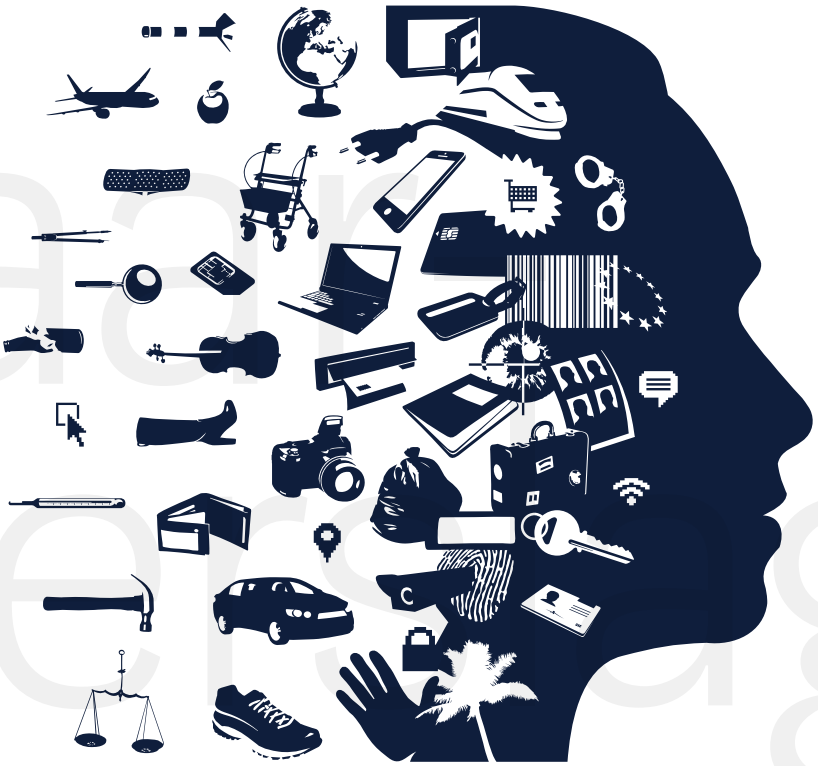
AUTORITEIT
PERSOONSGEGEVENS



Jaarverslag 2015

Jaarverslag 2015

Autoriteit Persoonsgegevens

Bezoekadres
Prins Clauslaan 60
2595 AJ 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)

autoriteitpersoonsgegevens.nl

Jaarverslag 2015

Van College bescherming persoonsgegevens naar Autoriteit Persoonsgegevens

Met ingang van 1 januari 2016 heeft het College bescherming persoonsgegevens een nieuwe naam: Autoriteit Persoonsgegevens. De naamswijziging hangt samen met de uitbreiding van de boetebevoegdheden van de toezichthouder per 1 januari 2016. De nieuwe naam van de privacytoezichthouder past bovendien bij Europese ontwikkelingen, waaronder de verwachte aanvaarding van een nieuwe EU-verordening en richtlijn voor gegevensbescherming in het voorjaar van 2016. In dit jaarverslag zal in verband met de leesbaarheid consequent de nieuwe naam worden gebruikt, ook waar het strikt genomen werkzaamheden van vóór de naamswijziging betrof.

Voorwoord 5

Inleiding 8

Internet & telecom **14**

Overheid **24**

Werk & inkomen **32**

Gezondheid **40**

Politie & justitie **46**

Internationaal **52**

Organisatie 62

Voorwoord

De wereld is bezien vanuit de Autoriteit Persoonsgegevens, zelfs als we maar vijf jaar terugkijken, sluipenderwijs ingrijpend veranderd. De smartphone, internet en de ontwikkelingen van het Internet der Dingen zijn niet meer uit ons dagelijks leven weg te denken. Mensen kunnen er onmogelijk aan ontkomen om dagelijks ontelbare hoeveelheden digitale sporen van persoonsgegevens achter te laten.

Apps, zoekmachines, sociale media: zij worden vaak alleen nog tegen betaling met persoonsgegevens aangeboden. Persoonsgegevens worden zodoende vermarkt. Geld wordt op deze terreinen als ruilmiddel langzaamaan vervangen door persoonsgegevens. Maar waar het uitgeven van geld eenmalig en zichtbaar is, is afgifte van persoonsgegevens veel minder zichtbaar en blijft het hergebruik daarvan buiten ieders zicht of controle. Met behulp van die gegevens – Big Data – worden wij allemaal geprofileerd. Mensen van vlees en bloed worden profielen. Zij worden benaderd en behandeld op grond van onnavolgbare wiskundige formules.

Is adequate bescherming van persoonsgegevens daardoor een illusie geworden, een vorm van dweilen met de kraan open? Of blijft de naleving van het grondrecht op bescherming van persoonsgegevens en de daarmee beoogde persoonlijke vrijheid essentieel voor het vertrouwen in en het functioneren van de samenleving? En als dit zo is, wat moet er dan gebeuren om bescherming van persoonsgegevens hoog op de prioriteitenlijst van publiek, politiek en pers te krijgen?

De Europese privacyverordening en de daarvan afgeleide Europese Richtlijn voor Politie en Justitie die in de zomer van 2016 naar verwachting definitief worden vastgesteld, geven een betekenisvol begin van een antwoord op de laatstgenoemde vraag. De privacyverordening herbevestigt een aantal belangrijke principes zoals deze sinds 1995 in de Europese Unie golden en bevat nieuwe elementen die een robuustere dijk kunnen opwerpen tegen aantasting van het recht op bescherming van persoonsgegevens.

Zo is sprake van versteviging van de rechten van burgers en consumenten en van grotere verantwoordelijkheid voor publieke en private organisaties voor naleving van

de verplichtingen op privacygebied. Accountability, *privacy by design*, *privacy by default* en de verplichting tot het aanstellen van een functionaris voor de gegevensbescherming voor alle publieke organisaties en voor bedrijven waarvoor het verzamelen en verwerken van persoonsgegevens een relevante activiteit is, zijn voorbeelden daarvan.

Daarnaast wordt in de privacyverordening een aantal meer formele zaken geregeld die naleving ten goede zullen komen. De sterke positie van de toezichthouder, toegerust met een stevige boetebevoegdheid, en het openen van de mogelijkheid voor belangenorganisaties om namens burgers in rechte op te treden en de door hen geleden schade vergoed te krijgen, dragen daartoe zeker bij.

