COLLEGE **BESCHERMING** PERSOONSGEGEVENS

HET CBP IN 2014

Het CBP staat voor het grondrecht op bescherming van persoonsgegevens

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. Het CBP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Het grondrecht op bescherming van persoonsgegevens is fundamenteel voor de werking van de rechtstaat. Het CBP beschermt dit grondrecht door:

- overtredingen van de wet aan te pakken;
- over nieuwe regelgeving te adviseren;
- op de hoogte te zijn van de dilemma's die in de samenleving spelen op het gebied van de privacy;
- overheid, bedrijfsleven en andere maatschappelijke organisaties alert te maken op hun verantwoordelijkheid bij de bescherming van persoonsgegevens;
- informatie te verstrekken waarmee mensen hun recht kunnen uitoefenen;
- resultaten van toezicht en handhaving openbaar te maken;
- nationaal en internationaal samenwerking te zoeken ten behoeve van de bescherming van persoonsgegevens.

HET CBP IN 2014

INHOUD

VOORWOORD

Eind oktober 2015 zal ongetwijfeld voor iedereen die betrokken is bij het College bescherming persoonsgegevens (CBP) een paar spannende dagen opleveren. Het CBP is dan gastheer van de 37e Internationale Privacyconferentie in Amsterdam. Naar verwachting zullen achthonderd toonaangevende privacyexperts uit de private en de publieke sector, van universiteiten en non-gouvernementele organisaties evenals de autoriteiten persoonsgegevens van over de hele wereld bijeenkomen om met elkaar in discussie te gaan over de 'stand van de privacy'.

Die stand van de privacy is meer dan het bespreken waard. De verontrustende mate waarin veiligheidsdiensten het leven van Jan en alleman lijken te registreren, maar ook de zoektocht naar de wijze waarop effectieve controle op het doen en laten van die veiligheidsdiensten kan worden georganiseerd, heeft sinds de onthullingen van Edward Snowden volop in de schijnwerpers gestaan. Daarnaast baart de ongekend omvangrijke verzameling van persoonsgegevens door grote, veelal in de VS gevestigde, IT-multinationals zorgen.

Omdat landsgrenzen door internet en ontwikkelingen in de IT niet of nauwelijks meer bestaan, leidt het geen twijfel dat het bepalen van de maatschappelijke randvoorwaarden waarbinnen het verzamelen en verwerken van persoonsgegevens dient plaats te vinden, al lang geen louter nationale aangelegenheid meer is.

In de Europese Unie wordt daarom terecht gewerkt aan de totstandkoming van een nieuwe privacyverordening. In alle lidstaten zullen op het terrein van de bescherming van persoonsgegevens dezelfde rechten en plichten gaan gelden. Het principiële uitgangspunt bij de totstandkoming van de verordening is dat bescherming van persoonsgegevens een grondrecht is, waardoor het verzamelen en verwerken van persoonsgegevens alleen is toegestaan op basis van een beperkt aantal rechtsgronden, bijvoorbeeld omdat de wet daartoe verplicht, omdat sprake is van een gerechtvaardigd belang, dan wel omdat de burger daarvoor uitdrukkelijk en geïnformeerd toestemming heeft gegeven.

In de Verenigde Staten wordt heel anders tegen 'privacy' aangekeken. De bescherming van persoonsgegevens is in de VS een consumentenrecht: verzamelen en verwerken van

persoonsgegevens is toegestaan tenzij daarvan op valse of bedrieglijke wijze ('false or deceptive') gebruik wordt gemaakt, bijvoorbeeld strijdig met de algemene voorwaarden die behoren bij het desbetreffende product of de desbetreffende dienst.

De verschillen in de wijze waarop de bescherming van persoonsgegevens aan beide zijden van de Atlantische Oceaan in wetgeving is verankerd, leiden tot ingrijpende problemen. Veel nieuwe, nuttige en leuke producten en diensten zijn afkomstig uit Silicon Valley en vinden buitengewoon succesvol hun weg naar de Europese markt. Maar omdat voor deze producten en diensten meestal 'slechts' wordt betaald door middel van het weggeven van persoonsgegevens, zonder dat het bedrijf zich op een rechtsgrond in de EU kan beroepen, zijn deze gegevensverwerkingen in flagrante strijd met het hier geldende recht. Burgers, overheden en bedrijven in de EU worden daardoor geconfronteerd met duivelse dilemma's, temeer omdat de bedrijven die deze diensten en producten leveren veelal een aan monopolie grenzend marktaandeel hebben.

Het feit dat in de EU hopelijk spoedig een definitieve knoop zal worden doorgehakt over de nieuwe privacyverordening terwijl in de VS de tegenstelling tussen Republikeinen en Democraten ook op het terrein van eventuele privacywetgeving besluitvorming in de weg staat, maakt het aannemelijk dat de principiële trans-Atlantische verschillen op dit punt niet spoedig door nieuwe wetgeving zullen verdwijnen.

Het Massachusetts Institute of Technology (MIT) en het Instituut voor Informatierecht van de Universiteit van Amsterdam (IViR) hebben op grond van deze analyse tot onze erkentelijkheid een twintigtal privacyexperts afkomstig van beide zijden van de oceaan bijeengebracht in het zogeheten Privacy Bridges Project. Dit project heeft tot doel om – onverlet de verschillen in privacywetgeving in de EU en de VS – een aantal pragmatische, praktische en/of technologische oplossingen te bedenken en uit te werken. Dit zal per saldo moeten leiden tot een hoger niveau van bescherming van persoonsgegevens, terwijl de verschillen in de rechtsstelsels als minder storend zullen worden ervaren. De werkhypothese gaat er bovendien van uit dat de door het project uit te denken 'privacybruggen' ook kunnen helpen om de verschillen in privacywetgeving tussen de VS, de EU en andere werelddelen voor burgers, bedrijven en overheden hanteerbaarder te maken.

De resultaten van het project zullen eind oktober 2015 worden gepresenteerd en bediscussieerd tijdens de 37e Internationale Privacyconferentie, die op grond daarvan het thema 'Building Bridges' heeft gekregen. De ambitie van MIT, IViR en het CBP – dat zich tegen die tijd overigens Autoriteit Persoonsgegevens hoopt te mogen noemen – is om ervoor te zorgen dat het project en de conferentie tot heel concrete en directe acties zullen leiden.

De Internationale Privacyconferentie vindt plaats aan de vooravond van het Nederlandse voorzitterschap van de EU (in de eerste helft van 2016). Het zou natuurlijk prachtig zijn als tijdens dit EU-voorzitterschap in samenwerking met de Europese Commissie en de Amerikaanse regering een aantal van de geformuleerde 'privacybruggen' in gebruik kan worden genomen, waardoor uiteindelijk wereldwijd een handzamer en vooral hoger niveau van bescherming van persoonsgegevens kan worden gerealiseerd.

Jacob Kohnstamm
Voorzitter College bescherming persoonsgegevens

INLEIDING

Het College bescherming persoonsgegevens (CBP) staat voor het grondrecht op bescherming van persoonsgegevens. Het CBP bewaakt dit grondrecht door toezicht te houden op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en door te adviseren over nieuwe regelgeving. Elk jaar bepaalt het CBP een aantal thema's waaraan het speciale aandacht geeft. In 2014 waren de belangrijkste thema's profilering, decentralisatie en gegevensverwerking in de arbeidsrelatie.

Het CBP komt tot de keuze voor de jaarlijkse thema's door ontwikkelingen bij te houden op het gebied van technologie en wetgeving en gesprekken te voeren met diverse stakeholders, zoals branche-, consumenten- en mensenrechtenorganisaties. Ook de vragen en tips over mogelijke privacyovertredingen die het CBP ontvangt – gemiddeld zo'n 7.000 per jaar – zijn een belangrijke bron van informatie, net als contacten met de pers en berichten in de media.

In 2014 heeft het CBP bij zijn werkzaamheden in het bijzonder gelet op de wijze waarop organisaties mensen informeren over het verwerken van persoonsgegevens en hiervoor – voor zover dit wettelijk is voorgeschreven – toestemming vragen. Door de omvang en complexiteit van veel gegevensverwerkingen hebben mensen vaak geen zicht op de aard en de gevolgen van het (her)gebruik van hun persoonsgegevens. Het is daarom van groot belang dat organisaties hierover transparant zijn. Een van de rechtsgronden waarop persoonsgegevens mogen worden verwerkt, is toestemming van de betrokkene. Vaak wordt die toestemming niet op de juiste wijze verkregen. Daarom bestudeerde het CBP in meerdere onderzoeken of aan de vereisten van een rechtsgeldige toestemming was voldaan. Ook had het CBP in 2014 speciale aandacht voor adequate beveiliging van persoonsgegevens en onderzocht het of organisaties hiertoe de vereiste technische en organisatorische maatregelen hadden getroffen.

Hieronder volgt een selectie uit de werkzaamheden van het CBP in 2014:

Profilering

Met behulp van zogeheten tracking cookies, waarmee het gedrag van internetters over meerdere websites kan worden gevolgd, kunnen organisaties grote hoeveelheden persoonsgegevens verzamelen. Door deze gegevens vervolgens te analyseren en/of te combineren kunnen zij mensen in bepaalde categorieën (profielen) indelen en hen vervolgens anders behandelen of gerichter benaderen. Dat kan prettig zijn, denk bijvoorbeeld aan op maat gesneden advertenties, maar dan moeten mensen nadat zij goed zijn geïnformeerd hiertoe zelf een keuze hebben kunnen maken.

Het CBP deed onderzoek naar advertentiebedrijf YD (inmiddels: Yieldr) en concludeerde dat dit bedrijf de wet overtrad door via tracking cookies persoonsgegevens te verzamelen om internetgebruikers gepersonaliseerde advertenties te tonen. Yieldr vroeg hiervoor geen toestemming maar bood alleen een opt-out, hetgeen in strijd is met de wet. Ook de Nederlandse Publieke Omroep (NPO) bleek tijdens onderzoek van het CBP onrechtmatig te handelen door via tracking cookies het surfgedrag van bezoekers van verschillende omroepwebsites te volgen, zonder hiervoor vooraf om toestemming te vragen. Het CBP constateerde onder meer dat op alle NPO-websites al bij het laden van een webpagina analytische tracking cookies werden geplaatst, dus vóórdat de websitebezoeker een keuze kon maken. Tevens stelde het CBP vast dat de NPO bezoekers onvolledig, inconsistent en soms feitelijk onjuist informeerde over de verschillende soorten cookies en welke persoonsgegevens waarvoor werden gebruikt.

In 2013 publiceerde het CBP onderzoek naar de aangepaste privacyvoorwaarden van Google. Uit dit onderzoek bleek dat Google persoonsgegevens van internetgebruikers combineerde, onder meer voor het tonen van gepersonaliseerde advertenties. Google kon gegevens over bijvoorbeeld zoekopdrachten, locatiedata, bekeken video's en e-mails met elkaar combineren, terwijl de diverse diensten heel verschillende doelen dienen. Dit gebeurde bovendien zonder dat Google internetgebruikers hierover vooraf goed informeerde en zonder dat het bedrijf hiervoor toestemming vroeg. In 2014 legde het CBP daarom een last onder dwangsom op aan Google. De dwangsom kon oplopen tot 15 miljoen euro.

Decentralisatie

Op 1 januari 2015 hebben gemeenten nieuwe taken gekregen op het gebied van jeugdzorg, werk & inkomen en zorg aan langdurig zieken en ouderen (ook wel het 'sociaal domein' genoemd). De voorbereiding op deze decentralisatie (overheveling) van taken van de rijksoverheid en provincies naar de gemeenten vond plaats in 2014. Het CBP reageerde onder meer op de beleidsvisie van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties over privacy in het sociaal domein, waarin wordt gesproken over een 'lerende praktijk' binnen gemeenten die na enige tijd wordt geëvalueerd. Het CBP benadrukte dat gemeenten de naleving van de Wet bescherming persoonsgegevens niet kunnen opschorten als gevolg van een 'lerende praktijk'.

Het CBP kreeg daarnaast het verzoek om de uitkomsten van een *privacy impact assessment* voor het jeugddomein te beoordelen. De belangrijkste boodschap van het CBP was dat een deugdelijke, overkoepelende wettelijke basis ontbreekt voor de verwerking van persoonsgegevens bij de uitvoering van nieuwe taken binnen de verschillende onderdelen van het sociaal domein. Gemeenten kunnen voor diverse varianten kiezen om de nieuwe taken uit te voeren, met verschillende partijen en werkwijzen. Daarbij moeten zij steeds vaststellen op welke wettelijke grondslag zij de gegevensverwerking kunnen baseren. Het CBP constateerde dat het vinden van een grondslag in de praktijk tijdrovend, ingewikkeld en soms zelfs onmogelijk is. Dit geldt niet alleen voor het jeugddomein, maar voor het gehele sociaal domein. Het dringende advies van het CBP aan de bewindspersonen was daarom om alsnog te zorgen voor een overkoepelende wettelijke basis.

Arbeidsrelatie

Randstad en Adecco, twee van de grootste Nederlandse uitzendbureaus, bleken tijdens onderzoek van het CBP op verschillende punten de wet te overtreden bij de verwerking van gegevens van uitzendkrachten. Zo vroegen beide uitzendbureaus aan uitzendkrachten die zich ziek meldden naar de aard en oorzaak van de ziekte en registreerden dit in een systeem. Daarnaast maakten Randstad en Adecco kopieën van identiteitsbewijzen van mensen tijdens een intakegesprek, hetgeen in dat stadium nog niet is toegestaan. Adecco verstrekte bovendien in strijd met de wet kopieën van ID-bewijzen aan opdrachtgevers. Tot slot bleek uit de onderzoeken dat zowel Randstad als Adecco persoonsgegevens van uitzendkrachten langer dan noodzakelijk bewaarden.

Het CBP onderzocht de beveiliging van Suwinet, een systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen op het gebied van werk en inkomen. Het is van groot belang dat deze gegevens goed zijn beschermd en dat alleen de daartoe bevoegde medewerkers er toegang toe hebben. Zowel bij het UWV (als beheerder van Suwinet) als bij de gemeente 's-Hertogenbosch (als afnemer) bleken de maatregelen niet toereikend om deze bescherming te kunnen bieden. Veel van de vereiste plannen of procedures waren niet up-to-date, niet compleet of niet afgemaakt. Het UWV en 's-Hertogenbosch hadden beide geen beveiligingsplan specifiek gericht op Suwinet. Ook werden beveiligingsincidenten niet centraal geanalyseerd en afgewikkeld.

Werkwijze CBP

Het College bescherming persoonsgegevens is de autoriteit die toezicht houdt op de naleving van de Wet bescherming persoonsgegevens en aanverwante wetgeving. Om naleving te bevorderen, zet het CBP een mix van instrumenten in op het gebied van toezicht, handhaving en communicatie.

Toezicht
Het CBP kan lang niet alle vermeende overtredingen van de wet onderzoeken. Daarom hanteert het een aantal criteria om te bepalen of het tot onderzoek overgaat. Het CBP doet onderzoek bij een vermoeden van ernstige en structurele overtredingen die veel mensen treffen, waarbij het met zijn bevoegdheden verschil kan maken en die vallen binnen de thema's die het jaarlijks vaststelt.

Het CBP kan er ook voor kiezen om bijvoorbeeld een waarschuwingsbrief aan een organisatie te sturen of een gesprek te voeren. Dit doet het CBP met name bij mogelijke overtredingen die niet aan bovengenoemde criteria voldoen. Zo'n brief of gesprek kan al voldoende zijn om de overtreding te laten beëindigen. Werkt de organisatie echter niet mee of krijgt het CBP opnieuw klachten over deze organisatie, dan kan het alsnog een onderzoek starten.

Handhaving
Heeft het CBP tijdens het onderzoek overtredingen geconstateerd die voortduren, dan kan het handhavend optreden. Het CBP heeft de bevoegdheid om organisaties een last onder dwangsom op te leggen. Zij krijgen dan een bepaalde periode om de overtredingen te beëindigen. Als dit niet gebeurt, moeten zij een dwangsom betalen die kan oplopen tot een bepaald maximumbedrag.

