruikers van de diverse Googlediensten combineert zonder de gebruikers daarover vooraf goed te informeren en zonder daarvoor vervolgens toestemming te vragen. Het zonder toestemming combineren van persoonsgegevens voor online marketing- en reclamedoeleinden is in strijd met de Europese privacyrichtlijn. De toezichthouders hebben verschillende aanbevelingen gedaan aan Google om het privacybeleid aan te passen, met het verzoek deze door te voeren in het eerste kwartaal van 2013.

Biometrie

In maart 2012 nam WP29 twee opinies aan over ontwikkelingen op het gebied van het gebruik van biometrische technologieën. Biometrische gegevens, zoals vingerafdrukken, opnamen van stemgeluid en gezichtskenmerken, zijn afgeleid van unieke eigenschappen van een persoon. Dergelijke gegevens kunnen worden gebruikt in automatische systemen om individuele personen te volgen, traceren of profileren.

In de eerste opinie kijkt WP29 naar de risico's van het gebruik van biometrie voor gegevensbescherming en privacy, zoals genetische discriminatie en identiteitsdiefstal. WP29 geeft hierbij concrete adviezen voor technische en organisatorische beveiligingsmaatregelen om deze risico's te beheersen.

In de tweede opinie, die specifiek gaat over gezichtsherkenning bij internet- en mobiele diensten, legt WP29 uit dat gezichtsherkenning alleen met toestemming van de betrokken personen mag worden ingezet. Mede naar aanleiding van deze opinie en door optreden van toezichthouders in Ierland en Schleswig-Holstein heeft Facebook het gezichtsherkenningsprogramma stopgezet in Europa, omdat dit systeem niet op toestemming was gebaseerd.

Cloud computing

In juli 2012 bracht WP29 een opinie uit over cloud computing: een verzamelnaam voor technologieën en diensten die gericht zijn op het gebruik van IT-applicaties, rekenkracht en opslag op afstand via internet. In de opinie analyseert WP29 alle relevante privacykwesties bij het gebruik van cloud computing. De belangrijkste conclusie luidt dat bedrijven en (overheids)organisaties die gebruik willen maken van cloud computing, als eerste stap een uitgebreide risicoanalyse zouden moeten maken. Bovendien moeten alle aanbieders die clouddiensten aanbieden in Europa hun klanten goed informeren, zodat deze de voor- en nadelen van cloud computing kunnen afwegen voordat zij besluiten hiervan gebruik te maken. Beveiliging, transparantie en rechtszekerheid voor de klant zijn essentiële elementen bij het aanbieden van clouddiensten, aldus WP29.

Op basis van de opinie van WP29 publiceerde het CBP in september 2012 een zienswijze over cloud computing. Meer informatie over deze zienswijze is te vinden in het hoofdstuk 'Internet & telecom'.

Online volgen van surfgedrag

Het CBP heeft WP29 vertegenwoordigd in een overleg van het World Wide Web Consortium (W3C), een organisatie die standaarden voor het internet ontwikkelt. In oktober 2012 vergaderde W3C over tracking, het volgen van het surfgedrag van internetgebruikers over meerdere websites. W3C is bezig met een 'do not track'-standaard, die digitale vormen van marketing betreft. Hiermee zouden mensen eenvoudig 'ja' of 'nee' kunnen zeggen tegen tracking.

Het CBP benadrukte in dat verband dat een wereldwijde 'do not track'-standaard in overeenstemming moet zijn met Europese privacyregelgeving. Dat betekent dat surfgedrag op internet alleen gevolgd mag worden als mensen daar hun uitdrukkelijke toestemming voor hebben gegeven. 'Do not track' betekent volgens de Europese privacyregelgeving 'do not collect' (verzamel geen persoonsgegevens over surfgedrag). Een 'do not track'-systeem waarbij mensen feitelijk alleen kunnen aangeven dat zij geen gepersonaliseerde advertenties willen ontvangen, volstaat niet. Naar verwachting wordt in 2013 het eindresultaat van het W3C-overleg gepresenteerd.