Zoals uit dit jaarverslag blijkt, heeft de Autoriteit Persoonsgegevens in 2015 opnieuw bijgedragen aan de naleving van de wettelijke bepalingen die zien op de bescherming van persoonsgegevens. Door vernieuwing van de website waardoor burgers en organisaties sneller en gemakkelijker van hun rechten en plichten kennis kunnen nemen, door optredens in media, in het parlement en in andere bijeenkomsten, door de wetgevingsadviezen, maar bovenal door onderzoek en handhaving en door actief daarover te communiceren.

Uit de onderzoeken in de publieke en de private sector wordt duidelijk dat het merendeel van de aangeschreven organisaties reeds tijdens de looptijd van de onderzoeken bereid is de handelwijze in overeenstemming te brengen met de wettelijke verplichtingen tot de bescherming van persoonsgegevens. De meeste door ons aangesproken verantwoordelijken lieten de verplichtingen vaak onbewust of zonder opzet links liggen. De uit zichzelf gevoelde noodzaak om conform de wet te handelen blijkt echter gering.

Externe prikkels om overtredingen van de Wbp te voorkómen zijn er blijkbaar onvoldoende. Consumenten komen zelden in actie bij overtredingen omdat zij zich daarvan niet bewust zijn en omdat deze meestal niet tot aantoonbare financiële schade leiden. Bovendien is de pakkans klein. Naar schatting van het kabinet staan in Nederland ruim 130.000 organisaties onder toezicht van de Autoriteit Persoonsgegevens omdat zij persoonsgegevens verwerken. Het budget liet in 2015 toe dat wij ongeveer vijftig daarvan onderzochten. Voor een verantwoordelijke die eens een gok wil wagen: zo bezien is de kans dat de toezichthouder aan de deur klopt kleiner dan eens in de duizend jaar!

Omdat echter in onze samenleving mensen steeds vaker worden verleid om met persoonsgegevens te betalen voor allerhande producten en diensten en hergebruik van dat 'geld' even onzichtbaar als onnavolgbaar is, zal aan een aantal maatregelen om bescherming van persoonsgegevens op moderne leest te schoeien niet te ontkomen zijn.

Spoedige inwerkingtreding van de nieuwe Europese privacywetgeving is er daar dus één van. Alle publieke en de meeste private organisaties die persoonsgegevens verzamelen en verwerken, zullen verplicht worden een eigen privacywaakhond (functionaris voor de gegevensbescherming) in dienst te nemen. Door die EU-wetgeving zal daarnaast certificering van organisaties meer in zwang komen en zullen privacykeurmerken ontstaan. De wijze waarop privacy gewaarborgd wordt, is steeds meer deel van de marketingstrategie. Privacy als *selling point*.

Daarnaast is het onvermijdelijk dat het budget van de Autoriteit Persoonsgegevens aanzienlijk wordt verhoogd. Het aantal medewerkers van de toezichthouder neemt al jaren af, terwijl het aantal persoonsgegevens dat van ieder van ons dagelijks wordt verwerkt, juist meer dan exponentieel is toegenomen.

Bescherming van persoonsgegevens is niet voor niets een fundamenteel recht. Omdat zonder dat recht de vrije ontwikkeling en ontplooiing van mensen in het geding is. En omdat zonder effectieve bescherming van dat grondrecht het vertrouwen in elkaar en uiteindelijk in de samenleving op het spel staat.

Jacob Kohnstamm
Voorzitter van de Autoriteit Persoonsgegevens

Inleiding

Persoonsgegevens zijn het 'nieuwe goud', zowel in de private als de publieke sector. Het werkterrein van de Autoriteit Persoonsgegevens is politiek en maatschappelijk volop in ontwikkeling. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving. Het toetsen van de praktijk aan de wet en het maken van afwegingen op het snijvlak van het grondrecht op bescherming van persoonsgegevens en innovatieve diensten en producten is haar dagelijkse werk.

De Autoriteit Persoonsgegevens stelt ieder jaar een aantal thema's vast waarop zij zich in het bijzonder richt. In 2015 waren dat profiling, bijzondere persoonsgegevens, lokale overheden, de arbeidsrelatie en beveiliging. De rode draad daarbij was de manier waarop bedrijven en organisaties mensen informeren over het verwerken van hun persoonsgegevens. Mensen hebben namelijk vaak geen zicht op wat bedrijven en organisaties precies doen met hun gegevens en wat de (soms verstrekkende) gevolgen hiervan zijn. Door de enorme hoeveelheid persoonsgegevens die van vrijwel iedereen in omloop is en de complexiteit van de verwerkingen is dat ook nauwelijks bij te houden. Het is daarom essentieel dat bedrijven en organisaties hierover transparant zijn.

De Autoriteit Persoonsgegevens selecteert de jaarlijkse thema's op basis van haar kennis over ontwikkelingen in technologie en wetgeving en op basis van gesprekken met stakeholders. Ook de vragen en tips over mogelijke overtredingen die de toezichthouder ontvangt, zijn een belangrijke informatiebron. Net als de vele perscontacten en berichten in de media over privacy en gegevensbescherming.

Het werk van de toezichthouder zorgde er in 2015 voor dat adequate gegevensbescherming steeds meer aandacht krijgt. Bovendien beëindigden uiteindelijk de meeste onderzochte bedrijven de geconstateerde overtredingen na optreden van de Autoriteit Persoonsgegevens. Vaak gebeurde dit naar aanleiding van het onderzoek, maar soms was daar dreiging met een sanctie voor nodig.

Hieronder volgt een selectie uit de werkzaamheden van de Autoriteit Persoonsgegevens in 2015.

Profiling

Profiling is het categoriseren van individuen op basis van patronen en (toevallige) correlaties binnen gegevensbestanden. Belangrijke risico's hiervan zijn het gebrek aan transparantie over informatieverzameling en het gevaar van verkeerde beslissingen, bijvoorbeeld bij grenscontroles en in de sociale zekerheid. De onderzoeken in de internet- en telecomsector waarover de Autoriteit Persoonsgegevens in 2015 publiceerde, laten bovendien zien hoe veelzijdig en wijdverspreid profiling is. Websites, sociale media, zoekmachines, apps, smart tv's – het gebruik van profiling is eerder regel dan uitzondering. Mensen worden aldus op basis van profielen bejegend.

De Autoriteit Persoonsgegevens onderstreepte in deze onderzoeken de wettelijke eis dat mensen vooraf moeten worden geïnformeerd over de verwerking van hun persoonsgegevens. In reactie op het onderzoek van de toezichthouder informeren bijvoorbeeld de Nederlandse Publieke Omroep, Ziggo en TP Vision (producent van Philips smart tv's) hun gebruikers nu beter. En de last onder dwangsom die de Autoriteit Persoonsgegevens oplegde aan Google leidde tot een aangescherpt privacybeleid en een publiekscampagne.