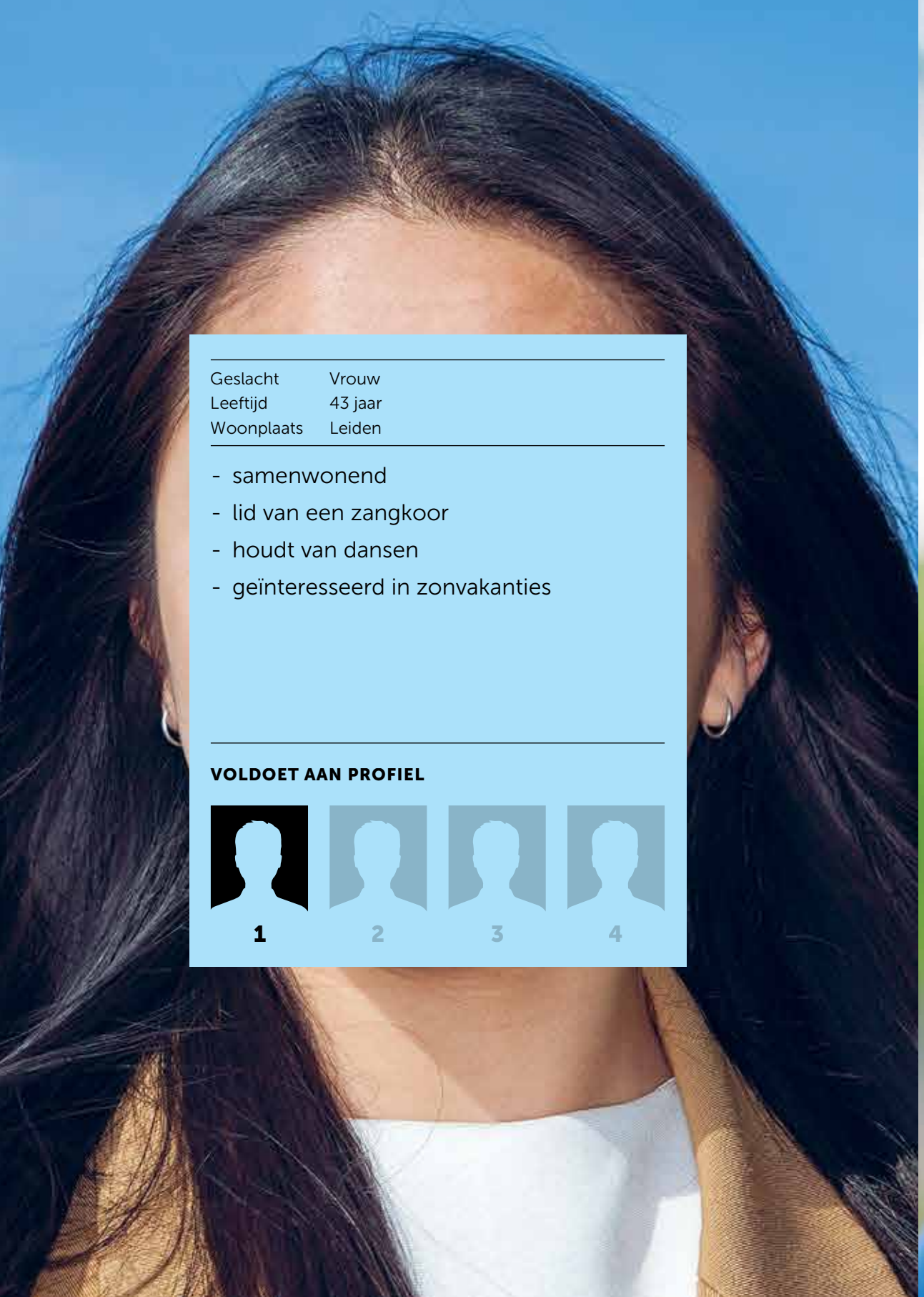
Communicatie
Ook externe communicatie is een belangrijk instrument om naleving van de wet te bevorderen. Het CBP onderhoudt contacten met de media, voert gesprekken met brancheorganisaties en andere stakeholders en verzorgt regelmatig externe optredens. Daarnaast geeft het CBP voorlichting via het telefonisch spreekuur en de – in 2014 geheel vernieuwde – website **cbpweb.nl**.

Jaarverslag
Deze publicatie behandelt de belangrijkste werkzaamheden van het CBP in 2014. Meer informatie en de cijfers van dat jaar zijn te vinden in de online bijlage: **www.cbpweb.nl/14/2**

Daarnaast is er de samenvatting *2014 - Het CBP in vogelvlucht*, die zowel op papier als online beschikbaar is: **www.cbpweb.nl/14/3**

Over de grens

Het CBP neemt deel aan verschillende Europese samenwerkingsverbanden, zoals de Artikel 29-werkgroep, de Berlijn Telecomgroep en de toezichthoudende organen voor onder meer Europol en Eurojust. Binnen deze samenwerkingsverbanden hield het CBP zich in 2014 onder meer bezig met big data en surveillance door inlichtingendiensten. Ook besteedde het CBP, net als in 2013, veel tijd aan de herziening van de Europese privacyregelgeving. Daarnaast is in 2014 het Privacy Bridges Project van start gegaan, op initiatief van de CBP-voorzitter. Amerikaanse en Europese privacydeskundigen zoeken hierbij naar praktische oplossingen om de trans-Atlantische verschillen in de juridische benadering van het recht op bescherming van persoonsgegevens te overbruggen.

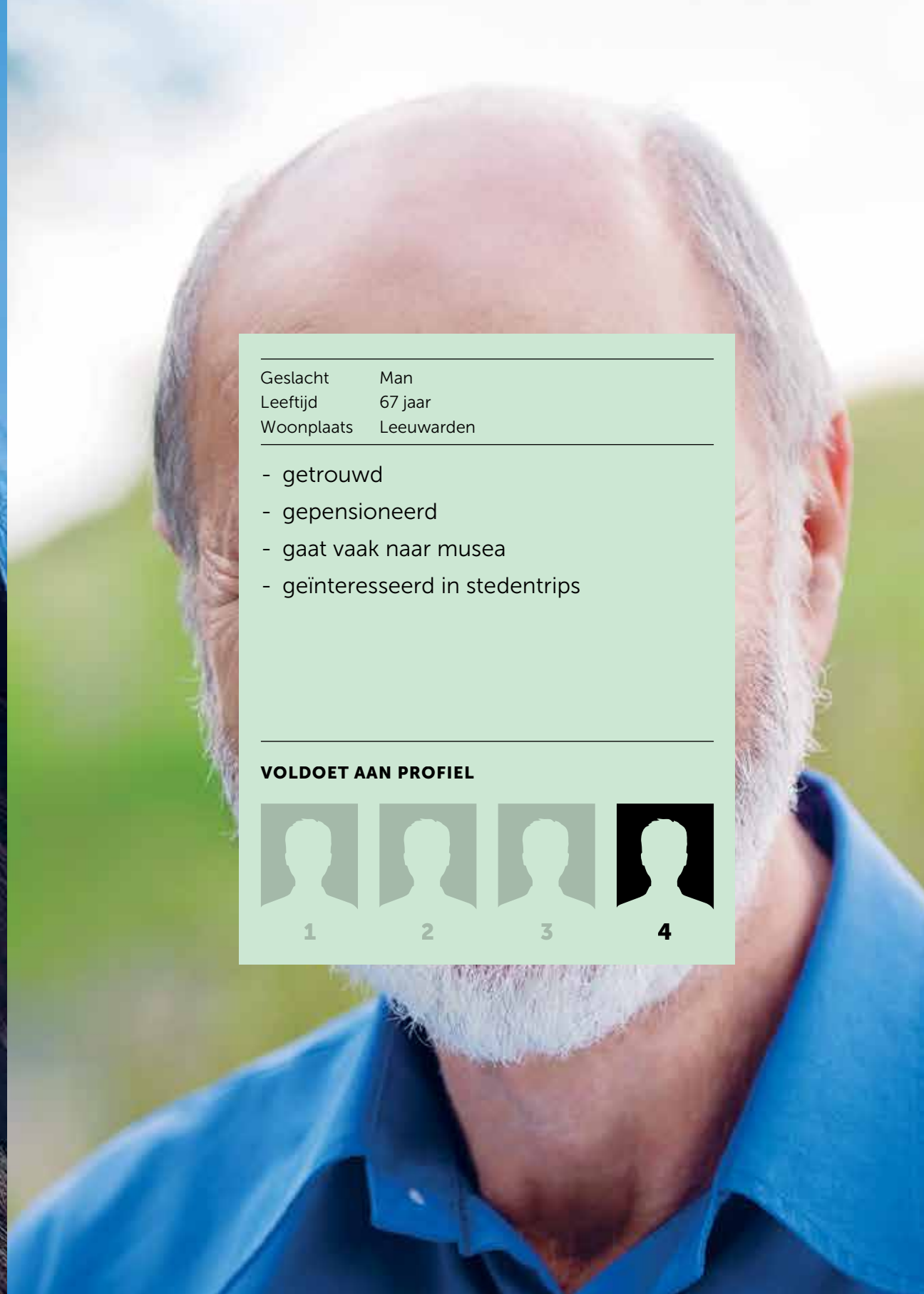


Geslacht	Vrouw
Leeftijd	43 jaar
Woonplaats	Leiden

- samenwonend
- lid van een zangkoor
- houdt van dansen
- geïnteresseerd in zonvakanties

VOLDOET AAN PROFIEL

1 2 3 4



Geslacht	Man
Leeftijd	67 jaar
Woonplaats	Leeuwarden

- getrouwd
- gepensioneerd
- gaat vaak naar musea
- geïnteresseerd in stedentrips

VOLDOET AAN PROFIEL

1 2 3 **4**

INTERNET EN TELECOM

Profilering was een van de thema's waaraan het CBP in 2014 speciale aandacht besteedde. Profilering houdt in dat organisaties (persoons)gegevens verzamelen en vervolgens analyseren en/of combineren met als doel mensen in te delen in bepaalde categorieën (profielen). Vervolgens kunnen de organisaties deze mensen – vaak zonder dat zij dat weten – op basis van die profielen anders behandelen of gerichter benaderen. Dat kan prettig zijn, denk bijvoorbeeld aan op maat gesneden advertenties, maar dan moeten mensen hierover wel goed zijn geïnformeerd en zelf een keuze hebben kunnen maken. Internetgebruikers hebben het recht om te weten wie welke persoonsgegevens waarvoor verzamelt. Vervolgens moeten zij zelf kunnen beslissen of ze hiervoor toestemming geven.

Google

In 2013 publiceerde het CBP onderzoek naar de in 2012 aangepaste privacyvoorwaarden van Google. Uit dit onderzoek bleek dat Google persoonsgegevens van internetgebruikers combineerde, onder meer voor het tonen van gepersonaliseerde advertenties. Het ging daarbij niet alleen om mensen die waren ingelogd op een Google-account, maar ook om mensen die de zoekmachine gebruikten of een website bezochten met cookies van Google. Het bedrijf kon gegevens over bijvoorbeeld zoekopdrachten, locatiedata, bekeken video's en e-mails met elkaar combineren, terwijl de diverse diensten heel verschillende doelen dienen. Dit gebeurde bovendien zonder dat Google internetgebruikers hierover vooraf goed informeerde en zonder dat het bedrijf hiervoor toestemming vroeg.

Het CBP legde in december 2014 een last onder dwangsom op aan Google omdat de aangepaste privacyvoorwaarden in strijd waren met de wet. De dwangsom kon oplopen tot 15 miljoen euro. Het CBP eiste onder meer dat Google ondubbelzinnige toestemming vraagt aan de gebruikers voor het combineren van persoonsgegevens uit de verschillende Googlediensten. Dit kan bijvoorbeeld via een duidelijk toestemmingsscherm. Ook eiste het CBP dat Google de informatie in het privacybeleid verder aanpast, zodat mensen heldere en consistente informatie krijgen over welke persoonsgegevens de verschillende diensten van Google gebruiken.

Google treft maatregelen om de geconstateerde overtredingen te beëindigen. Het CBP controleert of door deze maatregelen de overtredingen daadwerkelijk opgeheven zijn.
→ Lees verder: www.cbpweb.nl/14/4

Cookies

Organisaties passen profilering vaak toe op basis van gegevens die zij hebben verzameld via zogeheten tracking cookies. Met behulp van deze cookies kunnen zij het gedrag van internetters over meerdere websites volgen. Het plaatsen en lezen van tracking cookies is alleen toegestaan als websitebezoekers hierover adequate informatie krijgen en zij hiervoor vooraf hun ondubbelzinnige toestemming hebben gegeven.

Online advertenties

In mei 2014 publiceerde het CBP zijn onderzoek naar YD Display Advertising Benelux B.V. (inmiddels: Yieldr), een bedrijf dat bemiddelt tussen adverteerders en websites bij het plaatsen van online advertenties. Het CBP concludeerde dat Yieldr de wet overtrad door zonder toestemming persoonsgegevens van internetgebruikers te verzamelen om vervolgens gepersonaliseerde advertenties aan hen te tonen.

Yieldr verzamelde met tracking cookies onder meer informatie over producten of diensten die internetgebruikers bekeken op websites van zijn adverteerders. Vervolgens liet het bedrijf op verschillende andere sites advertenties van die adverteerders zien *(retargeting)*. Yieldr vroeg hiervoor geen toestemming aan internetgebruikers, maar bood alleen een opt-out. Dat is in strijd met de wet.

Surfgedrag hoort privé te blijven, tenzij je toestemming geeft om gevolgd te worden op internet.
Wilbert Tomesen, vicevoorzitter van het CBP

Het CBP heeft Yieldr desgevraagd in de gelegenheid gesteld om samen met de marketingbranche aan een branche-brede oplossing te werken om de geconstateerde overtredingen te beëindigen. Hierna controleert het CBP in hoeverre de overtredingen voortduren en beslist het over eventuele inzet van handhavende maatregelen.

Omroepwebsites

Het CBP maakte in juli 2014 de resultaten van onderzoek naar het gebruik van tracking cookies door de Nederlandse Publieke Omroep (NPO) openbaar. Het CBP concludeerde dat de NPO in strijd met de wet handelde door via deze cookies het surfgedrag van bezoekers

van verschillende omroepwebsites te volgen, zonder hiervoor vooraf om toestemming te vragen. Het CBP constateerde dat op alle NPO-websites al bij het laden van een webpagina analytische tracking cookies werden geplaatst. Dit gebeurde dus vóór de websitebezoeker een keuze kon maken. Op de NPO-websites werden daarnaast andere tracking cookies geplaatst zonder dat bezoekers hiervoor ondubbelzinnige toestemming hadden gegeven.

Websitebezoekers moeten eerst informatie krijgen over de verschillende soorten cookies en over welke persoonsgegevens waarvoor worden gebruikt, zodat zij weten waarvoor zij precies toestemming geven. Het CBP stelde vast dat de NPO de bezoekers onvolledig, inconsistent en soms feitelijk onjuist informeerde. De NPO verzamelde gegevens van websitebezoekers onder meer om het publieksbereik te meten, gepersonaliseerde advertenties te tonen en het delen via social media mogelijk te maken. De informatie hierover schoot op verschillende punten tekort.

De NPO treft maatregelen om de geconstateerde overtredingen te beëindigen. Het CBP controleert of door deze maatregelen de overtredingen daadwerkelijk zijn beëindigd.
→ Lees verder: www.cbpweb.nl/14/5

Apps

Het is cruciaal dat duidelijk is wat er met de gegevens van app-gebruikers gebeurt. Zeker als het om de gegevens van een kwetsbare groep als kinderen gaat. De kinderen en/of degenen die namens hen toestemming verlenen voor het gebruik van hun gegevens, zoals hun ouders, moeten vooraf voldoende begrijpelijke en specifieke informatie krijgen over de werking van de app. Ook adequate beveiliging van de persoonsgegevens die via de app worden verzameld, onder meer opdat onbevoegden daarvan geen kennis kunnen nemen, is een wettelijk vereiste.

Tablets in basisonderwijs

Snappet, een organisatie die tablets met ingebouwde apps verhuurt aan meer dan vierhonderd basisscholen, verwerkte leerresultaten van kinderen in strijd met de wet. Op de Snappet-tablets kunnen kinderen onder meer oefeningen doen voor vakken als taal, spelling en rekenen. Uit onderzoek van het CBP bleek dat Snappet de persoonsgegevens van kinderen niet alleen verwerkte voor doelen die redelijkerwijs voortvloeien uit het gebruik van onderwijstablets, zoals het teruggeven van de resultaten aan de kinderen en hun eigen leraar.

Tablets en andere digitale leermiddelen zijn een prachtige verrijking van het onderwijs. Maar scholen moeten wel weten wat er met de gegevens van de kinderen gebeurt, zodat ze zelf kunnen bepalen waarvoor de gegevens mogen worden gebruikt. Wilbert Tomesen, vicevoorzitter van het CBP

Snappet bleek de persoonsgegevens bijvoorbeeld ook te gebruiken om kinderen voortdurend per opgave te beoordelen en te kwalificeren in vergelijking met alle andere kinderen die de Snappet-tablets gebruiken. Dit deed Snappet zonder dat de scholen hiervoor een expliciete schriftelijke opdracht hadden gegeven. Het bedrijf gaf de scholen onvoldoende informatie over de verwerking van de gegevens van de kinderen. Ook had Snappet de dienst onvoldoende beveiligd tegen onrechtmatige verwerking van de persoonsgegevens door onbevoegde derde partijen.

Snappet heeft toegezegd scholen beter te informeren over de gegevensverwerkingen. De scholen kunnen dan vervolgens de ouders informeren. Verder heeft het bedrijf inmiddels een maatregel getroffen waardoor leerresultaten in de algemene overzichtstabellen niet meer te herleiden zouden zijn tot de kinderen. Tot slot heeft Snappet beveiligingsmaatregelen genomen. Het CBP controleert of Snappet de geconstateerde overtredingen daadwerkelijk heeft beëindigd.
→ Lees verder: www.cbpweb.nl/14/6

App voor kinderen

Het CBP deed in 2014 onderzoek naar de kinderapp Okki Gekke-bekken-club. Hierbij constateerde het CBP dat de app, die jonge kinderen helpt om hun tanden goed te poetsen, op meerdere punten in strijd was met de wet. Via de app konden kinderen gegevens van zichzelf op internet publiceren, waaronder foto's. De app bevatte geen waarschuwing dat de kinderen hiervoor eerst toestemming moeten vragen aan hun ouders. Bovendien was er geen mogelijkheid voor de kinderen en hun ouders om deze gegevens van internet te verwijderen. Tot slot stelde het CBP vast dat de gegevens onversleuteld via internet werden verzonden.