Toestemming voor cookies

WP29 hield zich in 2012 ook bezig met alle ontwikkelingen rondom cookies, kleine bestandjes die bedrijven en organisaties op computers van hun websitebezoekers plaatsen. Hiermee kunnen zij onder meer het zoek- en klikgedrag van de bezoekers volgen, al dan niet over meerdere websites. Op grond van Europese regelgeving dient in de meeste gevallen toestemming gevraagd te worden voor het plaatsen en uitlezen van cookies. Over de uitzonderingen op dit toestemmingsvereiste nam WP29 in juni een opinie aan, om hierover meer duidelijkheid te verschaffen aan het bedrijfsleven.

In de opinie is uiteengezet voor welk soort cookies en onder welke voorwaarden geen toestemming van de gebruiker nodig is. Zo is toestemming bijvoorbeeld niet nodig voor het plaatsen van cookies die strikt noodzakelijk zijn voor het leveren van een door de gebruiker gevraagde dienst, zoals cookies die nodig zijn voor het onthouden van de artikelen in een online winkelmandje. Ook voor cookies die bijvoorbeeld een bepaalde taalvoorkeur op een site vastleggen, hoeft geen toestemming te worden gevraagd.

Zie voor de opinie van WP29 over cookies:
www.cbpweb.nl/12/4

COLLEGE & ORGANISATIE

Externe werkzaamheden collegeleden

Het uitdragen en toelichten van het werk van het CBP in binnen- en buitenland is een belangrijke taak van de collegeleden. Het CBP signaleert een toenemende aandacht voor de bescherming van persoonsgegevens en het werk van het CBP, hetgeen resulteert in vele verzoeken tot deelname aan externe bijeenkomsten en mediaoptredens. Het CBP zoekt daarnaast ook zelf actief contact met media en maatschappelijke organisaties.

In 2012 bestond een aanzienlijk deel van de werkzaamheden van de collegeleden dan ook uit externe optredens. Het CBP blikt terug op een breed scala aan externe activiteiten, variërend van radio- en televisie-interviews tot (keynote-)speeches tijdens conferenties. Een belangrijk deel van de optredens had een internationaal karakter. Een selectie uit de externe werkzaamheden van de collegeleden in 2012:

Nationaal

- De collegeleden gaven talrijke interviews aan radio, televisie en de geschreven pers. De interviews kwamen vaak voort uit door het CBP gepresenteerde onderzoeksrapporten en richtsnoeren, maar het CBP kreeg ook veel mediaverzoeken om naar aanleiding van actuele gebeurtenissen op het gebied van privacy een reactie te geven.
- De bescherming van medische gegevens was een veelvuldig terugkerend onderwerp tijdens persoptredens. In het begin van het jaar ontstond onrust over het maken van televisieopnamen op de afdeling spoedeisende hulp van het VUmc. Het CBP heeft naar aanleiding van deze zaak en zijn eigen onderzoek hiernaar verschillende (radio)interviews gegeven. Niet lang daarna speelde in de media een kwestie over de verwerking van medische gegevens van werknemers door het bedrijf VerzuimReductie, waarover het CBP zich ook duidelijk heeft uitgesproken. De verwerking van medische gegevens binnen de arbeidsrelatie is een belangrijk thema geweest tijdens speeches en contacten met de media.
- De collegeleden voerden ook in 2012 regelmatig gesprekken met externe stakeholders. Naast het onderhouden van de contacten hebben deze tot doel algemene beginselen van de Wet bescherming persoonsgegevens en specifieke onderzoeksresultaten van het CBP over het voetlicht te brengen. Het CBP organiseerde in dit kader ook twee besloten rondetafelgesprekken; een met vertegenwoordigers van politie en justitie en een met advocaten met wie het CBP in gerechtelijke procedures te maken heeft gehad. Deze rondetafelgesprekken waren erop gericht te vernemen hoe de effectiviteit en de rol van het CBP werden ervaren en hoe deze verder kunnen worden verbeterd.
- De aangekondigde wijziging van de wetgeving voor het gebruik van cookies heeft gedurende 2012 geleid tot deelname aan uiteenlopende externe activiteiten. Daarbij heeft het CBP onder meer aandacht besteed aan de risico's van profilering die mogelijk is door het plaatsen van cookies.
- In de zomer van 2012 presenteerde het CBP richtsnoeren voor het gebruik van een 'kopietje paspoort' in de private sector. Tijdens verschillende mediaoptredens gaven de collegeleden een toelichting op de regels voor het overnemen van persoonsgegevens en het kopiëren en/of scannen van identiteitsdocumenten.