Bijzondere persoonsgegevens

Gegevens over iemands godsdienst, ras, politieke gezindheid, gezondheid en strafrechtelijk verleden vallen in de categorie bijzondere persoonsgegevens. Omdat het gaat om gevoelige persoonlijke informatie, is het alleen toegestaan deze gegevens onder strikte voorwaarden te verzamelen, bewaren en gebruiken. In 2015 besteedde de Autoriteit Persoonsgegevens speciale aandacht aan medische en strafrechtelijke gegevens.
Deze focus is gekozen omdat steeds meer mensen met apps en apparaten hun gezondheid en levensstijl monitoren – met alle gevolgen van dien voor de verwerking en beveiliging van gezondheidsgegevens. Daarnaast signaleert de toezichthouder de opmars van publiek-private samenwerkingsverbanden in het veiligheidsdomein, die leidt tot nieuwe gegevensuitwisselingen tussen overheidsorganisaties, bedrijven en burgers.

Uit onderzoek van de Autoriteit Persoonsgegevens uit 2015 blijkt onder meer dat lifestyle apps – vaak zonder dat gebruikers zich ervan bewust zijn – gezondheidsgegevens kunnen verzamelen en analyseren. De toezichthouder wees aanbieders van de software op de noodzaak om hiervoor extra privacybeschermende maatregelen te nemen, waaronder duidelijke informatie aan de gebruikers. In de context van strafrechtelijke gegevens, zoals in politieregisters, benadrukte de Autoriteit Persoonsgegevens in 2015 het belang van een

proportionaliteits- en subsidiariteitstoets. Zo reageerde de Autoriteit op de Verkenning kaderwet gegevensuitwisseling, waarmee het kabinet enkele knelpunten bij de fraude-aanpak vanuit samenwerkingsverbanden wil wegnemen. De brede grondslag voor gegevensuitwisseling staat echter op gespannen voet met de wettelijke eisen van proportionaliteit en subsidiariteit, aldus de Autoriteit.

Persoonsgegevens bij lokale overheden

Sinds een aantal taken van de rijksoverheid en provincies is overgeheveld naar gemeenten, heeft de lokale overheid nieuwe verantwoordelijkheden op het terrein van jeugdzorg, maatschappelijke ondersteuning, arbeidsparticipatie en zorg voor chronisch zieken en gehandicapten. De Autoriteit Persoonsgegevens vroeg in 2015 op verschillende manieren aandacht voor de privacyrisico's van de decentralisaties in het sociaal domein.

Allereerst maakte de Autoriteit Persoonsgegevens in 2015 het resultaat van een quickscan van de websites van circa vijftig gemeenten bekend. Hieruit bleek dat het op veel websites lastig is om informatie te vinden over gegevensverwerkingen binnen het sociaal domein. De toezichthouder stelde in het onderzoek dat volgde op de quickscan onder meer de vraag in welke mate gemeenten transparant zijn over de verwerking van de persoonsgegevens van hun inwoners.

Verder beoordeelde de Autoriteit Persoonsgegevens gegevensverwerkingen binnen de jeugdzorg. De toezichthouder publiceerde de resultaten van onderzoek bij twee Bureaus Jeugdzorg waarbij de registratie van persoonsgegevens van cliënten niet goed verliep. Daarnaast adviseerde de Autoriteit over de geheimhoudingsplicht binnen de Jeugdwet. In de zogenoemde Veegwet VWS 2015 is het rechtmatig doorbreken van de geheimhoudingsplicht om persoonsgegevens te verstrekken volgens de toezichthouder niet goed geregeld. Aan de Tijdelijke regeling persoonsgegevens op facturen Jeugdwet, die vooruitloopt op een formele wijziging van de Jeugdwet, is op aandringen van de Autoriteit Persoonsgegevens een aantal strikte voorwaarden verbonden.

Persoonsgegevens in de arbeidsrelatie

Camera's die winkelpersoneel in het oog houden. Werkgevers die gegevens over zieke werknemers verzamelen. Uitzendbureaus die het verleden van werkzoekenden natrekken. Voor werknemers en werkzoekenden zijn privacy en gegevensbescherming in de praktijk geen vanzelfsprekendheid. In 2015 vroeg de Autoriteit Persoonsgegevens onder meer aandacht voor de bescherming van medische gegevens in verzuimsystemen en voor de beveiliging van Suwinet.

De Autoriteit Persoonsgegevens stuurde in 2015 een brief aan tientallen beheerders van verzuimsystemen om hen te wijzen op hun verantwoordelijkheid voor de beveiliging van software en applicaties. Eerder onderzoek naar het verzuimsysteem Humannet had uitgewezen dat de beveiliging onvoldoende was. Net als in 2014 onderzocht de Autoriteit Persoonsgegevens in 2015 de beveiliging van Suwinet, het systeem waarmee onder andere gemeenten, het UWV en de Sociale Verzekeringsbank persoonsgegevens uitwisselen op het gebied van werk en inkomen. Voortbouwend op onderzoek naar het UWV en de gemeente 's-Hertogenbosch startte de Autoriteit in 2015 onderzoek naar de werkwijze in andere gemeenten.

Beveiliging van persoonsgegevens

De persoonsgegevens van de gemiddelde Nederlander kunnen zijn opgeslagen in honderden of zelfs wel duizenden databestanden, van zowel bedrijven als overheidsorganisaties. De wet eist dat deze gegevens adequaat worden beveiligd. Bijvoorbeeld om datalekken en misbruik, zoals identiteitsfraude, te voorkomen. Net als in voorgaande jaren deed de Autoriteit Persoonsgegevens in 2015 onderzoek naar overtredingen van de wettelijke eis om persoonsgegevens adequaat te beveiligen.

Zo wees de Autoriteit Persoonsgegevens er in oktober 2015 op dat bij de huidige staat van de beveiligingssituatie niet valt uit te sluiten dat onbevoegden DigiD-inloggegevens van gebruikers achterhalen. Onbevoegden kunnen zo misbruik maken van gevoelige gegevens die toegankelijk zijn met DigiD. De Autoriteit Persoonsgegevens pleitte daarom voor een extra veiligheidsvoorziening voor overheidsinstanties die zijn aangesloten bij DigiD. De Autoriteit bracht tegelijkertijd de resultaten van haar onderzoek bij reclamebureau Digi-D naar buiten, dat de inloggegevens van 8.500 DigiD-gebruikers in handen kreeg. Het reclamebureau heeft naar aanleiding van het onderzoek maatregelen genomen.