Blink Uitgevers heeft naar aanleiding van het onderzoek van het CBP de app uit de app stores verwijderd en alle foto's en overige persoonsgegevens van de kinderen verwijderd van de bijbehorende website. Ook heeft Blink Uitgevers aangekondigd maatregelen te nemen om verdere overtredingen in de toekomst te voorkomen. De uitgever heeft toegezegd de app pas terug te plaatsen als ondubbelzinnige toestemming wordt gevraagd aan de ouders van kinderen en ook op alle andere punten aan de wet is voldaan.

→ Ook in het hoofdstuk Internationaal van dit jaarverslag zijn onderwerpen te vinden op het gebied van internet & telecom, zoals big data en verwijderverzoeken aan zoekmachines.

Verwerking van internet- en telefoongegevens

Zowel de overheid als het bedrijfsleven kunnen baat hebben bij de verwerking van telecomgegevens. De politie bijvoorbeeld voor opsporingsdoeleinden en telecomaanbieders voor netwerkbeheer. Omdat deze gegevens veel kunnen zeggen over het gedrag en de voorkeuren van mensen, raakt dit echter direct aan de persoonlijke levenssfeer. Het is daarom uiterst belangrijk dat bedrijven zich bij deze gegevensverwerking aan de wet houden en dat bij nieuwe (wettelijke) bevoegdheden hieromtrent de noodzaak van de verwerking goed is onderbouwd.

Bewaarplicht verkeersgegevens

Het Europees Hof van Justitie bepaalde in mei 2014 dat een algemene bewaarplicht van verkeersgegevens in strijd is met het fundamentele recht op de bescherming van persoonsgegevens zoals dat is verankerd in Europees recht. Uit de uitspraak blijkt dat de bewaarplicht een te grote inbreuk maakt op de persoonlijke levenssfeer en mensen het idee kan geven dat zij voortdurend onder observatie staan. In november bleek het Nederlandse kabinet vast te houden aan de opslag van verkeersgegevens en deed het een voorstel voor een aanpassing van de betreffende wet. Het CBP liet weten de kabinetsreactie en het bijbehorende in consultatie gegeven wetsvoorstel zorgvuldig te bestuderen.

In februari 2015 bracht het CBP een advies over het wetsvoorstel uit. Het bewaren van de telefoon- en internetgegevens van bijna alle Nederlanders gedurende zes tot twaalf maanden is een zeer ingrijpende maatregel, waarvan de noodzaak onweerlegbaar moet worden aangetoond. Het CBP constateerde dat in het wetsvoorstel deze noodzaak onvoldoende is onderbouwd. Daarnaast beperkt de bewaarplicht zich niet tot enkel die gegevens die noodzakelijk zijn voor het bestrijden van zware criminaliteit. Het CBP concludeerde dat hiermee de inbreuk op de persoonlijke levenssfeer van feitelijk alle Nederlanders te groot en oneven-redig is. Het CBP adviseerde het wetsvoorstel niet in te dienen.

Data-analyse telecomaanbieders

In 2014 controleerde het CBP of telecomaanbieders Tele2, T-Mobile en Vodafone maatregelen hadden getroffen om eerder geconstateerde overtredingen van de wet te beëindigen. Uit onderzoek van het CBP was gebleken dat deze aanbieders bij de analyse van het dataverkeer over hun mobiele netwerk *(deep packet inspection)* in strijd met de wet op detailniveau gegevens bewaarden over bezochte websites en gebruikte apps. Uit het onderzoek kwam ook naar voren dat de aanbieders hierover hun klanten niet of onjuist informeerden.

Het is in veel gevallen niet noodzakelijk om deze gegevens op klantniveau te bewaren. De telecomaanbieders hebben onder meer de gebruikte apparatuur en technologie, bewaartermijnen van klantgegevens en de informatie hierover aangepast. Hiermee werden de overtredingen beëindigd. Het onderzoek vond oorspronkelijk plaats bij vier telecomaanbieders, maar KPN beëindigde de geconstateerde overtredingen al tijdens het onderzoek.

Recht op inzage gegevens bij telecomaanbieders

Telecomaanbieders mogen in beginsel geen kennis nemen van de inhoud van het dataverkeer, zoals welke websites iemand heeft bezocht of welke apps iemand heeft gebruikt. Hiervoor is analyse van het dataverkeer *(deep packet inspection)* nodig. Telecomaanbieders mogen dergelijke analyses alleen toepassen als dat strikt noodzakelijk is voor technische doeleinden zoals het beheer van het netwerk, mits ze de gegevens direct anonimiseren. Ze mogen geen analyses op individueel niveau bewaren, tenzij de klant daarvoor vooraf toestemming heeft gegeven.

Het tv-programma Radar besteedde op 15 september 2014 aandacht aan de ophef onder klanten van telecomaanbieders over onverklaarbaar hoge rekeningen voor dataverbruik. Zij wilden weten welke websites of apps op welk moment hoeveel data hadden verbruikt. De aanbieders zeiden echter geen inzicht te kunnen geven in de details van dit dataverbruik en beriepen zich hierbij op de privacywetgeving, die zou verbieden dergelijke gegevens op te slaan. In de uitzending onderstreepte de voorzitter van het CBP dat de wet aanbieders niet verbiedt telecomgegevens op te slaan om klanten inzicht te kunnen geven in hun verbruik, mits zij hiervoor vooraf toestemming hebben gegeven. Telecomaanbieders zouden nieuwe klanten hierover goed moeten informeren, aldus de CBP-voorzitter.

Nieuwe privacyvoorwaarden Facebook

Het CBP besloot in december 2014 om het nieuwe privacybeleid van Facebook te onderzoeken. Aanleiding hiervoor was de aankondiging van het bedrijf dat per 1 januari 2015 nieuwe privacyvoorwaarden zouden gelden voor Facebook-gebruikers. Deze voorwaarden geven Facebook onder meer het recht om gegevens en foto's uit Facebook-profielen te gebruiken voor commerciële doeleinden. Het CBP wil weten welke gevolgen dit heeft voor de privacy van Facebook-gebruikers in Nederland. Het wil onder meer weten hoe Facebook toestemming verkrijgt voor het gebruiken van hun persoonsgegevens.

Privacychecklist slimme meters

Wie een slimme energiemeter heeft, kan een zogeheten energiebesparingsdienst gebruiken. Besparingsdiensten zijn handige tools die consumenten inzicht geven in hun energieverbruik, bijvoorbeeld via een website of app. Maar hoe gaan de bedrijven die deze diensten aanbieden om met de privacy van consumenten? Hoe vaak lezen zij bijvoorbeeld de gegevens van de slimme meter uit? En wat doen zij vervolgens met deze gegevens? Het CBP en de Autoriteit Consument en Markt (ACM) ontwikkelden in 2014 samen een privacychecklist, zodat mensen dit eenvoudig kunnen nagaan.

De aanbieders van de besparingsdiensten zijn wettelijk verplicht om consumenten vooraf duidelijk te informeren over een aantal belangrijke punten op het gebied van privacy. Ook mogen deze bedrijven niet zonder de expliciete toestemming van de klanten hun meetgegevens verzamelen en gebruiken. In de privacychecklist zijn deze punten op een rij gezet. Zo kunnen consumenten weloverwogen een keuze maken en zelf bepalen of het gemak van een besparingsdienst wel opweegt tegen het prijsgeven van een deel van hun privacy.
→ Bekijk de checklist: www.cbpweb.nl/14/7

OVERHEID

Een onderwerp dat in 2014 sterk in de belangstelling stond was de naderende decentralisatie van taken in het sociaal domein. Deze overheveling van taken van de rijksoverheid en provincies naar de gemeenten is op 1 januari 2015 ingegaan; 2014 stond in het teken van de voorbereiding hierop. Gemeenten hebben er nieuwe taken bij gekregen op het gebied van jeugdzorg, werk & inkomen en zorg aan langdurig zieken en ouderen. Het CBP vroeg in 2014 opnieuw aandacht voor de privacyrisico's hiervan.

De decentralisatie heeft tot gevolg dat meerdere instellingen meer gegevens van meer mensen verwerken. Hier zijn bijzondere persoonsgegevens bij, zoals medische en strafrechtelijke gegevens. Voor het CBP was de decentralisatie dan ook een van de speerpunten in 2014. Het CBP gaf, net als in 2013, advies over de bescherming van persoonsgegevens bij de decentralisatie. Hierbij benadrukte het CBP dat de gemeenten zich ook bij de uitvoering van hun nieuwe taken aan de Wet bescherming persoonsgegevens (Wbp) moeten houden. Het CBP constateerde echter, op basis van intensieve gesprekken met gemeenten, dat dit in de praktijk lastig kan zijn. Ook voerde het CBP verschillende gesprekken met de betrokken ministeries en andere organisaties die zich bezighouden met de decentralisatie.

Reactie op beleidsvisie privacy in sociaal domein

In vervolg op zijn adviezen uit 2013 stuurde het CBP in juni 2014 een brief naar de minister van Binnenlandse Zaken en Koninkrijksrelaties. Met deze brief reageerde het CBP op de beleidsvisie over privacy in het sociaal domein van 27 mei 2014. In deze visie wordt gesproken over een 'lerende praktijk'. Dit houdt in dat de gemeenten in de praktijk kijken welke privacyrisico's zich voordoen en welke oplossingen zij daarvoor kunnen vinden. Het CBP benadrukte in de brief onder meer dat gemeenten de naleving van de Wbp niet kunnen opschorten als gevolg van een 'lerende praktijk'.

Zo mogen de gemeenten en andere betrokken partijen op grond van de Wbp niet meer gegevens delen dan noodzakelijk, mogen zij de verzamelde gegevens niet gebruiken voor een doel dat onverenigbaar is met het oorspronkelijke verzameldoel en moeten zij de gegevens adequaat beveiligen. Ook wees het CBP erop dat gemeenten toestemming van mensen om hun gegevens te verwerken niet kunnen gebruiken als legitimatie voor een eventuele onrechtmatige gegevensverwerking, zoals het verzamelen van te veel gegevens of gegevens die niet noodzakelijk zijn.

→ Lees verder: www.cbpweb.nl/14/8

Gemeenten verwerken voor hun nieuwe taken veel gevoelige persoonsgegevens, wat het extra belangrijk maakt dat zij zich aan de privacywetgeving houden.
Wilbert Tomesen, vicevoorzitter van het CBP

Beoordeling privacytoets jeugddomein

In oktober 2014 werd het CBP gevraagd om de uitkomsten van een *privacy impact assessment* (PIA) voor het jeugddomein te beoordelen. Het CBP heeft zijn reactie op dit verzoek openbaar gemaakt. De belangrijkste boodschap van het CBP was dat een deugdelijke wettelijke basis voor de verwerking van persoonsgegevens bij de uitvoering van nieuwe taken binnen de verschillende onderdelen van het sociaal domein ontbreekt. Daarom is het in de praktijk lastig voor gemeenten om te beoordelen welke risico's de verwerking van persoonsgegevens met zich meebrengt en wat wel en niet mag. Dit geldt niet alleen voor het jeugddomein, maar voor het gehele sociaal domein.

Gemeenten kunnen voor verschillende varianten kiezen om de nieuwe taken uit te voeren, met verschillende partijen en werkwijzen. Daarbij moeten zij steeds vaststellen op welke wettelijke grondslag zij de gegevensverwerking kunnen baseren. Zonder zo'n grondslag is de verwerking van persoonsgegevens niet toegestaan. Het CBP constateerde dat het vinden van een grondslag in de praktijk tijdrovend, ingewikkeld en soms zelfs onmogelijk is. Dat komt omdat integraal werken (problemen uit verschillende domeinen tegelijk oppakken) niet als zodanig is geregeld in de decentralisatiewetten (Jeugdwet, Participatiewet en Wmo 2015).

Bovendien zijn twee grondslagen voor het verwerken van persoonsgegevens die op het eerste gezicht voor de hand lijken te liggen – toestemming van betrokkenen en uitvoering van publiekrechtelijke taken – meestal niet van toepassing. Toestemming moet volgens de wet in vrijheid zijn gegeven, maar er is vaak een afhankelijkheidsrelatie tussen de betrokkenen en de gemeente. Daarnaast zijn niet alle taken van de gemeente te kwalificeren als publiekrechtelijke taken. Het dringende advies van het CBP was daarom om alsnog te zorgen voor een deugdelijke, overkoepelende wettelijke basis voor de verwerking van persoonsgegevens in het sociaal domein.

→ Lees verder: www.cbpweb.nl/14/9

Jeugdzorg

Onder jeugdzorg valt de ondersteuning van en hulp aan kinderen en hun ouders bij (dreigende) opgroei-, opvoedings- of psychiatrische problemen. Sinds 1 januari 2015 is de nieuwe Jeugdwet van kracht. Hierdoor zijn gemeenten verantwoordelijk geworden voor de jeugdzorg. In 2014 adviseerde het CBP over het ontwerpbesluit Jeugdwet. Ook deed het CBP onderzoek naar de gegevensverwerking bij Bureau Jeugdzorg (BJZ) Limburg en BJZ Noord-Holland.

Advies ontwerpbesluit Jeugdwet

Het CBP adviseerde in mei 2014 over het ontwerpbesluit Jeugdwet. Dit besluit regelt onder meer een verruiming van de verwijsindex risicojongeren (VIR) door de kring van meldingsbevoegden aan de VIR uit te breiden. Het CBP miste hierbij een onderbouwing van de noodzaak van deze verruiming, mede gezien een uitgevoerde evaluatie van de VIR, die aanleiding gaf om de effectiviteit en daarmee de continuering van de VIR opnieuw te bezien. Verder wees het CBP erop dat noch in dit ontwerpbesluit, noch in de Jeugdwet zelf voldoende is geregeld hoe gemeenten hun taken bij de VIR – en de bijbehorende noodzakelijke verwerking van persoonsgegevens – dienen in te richten.

Beleidsinformatie

Naast de verruiming van de VIR regelt het ontwerpbesluit dat enkele partijen (waaronder jeugdhulpaanbieders en Advies- en Meldpunten Kindermishandeling (AMK's)) verplicht zijn gegevens te verstrekken aan de rijksoverheid voor beleidsinformatie. Het gaat hierbij om direct tot de persoon herleidbare gegevens, terwijl dat eerder gepseudonimiseerde gegevens waren. Het CBP adviseerde daarom te onderbouwen waarom een minder ingrijpende methode niet voldoet en als dat niet mogelijk is, af te zien van de verplichting om deze gegevens te verstrekken.

Ook bevat het ontwerpbesluit de bevoegdheid voor gemeenten om partijen als AMK's te verplichten gegevens te verstrekken voor de gemeentelijke beleidsdoelen. Het CBP adviseerde om aan deze bevoegdheid voorwaarden te verbinden, die er in ieder geval voor zorgen dat gemeenten expliciet afwegen wat de privacyrisico's zijn en maatregelen nemen om deze te voorkomen.

Justitiële gegevens

Het CBP adviseerde ook over een aanvulling van het Besluit Jeugdwet. Dit artikel regelt onder meer dat de minister van Veiligheid en Justitie justitiële gegevens mag verstrekken aan de gemeente, omdat gemeenten verantwoordelijk zijn voor de uitvoering van maatregelen die volgen uit een strafrechtelijke beslissing (zoals jeugdreclassering).

Het CBP merkte op dat de taak waarvoor gemeenten justitiële gegevens mogen ontvangen heel algemeen geformuleerd is. Daardoor is onduidelijk welk doel de verwerking van deze gegevens dient. Het CBP adviseerde daarom de noodzaak van de verstrekking per (deel)doel te onderbouwen. Vervolgens moet in het ontwerpbesluit worden omschreven voor welke specifieke doelen justitiële gegevens mogen worden verstrekt en voor welke specifieke taken de gemeente deze gegevens mag verwerken.

Het ontbreken van deze onderbouwing en specificatie van de doelen maakt het ook lastig te bepalen of de gegevens toereikend, ter zake dienend en niet bovenmatig zijn. Daardoor ontstaat het risico dat er meer gegevens worden verwerkt dan noodzakelijk is. Het CBP adviseerde dan ook om, op basis van de nadere specificatie van de doeleinden, een onderbouwing te geven van de aard en omvang van de daartoe te verstrekken gegevens.

Onderzoek Bureaus Jeugdzorg

Het CBP deed in 2014 onderzoek naar de kwaliteit van de persoonsgegevens in de dossiers van twee Bureaus Jeugdzorg (BJZ's). Het CBP concludeerde dat de werkwijzen van deze BJZ's onvoldoende waren om te waarborgen dat de gegevens juist en nauwkeurig zijn. Op basis van de informatie bij BJZ's kunnen ingrijpende beslissingen worden genomen over kinderen en jongeren. Deze beslissingen gaan bijvoorbeeld over de zorg die een jeugdige krijgt of over een verzoek aan de Raad voor de Kinderbescherming om onderzoek te doen. Bovendien bevinden de kinderen en jongeren en hun ouders zich in een afhankelijke positie ten opzichte van de BJZ's. Het is daarom van groot belang dat de informatie waarmee een BJZ werkt, juist en nauwkeurig is.