Internationaal

- Het voorzitterschap van de Artikel 29-werkgroep van Europese privacytoezichthouders bracht veel overleg met vertegenwoordigers van de EU-instellingen mee, vooral nadat de Europese Commissie begin 2012 de voorstellen voor de herziening van de Europese privacyrichtlijn presenteerde. Het afgelopen jaar zijn over de voorstellen voor de toekomstige Europese privacyregelgeving veelvuldig interviews gegeven aan (inter)nationale media.
- De collegeleden namen ook deel aan verschillende mondiale conferenties en bijeenkomsten. Zo vond eind oktober 2012 in Uruguay de jaarlijkse internationale conferentie van privacytoezichthouders plaats, waarbij het centrale thema profilering was. De CBP-voorzitter is sinds 2011 de eerste voorzitter van het Uitvoerend Comité van de internationale conferentie, dat is ingesteld om ervoor te zorgen dat de besloten sessie van de conferentie meer structuur krijgt.
- Begin 2012 besloten de Europese privacytoezichthouders, mede op initiatief van het CBP, gezamenlijk onderzoek te doen naar de privacyvoorwaarden van Google. Het betrof een unieke internationale samenwerking, waarvan het CBP een groot pleitbezorger is. In het najaar van 2012 presenteerden de Europese privacytoezichthouders tijdens een persconferentie in Parijs de resultaten van het onderzoek.

College & Directie

College

Mr. J. Kohnstamm
Voorzitter

Mr. W.B.M. Tomesen
Collegelid, plv. voorzitter

Directie

Drs. P.J.J. Frencken
Directeur

Collegelid mr. M.W. McLaggan is eind 2012 na overleg met de voorzitter van het CBP door de staatssecretaris van Veiligheid en Justitie gevraagd een onderzoeksrapport te schrijven over de ontwikkelingen op het raakvlak van bescherming van persoonsgegevens en mededinging. De bescherming van persoonsgegevens in de private sector interfereert steeds vaker met mededingingsrecht en de vraag is welke consequenties dit heeft voor de betreffende wetgeving en het toezicht daarop. Mevrouw McLaggan was bereid op dit verzoek in te gaan en is voor de duur van het onderzoek ontheven van haar reguliere taken als lid van het college.

Organisatie

In 2012 startte het CBP met de ontwikkeling van een vernieuwde missie en visie, waarin de ambitie van het CBP wordt neergelegd, en van een strategie om deze te realiseren. Ook worden kernwaarden en kernkwaliteiten ontwikkeld die passen bij de missie, visie en strategie. Het doel van dit traject is voor de komende jaren een heldere focus te hebben binnen de taken van het CBP én om de toekomstige veranderingen rond de nieuwe Europese privacywetgeving, de boetebevoegdheid en de meldplicht voor datalekken goed te kunnen integreren in de interne organisatie.

Het budget van het CBP bedroeg in 2012 7.679.000 euro (in 2011: 7.737.000 euro). Gelet op de bezuinigingen van rijkswege daalt het budget van het CBP en neemt de bezetting – in 2012 gemiddeld 75,8 fte – wellicht verder af. Daarom is in 2012 de selectieve vacaturestop voortgezet die in 2011 is gestart.

Productie

- In 2012 zijn 58 onderzoeken afgerond. In 12 gevallen is een last onder dwangsom opgelegd.
- Het aantal voorafgaande onderzoeken was 93. Het CBP doet deze onderzoeken naar voorgenomen verwerkingen van persoonsgegevens die bijzondere risico's opleveren voor de persoonlijke levenssfeer van de betrokkenen, zoals zwarte lijsten.
- Het aantal adviezen aan de regering over voorgenomen wetgeving bedroeg 41.
- Over doorgifte van persoonsgegevens aan zogeheten derde landen (landen buiten de Europese Unie) is 61 keer advies uitgebracht. Voor deze doorgifte is een vergunning nodig van de minister van Veiligheid en Justitie. Het CBP adviseert de minister over de afgifte van de vergunningen.