Over de grens

In een geglobaliseerde samenleving is internationale samenwerking tussen privacytoezichthouders onmisbaar. Bijvoorbeeld omdat internet grenzeloos is. De Autoriteit Persoonsgegevens werkt dan ook intensief samen met collega-toezichthouders in Europa en daarbuiten. Zo is de Autoriteit Persoonsgegevens een zeer actieve deelnemer aan Europese samenwerkingsverbanden, zoals de Artikel 29-werkgroep, de Berlijn Telecomgroep en de toezichthoudende organen voor onder meer Europol en Eurojust. In 2015 ondertekende de Autoriteit bovendien twee samenwerkingsovereenkomsten.

Binnen deze internationale samenwerkingsverbanden hield de Autoriteit Persoonsgegevens zich in 2015 onder meer bezig met de verwerking van medische gegevens bij

gezondheids-apps, de doorgifte van persoonsgegevens aan de Verenigde Staten en het Europese Passenger Name Record-systeem, dat persoonlijke reisinformatie uit computer-reserveringssystemen opslaat. Daarnaast besteedde de toezichthouder, net als in 2014, veel tijd aan de herziening van de Europese privacyregelgeving. Tot de hoogtepunten uit de internationale activiteiten van de Autoriteit Persoonsgegevens behoort de 'Internationale Conferentie van Toezichthouders voor Gegevensbescherming en Privacy', die in oktober 2015 in Amsterdam plaatsvond. Met ruim zevenhonderd deelnemers uit de hele wereld fungeerde de conferentie als een multidisciplinair platform om ervaringen uit te wisselen, kennis te delen en gezamenlijke plannen te maken. Tijdens de conferentie werden de eindresultaten gepresenteerd van het Privacy Bridges Project met tien voorstellen om de trans-Atlantische verschillen in gegevensbescherming te overbruggen.

Nieuwe bevoegdheid en nieuwe taak

Tot 1 januari 2016 beschikte de Nederlandse privacytoezichthouder over een zeer beperkte bevoegdheid om boetes op te leggen bij overtredingen van de Wet bescherming persoons-gegevens. Zij kon alleen een last onder dwangsom opleggen, waarbij de overtreder eerst een termijn krijgt om de overtredingen te beëindigen. Sinds 1 januari 2016 is de boetebevoegdheid sterk uitgebreid. De Autoriteit Persoonsgegevens kan nu ook boetes opleggen als een over-heidsinstelling of bedrijf persoonsgegevens bijvoorbeeld onzorgvuldig verwerkt, langer bewaart dan noodzakelijk is of onvoldoende beveiligt. De nieuwe boetebevoegdheid zal naar verwachting de naleving van de wet bevorderen door de preventieve werking die ervan uitgaat.

Op 1 januari 2016 is ook de meldplicht datalekken in werking getreden. Alle overheidsorgani-saties en bedrijven die persoonsgegevens verwerken zijn sindsdien verplicht een ernstig datalek direct te melden aan de Autoriteit Persoonsgegevens. In 2015 publiceerde de toezicht-houder beleidsregels die organisaties helpen om te bepalen of er sprake is van een datalek dat zij moeten melden.

> 'De verwachting is dat beveiliging van persoons-gegevens een veel hogere prioriteit krijgt bij de ont-wikkeling van producten en diensten. De meldplicht datalekken is geen doel op zich, maar een middel om te zorgen dat datalekken worden voorkomen'.
>
> Jacob Kohnstamm, voorzitter Autoriteit Persoonsgegevens

Werkwijze

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de Wet bescherming persoonsgegevens en aanverwante wetgeving. Om naleving te bevorderen, gebruikt de Autoriteit een mix van instrumenten op het gebied van toezicht, handhaving en communicatie.

Toezicht

De Autoriteit Persoonsgegevens moet keuzes maken bij het onderzoeken van vermeende overtredingen van de wet. Zij hanteert een aantal criteria om te bepalen of er onderzoek wordt uitgevoerd. Zo doet de Autoriteit onderzoek bij een vermoeden van ernstige en structurele overtredingen die veel mensen treffen, waarbij de toezichthouder vanuit zijn bevoegdheden verschil kan maken en die vallen binnen de thema's die de toezichthouder jaarlijks vaststelt.

Behalve via onderzoek kan de Autoriteit Persoonsgegevens ook optreden door waarschuwingsbrieven te sturen en gesprekken te voeren. Dit gebeurt vooral in gevallen waarbij niet aan bovengenoemde criteria is voldaan. Vaak is zo'n brief of gesprek voldoende om een overtreding te beëindigen. De toezichthouder kan zo nodig alsnog een onderzoek uitvoeren als de overtreding voortduurt of na enige tijd opnieuw begint.

Handhaving

Wanneer de Autoriteit Persoonsgegevens tijdens een onderzoek overtredingen constateert die blijven voortduren, kan zij handhavend optreden. De Autoriteit beschikt over de bevoegdheid om een last onder dwangsom op te leggen. Wetsovertreders krijgen dan een bepaalde periode om de werkwijze aan te passen. Als dit niet gebeurt, moeten zij een dwangsom betalen. Sinds 1 januari 2016 heeft de toezichthouder ook de bevoegdheid een boete op te leggen.

Communicatie

Communicatie is met toezicht en handhaving een belangrijk instrument om regelnaleving te bevorderen. De Autoriteit Persoonsgegevens onderhoudt daarom intensief contact met de media. Daarnaast vinden gesprekken plaats met brancheorganisaties en andere stakeholders en verzorgen de leden van de Autoriteit, leden van het managementteam en medewerkers regelmatig lezingen, presentaties en andere optredens. Ook geeft de Autoriteit voorlichting via een telefonisch spreekuur en biedt zij uitgebreide informatie en handreikingen via de website autoriteitpersoonsgegevens.nl.

Jaarverslag

Het jaarverslag geeft een overzicht van de belangrijkste werkzaamheden van de Autoriteit Persoonsgegevens. Deze editie, die verslag doet van 2015, bevat een bijlage met cijfermatige gegevens die online te vinden is via autoriteitpersoonsgegevens.nl/15/2. De samenvatting '2015 in vogelvlucht' is beschikbaar via autoriteitpersoonsgegevens.nl/15/3.

Profiling van internetgebruikers is een van de thema's waaraan de Autoriteit Persoonsgegevens in 2015 bijzondere aandacht besteedde. De toezichthouder vroeg aandacht voor de privacyrisico's – en voor de noodzaak van adequate gegevensbescherming – rond online profiling. Ook hield de Autoriteit andere privacykwesties in de internet- en telecomsector in het oog. Het werk van de toezichthouder droeg er onder meer aan bij dat de persoonsgegevens van Nederlanders bij het gebruik van zoekmachines, apps, smartphones en digitale televisie beter beschermd zijn.