Uit het onderzoek bleek dat bij de BJZ's onvoldoende werd voorgeschreven op welke wijze de persoonsgegevens moeten worden geregistreerd, opdat de kwaliteit ervan kan worden gewaarborgd. Zo ontbraken werkwijzen voor de zogeheten contactjournaals waarin de contacten van BJZ met hulpverleners, ouders en jeugdigen zijn vastgelegd. Ook was niet altijd genoeg uitgewerkt hoe onderscheid wordt gemaakt tussen 'harde' feitelijke gegevens en 'zachte' gegevens, die gaan over meningen, indrukken en vermoedens. Tot slot ontbrak een standaardwerkwijze voor onder meer het weergeven van de herkomst van informatie, het actueel houden ervan en het markeren van onjuistheden.

Naar aanleiding van het onderzoek hebben de twee onderzochte BJZ's, Noord-Holland (tegenwoordig De Jeugd- en Gezinsbeschermers) en Limburg, maatregelen aangekondigd om hun werkwijzen te verbeteren. Het CBP heeft hierover ook met Jeugdzorg Nederland gesproken. Het CBP bekijkt in hoeverre met deze maatregelen de geconstateerde overtredingen zijn beëindigd.

→ Lees verder: www.cbpweb.nl/14/10

Cameratoezicht in het verkeer

Camera's langs (snel)wegen scannen kentekens van passerende voertuigen. De politie gebruikt deze kentekens voor automatische kentekenherkenning, ook wel ANPR (*automatic numberplate recognition*) genoemd. ANPR is een methode om gescande kentekens op automatische wijze te vergelijken met kentekens in politiebestanden. Op deze manier kan de politie verdachten signaleren, bijvoorbeeld voortvluchtige personen. Rijkswaterstaat en de provincies zetten ook ANPR-camera's in. Zij gebruiken de verzamelde kentekens om de adressen van automobilisten op bepaalde trajecten te achterhalen en hen vervolgens te benaderen voor verkeersonderzoek.

Advies camera's voor verkeersonderzoek

Rijkswaterstaat (RWS) voert verkeersonderzoeken en zogeheten spitsmijdenprojecten uit. Het doel hiervan is de verkeersveiligheid en de doorstroming van het verkeer te vergroten. Om automobilisten te benaderen voor onderzoek, maakt RWS gebruik van ANPR. Het wetsvoorstel tot wijziging van de Wegenverkeerswet 1994 (Wvw 1994) bevat de wettelijke basis voor wegbeheerders om camera's te plaatsen langs wegen voor verkeersonderzoeken. In januari 2014 gaf het CBP advies over dit wetsvoorstel.

Het CBP adviseerde onder meer om de memorie van toelichting (MvT) op twee punten aan te passen. De MvT beperkt zich tot de verkeersonderzoeken van RWS. Dit wekt de indruk dat alleen RWS de bevoegdheid krijgt om camera's te plaatsen. Maar door de grondslag hiervoor neer te leggen in artikel 14 van de Wvw 1994, worden álle wegbeheerders hiertoe bevoegd. Het CBP adviseerde om dit explicieter aan te geven. Ook adviseerde het CBP om in de MvT duidelijker te maken dat het plaatsen van camera's alleen is toegestaan voor verkeersonderzoeken, niet voor andere doelen.

Convenant Belastingdienst en politie

In september 2014 sloten de Belastingdienst en de politie een convenant waarin is vastgelegd dat de Belastingdienst toegang krijgt tot de kentekengegevens die de politie verzamelt met ANPR-camera's. Met deze gegevens kan de Belastingdienst bijvoorbeeld controleren of mensen privé in hun leaseauto rijden. Het CBP zette vraagtekens bij het massaal verzamelen en opslaan van gegevens van alle automobilisten, ongeacht of ze iets op hun kerfstok hebben. Het CBP vroeg zich af of het verzamelen van al deze gegevens noodzakelijk is om de taak van de Belastingdienst uit te voeren. Daarnaast stelde het CBP dat er een principiële discussie moet worden gevoerd over het gebruik van ANPR nu dit niet is voorbehouden aan de politie voor opsporingsdoeleinden, maar de gegevens ook met andere overheidsdiensten worden gedeeld. Bovendien mag de politie de kentekengegevens slechts een beperkte tijd bewaren, maar mag de Belastingdienst de verstrekte gegevens veel langer – tot soms wel zeven jaar – bewaren.

Inkomensgegevens van huurders

In 2013 concludeerde het CBP na onderzoek dat de Belastingdienst van te veel huurders gegevens gebruikte bij de uitvoering van de inkomensafhankelijke huurverhoging. De Belastingdienst nam in dat jaar álle huurwoningen op in een bestand, in plaats van alleen die woningen waarvoor de inkomensafhankelijke huurverhoging geldt. Dit was bovenmatig en daarmee onrechtmatig, aldus het CBP. De Belastingdienst nam naar aanleiding van het onderzoek van het CBP maatregelen om de privacy van huurders beter te waarborgen en ervoor te zorgen dat verhuurders niet zonder noodzaak inkomensgegevens opvragen.

Het resultaat daarvan is dat er 750.000 minder woningen – en daarmee huurders – in het bestand van de Belastingdienst terecht zijn gekomen. Ook krijgen huishoudens bericht van de Belastingdienst als hun verhuurder voor hun woonadres een indicatie over alle gezamenlijke inkomensgegevens in een huishouden heeft opgevraagd. In 2014 concludeerde het CBP dan ook dat de Belastingdienst niet langer de wet overtreedt bij de uitvoering van de inkomensafhankelijke huurverhoging.

Overeenkomst CBP en Agentschap BPR

Op 6 januari 2014 is de Wet basisregistratie personen (BRP) ingegaan. De BRP is de opvolger van de gemeentelijke basisadministratie (GBA). Het CBP houdt toezicht op de naleving van de Wet BRP. Op 19 september 2014 hebben het CBP en het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) een samenwerkingsovereenkomst gesloten. Deze overeenkomst heeft als doel efficiënt en effectief toezicht op de gemeentelijke zelfevaluatie basisregistratie persoonsgegevens (BRP).

Alle gemeenten voeren jaarlijks een onderzoek uit naar de inrichting, werking en beveiliging van de BRP. Daarnaast onderzoeken zij de verwerking van de gegevens in de BRP. In de overeenkomst tussen het CBP en het Agentschap BPR zijn concrete afspraken gemaakt over de rol en werkwijze van beide partijen als gemeenten hun verplichtingen bij de zelfevaluatie niet (tijdig) nakomen. Zo is onder meer afgesproken dat het Agentschap BPR het CBP informeert als het situaties signaleert die mogelijk in strijd zijn met de Wet BRP of die op een andere manier het toezichtgebied van het CBP raken.

Geslacht	Man
Leeftijd	52 jaar
Woonplaats	Rotterdam

- heeft kinderen
- houdt van voetbal
- bezoekt vaak nieuwssites
- luistert veel muziek online

VOLDOET AAN PROFIEL

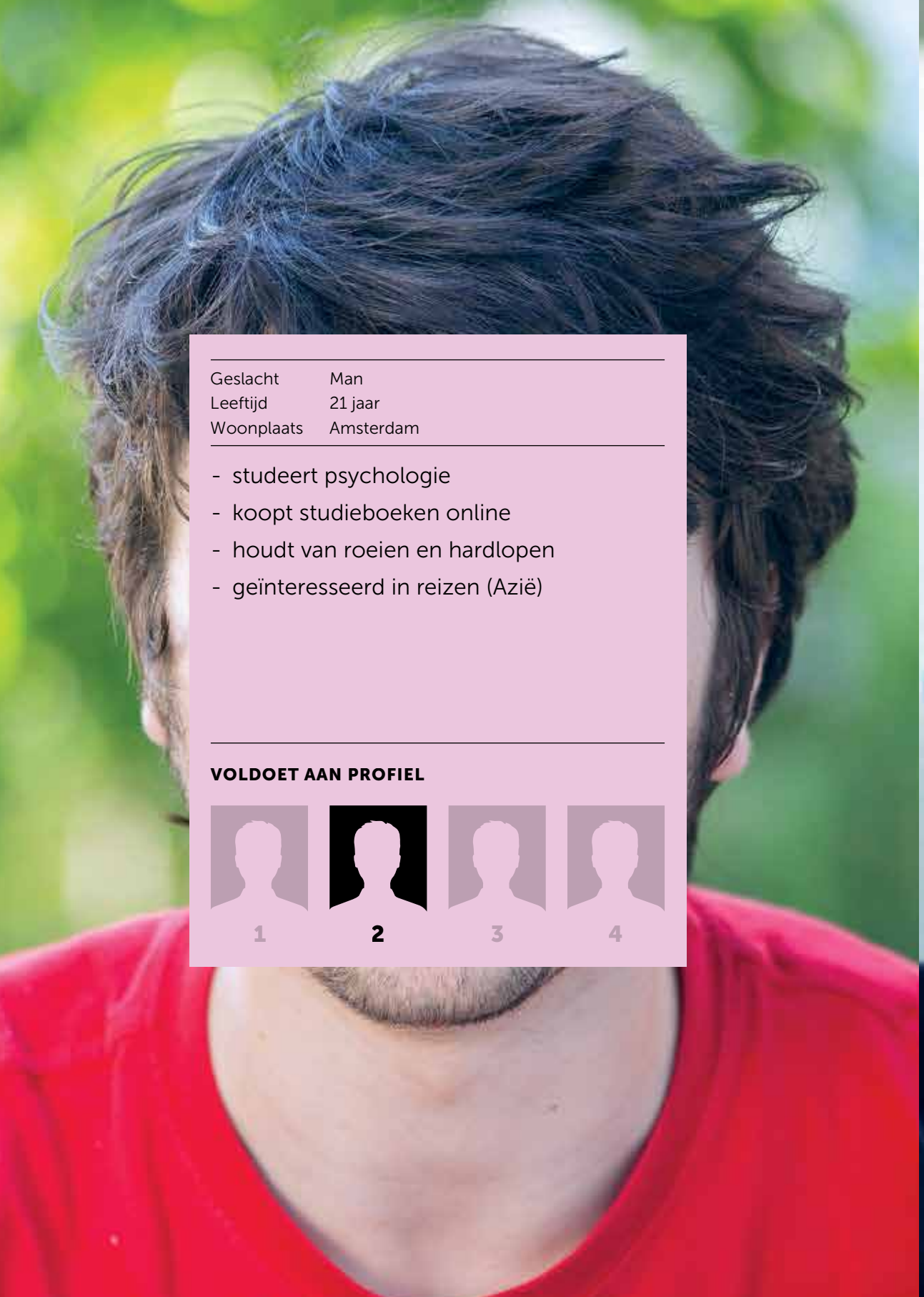
1 2 3 4

Geslacht	Vrouw
Leeftijd	51 jaar
Woonplaats	Groningen

- getrouwd
- geen kinderen
- bovenmodaal inkomen
- geeft aan goede doelen

VOLDOET AAN PROFIEL

1 2 3 **4**



Geslacht	Man
Leeftijd	21 jaar
Woonplaats	Amsterdam

- studeert psychologie
- koopt studieboeken online
- houdt van roeien en hardlopen
- geïnteresseerd in reizen (Azië)

VOLDOET AAN PROFIEL

1 **2** 3 4

Geslacht	Man
Leeftijd	15 jaar
Woonplaats	Helmond

- scholier, technisch profiel
- heeft bijbaantjes
- downloadt veel apps
- geïnteresseerd in games

VOLDOET AAN PROFIEL

1 2 **3** 4

WERK EN INKOMEN

In 2014 had het CBP, net als in 2013, speciale aandacht voor de verwerking van medische gegevens van werknemers. Twee speerpunten van het CBP voor 2014 waren hierin gebundeld: de verwerking van medische gegevens en de verwerking van persoonsgegevens binnen de arbeidsrelatie. Medische gegevens zijn bijzondere persoonsgegevens en niet voor niets gelden voor de verwerking hiervan extra strenge regels. Werknemers zijn in financieel en maatschappelijk opzicht afhankelijk van hun werkgever, wat hen kwetsbaar maakt. Ook staat de sector arbeid de laatste jaren onverminderd in de top drie van sectoren waarover het CBP de meeste vragen en tips krijgt over mogelijke overtredingen van de wet.

Zieke werknemers

Werkgevers mogen een beperkt aantal medische gegevens verwerken van hun zieke werknemers. Het gaat hierbij om gegevens die noodzakelijk zijn voor het vaststellen van de verplichting om loon door te betalen en voor de re-integratie. Zo mag een werkgever onder meer vragen naar de verwachte duur van het verzuim en of er mogelijkheden zijn voor het doen van (andere) werkzaamheden. Het is wettelijk niet toegestaan om te informeren naar de aard en oorzaak van de ziekte. Alleen de arbodienst of bedrijfsarts mag deze medische gegevens verwerken.

Onderzoek uitzendbureaus

Randstad en Adecco, twee van de grootste Nederlandse uitzendbureaus, bleken tijdens onderzoek van het CBP in 2014 op verschillende punten de wet te overtreden bij de verwerking van gegevens van uitzendkrachten. Een van die punten is dat beide uitzendbureaus vroegen naar de aard en oorzaak van de ziekte bij uitzendkrachten die zich ziek meldden en dit registreerden in een systeem.

Daarnaast maakten Randstad en Adecco kopieën van identiteitsbewijzen van mensen die een intakegesprek met het uitzendbureau voerden maar er nog niet voor werkten. Dit mogen de uitzendbureaus echter pas doen op het moment dat iemand voor het uitzendbureau aan de slag gaat en het uitzendbureau feitelijk de werkgever van de uitzendkracht wordt. Adecco verstrekte bovendien in strijd met de wet kopieën van ID-bewijzen aan opdrachtgevers.

In tijden van economische crisis hebben uitzendbureaus te maken met kritische opdrachtgevers. Tegelijkertijd zijn uitzendkrachten afhankelijk van uitzendbureaus. Ook in die spanningsvolle situatie moeten uitzendbureaus de wet strikt naleven. Jacob Kohnstamm, voorzitter van het CBP

Tot slot bleek uit de onderzoeken dat zowel Randstad als Adecco persoonsgegevens van uitzendkrachten langer dan noodzakelijk bewaarden. Randstad bewaarde gegevens soms meer dan 13 jaar, Adecco soms zelfs meer dan 24 jaar. De uitzendbureaus moeten de gegevens verwijderen als deze niet meer noodzakelijk zijn om bijvoorbeeld te voldoen aan fiscale regelgeving.

Randstad en Adecco hebben maatregelen aangekondigd om hun werkwijze aan te passen en hebben deze deels al ingevoerd. Het CBP controleert of de uitzendbureaus de geconstateerde overtredingen hebben beëindigd. Indien nodig zet het CBP handhavende maatregelen in.
→ Lees verder: www.cbpweb.nl/14/11

Onderzoek vervoersbedrijf

Het CBP publiceerde in december 2014 een onderzoek waaruit bleek dat personenvervoersbedrijf Noot Holding BV meer medische gegevens van zieke werknemers verwerkte dan noodzakelijk. Het bedrijf vroeg onder meer naar de aard en oorzaak van de ziekte en naar situationele omstandigheden (ziek kind, sterfgeval). Ook vroeg het in strijd met de wet werknemers om toestemming om hun gezondheidsgegevens op te vragen bij het UWV. Noot Holding BV heeft naar aanleiding van het onderzoek de werkwijze aangepast en de werknemers geïnformeerd over de onrechtmatig verzamelde gegevens. Ook heeft het bedrijf deze gegevens vernietigd. Hiermee zijn de geconstateerde overtredingen beëindigd.

Adviezen over gebruik medische gegevens werknemers

Ook in zijn wetgevingsadviezen heeft het CBP in 2014 gewezen op de strenge voorwaarden voor de verwerking van gegevens over iemands gezondheid. Bijvoorbeeld in het advies over het Tijdelijk besluit experimenten Ziektewet. Dit besluit houdt in dat in plaats van het UWV werkgevers verantwoordelijk worden voor de re-integratie van werknemers in de Ziektewet. Werkgevers mogen echter maar een beperkt aantal, strikt noodzakelijke

medische gegevens verwerken. Het CBP adviseerde om dit in de toelichting op het besluit duidelijk aan te geven.

Quotumwet
Een andere ingrijpende maatregel waarover het CBP adviseerde was het voorstel voor de Quotumwet en de lagere regelgeving hierbij. Deze wet introduceert de verplichting voor werkgevers om minimaal een bepaald percentage werknemers met een arbeidsbeperking in dienst te hebben. Om deze doelstelling te realiseren, neemt het UWV de gegevens van werknemers met een arbeidsbeperking op in een landelijk register.