Publieksvoorlichting en perswerk

Het CBP beantwoordt vragen en behandelt signalen over (mogelijke) overtredingen van de privacywetgeving. In 2012 ging het om 6042 vragen en signalen, een stijgende lijn ten opzichte van de voorgaande jaren. Het CBP analyseert de signalen en kan naar aanleiding daarvan besluiten een onderzoek in te stellen. In 2012 is de algemene voorlichting via de website Mijnprivacy.nl verder uitgebreid met nieuwe vragen en antwoorden over uiteenlopende thema's, onder meer naar aanleiding van signalen.

Door het actieve en reactieve perswerk van het CBP hebben de onderzoeken en andere werkzaamheden van de toezichthouder geregeld een uitstralende werking die verder reikt dan de onderzochte bedrijven en organisaties. Dit heeft een positief effect op het niveau van de naleving van de wet. In 2012 was het aantal perscontacten 587.

Raad van advies

De Raad van advies heeft tot taak het college te adviseren over de hoofdlijnen van het beleid van het CBP en andere algemene aspecten van de bescherming van persoonsgegevens. In 2012 waren de leden van de Raad van advies:

Mevrouw drs. T.A. Maas-de Brouwer
Voorzitter, lid raad van commissarissen van onder meer PEN, Schiphol Groep, Arbo Unie en Van Leer Group Foundation, voormalig senator PvdA

De heer drs. H.G.M. Blocks
Adviseur/bestuurder, oud-directeur Nederlandse Vereniging van Banken

De heer H.W. Broeders
Voorzitter directieraad Capgemini Nederland, lid dagelijks bestuur VNO-NCW

Mevrouw H.C.J. van den Burg
Commissaris ASML en APG, lid Monitoring Commissie Corporate Governance, voorheen lid Europees Parlement en federatiebestuur FNV

De heer drs. B.R. Combée
Directeur Consumentenbond

De heer prof. mr. E.J. Dommering
Emeritus hoogleraar informatierecht Universiteit van Amsterdam, lid Commissie Mensenrechten van de Adviesraad Internationale Vraagstukken

Mevrouw prof. dr. H.M. Dupuis
Lid van de Eerste Kamer voor de VVD, voorzitter van de brancheorganisatie Vereniging Gehandicaptenzorg Nederland, voorzitter van twee raden van toezicht in de gezondheidszorg, emeritus hoogleraar medische ethiek Universiteit Leiden

De heer mr. T.H.J. Joustra
Voorzitter Onderzoeksraad voor Veiligheid, voorheen Nationaal Coördinator Terrorismebestrijding

De heer prof.mr. J. Legemaate
Hoogleraar gezondheidsrecht, AMC/Universiteit van Amsterdam

De heer mr. R.J. Manschot
Oud-hoofdofficier van Justitie, oud-vicevoorzitter Eurojust

De heer drs. L.J.E. Smits
Algemeen directeur PBLQ

De heer mr. A.A. Westerlaken
Voorzitter Raad van Bestuur Maasstadziekenhuis

De heer mr. A. Wolfsen
Burgemeester van Utrecht

De heer drs. L.J. Wijngaarden
Beroepscommissaris, voorheen CEO Postbank en CEO Nationale Nederlanden

Colofon

Het CBP in 2012

Ontwerp: Proforma | visual identity, Rotterdam
Fotografie college: Mark Kohn
Fotografie: Shutterstock, Nationale beeldbank, Hollandse Hoogte
Druk: OBT BV, Den Haag

COLLEGE BESCHERMING PERSOONSGEGEVENS

Juliana van Stolberglaan 4-10
2595 CL Den Haag

Postbus 93374
2509 AJ Den Haag

T 070 8888 500
F 070 8888 501

Telefonisch spreekuur
T 0900-2001 201 (5 cent per minuut)

www.cbpweb.nl

www.mijnprivacy.nl