Internet & telecom

Profiling

Online profiling draait om het verzamelen, combineren en analyseren van digitale (persoons)gegevens met als doel om mensen in te delen in bepaalde categorieën.

Een belangrijke rol bij profiling spelen zogeheten tracking cookies, waarmee bedrijven het surfgedrag van mensen door de tijd heen kunnen volgen. Vervolgens kunnen mensen – vaak zonder dat ze het weten – op basis van hun profiel specifiek benaderd en behandeld worden. Dat kan prettig zijn, bijvoorbeeld bij op maat gemaakte advertenties. Maar privacyrisico's zijn er ook. Internetgebruikers hebben het recht te weten welke gegevens over hen worden verzameld. En vóórdat bedrijven en instellingen persoonsgegevens mogen verwerken, is toestemming nodig van de betrokkenen. De Autoriteit Persoonsgegevens treedt op bij (potentiële) overtredingen van deze regels.

Google

Een aangescherpt privacybeleid en een publiekscampagne over privacybescherming zijn enkele resultaten van de last onder dwangsom die de Autoriteit Persoonsgegevens oplegde aan Google. De Autoriteit Persoonsgegevens constateerde eerder op basis van onderzoek dat Google uiteenlopende persoonsgegevens van internetgebruikers samenbracht, onder meer om gepersonaliseerde advertenties te kunnen maken. Omdat Google internetgebruikers hierover vooraf niet goed informeerde en hun ook geen toestemming vroeg, handelde het bedrijf in strijd met de wet.

Nadat de Autoriteit Persoonsgegevens eind 2014 een last onder dwangsom oplegde die kon oplopen tot 15 miljoen euro, trof Google in 2015 een aantal noodzakelijke maatregelen. Zo verduidelijkte Google de informatie in zijn privacybeleid. Verder vraagt Google gebruikers van een Google-account nu om toestemming voor het combineren van hun persoonsgegevens.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/4

Nederlandse Publieke Omroep

Na onderzoek van de Autoriteit Persoonsgegevens nam de Nederlandse Publieke Omroep (NPO) in 2015 maatregelen om het cookiebeleid in lijn te brengen met de wettelijke eisen. Tracking cookies worden nu alleen geplaatst en verwerkt nadat een websitebezoeker hiervoor ondubbelzinnige toestemming heeft gegeven. Daarnaast verbeterde de NPO de informatie over cookies op de aangesloten websites. Zo is de tekst in de cookiebanner

verduidelijkt en krijgen websitebezoekers betere informatie over de achterliggende advertentienetwerken.

Facebook

De nieuwe privacyvoorwaarden van Facebook, die sinds januari 2015 gelden, geven het bedrijf onder meer het recht om gegevens en foto's van Facebookprofielen te gebruiken voor commerciële doeleinden. De Autoriteit Persoonsgegevens onderzoekt of het privacybeleid van Facebook wel voldoet aan de regels uit de Wet bescherming persoonsgegevens. Het onderzoek richt zich bijvoorbeeld op de vraag of het bedrijf toestemming vraagt voor het gebruik van de persoonsgegevens van de ruim negen miljoen Nederlanders met een Facebookprofiel.

In 2015 startte de Autoriteit Persoonsgegevens het onderzoek naar de privacywaarborgen op Facebook. Zo heeft de toezichthouder Facebook Inc. een last onder dwangsom opgelegd omdat het bedrijf weigerde om een deel van de informatie te verstrekken die de toezichthouder had gevraagd. De informatie was onder meer nodig voor de vaststelling van de bevoegdheid van de Autoriteit Persoonsgegevens en de toepasselijkheid van de Wet bescherming persoonsgegevens. Facebook heeft in reactie op de last onder dwangsom toegezegd de gevraagde informatie te verstrekken, zodat kan worden vastgesteld of de Autoriteit Persoonsgegevens inderdaad de aangewezen partij is om toezicht te houden op de privacyvoorwaarden van het socialemediabedrijf.

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Een school mag foto's van leerlingen niet zomaar online zetten'

'Een moeder belde dat de basisschool van haar kind foto's van leerlingen op een openbare website en Facebookpagina plaatste. Toen ze hierover klaagde bij de directeur, zei hij dat het niet te doen was om bij elke foto eerst aan de ouders toestemming te vragen. Hierop heb ik direct met de school contact opgenomen. De school moet óf toestemming vragen aan de ouders óf ervoor zorgen dat de foto's op de website en Facebookpagina alleen toegankelijk zijn voor een beperkte groep mensen. De school heeft alles nu afgeschermd, zodat niet zomaar iedereen foto's van de kinderen kan bekijken.'

YD

De Autoriteit Persoonsgegevens legde het online advertentiebedrijf YD Display Advertising Benelux BV (YD) in 2015 een last onder dwangsom op. YD heeft inmiddels de verantwoordelijkheid voor de verwerking van persoonsgegevens naar een in het Verenigd Koninkrijk gevestigde vennootschap verplaatst. De Nederlandse Wet bescherming persoonsgegevens (Wbp) is niet van toepassing op de huidige activiteiten van de Engelse vennootschap, die vallen onder het toezicht van de Engelse privacytoezichthouder.

De Autoriteit Persoonsgegevens heeft de privacytoezichthouder van het Verenigd Koninkrijk geïnformeerd over deze zaak. Deze heeft laten weten in verband met de huidige verschillen tussen de Wbp en de in het Verenigd Koninkrijk geldende wetgeving geen mogelijkheid te zien om nadere maatregelen te nemen. Begin 2018 zal naar verwachting de Europese privacyverordening in werking treden. Deze verordening zal rechtstreeks gelden in alle lidstaten van de EU. Hierdoor zal er geen verschil meer zijn in het geldende privacyrecht in de verschillende lidstaten. Op het terrein van de bescherming van persoonsgegevens gelden dan dezelfde rechten en plichten. Bovendien moeten de Europese privacytoezichthouders dan in bepaalde gevallen verplicht samenwerken.

Apps

Naar schatting 86 procent van de tijd die we aan onze mobieltjes besteden, bestaat uit het gebruik van apps. Smartphonegebruikers raadplegen elke maand gemiddeld 27 apps.

De Autoriteit Persoonsgegevens doet regelmatig onderzoek naar de manier waarop aanbieders van apps de persoonlijke informatie van gebruikers verwerken. Bijvoorbeeld als het gaat om de beveiliging van gegevens die via apps worden verzameld. De Wet bescherming persoonsgegevens stelt daarnaast eisen aan de informatie die gebruikers krijgen over de gegevensverwerking via apps en aan de manier waarop hiervoor toestemming wordt gevraagd.