Het UWV kan een beoordeling uitvoeren of iemand tot de doelgroep behoort. Hierbij verwerkt het UWV medische gegevens.
Het CBP vraagt in zijn advies onder meer aandacht voor de eisen die de Wet bescherming persoonsgegevens stelt aan het verwerken van medische gegevens, de eisen die uit het medisch beroepsgeheim voortvloeien en de plicht om betrokkenen goed te informeren, bijvoorbeeld over het opvragen en verstrekken van hun medische gegevens.

Ook wijst het CBP erop dat toestemming van werknemers om hun medische gegevens te verwerken in deze situatie niet rechtsgeldig is, omdat er een sterke afhankelijkheidsrelatie bestaat tussen hen en het UWV.

Cameratoezicht op het werk

Het CBP krijgt veel vragen en tips over cameratoezicht op de werkvloer, vooral over heimelijke controle van personeel. Cameratoezicht op het werk kan helpen tegen diefstal of beschadiging van eigendommen. Ook kan een werkgever camera's gebruiken om het personeel en de eventuele klanten te beschermen. Werkgevers moeten echter aan een aantal voorwaarden voldoen voordat zij camera's mogen ophangen. De inbreuk op de privacy van de werknemers is immers groot. Verborgen camera's zijn alleen bij grote uitzondering toegestaan.

Toestemming in de arbeidsrelatie

In 2014 was toestemming een van de principes uit de Wet bescherming persoonsgegevens waaraan het CBP speciale aandacht gaf. Organisaties kunnen zich in bepaalde gevallen beroepen op iemands toestemming om zijn persoonsgegevens te verwerken. Maar de wet eist wel dat deze toestemming in vrijheid gegeven moet zijn. Dat houdt in dat iemand geen druk ervaart om toestemming te geven door de omstandigheden of door zijn relatie tot degene die toestemming vraagt. In een arbeidsverhouding is daarom over het algemeen geen sprake van vrije toestemming. Werknemers zijn namelijk in financieel en maatschappelijk opzicht in hoge mate afhankelijk van hun werkgever.

Het CBP heeft in 2014 een aantal keer ingegrepen in zaken die cameratoezicht op het werk betroffen. Zo filmde een ziekenhuis heimelijk de werknemers om te controleren of zij de hygiëneregels naleefden. Het CBP liet het ziekenhuis weten dat het dit ook op andere manieren had kunnen doen. Het ziekenhuis gaf aan dat het een eenmalig incident was en dat de beelden inmiddels vernietigd zijn. In een ander geval kregen filiaalleiders van een keten van tankstations een e-mail van het hoofdkantoor met de oproep om camerabeelden van werknemers te controleren. Bij navraag door het CBP onderkende het bedrijf de wettelijke regel dat camerabeelden alleen mogen worden gecontroleerd bij een aantoonbaar vermoeden van fraude. Het bedrijf heeft vervolgens een nieuwe e-mail aan de filiaalleiders gestuurd waarin dit duidelijk is aangegeven.

Ook een keten van telefoonwinkels controleerde medewerkers op basis van camerabeelden en sprak ze vervolgens aan op hun functioneren. Na contact met het CBP heeft het hoofdkantoor richtlijnen opgesteld voor het gebruik van camerabeelden, waarin duidelijk is aangegeven dat de camerabeelden voor niets anders dan beveiliging gebruikt mogen worden. Tot slot heeft het CBP twee werkgevers die van plan waren om het functioneren van hun medewerkers te controleren met beveiligingscamera's tijdig kunnen stoppen. De werkgevers deden de wettelijk verplichte melding van het cameratoezicht bij het CBP. Nadat het CBP contact met hen had opgenomen, gaven zij aan van hun plan af te zien en de camera's alleen te gebruiken voor beveiligingsdoeleinden.

Sociale zekerheid

Om te kunnen beoordelen of mensen recht hebben op een uitkering, hebben zogeheten uitvoeringinstanties (organisaties die wettelijke regelingen in de sociale zekerheid uitvoeren) als het UWV Werkbedrijf en de gemeentelijke sociale dienst veel persoonsgegevens nodig. Bijvoorbeeld gegevens over het arbeidsverleden van mensen en hun financiële gegevens. Dit zijn gevoelige gegevens waarmee alle organisaties in de keten werk en inkomen zorgvuldig moeten omspringen, onder meer door te zorgen voor adequate beveiliging van de gegevens.

Onderzoek beveiliging Suwinet

Uit onderzoek dat het CBP in december 2014 publiceerde, blijkt dat het UWV en de gemeente 's-Hertogenbosch onvoldoende maatregelen hadden getroffen om te zorgen voor een adequate beveiliging van de persoonsgegevens die met Suwinet worden uitgewisseld. Suwinet is een besloten systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen op het gebied van werk en inkomen.

Via Suwinet kan veel informatie over mensen worden verkregen, zoals gegevens over arbeidsverleden, opleiding, alimentatie, uitkering of boetes.

Het is van groot belang dat deze gegevens goed zijn beschermd en dat alleen de daartoe bevoegde medewerkers erbij kunnen. Zowel bij het UWV als bij de gemeente 's-Hertogenbosch bleken de maatregelen niet toereikend om deze bescherming te kunnen bieden. Veel van de vereiste plannen of procedures waren niet up-to-date, niet compleet of niet afgemaakt. Het UWV (als beheerder van Suwinet) en 's-Hertogenbosch (als afnemer) hadden beide geen beveiligingsplan specifiek gericht op Suwinet. Ook werden beveiligingsincidenten niet centraal geanalyseerd en afgewikkeld.

Het UWV en 's-Hertogenbosch hebben naar aanleiding van het onderzoek laten weten maatregelen te gaan treffen om de persoonsgegevens beter te beschermen. Het CBP controleert of zij de overtredingen hebben beëindigd en kan zo nodig handhavende maatregelen inzetten.
→ Lees verder: www.cbpweb.nl/14/12

Adequate beveiliging van persoonsgegevens bij de overheid is des te belangrijker gezien de decentralisatie: de overheveling van taken van het Rijk en de provincies naar de gemeenten. Jacob Kohnstamm, voorzitter van het CBP

→ Informatie over de decentralisatie per 1 januari 2015 is te vinden in het hoofdstuk 'Overheid' van dit jaarverslag.

Advies fraudeaanpak

In februari 2014 bracht het CBP advies uit over het Besluit SyRI. Systeem Risico Indicatie (SyRI) is een instrument dat verschillende overheidsdatabases koppelt om mogelijke fraudeurs in kaart te brengen. Het gaat hierbij om het voorkomen en bestrijden van onder meer uitkerings- en belastingfraude. Het CBP richtte zich in zijn advies op de wettelijke grondslag voor de gegevensverwerkingen en plaatste kanttekeningen bij de proportionaliteit en subsidiariteit van het voorstel. Het CBP wees onder meer op het principe 'select before you collect'. Dit betekent dat de persoonsgegevens vooraf, volgens objectiveerbare indicatoren, moeten worden geselecteerd. Anders ontstaat het risico dat de bestandskoppelingen te veel personen raken. Ook signaleerde het CBP het risico dat de privacybelangen van betrokkenen meer dan noodzakelijk, en dus buitenproportioneel, worden aangetast door het opstellen van profielen op basis van negatieve kenmerken als schulden, overtredingen en sancties. Verder moet het voornemen om bijzondere persoonsgegevens (zoals strafrechtelijke gegevens) te verwerken nader worden onderbouwd, aldus het CBP.

Screening van personeel

Voor werkgevers is het van belang om betrouwbaar personeel te selecteren en in dienst hebben. Screening is een hulpmiddel om de risico's te beperken. Voor bepaalde functies (bijvoorbeeld in de kinderopvang) is screening zelfs wettelijk verplicht. Screening kan echter zeer ingrijpend zijn voor de privacy van de betrokken werknemers. Daarom is screening alleen onder bepaalde wettelijke voorwaarden toegestaan. De belangrijkste voorwaarden zijn dat de werkgever een legitieme reden (gerechtvaardigd belang) heeft en dat de screening noodzakelijk is.

Advies screening personeel kinderopvang

In september 2014 adviseerde het CBP over een voorstel voor continue screening van werknemers in de kinderopvang. Het kabinet wil een systeem ontwikkelen van continue screening zonder direct van iedereen een nieuwe verklaring omtrent het gedrag (VOG) te vragen.
Op 1 maart 2014 is de eerste fase van de continue screening gestart. Hierbij worden bestaande gegevensbestanden gebruikt, maar die zijn niet altijd volledig en actueel. Daarnaast zijn er van stagiaires, uitzendkrachten, zelfstandigen en vrijwilligers geen gegevensbestanden, waardoor zij buiten de continue screening vallen.

Daarom stelt het kabinet voor om een personenregister te ontwikkelen waarin alle personen die werkzaam zijn in de kinderopvang en het peuterspeelzaalwerk zich moeten inschrijven. Met dit personenregister kunnen alle personen voor wie een VOG-plicht geldt continu worden gescreend. Het personenregister komt in de plaats van de koppeling van bestaande gegevensbestanden. Het CBP heeft in zijn advies onder meer aandacht gevraagd voor de onderbouwing van de noodzaak van de gegevensverwerking, de verschillende verantwoordelijkheden voor de gegevensverwerkingen en de beveiliging van de persoonsgegevens.

GEZONDHEID

Gegevens over iemands gezondheid zijn bijzondere persoonsgegevens. Voor de verwerking hiervan geldt een strenger wettelijk regime. In 2014 was verwerking van medische gegevens, net als in 2013, een van de thematische speerpunten van het CBP. De onderzoeken die het CBP in 2014 afrondde, waren gericht op beveiliging van patiëntgegevens en toestemming voor het verwerken van medische gegevens.

Onderzoek beveiliging ziekenhuis

Het CBP publiceerde eind 2014 een onderzoek naar de beveiliging van patiëntgegevens bij het Groene Hart Ziekenhuis. Het CBP constateerde tijdens het onderzoek dat het netwerk van het ziekenhuis kwetsbaar is voor toegang door onbevoegden. Dit komt omdat op het netwerk medische apparatuur is aangesloten die draait op zogeheten *end-of-life* besturingssoftware, zoals Windows 2000 en Windows XP. Bij dergelijke software worden bekende beveiligingsrisico's niet meer hersteld. Ook kunnen er onbekende beveiligingsrisico's aanwezig zijn, omdat de software niet meer wordt gecontroleerd. Dit vergroot het risico dat medische persoonsgegevens op het netwerk worden gestolen, vernietigd of gewijzigd. Tijdens het onderzoek bleek ook dat het ziekenhuisnetwerk niet was verdeeld in technisch gescheiden onderdelen, waardoor bijvoorbeeld een virus zich makkelijker had kunnen verspreiden tot andere onderdelen van het ziekenhuisnetwerk.

Om de beveiligingsrisico's tegen te gaan is het van belang dat ziekenhuizen die apparatuur met end-of-life besturingssoftware gebruiken deze zo snel mogelijk updaten of vervangen. Zolang dit niet mogelijk is, moeten de ziekenhuizen maatregelen nemen om de beveiligingsrisico's zo veel mogelijk te beperken. Zij moeten bijvoorbeeld kwetsbare apparatuur in een extra beveiligd segment van het netwerk plaatsen. Ook moeten zij beveiligingsrisico's voortdurend in kaart brengen en maatregelen treffen om geconstateerde kwetsbaarheden zo snel mogelijk te verhelpen.

Het Groene Hart Ziekenhuis heeft naar aanleiding van het onderzoek van het CBP maatregelen getroffen om patiëntgegevens beter te beveiligen. Zo monitort het ziekenhuis het netwerkverkeer nu continu om beveiligingsrisico's op te sporen. Ook is het ziekenhuis bezig de kwetsbare apparatuur zo veel mogelijk uit te faseren of in een apart, extra beveiligd segment van het netwerk te plaatsen. Het CBP controleert of het Groene Hart Ziekenhuis de overtredingen heeft beëindigd.

Door verouderde software in ziekenhuizen kunnen medische gegevens op straat komen te liggen. Wilbert Tomesen, vice-voorzitter van het CBP

De Nederlandse Vereniging van Ziekenhuizen (NVZ) liet tijdens het onderzoek weten dat er meer ziekenhuizen zijn die gebruikmaken van end-of-life software op apparaten die aan het netwerk verbonden zijn. De NVZ heeft inmiddels aangegeven met de bij de vereniging aangesloten ziekenhuizen maatregelen te hebben genomen om de kwetsbaarheid van systemen te minimaliseren.

→ Lees verder: www.cbpweb.nl/14/13

Vervolgonderzoeken beveiliging patiëntgegevens

Huisartsen en apothekers bieden steeds vaker de mogelijkheid om herhaalrecepten online aan te vragen en medicijnen te bestellen. De aanvraagformulieren bevatten gevoelige gegevens, zoals de benodigde medicatie. Huisartsen en apothekers zijn ervoor verantwoordelijk dat de persoonsgegevens van hun patiënten op een veilige manier worden verzonden, zodat derden hier geen toegang toe hebben. Daarom moeten zij het verkeer tussen de browser en de server goed beveiligen.

In 2013 constateerde het CBP na een steekproef onder 150 websites dat bijna een derde van de sites een onbeveiligde verbinding had. Hierdoor konden anderen de gevoelige, medische gegevens relatief eenvoudig meelezen, verwijderen of aanpassen. In 2014 deed het CBP een vervolgonderzoek naar de beveiliging van deze websites. Het CBP concludeerde dat alle eerder onderzochte huisartsen en apotheken inmiddels over een beveiligde verbinding beschikken.

Toegang tot patiëntgegevens

Apothekers zijn net als andere zorgverleners gebonden aan het medisch beroepsgeheim. Zij hebben de plicht hun patiëntgegevens vertrouwelijk te behandelen, adequaat te beschermen en te beveiligen. Het CBP deed in 2013 een steekproefonderzoek bij een aantal apotheken naar beveiliging van de toegang tot patiëntgegevens. Hieruit bleek dat vier apothekers onvoldoende maatregelen hadden genomen om te zorgen dat alleen bevoegde personen toegang hadden tot hun patiëntgegevens.

Zo maakten de apothekers alleen gebruik van wachtwoorden om in te loggen en dat is onvoldoende. Voor toegang tot het systeem is zogeheten tweefactorauthenticatie vereist, bijvoorbeeld een chipcard in combinatie met een pincode. In 2014 controleerde het CBP of de geconstateerde overtredingen bij deze vier apothekers inmiddels waren beëindigd. Het CBP stelde vast dat bij de vier apothekers inmiddels alleen kan worden ingelogd met tweefactorauthenticatie en dat zij daardoor op dit punt niet langer de Wet bescherming persoonsgegevens overtreden.

Onderzoek landelijk elektronisch patiëntendossier

Uitwisseling van medische gegevens via een landelijk elektronisch patiëntendossier is alleen toegestaan met voorafgaande, uitdrukkelijke toestemming van de patiënt. In 2014 deed het CBP onderzoek naar deze uitwisseling, die verloopt via het Landelijk Schakelpunt (LSP). Het CBP concludeerde dat via het LSP medische gegevens werden uitgewisseld van mensen zonder dat zij daarvoor aantoonbaar rechtsgeldige toestemming hadden gegeven.

Uit een steekproef van 149 dossiers bleek dat uiteindelijk in acht onderzochte dossiers niet kon worden aangetoond dat sprake was van rechtsgeldige, uitdrukkelijke toestemming. Zo ontbrak in enkele dossiers het bewijs dat iemand rechtsgeldige toestemming had gegeven. Bij andere dossiers bleek vooraf onvoldoende informatie over de uitwisseling aan de patiënt te zijn verstrekt.

Naar aanleiding van het onderzoek nam VZVZ, de verantwoordelijke partij voor de medische gegevensuitwisseling via het LSP, technische en organisatorische maatregelen om ervoor te zorgen dat alleen medische gegevens worden uitgewisseld van mensen die hiervoor uitdrukkelijke toestemming hebben gegeven.

Het CBP heeft er al verschillende malen op gewezen dat een grootschalige uitwisseling van medische gegevens via het LSP alléén kan als mensen daarvoor op basis van heldere informatie hun uitdrukkelijke toestemming hebben gegeven. Zo moet onder meer duidelijk zijn wie welke persoonsgegevens verwerkt, met welk doel dit gebeurt en aan wie deze gegevens worden doorgegeven.

De wet vraagt dat zorgverleners de informatie daadwerkelijk aan de patiënt verstrekken. Het is niet genoeg als zij folders op de balie neerleggen, deze aanbieden in een folderrek of een downloadmogelijkheid op hun website hebben. Artsen moeten hun patiënten goed informeren en daarna om hun uitdrukkelijke toestemming vragen voor de gegevensuitwisseling via het LSP.

Advies Besluit langdurige zorg

In juli 2014 adviseerde het CBP over het Besluit langdurige zorg, een uitwerking van bepalingen in het wetsvoorstel langdurige zorg. In dit besluit wordt de werkwijze van het Centrum indicatiestelling zorg (CIZ) uitgewerkt bij het stellen van een indicatie. Het CIZ toetst dan of iemand aanspraak op zorg heeft vanuit de Wet langdurige zorg. Het CIZ vraagt, als dat nodig is voor een goede indicatiestelling, informatie op bij behandelend artsen. In het besluit is aangegeven dat het CIZ de betrokkene daarvoor direct bij de aanvraag om toestemming vraagt. Geeft iemand geen toestemming, dan kan het CIZ de informatie toch opvragen.