Internationale apps voor kinderen

In 2015 leverde de Autoriteit Persoonsgegevens een bijdrage aan een internationale privacyscan van apps voor kinderen. In totaal 29 verschillende privacytoezichthouders uit de hele wereld namen bijna 1.500 van de populairste apps en websites voor kinderen onder de loep. Bij de scan werd gekeken naar privacyaspecten als de informatie-

verstrekking in de app-store, de verplicht in te vullen persoonsgegevens en het gebruik van advertentienetwerken.

Het gros van de onderzochte apps (67%) verzamelt persoonsgegevens van kinderen. En bijna de helft deelt persoonlijke informatie met derden, zoals reclamemakers. Slechts 31% van de onderzochte apps biedt voldoende mogelijkheden om het verzamelen van persoonlijke informatie te beperken. Bovendien bestaat er een reëel risico dat kinderen via links buiten de veilige online omgeving van de app terechtkomen.

De Autoriteit Persoonsgegevens concludeerde uit haar nationale scan onder meer dat het bij de meeste onderzochte apps niet mogelijk is te beoordelen wat de app precies doet, welke persoonsgegevens ermee worden verwerkt en voor welk doel. De Autoriteit Persoonsgegevens bepleitte daarom onder meer dat ouders in de app-store op een makkelijke manier begrijpelijke informatie kunnen vinden over de verwerking en bescherming van persoonsgegevens van hun kinderen.

Uit de internationale privacyscan zijn ook goede voorbeelden naar voren gekomen van apps die privacybescherming ondersteunen, zoals virtuele online assistenten die voorkomen dat kinderen onbedoeld persoonlijke informatie delen.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/5

WhatsApp

Zo'n 9,5 miljoen Nederlanders gebruikten in 2015 berichtendienst WhatsApp. Maar hoe zit het met de privacy van niet-gebruikers? Uit onderzoek van de Canadese privacytoezichthouder en de Autoriteit Persoonsgegevens bleek eerder dat WhatsApp via de adresboeken van gebruikers toegang kon krijgen tot de mobiele telefoonnummers van niet-gebruikers.

WhatsApp heeft toegelicht dat het technisch niet mogelijk is om te voorkomen dat gebruikers bij het uploaden van telefoonnummers uit hun elektronische adresboek ook de gegevens van niet-gebruikers delen met de berichtendienst. Maar in afstemming met de Autoriteit Persoonsgegevens zorgde WhatsApp wel voor passende beveiligingsmaatregelen. Hierdoor heeft WhatsApp een wettelijke basis gekregen om de gegevens van niet-gebruikers te verwerken.

Snappet

Het is essentieel dat gebruikers van apps duidelijk weten wat er met hun gegevens gebeurt. Zeker als het gaat om een kwetsbare groep zoals kinderen. Uit onderzoek van de Autoriteit Persoonsgegevens bleek dat Snappet, een organisatie die tablets met

ingebouwde apps verhuurt aan bijna duizend basisscholen, gegevens over leerlingen verwerkte in strijd met de Wet bescherming persoonsgegevens. In 2015 heeft Snappet de informatievoorziening aangepast, zodat deelnemende scholen weten wat er met de gegevens van hun leerlingen gebeurt en hierover bewuste keuzes kunnen maken. Daarnaast zijn er beveiligingsmaatregelen genomen om ongeoorloofd gebruik te voorkomen.

→ In het hoofdstuk 'Gezondheid' van dit jaarverslag staat het onderzoek beschreven dat de Autoriteit Persoonsgegevens deed naar de verwerking van gezondheidsgegevens via de Nike+ Running App.

Internet- en telefoongegevens

De websites die we bezoeken, de woorden die we invullen in zoekmachines, de telefoonnummers die we bellen, de berichten die we appen. Internet- en telefoonverkeer is een aantrekkelijke informatiebron voor overheden en bedrijven.

De politie maakt in de opsporingspraktijk veelvuldig gebruik van telecomgegevens. Telecomproviders kunnen hun netwerkbeheer en dienstverlening ermee verbeteren. Tegelijkertijd raakt de verwerking van internet- en telefoongegevens aan onze persoonlijke levenssfeer. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor het verwerken van deze persoonsgegevens. De toezichthouder wijst erop dat ook bij nieuwe wettelijke bevoegdheden op dit terrein altijd rekening moet worden gehouden met de eisen van de Wet bescherming persoonsgegevens.

Wifi-tracking in winkels

Het volgen van mensen in en rond winkels via de wifi-signalen van hun mobiele apparaten. Dat kan met een technologie waarmee winkeliers achterhalen hoeveel mensen langs hun pui lopen, de winkel binnenkomen en verschillende schappen bekijken. De Autoriteit Persoonsgegevens tikte het Nederlandse bedrijf Bluetrace in 2015 op de vingers vanwege overtredingen van de Wet bescherming persoonsgegevens.

Bluetrace verzamelde via wifi-tracking locatiegegevens van winkelbezoekers zonder hen hierover te informeren. Bovendien verzamelde en bewaarde Bluetrace meer gegevens dan noodzakelijk is voor het in kaart brengen van bezoekersaantallen in winkels.

Zo werden ook gegevens van voorbijgangers opgeslagen. En alle informatie werd voor onbeperkte tijd bewaard.

In reactie op het onderzoek heeft Bluetrace aangekondigd de werkwijze aan te passen. Bijvoorbeeld door een maximale opslagtermijn van 48 uur te hanteren en door persoonsgegevens te versleutelen. De Autoriteit Persoonsgegevens controleert of de maatregelen van Bluetrace een einde maken aan alle geconstateerde overtredingen.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/6

Bewaarplicht telecommunicatiegegevens

Het bewaren van de telefoon- en internetgegevens van bijna alle Nederlanders gedurende zes tot twaalf maanden is het uitgangspunt van een wetsvoorstel over de bewaarplicht van telecommunicatiegegevens, dat de minister van Veiligheid en Justitie in 2015 ter advies aan de Autoriteit Persoonsgegevens voorlegde. De toezichthouder oordeelde dat de noodzaak voor de uitvoerige en langdurige gegevensverwerking onvoldoende onderbouwd was.

De door de regering voorgestelde bewaarplicht voor gegevens over telefoon- en internetverkeer is bedoeld om de Telecommunicatiewet en het Wetboek van Strafvordering te wijzigen. Het wetsvoorstel is een reactie op een uitspraak van het Europese Hof van Justitie, dat in 2014 bepaalde dat een algemene bewaarplicht in strijd is met het fundamentele recht op de bescherming van persoonsgegevens. Het wetsvoorstel van de Nederlandse regering beoogt de nationale wetgeving in lijn te brengen met het Europese recht. Het voorstel bevat daartoe onder andere een bepaling dat het Openbaar Ministerie pas telefoon- en internetgegevens kan inzien nadat een rechter-commissaris hiervoor toestemming heeft gegeven. Daarnaast maakt het wetsvoorstel een onderscheid tussen een bewaartermijn van zes en twaalf maanden, afhankelijk van het soort misdrijf waarnaar politie en justitie onderzoek doen.

Volgens de Autoriteit Persoonsgegevens schiet de onderbouwing van de voorgestelde bewaartermijn echter tekort. In het wetsvoorstel wordt voorbijgegaan aan de vraag of er geen andere, minder ingrijpende middelen mogelijk zijn om zware criminaliteit te bestrijden. Bovendien gaat het om veel meer gegevens dan noodzakelijk is voor dit doel. De Autoriteit Persoonsgegevens concludeerde in 2015 dan ook dat de inbreuk op de persoonlijke levenssfeer van feitelijk alle Nederlanders te groot en onevenredig is.

Ook merkte de Autoriteit Persoonsgegevens over het voorgestelde artikel 18.7, tweede lid, van de Telecommunicatiewet op dat niet alleen het Agentschap Telecom toezicht houdt maar ook de Autoriteit Persoonsgegevens. De memorie van toelichting lijkt het toezicht door de Autoriteit echter uit te sluiten.

Data-analyse door telecomaanbieders

Telecomaanbieders kunnen bij hun analyses van het dataverkeer over het mobiele netwerk gedetailleerde informatie over telefoongebruikers verzamelen. De Autoriteit Persoonsgegevens onderzocht eerder bij vier telecomaanbieders of de verwerking van persoonsgegevens bij deze zogenoemde *packet inspection* wel in overeenstemming met de wet gebeurde.

In 2015 constateerde de Autoriteit Persoonsgegevens dat KPN, Tele2, T-Mobile en Vodafone maatregelen hebben getroffen om aan de wettelijke regels te voldoen. Onder andere de bewaartermijnen van klantgegevens en de informatie aan telecomgebruikers zijn aangepast. Daarom heeft de Autoriteit besloten verder niet handhavend op te treden.

Tv-gegevens

Met de komst van digitale televisie is tv-kijken tweerichtingsverkeer geworden: wij kijken tv en de tv-aanbieder kijkt als het ware mee. Op die manier verzamelen de televisiemaatschappijen gegevens over ons kijkgedrag, bijvoorbeeld om ons vervolgens met gerichte reclame te benaderen.

Informatie over het kijkgedrag van consumenten behoort tot de gevoelige gegevens waarop de Wet bescherming persoonsgegevens van toepassing is. De Autoriteit Persoonsgegevens plaatste in 2015 de schijnwerpers op de gegevensverwerkingen bij digitale televisie en smart tv's.

Ziggo

Ziggo, de grootste aanbieder van digitale televisie in Nederland, beschikt over een grote hoeveelheid informatie over het kijkgedrag van abonnees. Daarmee kunnen profielen worden opgesteld en op maat gemaakte aanbiedingen worden gedaan. Op basis van onderzoek constateerde de Autoriteit Persoonsgegevens in 2015 dat Ziggo bij deze activiteiten de Wet bescherming persoonsgegevens heeft overtreden.

Ziggo verzamelde gegevens over het kijkgedrag van abonnees om kijkcijferanalyses te maken. Daarnaast verwerkte het bedrijf gegevens van klanten van *video on demand* om hun persoonlijke aanbiedingen te doen. Bovendien ontdekte de Autoriteit Persoons-

gegevens dat Ziggo zeker één keer gegevens over betaalde sportuitzendingen (*pay per event*) gebruikte voor gerichte direct marketing. Dit alles gebeurde zonder klanten goed te informeren over de dataverwerking en zonder hun hiervoor om toestemming te vragen. Dat is in strijd met de wet.

Al tijdens het onderzoek van de Autoriteit Persoonsgegevens veranderde Ziggo de werkwijze om de privacy van klanten beter te beschermen. Zo worden gegevens over het kijkgedrag voortaan geanonimiseerd verwerkt. Daarnaast vraagt Ziggo tegenwoordig aan tv-kijkers toestemming voor het verwerken van hun gegevens, waarbij het bedrijf duidelijk aangeeft wat er met de informatie gebeurt. Daarmee heeft Ziggo de eerder geconstateerde overtredingen van de Wet bescherming persoonsgegevens beëindigd.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/7