In het advies over het wetsvoorstel langdurige zorg dat het CBP eerder gaf, wees het er al op dat geen sprake is van in vrijheid gegeven toestemming. De aanvrager staat namelijk in een afhankelijke positie ten opzichte van het CIZ. Deze constructie is daarom in strijd met de Wet bescherming persoonsgegevens (Wbp). Het CBP gaf aan dat de Wet langdurige zorg zou moeten voorzien in een verplichting voor behandelend artsen om hun geheimhoudingsplicht te doorbreken, indien en voor zover dat nodig is voor de indicatiestelling. Hoewel de bepalingen in het wetsvoorstel in die zin zijn aangepast, komt de genoemde constructie nu in het Besluit langdurige zorg terug. Deze bepalingen zijn in strijd met de Wbp en met de Wet langdurige zorg zelf, aldus het CBP.

Het CBP drong ook nogmaals aan op een precisering van de (bijzondere) persoonsgegevens die partijen die betrokken zijn bij de uitvoering van de Wet langdurige zorg met elkaar mogen uitwisselen.

→ De verwerking van medische gegevens komt ook aan bod in de hoofdstukken ‘Overheid’ en ‘Werk & uitkering’ van dit jaarverslag

POLITIE EN JUSTITIE

Politie en justitie verwerken persoonsgegevens voor onder meer de opsporing en vervolging van strafbare feiten. Het gaat hierbij ook om bijzondere persoonsgegevens, zoals strafrechtelijke gegevens. Er gelden dan ook strenge wettelijke eisen voor het gebruik ervan. Zo mogen politie en justitie niet meer gegevens verwerken dan noodzakelijk voor het doel en moeten zij de gegevens verwijderen zodra deze niet langer noodzakelijk zijn.

Advies 'hackbevoegdheid' politie

Het CBP bracht in februari 2014 een kritisch advies uit over het conceptwetsvoorstel Computercriminaliteit III. In dit advies besprak het CBP de voorgestelde bevoegdheid voor de politie en opsporingsdiensten tot zogeheten onderzoek in een geautomatiseerd werk, ook wel aangeduid als 'hackbevoegdheid'. Volgens het CBP blijkt uit het voorstel onvoldoende hoe enorm ver deze nieuwe bevoegdheid reikt. Het gaat namelijk om heel veel gegevens van een zeer grote groep mensen.

De 'hackbevoegdheid' maakt onder meer volledige toegang mogelijk tot alle historische – en ook toekomstige – gegevens opgeslagen op randapparatuur en uitgewisseld met alle hiermee verbonden communicatiekanalen. Dit zijn niet alleen gegevens die de verdachte zelf betreffen, maar ook gegevens van iedereen die in documenten voorkomt of met wie er digitaal contact is geweest. Daarmee raakt de toepassing van deze bevoegdheid een grote groep mensen die geen verdachten zijn.

Daarom moet het wetsvoorstel blijk geven van een zorgvuldige afweging tussen het belang van de voorgestelde bevoegdheid en het grondrecht op eerbiediging van de persoonlijke levenssfeer, aldus het CBP. Inbreuken op grondrechten zijn alleen rechtmatig als wordt voldaan aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Uit de toelichting op het wetsvoorstel blijken echter onvoldoende de gronden en overwegingen die de noodzaak van invoering van een zo ingrijpende bevoegdheid rechtvaardigen. Het CBP adviseerde daarom het wetsvoorstel beter te onderbouwen. Ook adviseerde het CBP in een aanvullend advies een *privacy impact assessment* uit te voeren.

→ Lees het advies: www.cbpweb.nl/14/14

Je hoeft geen zware crimineel te zijn om in het Boaregistratie-systeem terecht te komen. Het kan ook gaan om bijvoorbeeld een incidentele plukker van een beschermde bloemsoort of iemand die zwartrijdt in het openbaar vervoer, die wellicht een keer zijn kaartje is vergeten.
Wilbert Tomesen, vice-voorzitter van het CBP

Onderzoek Boaregistratiesysteem

In 2014 rondde het CBP een onderzoek af naar het Boaregistratiesysteem, een informatiesysteem voor buitengewoon opsporingsambtenaren (boa's). Het systeem bevat veel gegevens, waaronder strafrechtelijke gegevens, van mensen die regelgeving voor de bijzondere opsporing op het gebied van lokale orde en veiligheid hebben overtreden, zoals lokale milieuwetgeving of parkeerregelingen. Strafrechtelijke gegevens zijn gevoelige gegevens, waarvoor strenge wettelijke eisen gelden. Zo is er een verbod om deze gegevens te verwerken, tenzij de wet daarop een uitzondering maakt. Het CBP constateerde echter dat de particuliere organisatie NatuurNetwerk BV strafrechtelijke gegevens verwerkte in het systeem, terwijl voor deze organisatie geen uitzondering geldt.

Naar aanleiding van het onderzoek van het CBP is onder regie van het ministerie van Veiligheid en Justitie een publiek samenwerkingsverband opgericht dat wel strafrechtelijke gegevens mag verwerken. Dit is geregeld in een convenant, waarin is vastgelegd dat de gezamenlijke werkgevers en de boa's verantwoordelijk zijn voor de gegevensverwerking. Na ondertekening van dit convenant is de overtreding beëindigd. In het convenant is ook geregeld dat binnen het systeem niet meer persoonsgegevens kunnen worden uitgewisseld dan noodzakelijk voor boa's om hun taak goed te kunnen uitoefenen. Hiermee is een andere overtreding van de wet beëindigd die het CBP tijdens het onderzoek constateerde, namelijk dat boa's gegevens konden raadplegen die waren geregistreerd door opsporingsambtenaren uit een ander, niet-gerelateerd domein.

Onderzoek afloopberichten OM

Het CBP concludeerde tijdens onderzoek dat het Openbaar Ministerie (OM) zogeheten afloopberichten over de afloop van een strafzaak niet tijdig doorstuurde aan het Justitieel Documentatiesysteem (JDS) en de DNA-databank. Hierdoor stonden mensen onterecht in het systeem als verdachte, terwijl zij niet langer verdacht zijn dan wel onherroepelijk zijn vrijgesproken door de rechter.

Het CBP constateerde dat het OM ruim 95% van de afloopberichten over een vrijspraak te laat doorstuurde. Bovendien kwam uit het onderzoek naar voren dat in ongeveer 40% van de door het CBP onderzochte zaken het DNA-profiel van de – achteraf – onterecht verdachte persoon niet direct werd vernietigd. Ook werden de afloopberichten niet snel genoeg verwerkt door de beheerder van het JDS.

Databestanden als het JDS en de DNA-databank moeten tijdig worden bijgewerkt, zodat de gegevens over iemands strafrechtelijk verleden juist en actueel zijn. Dit is belangrijk omdat de gevolgen voor mensen die in het systeem staan zeer groot kunnen zijn. Bijvoorbeeld als een belangrijke beslissing als het weigeren van een VOG-verklaring wordt gebaseerd op onjuiste informatie. Bovendien zijn strafrechtelijke gegevens en DNA-gegevens bijzondere persoonsgegevens en moet hiermee extra zorgvuldig worden omgegaan.

Het OM en de minister van Veiligheid en Justitie hebben inmiddels verbetermaatregelen aangekondigd, maar deze beëindigen de geconstateerde overtredingen vooralsnog niet. Het CBP controleert in hoeverre de overtredingen voortduren en beslist daarna over eventuele handhavende maatregelen.

Advies Wet terugkeer en vreemdelingenbewaring

In juli 2014 adviseerde het CBP over het wetsvoorstel Wet terugkeer en vreemdelingenbewaring. Dit voorstel bevat een nieuw bestuursrechtelijk kader voor vreemdelingenbewaring, waarin de rechten, plichten en omstandigheden in bewaring zijn opgenomen. De overheid kan vreemdelingen die geen recht hebben in Nederland te verblijven het land uitzetten. Voor dit doel beschikt de overheid over verschillende bestuursrechtelijke dwangmiddelen. Hiervan is vreemdelingenbewaring de meest vergaande. Dit middel houdt in dat vreemdelingen in detentie worden gezet, om te voorkomen dat zij zich aan de gedwongen uitzetting onttrekken.

Het CBP adviseerde onder meer over een voorstel tot het inzetten van de bodyscan voor onderzoek aan en in het lichaam van vreemdelingen. Volgens het wetsvoorstel is dit voor de vreemdeling de minst belastende wijze van onderzoek, vergeleken met handmatige visitatie. Het CBP wees erop dat er een wettelijke grondslag voor deze gegevensverwerking nodig is. De gegevens die de scan verzamelt, zijn namelijk bijzondere persoonsgegevens waarvoor in principe een verwerkingsverbod geldt. Het CBP merkte hierbij op dat de grondslag toestemming niet in aanmerking komt. De bodyscan ofwel visitatie (en de bijbehorende verwerking van persoonsgegevens) is namelijk verplicht, dus vreemdelingen hebben geen mogelijkheid om toestemming te weigeren. Ook adviseerde het CBP om de bewaartermijn van zes maanden voor de gegevens die de scan verzamelt nader te onderbouwen.

Advies 'Mijn Zaak' op Rechtspraak.nl

Het CBP adviseerde in januari 2014 over het wetsvoorstel Vereenvoudiging en digitalisering procedures burgerlijk recht en bestuursrecht. Dit voorstel vormt de wettelijk basis voor het webportaal 'Mijn Zaak' op Rechtspraak.nl. Dit portaal heeft als doel procederen toegankelijker te maken voor rechtzoekenden en de rechtspraak aan de eisen van de tijd aan te passen. Het CBP adviseerde onder meer om aandacht te besteden aan het periodiek evalueren van de beveiliging van het systeem. In het informatiesysteem kunnen immers gevoelige persoonsgegevens opgenomen worden.

In diverse artikelen van het wetsvoorstel is bepaald dat beeld- en geluidsopnamen van een zitting gemaakt kunnen worden en dat deze eventueel als vervanging van de schriftelijke versie kunnen dienen. Bij algemene maatregel van bestuur (AmvB) kunnen nadere regels worden gesteld over de toepassing van beeld- en geluidsopnamen. Het CBP adviseerde om in deze AmvB in elk geval aandacht te besteden aan de informatieplicht richting de procesdeelnemers.

Advies centraal register voor gerechtsdeurwaarders

Het CBP adviseerde in januari 2014 over wijziging van de Gerechtsdeurwaarderswet. Deze wijziging houdt onder meer in dat er een centraal register voor gerechtsdeurwaarders wordt ingesteld. In het register wordt iedereen opgenomen die bevoegd is of was om ambtshandelingen te verrichten op grond van de Gerechtsdeurwaarderswet. De doelen van het register zijn onder meer zekerheid te verschaffen over de bevoegdheid van gerechtsdeurwaarders en de kwaliteit en integriteit van het beroep te waarborgen.

Het CBP richtte zich in het advies op de bewaartermijn van de gegevens in dit register. Ook als gerechtsdeurwaarders inmiddels zijn ontslagen en dus niet meer bevoegd zijn, blijven zij in het register staan. De reden hiervoor is dat het altijd nodig kan zijn om achteraf vast te stellen dat een ambtshandeling nietig was. Het CBP wees hierbij op de mogelijkheid dat rechtshandelingen verjaren. Is een rechtshandeling verjaard, dan is het niet meer noodzakelijk om deze persoonsgegevens te bewaren.

Geslacht	Man
Leeftijd	44 jaar
Woonplaats	Maastricht

- gescheiden
- bovenmodaal inkomen
- actief op datingsites
- geïnteresseerd in auto’s

VOLDOET AAN PROFIEL

Geslacht	Man
Leeftijd	7 jaar
Woonplaats	Emmen

- geen broertjes of zusjes
- speelt spelletjes online
- kijkt filmpjes online
- gaat vaak naar de dierentuin

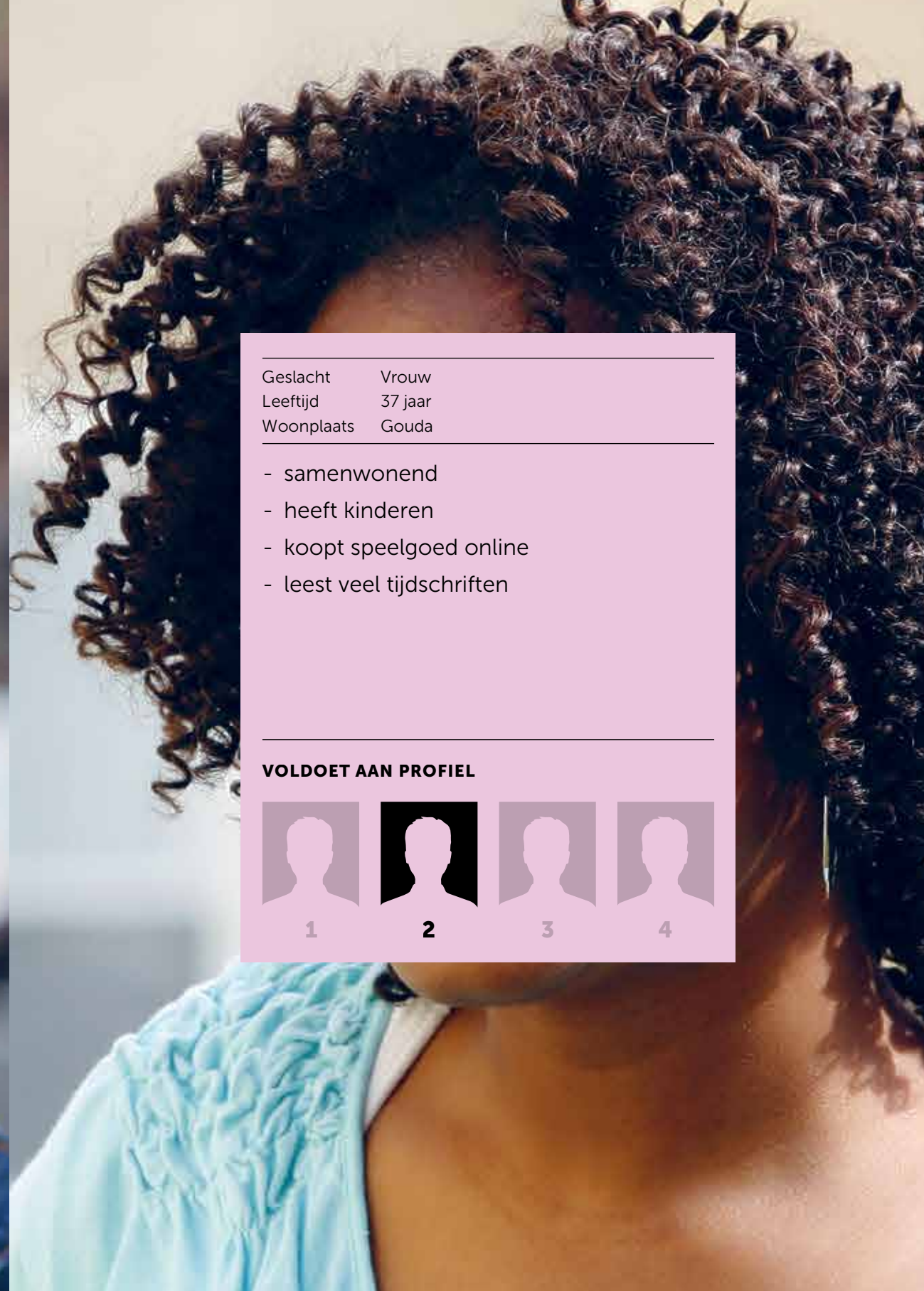
VOLDOET AAN PROFIEL

Geslacht	Vrouw
Leeftijd	41 jaar
Woonplaats	Breda

- gescheiden
- geen kinderen
- heeft een hond
- geïnteresseerd in singlereizen

VOLDOET AAN PROFIEL

1 2 3 **4**



Geslacht	Vrouw
Leeftijd	37 jaar
Woonplaats	Gouda

- samenwonend
- heeft kinderen
- koopt speelgoed online
- leest veel tijdschriften

VOLDOET AAN PROFIEL

1 **2** 3 4

INTERNATIONAAL

Gegevensstromen houden zich niet aan landsgrenzen. Internationale samenwerking tussen privacytoezichthouders is daarom steeds belangrijker. Het CBP heeft dan ook regelmatig overleg met collega-toezichthouders van over de hele wereld, zowel over concrete beleidsonderwerpen als op strategisch niveau. Daarnaast wisselt het CBP met de buitenlandse collega's kennis, ervaring en onderzoeksmethodes uit. In internationaal verband had het CBP in 2014 onder meer speciale aandacht voor big data. Dit is een fenomeen dat samenhangt met profilering, een van de speerpunten van het CBP dat jaar.

Big data

Het verzamelen en gebruiken van persoonsgegevens – online en offline – neemt explosief toe. Overheden gebruiken deze gegevens bijvoorbeeld om belastingfraude tegen te gaan, bedrijven onder meer om mensen gerichter aanbiedingen te doen. Via digitale apparatuur worden voortdurend grote hoeveelheden gegevens vastgelegd over het gedrag van mensen. Het verzamelen en bewaren van zo veel mogelijk informatie in snel groeiende databanken wordt ook wel 'big data' genoemd. Uit deze enorme hoeveelheid data kunnen organisaties vervolgens met behulp van algoritmes allerlei nieuwe verbanden en nieuwe informatie destilleren.

Artikel 29-werkgroep

Eind mei 2014 werd het in opdracht van de president van de Verenigde Staten geschreven rapport 'Big data: seizing opportunities, preserving values' gepresenteerd. In reactie op dit rapport heeft de Artikel 29-werkgroep een brief gestuurd aan de adviseur met de eerste gedachten van de werkgroep over diens aanbevelingen. De werkgroep steunt vooral de aanbeveling in het rapport om de privacyrechten van Amerikaanse en niet-Amerikaanse burgers gelijk te trekken. Daarnaast vindt de Artikel 29-werkgroep het goed om te zien dat in het rapport wordt erkend dat het gebruik van big data soms kan leiden tot discriminatie. Het is daarom belangrijk te waarborgen dat het recht op non-discriminatie niet wordt geschonden.

De Artikel 29-werkgroep is het onafhankelijke advies- en overlegorgaan van Europese privacy-toezichthouders, waaronder het CBP. In maart 2014 legde CBP-voorzitter Jacob Kohnstamm het voorzitterschap van de Artikel 29-werkgroep, dat hij sinds 2010 bekleedde, neer.

Berlijn Telecomgroep

De Berlijn Telecomgroep bracht in september 2014 een *working paper* uit over big data. De Berlijn Telecomgroep is een internationale werkgroep waaraan privacytoezichthouders (waaronder het CBP), wetenschappers en organisaties uit de hele wereld deelnemen.
In dit paper vraagt de werkgroep aandacht voor de privacyrisico's van big data, voornamelijk binnen de telecommunicatie-industrie. De werkgroep ziet onder meer als risico's dat organisaties zo veel mogelijk gegevens verzamelen en bewaren die mogelijk ooit van pas komen, dat zij gegevens voor andere doelen gebruiken en dat zij niet transparant zijn over de gegevensverwerkingen. Ook doet de werkgroep aanbevelingen voor een juist gebruik van big data, zoals hoe organisaties moeten omgaan met het toestemmingsvereiste en hoe zij gegevens kunnen anonimiseren.

Internationale Conferentie

Van 13 tot en met 16 oktober 2014 vond de International Data Protection and Privacy Commissioners Conference plaats (ook wel de Internationale Conferentie genoemd).
Sinds 1979 komen privacytoezichthouders uit de hele wereld jaarlijks bijeen voor overleg. Deze Internationale Conferentie is deels ook toegankelijk voor vertegenwoordigers van het bedrijfsleven, niet-overheidsorganisaties en de wetenschap. De toezichthouders bespreken nieuwe (technologische) ontwikkelingen en delen ervaringen op onderzoeksgebied.
De uitkomsten van de besprekingen worden vastgelegd in resoluties en een slotverklaring. Jacob Kohnstamm legde aan het einde van de Internationale Conferentie 2014 het voorzitterschap van de Executive Committee, dat hij sinds 2011 bekleedde, neer.

In 2015 vindt de Internationale Conferentie plaats in Amsterdam en is het CBP gastheer van de conferentie. Tijdens de conferentie worden de resultaten gepresenteerd van het Privacy Bridges Project dat in april 2014 van start is gegaan, op initiatief van de CBP-voorzitter. Amerikaanse en Europese privacydeskundigen onderzoeken binnen dit project praktische oplossingen om de trans-Atlantische verschillen in de juridische benadering van het recht op bescherming van persoonsgegevens te overbruggen.

Resolutie over big data

In 2014 was een van de resoluties van de Internationale Conferentie gewijd aan big data. CBP-voorzitter Jacob Kohnstamm riep hierbij op tot een internationaal maatschappelijk debat over de privacyrisico's van big data, met als doel te zorgen voor een maatschappelijk verantwoorde toepassing van dit fenomeen. Kohnstamm stelde dat de inzet van big data kan uitmonden in een vorm van 'digitale predestinatie' waarbij mensen gehinderd zullen worden in hun vrije ontwikkeling en vrije keuzes.

Verder riepen de gezamenlijke privacytoezichthouders alle partijen die gebruikmaken van big data op om onder meer de algemene privacyregels in acht te nemen. Zo mogen zij niet meer gegevens verzamelen dan noodzakelijk en moeten zij bovendien privacy impact assessments uitvoeren en privacy by design toepassen bij nieuwe big data-technologieën. De privacytoezichthouders sloten hiermee aan bij eerdere initiatieven om de privacyrisico's van big data te verkleinen, waaronder die van de Berlijn Telecomgroep.

Slotverklaring over 'Internet of Things'

De slotverklaring van de Internationale Conferentie 2014 betrof het fenomeen 'Internet of Things'. Steeds meer apparaten zijn verbonden met het internet en kunnen onderling communiceren. Deze apparaten verzamelen persoonsgegevens en wisselen deze uit. De privacytoezichthouders deden in hun slotverklaring een oproep aan bedrijven die zulke apparaten aanbieden. Zij moeten in hun privacyvoorwaarden duidelijk(er) zijn over welke gegevens zij precies verzamelen en gebruiken, voor welk doel dat gebeurt en hoe lang ze deze gegevens bewaren. Transparantie moet leidend zijn bij het opstellen van de privacy-voorwaarden.

→ Lees de resoluties en slotverklaring: www.cbpweb.nl/14/15

Surveillance

In 2013 ontstond grote commotie door de onthullingen over de NSA-praktijken door klokkenluider Edward Snowden. Amerikaanse en ook Europese inlichtingendiensten bleken met surveillanceprogramma's op grote schaal persoonsgegevens te verzamelen, op te slaan en te doorzoeken. Zowel het CBP als de Artikel 29-werkgroep van Europese privacytoezichthouders hield zich in 2014 actief met dit onderwerp bezig.

Beveiliging bankgegevens

Eind 2013 verschenen diverse berichten dat Amerikaanse veiligheidsdiensten zich mogelijk onrechtmatig toegang zouden hebben verschaft tot de bankgegevens van Europeanen bij de Society for Worldwide Interbank Financial Telecommunication (SWIFT). Dit zou strijdig zijn met de privacyafspraken in het Terrorist Finance and tracking Program II Agreement (TFTP-verdrag) waar SWIFT onder valt. SWIFT regelt het internationale betalingsverkeer voor meer dan 10.000 financiële instellingen uit ongeveer 200 landen.

Het CBP en de CBPL, de Belgische privacytoezichthouder, startten hierop een gezamenlijk onderzoek naar de beveiliging van de computernetwerken van SWIFT. In 2014 publiceerden zij de resultaten. De toezichthouders konden geen overtredingen van de wettelijke beveiligingseisen achterhalen. Ook vonden zij geen aanwijzingen dat derden onrechtmatig toegang hadden tot het financiële berichtenverkeer over Europese burgers.

Gegevens bij Europol

De Joint Supervisory Body (JSB), die onafhankelijk toezicht houdt op de verwerking van persoonsgegevens door Europol en waarin het CBP Nederland vertegenwoordigt, publiceerde in december 2014 de resultaten van een inspectie. Deze inspectie voerde de JSB op verzoek van het Europees Parlement uit en was bedoeld om na te gaan of de gegevens die Europol verwerkt rechtmatig zijn verkregen. Daarbij keek de JSB specifiek of Europol gegevens verwerkt die van geheime diensten afkomstig zijn en/of gegevens die strijdig met de mensenrechten zijn verkregen. Een uitgebreide steekproef van de JSB Europol leverde geen aanwijzingen op dat dit zo is.

Europese privacytoezichthouders

Inlichtingendiensten in de Europese Unie (EU) die met hun surveillanceprogramma's op grote schaal gegevens van en over Europese burgers verzamelen, handelen in strijd met de in Europa geldende grondrechten. Deze conclusie trok de Artikel 29-werkgroep van gezamenlijke Europese privacytoezichthouders in een in april 2014 gepubliceerde opinie. Deze opinie verscheen tegelijkertijd met een belangrijke uitspraak van het Europees Hof van Justitie, waarin de Europese richtlijn over de bewaarplicht voor telecom- en internet-gegevens – die grote hoeveelheden gegevens van en over alle Europeanen toegankelijk maakt voor politie en justitie – ongeldig werd verklaard.

Hoewel de inlichtingendiensten niet onder de reikwijdte van het EU-recht vallen maar onder nationaal recht, stelde de Artikel 29-werkgroep vast dat de algemene grondrechten, zoals vastgelegd in onder meer het Europees Verdrag voor de Rechten van de Mens, wel van toepassing zijn. Het is de plicht van de EU-lidstaten om ervoor te zorgen dat die rechten ook daadwerkelijk worden gerespecteerd. Volgens de werkgroep betekent dit onder meer dat het onrechtmatig is om met geheime surveillanceprogramma's gegevens op te slaan van grote groepen – vaak onverdachte – personen. De opinie bevat een aantal aanbevelingen om de balans tussen privacy en veiligheid te herstellen, zoals meer transparantie over de surveillanceprogramma's en effectief en onafhankelijk toezicht op de veiligheidsdiensten.

Conferentie

Kort na de publicatie van de opinie vond in Parijs het European Data Governance Forum plaats. Tijdens deze conferentie van de Artikel 29-werkgroep stonden surveillance en de reactie daarop door het Europese en internationale bedrijfsleven en maatschappelijk middenveld centraal. Daarnaast is besproken hoe de nieuwe Europese privacywetgeving de rechten van burgers bij surveillance door niet-Europese landen kan helpen beschermen.

Werkdocument
Tot slot nam de werkgroep in december 2014 een werkdocument aan over surveillance van elektronische communicatie voor inlichtingendoeleinden en nationale veiligheid. Dit document bevat de juridische analyse achter de eerdergenoemde opinie en gaat onder meer in op de noodzaak van een goede definitie van het begrip nationale veiligheid.

→ Meer informatie over de bewaarplicht verkeersgegevens en inzage in internet- en telecomgegevens is te vinden in het hoofdstuk 'Internet & telecom' van dit jaarverslag

Verwijderverzoeken zoekmachines

Het Europees Hof van Justitie heeft op 13 mei 2014 geoordeeld dat zoekmachines, zoals Google, verantwoordelijk zijn voor de verwerking van persoonsgegevens via de zoekmachine. Schaden zoekresultaten op iemands naam de privacy van deze persoon, dan kan diegene een verwijderverzoek indienen bij de zoekmachine. De zoekmachine mag het verzoek alleen weigeren als het maatschappelijk belang om de resultaten te tonen zwaarder weegt dan het recht op privacy, bijvoorbeeld als iemand een rol speelt in het publieke leven.

Criteria bemiddeling

Weigert een zoekmachine iemands verwijderverzoek, dan kan diegene om bemiddeling vragen bij een privacytoezichthouder in Europa. In Nederland is dat het CBP. De Europese privacytoezichthouders, verzameld in de Artikel 29-werkgroep, stelden daarom criteria op voor een eenduidige behandeling van deze bemiddelingsverzoeken. Hiertoe voerde de werkgroep onder meer gesprekken met vertegenwoordigers van Google, Microsoft en Yahoo!. De Artikel 29-werkgroep stelde hierin vragen over onderdelen van het verwijderingsproces, zoals de omvang van de toepassing van de rechterlijke uitspraak, het melden van verwijdering aan derden en de redenen voor zoekmachines om verzoeken te weigeren. Het CBP benadrukte daarnaast dat het belangrijk is dat zoekmachines hun eigen criteria openbaar maken en dat zij geanonimiseerde overzichten publiceren van zowel toegekende als afgewezen verzoeken.

Bemiddeling door CBP

Tussen juli en december 2014 hebben ruim dertig personen het CBP om bemiddeling gevraagd nadat hun verwijderverzoek was afgewezen door Google. Over andere zoekmachines ontving het CBP geen signalen. Het CBP heeft in een aantal gevallen Google gevraagd de beslissing te heroverwegen. In alle andere gevallen zag het CBP geen aanleiding om te bemiddelen en volstond het met het doorverwijzen van de betrokkenen naar de rechter. Het merendeel van deze verzoeken was afkomstig van personen met een rol in het publieke leven, zoals (oud-) bestuurders en professionals uit de financiële sector en de zorgsector.

Herziening EU-privacyregelgeving

Op 25 januari 2012 publiceerde de Europese Commissie (EC) voorstellen voor een algemene Europese privacyverordening, die de huidige privacyrichtlijn moet gaan vervangen, en een nieuwe Europese richtlijn voor gegevensverwerking door politie en justitie. Hierna zijn de wetgevingsprocedures in het Europees Parlement (EP) en de Raad van ministers van Justitie en Binnenlandse Zaken van de Europese Unie (Raad) van start gegaan. Het CBP heeft zich ook in 2014 intensief met dit dossier beziggehouden.

Europees Parlement

In oktober 2013 is in het comité voor burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE) van het EP overeenstemming bereikt over de compromis-amendementen op het voorstel van de EC. In maart 2014 is deze overeenstemming met grote meerderheid van stemmen door het voltallige parlement bevestigd. Dit resultaat vormt de basis van het EP in de onderhandelingen tussen EP, EC en Raad over de beide instrumenten (Verordening en Richtlijn), de zogeheten triloog. Voordat de triloog van start kan gaan, moet er eerst overeenstemming zijn in de Raad.

Raad

In de Raad is in 2014, net als in 2013, minder voortgang geboekt dan gehoopt. Hieraan heeft niet alleen politieke verdeeldheid tussen de lidstaten ten grondslag gelegen, maar ook het feit dat zowel de zittingstermijn van het EP als die van de EC in 2014 ten einde kwamen. Desondanks is er op grote onderwerpen, zoals de keuze voor het instrument van een Verordening, in de zomer van 2014 wel politieke consensus bereikt. Ook konden op diverse onderwerpen technisch-inhoudelijke en juridische discussies worden gevoerd, die hebben geleid tot het vaststellen van zogeheten *partial general approaches*.

Een punt van verdeeldheid bleek, net als in 2013, de discussie over onderlinge samenwerking tussen de Europese toezichthouders. De invulling van de door het EC voorgestelde 'éénloketfunctie' (bedrijven die in meerdere EU-lidstaten actief zijn, hoeven zich slechts tot één toezichthouder te wenden), leidde tot veel discussies tussen de lidstaten. Dit gold ook voor de verdeling van bevoegdheden en verplichtingen tussen de toezichthouders bij het onderzoeken van klachten over schendingen van de privacywetgeving.

Europese toezichthouders

De Artikel 29-werkgroep van gezamenlijke Europese privacytoezichthouders heeft ook in 2014 op verschillende manieren bijgedragen aan de discussies over het nieuwe wettelijke kader voor gegevensbescherming in de EU. Zo heeft de werkgroep zowel aan het Griekse voorzitterschap (eerste helft 2014) als aan het Italiaanse voorzitterschap (tweede helft 2014) van de Raad brieven geschreven met nadere inbreng over onderwerpen als de éénloketfunctie.

Toezicht op Europese informatiesystemen

De EU-lidstaten wisselen (persoons)gegevens uit om de grenzen van het Schengengebied te bewaken en justitiële taken uit te voeren, zoals visa afgeven en bepalen welke lidstaat een asielverzoek in behandeling neemt. De bevoegde autoriteiten in de lidstaten, zoals politie en justitie, wisselen deze gegevens uit via verschillende informatiesystemen. Op deze verwerking van persoonsgegevens bestaat onafhankelijk toezicht, waaraan het CBP namens Nederland deelneemt.

Douane Informatiesysteem

Op initiatief van de Supervision Coordination Group (SCG) voor het Douane Informatiesysteem (DIS) zijn twee onderzoeken uitgevoerd in de aangesloten lidstaten. In Nederland heeft het CBP de onderzoeken uitgevoerd. Het DIS wordt gebruikt voor het uitwisselen van douanegegevens tussen autoriteiten van de lidstaten. Bijvoorbeeld gegevens over fraude of drugssmokkel.

Eerst is onderzocht welke nationale autoriteiten per land toegang hebben tot de database van het DIS. Vervolgens is onderzocht of deze autoriteiten volgens de Europese regels ook toegang mogen hebben tot het systeem. Dit bleek over het algemeen op de juiste manier te gebeuren. Wel geeft het onderzoeksrapport nog enkele aanbevelingen aan de lidstaten en aan de Europese anti-fraude autoriteit OLAF om de aanwijzing van daarvoor bevoegde autoriteiten te verbeteren. Er is geen actie vereist voor Nederland op dit punt.

Het tweede onderzoek inventariseerde hoe de privacyrechten van burgers zijn geregeld in de verschillende lidstaten. Is er bijvoorbeeld voldoende informatie beschikbaar over die rechten, zoals het recht van mensen op inzage van hun persoonsgegevens in het DIS? In het rapport dat hierover is uitgebracht, staan aanbevelingen aan de lidstaten om te zorgen voor een effectieve uitoefening van de rechten van betrokkenen. Voor Nederland adviseert het CBP om in de Douaneorganisatie aandacht te besteden aan de informatievoorziening over de rechten van betrokkenen.

Schengen Informatiesysteem II

Op initiatief van de Supervision Coordination Group (SCG) voor het Schengen informatiesysteem II (SIS II) is in de aangesloten lidstaten een onderzoek uitgevoerd naar de uitoefening van de privacyrechten van betrokkenen (in het SIS II opgenomen personen). In Nederland heeft het CBP dit onderzoek uitgevoerd. Het SIS II bevat informatie over signaleringen binnen het Schengengebied, zoals gegevens over gezochte of vermiste personen of over gestolen voertuigen.

Het onderzoeksrapport bevat allereerst een overzicht van de vormen waarin deze rechten in de verschillende lidstaten worden uitgeoefend. Daarnaast beschrijft het rapport de samenwerking tussen de bevoegde autoriteiten van de lidstaten als aan de signalerende lidstaat wordt gevraagd of een betrokkene kennis mag nemen van zijn gegevens. Verder vermeldt het rapport in welke taal de communicatie plaatsvindt en hoe de samenwerking verloopt tussen de privacytoezichthouders. Tot slot is beschreven hoe de lidstaten omgaan met verschillen van inzicht over de handhaving van specifieke signaleringen en het vinden van oplossingen voor eventuele problemen in de samenwerking. Voor de Nederlandse situatie stelt het CBP vast dat er geen verbeteringen noodzakelijk zijn.

ORGANISATIE

In 2014 stegen de productiecijfers van het CBP en werd fors geïnvesteerd in de verdere ontwikkeling van de organisatie. In dat jaar zag onder meer een totaal vernieuwde website het licht en werkte het CBP aan de voorbereidingen op de nieuwe boetebevoegdheid en de algemene meldplicht datalekken.

Het budget van het CBP in 2014 was € 8.185.000. De bezetting bedroeg in dat jaar gemiddeld 74,2 fte, een lichte daling ten opzichte van 2013.

2014 liet een stijging zien van onder meer het aantal onderzoeken, internationale verzoeken om medewerking, voorafgaande onderzoeken naar risicovolle verwerkingen van persoonsgegevens en meldingen van gegevensverwerkingen bij het CBP.

Publieksvoorlichting en perswerk

Ook steeg het aantal vragen en tips dat het CBP ontving. Dit waren er 7.468 in 2014, bijna 9% meer dan in 2013. Hiermee zet de stijgende lijn van de afgelopen jaren door. Veruit de meeste vragen en tips – een derde van het totaal – gingen in 2014 over de sector handel & dienstverlening. Daarna kwamen de sectoren overheid en arbeid. Het aantal perscontacten in 2014 was 653.

→ Alle cijfers over het CBP in 2014 zijn te vinden in de online bijlage bij dit jaarverslag: www.cbpweb.nl/14/2

College en directie

College

Mr. J. Kohnstamm
Voorzitter

Mr. W.B.M. Tomesen
Collegelid, vicevoorzitter

Directie

Drs. P.J.J. Frencken
Directeur

Mr. M.W. McLaggan maakt sinds september 2014 – het einde van haar tweede zittingstermijn – geen deel meer uit van het college.

Externe optredens collegeleden

De onderwerpen privacy en de bescherming van persoonsgegevens konden in 2014 weer rekenen op veel maatschappelijke en publicitaire aandacht. De leden van het college en het MT van het CBP droegen het werk van het CBP in binnen- en buitenland veelvuldig uit en gaven geregeld toelichting op diverse onderwerpen. Het CBP zocht zelf actief contact met de pers en maatschappelijke organisaties. Andersom wisten de media het CBP goed te vinden. Het CBP werd om een reactie gevraagd over uiteenlopende onderwerpen, variërend van de omgang met persoonsgegevens door gemeenten bij hun nieuwe taken tot het verhandelen van klantgegevens door banken en de privacyvoorwaarden van grote internetbedrijven. Ook kreeg het CBP veel uitnodigingen om toespraken te houden op congressen.

In 2014 bestond een belangrijk deel van de werkzaamheden van de collegeleden dan ook uit externe optredens. De collegeleden hielden (keynote)speeches tijdens conferenties, namen deel aan debatten en gaven interviews aan zowel radio en televisie als geschreven pers. Veel van de werkzaamheden hadden een internationaal karakter.

Een selectie uit de externe werkzaamheden van de collegeleden in 2014:

Nationaal

De collegeleden van het CBP gaven in 2014 diverse interviews, vaak over door het CBP gepresenteerde onderzoeken en wetgevingsadviezen. Daarnaast kreeg het CBP geregeld interviewverzoeken van de media om naar aanleiding van actuele gebeurtenissen op het gebied van privacy een reactie te geven.

Profilering

Er was in 2014 veel media-aandacht voor het volgen van mensen op internet en het op basis daarvan indelen in profielen. In januari ontstond veel ophef over winkeliers die gedrag van consumenten in de gaten hielden met wifi-tracking. Het CBP heeft hier in diverse media, waaronder het NOS-journaal en NRC Handelsblad, op gereageerd en aangegeven dat winkels hun klanten in ieder geval hierover moeten informeren. Nog diezelfde week hingen er bij winkels stickers op de deur waarmee klanten werden geïnformeerd. In mei bracht NRC Handelsblad een groot artikel naar aanleiding van het CBP-onderzoek naar het advertentiebedrijf YD (inmiddels: Yieldr). Het CBP concludeerde dat dit bedrijf de privacywetgeving schond door het surf- en klikgedrag van websitebezoekers zonder hun toestemming te volgen en vast te leggen. In december besteedde Kassa een uitzending aan apps voor kinderen. De voorzitter van het CBP vertelde in deze uitzending waar appontwikkelaars zich aan moeten houden.

Big data

Het fenomeen big data was gedurende heel 2014 een onderwerp waarover het CBP zich liet horen. De voorzitter van het CBP hield onder meer toespraken over big data voor privacyprofessionals van over de hele wereld tijdens de internationale privacyconferentie en tijdens het Nationale Denktank Expertforum in oktober 2014. Ook gaf hij interviews waarin hij de essentie van dataprotectie, *surprise minimisation*, afzette tegen de essentie van big data, *surprise maximisation*. Hij waarschuwde voor 'digitale predestinatie'. Volledige individuele ontplooiing en ontwikkeling zijn een illusie op het moment dat op basis van iemands profiel keuzes al vóór hem worden gemaakt in plaats van dóór hem. De CBP-voorzitter riep op tot een maatschappelijk debat over hoe de risico's en ongewenste gevolgen van big data effectief kunnen worden aangepakt en ingedamd. Een debat met als gedroomde uitkomst dat gezamenlijke eisen worden geformuleerd die zorgen voor een maatschappelijk verantwoorde toepassing van dit fenomeen.

Decentralisatie

Het CBP vroeg in 2014 verschillende keren aandacht voor de privacyrisico's van de naderende decentralisatie van taken in het sociaal domein. Zo waarschuwde het CBP de minister van BZK dat gemeenten bij de voorbereidingen op de decentralisatie de bescherming van persoonsgegevens niet uit het oog mochten verliezen. Ook beoordeelde het CBP de uitkomsten van een *privacy impact assessment* voor het jeugddomein. Zowel de voorzitter als de vicevoorzitter gaven verschillende interviews in zowel de landelijke pers, waaronder een groot artikel in NRC Handelsblad, als de vakpers.

Financiële sector

'ING wil bedrijven als Albert Heijn inzicht gaan geven in het betalingsgedrag van hun klanten om hun op maat gesneden advertenties te kunnen aanbieden', schreef het Financieele Dagblad (FD) op 10 maart 2014. Dit artikel bracht dagenlang veel media-aandacht en maatschappelijke onrust teweeg. Het CBP werd overspoeld door persverzoeken. In de woordvoering benadrukte het CBP dat banken vertrouwen verkopen. En dat banken en de wetgever nog een keer goed zouden moeten nadenken over de vraag of banken – gezien hun functie en gezien de afhankelijkheid van klanten/burgers – op een dergelijke manier met persoonsgegevens/big data moeten omgaan. Daags hierna kondigde ING aan het plan voorlopig in de ijskast te zetten. Verder hielden leden van het college en het MT van het CBP gedurende het jaar diverse toespraken over het verwerken van persoonsgegevens en de financiële sector, onder meer op het congres 'Big Data in de financiële sector', tijdens het 'Risk Forum Verzekeraars' en op het privacycongres 'Privacy with a view' over het commercieel gebruik van persoonsgegevens.

Google en Facebook

In december heeft het CBP Google een last onder dwangsom opgelegd die kon oplopen tot 15 miljoen euro. De reden voor deze sanctie was dat de in 2012 aangepaste privacyvoorwaarden van Google in strijd waren met de Wet bescherming persoonsgegevens. Onder meer Radio 1 besteedde hier aandacht aan. CBP-voorzitter Jacob Kohnstamm zei daar: "Google, ga door met het maken van mooie, leuke, nieuwe, handige, vrolijke producten. Maar houd ons niet voor de gek door achter onze rug om onze persoonsgegevens tot geld te maken, zonder dat ons iets gevraagd is." In dezelfde week kondigde het CBP aan onderzoek te gaan doen naar Facebook. Ook hiervoor was veel media-aandacht.

Kohnstamm tien jaar voorzitter CBP

Jacob Kohnstamm was in 2014 tien jaar voorzitter van het CBP. Hij gaf verschillende interviews waarin hij terugblikte op deze tien jaar, onder meer op BNR en in Trouw. Het onderwerp privacy is in vergelijking met 2004 een veelbesproken onderwerp. De beleving van privacy veranderde van 'een plek waar het kwaad zich schuil kon houden' tot een onderwerp waaraan de maatschappij veel waarde hecht. Door technologische ontwikkelingen en ernstige datalekken is de achteloosheid van 'ik heb toch niets te verbergen, dus laat ze maar alles verzamelen' van mensen weg. Mensen beseffen dat hun persoonsgegevens voor veel bedrijven geld waard zijn en dat verlies van hun data vervelende gevolgen kan hebben.

Rondetafelgesprek Tweede Kamer

De voorzitter van het CBP nam in mei 2014 op uitnodiging van de vaste commissie voor Financiën deel aan een rondetafelgesprek in de Tweede Kamer over het gebruik van klantgegevens door banken. De publiciteit over voornemens van ING eerder in het jaar waren aanleiding voor dit gesprek. Jacob Kohnstamm gaf aan dat voor het uitbaten van klantgegevens met het doel om klanten persoonlijke aanbiedingen te doen, mogelijk een wettelijke grondslag is te vinden in de Wet bescherming persoonsgegevens. Hij benadrukte echter dat de banken en de wetgever zich los hiervan zouden moeten afvragen of het maatschappelijk wenselijk en aanvaardbaar is om het commerciële gebruik van individuele bankgegevens onderdeel uit te laten maken van het verdienmodel van banken.

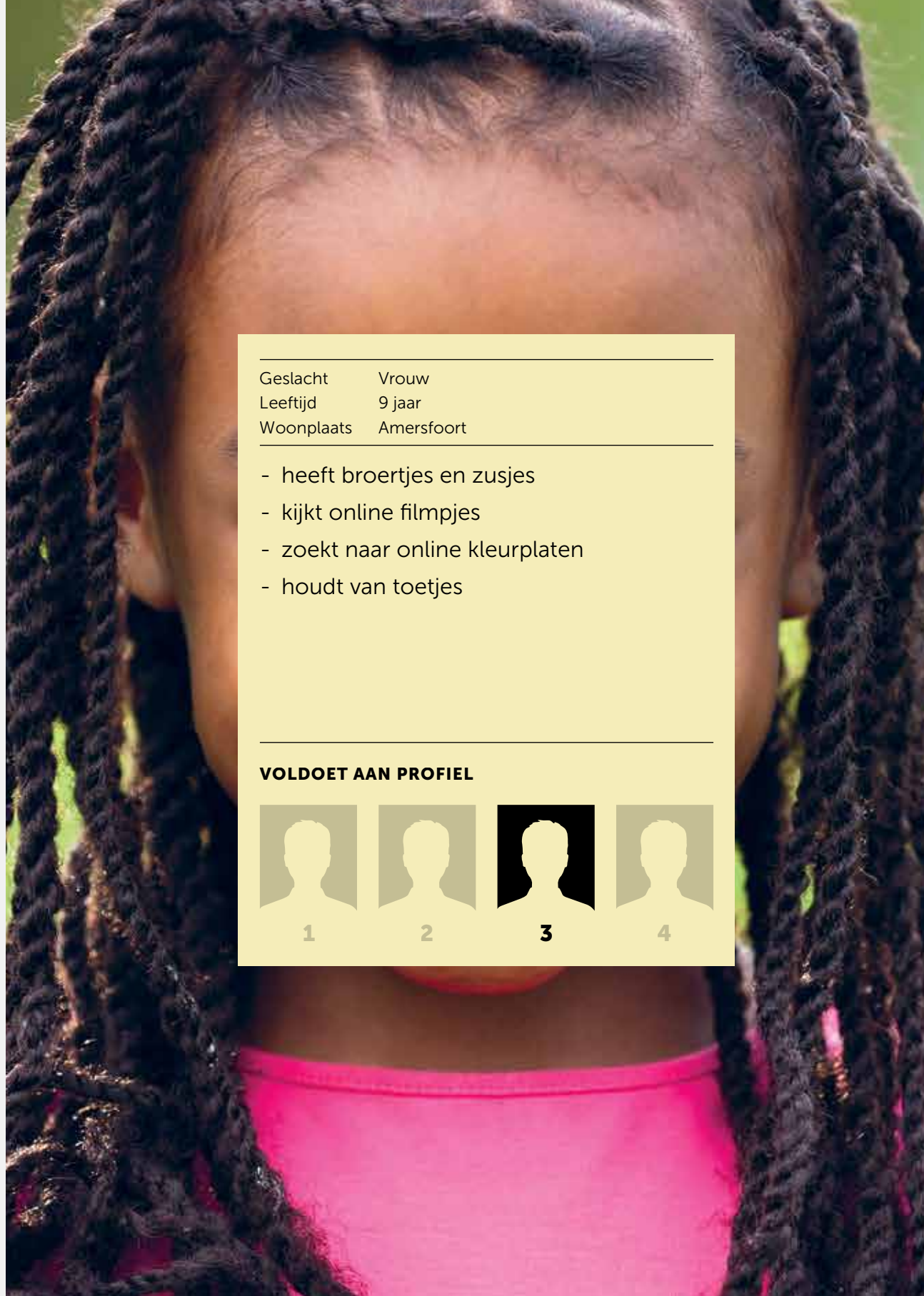
Markttoezichthoudersberaad

De collegeleden namen ook in 2014 actief deel aan het Markttoezichthoudersberaad (MTB), een samenwerkingsverband van Nederlandse toezichthouders. Hoewel elke toezichthouder een specifieke taak vervult, zijn de vraagstukken en ontwikkelingen binnen het toezicht vaak vergelijkbaar. Het MTB heeft als doel kennis en ervaringen uit te wisselen en de krachten te bundelen bij gezamenlijke thema's en vraagstukken. Een dergelijke gezamenlijke aanpak leidt tot effectiever en efficiënter toezicht.

De overige deelnemers aan dit samenwerkingsverband zijn de Autoriteit Consument en Markt (ACM), de Autoriteit Financiële Markten (AFM), De Nederlandsche Bank (DNB), de Kansspelautoriteit (KSa), de Nederlandse Zorgautoriteit (NZa) en het Commissariaat voor de Media (CvdM). Laatstgenoemde trad in 2014 toe. Het MTB organiseerde in 2014 wederom twee seminars voor zijn bestuurders en medewerkers. De onderwerpen waren techniek en big data en het toezien op integriteit binnen organisaties die onder het toezicht vallen.

Internationaal

De collegeleden gaven in 2014 diverse interviews aan nationale en internationale media over onderwerpen met een internationaal karakter, zoals big data, de herziening van de Europese privacyregelgeving en surveillance. Ook namen de collegeleden en andere CBP-werknemers deel aan verschillende Europese en internationale conferenties, workshops en andere bijeenkomsten. Bijvoorbeeld de Europese conferentie van privacytoezichthouders in Straatsburg, de internationale conferentie van privacytoezichthouders in Mauritius en de Global Privacy Summit van de International Association of Privacy Professionals in Washington. In het hoofdstuk 'Internationaal' van dit jaarverslag is meer informatie te vinden over de internationale werkzaamheden van de collegeleden en het CBP.



Colofon

Het CBP in 2014

De profielen in deze uitgave zijn fictief. Elke gelijkenis met bestaande personen berust op toeval.

Ontwerp: T2 Ontwerp, Katwijk
Fotografie: Shutterstock
Fotografie college: Mark Kohn
Druk: Xerox/OBT, Den Haag

COLLEGE BESCHERMING PERSOONSGEGEVENS

BEZOEKADRES	Juliana van Stolberglaan 4-10 2595 CL Den Haag
POSTADRES	Postbus 93374 2509 AJ Den Haag
TELEFOON	070 8888 500
FAX	070 8888 501
TELEFONISCH SPREEKUUR	maandag t/m vrijdag 09.30 - 12.30 uur: 0900 2001 201 (5 ct p/m)
	www.cbpweb.nl