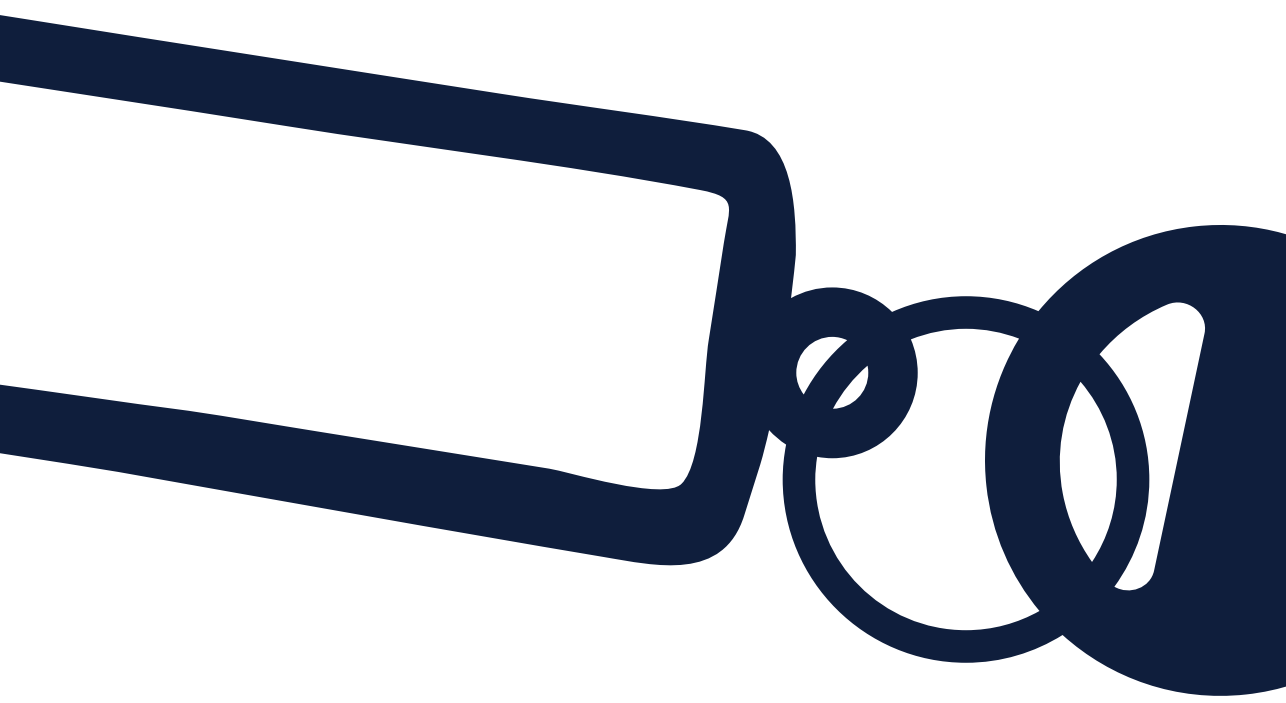
TP Vision

De Autoriteit Persoonsgegevens nam eerder het privacy- en cookiebeleid van TP Vision, producent van Philips' smart tv's, onder de loep. Het onderzoek liet zien dat het bedrijf tv-kijkers onvoldoende en onvolledige informatie gaf over de verwerking van hun persoonsgegevens via de tv's met internetfunctionaliteiten.

> 'Smart tv's bieden fantastische nieuwe mogelijkheden, maar je moet de tv-kijkers wél vertellen dat die diensten gepaard gaan met een grootschalige verwerking van gegevens over hun privésfeer.'
>
> Wilbert Tomesen, vicevoorzitter van de Autoriteit Persoonsgegevens

In 2015 wijzigde TP Vision het privacy- en cookiebeleid voor de onderzochte tv's. Daardoor krijgen gebruikers meer duidelijkheid over het verwerken van persoonsgegevens voor advertentiedoeleinden. Ook de informatie die TP Vision verstrekt als een tv in gebruik wordt genomen is aangepast. Tv-kijkers krijgen nu duidelijk te horen hoe cookies het kijkgedrag bijhouden en hoe toestemming kan worden gegeven (of geweigerd) voor het ontvangen van persoonlijke kijkaanbiedingen.

→ Onderwerpen op het gebied van internet en telecom staan ook in de hoofdstukken 'Overheid' (DigID) en 'Gezondheid' (e-health).



In januari 2015 is een aantal taken van de rijksoverheid en provincies op het gebied van het sociaal domein overgeheveld naar gemeenten. Daarmee heeft de lokale overheid nieuwe verantwoordelijkheden gekregen op het terrein van jeugdzorg, maatschappelijke ondersteuning, arbeidsparticipatie en zorg voor chronisch zieken en gehandicapten. De Autoriteit Persoonsgegevens vraagt al enkele jaren aandacht voor de privacyrisico's van deze decentralisaties. Door de ontwikkelingen in 2015 stond de gegevensuitwisseling in het sociaal domein extra in de schijnwerpers. Daarnaast onderzocht de Autoriteit Persoonsgegevens een aantal andere gegevensverwerkingen binnen de overheid.

Overheid

Gemeenten

Bij de uitvoering van de nieuwe taken van de gemeenten in het sociaal domein wisselen verschillende partijen allerlei persoonsgegevens uit. De Autoriteit Persoonsgegevens onderzoekt hoe gemeenten burgers hierover informeren en hiervoor toestemming vragen.

Ook buiten het sociaal domein horen gemeenten zorgvuldig om te gaan met de persoonsgegevens van hun inwoners. De Autoriteit Persoonsgegevens gaf onder meer advies over de privacygevolgen van screening van woningzoekenden.

Persoonsgegevens in het sociaal domein

In 2015 maakte de Autoriteit Persoonsgegevens een eerste quickscan van de websites van circa vijftig gemeenten. Hieruit bleek dat het op veel websites lastig is om informatie te vinden over gegevensverwerking binnen het sociaal domein. Vervolgens zijn 41 gemeenten aangeschreven met het verzoek inzicht te geven in hun omgang met persoonsgegevens in het sociaal domein. De vragen gaan bijvoorbeeld over de transparantie over de gegevensverwerkingen en over de toestemming die noodzakelijk is om persoonsgegevens van burgers uit te wisselen tussen de verschillende diensten. De uitkomsten van het onderzoek worden in het voorjaar van 2016 verwacht.

Screening van woningzoekenden

In wooncomplexen, straten of buurten met ernstige leefbaarheidsproblemen willen gemeenten voorkomen dat zich nieuwe bewoners met een strafblad of overlastverleden vestigen. Maar screening van woningzoekenden kan een te grote inbreuk maken op de persoonlijke levenssfeer. Dat stelde de Autoriteit Persoonsgegevens in 2015 in haar advies over de wijziging van de Wet bijzondere maatregelen grootstedelijke problematiek. Volgens de toezichthouder was de voorgestelde wijze van screening niet noodzakelijk en niet proportioneel.

Uitgangspunt van het wetsvoorstel dat het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ter advies aan de Autoriteit Persoonsgegevens voorlegde was dat gemeenten over woningzoekenden een verklaring omtrent het gedrag (VOG) aanvragen of onderzoek binnen politieregisters uitvoeren. In 2013 oordeelde de Raad van State in een advies over een vergelijkbaar wetsvoorstel dat de noodzaak en proportionaliteit van dergelijke screenings onvoldoende aangetoond waren.

Volgens de Autoriteit Persoonsgegevens schiet ook de onderbouwing van het nieuwe wetsvoorstel tekort. Het wetsvoorstel geeft bijvoorbeeld geen overtuigend antwoord op de vraag of de inbreuk op de privacy van de betrokkenen te ver gaat. Daarbij merkte de toezichthouder op dat niet alleen de privacy van woningzoekenden maar ook van hun buurtgenoten op het spel staat, omdat de aanwijzing van probleemgebieden stigmatiserend kan werken. Daarnaast pleitte de Autoriteit voor een *privacy impact assessment* van de VOG-procedure, zodat een volledig beeld ontstaat van alle privacyrisico's van de voorgestelde screeningsmethode.

Digitale overheid

Niet alleen de Belastingdienst en gemeenten, maar ook verschillende organisaties die overheidsdiensten uitvoeren (zoals ziekenhuizen, zorgverzekeraars en pensioenfondsen) maken gebruik van DigiD. Dat maakt de privacybescherming en beveiliging van de digitale handtekening voor overheidsdienstverlening belangrijker dan ooit.

De Autoriteit Persoonsgegevens pleitte in 2015 voor een hoger beveiligingsniveau voor DigiD. Daarnaast lette de toezichthouder op de privacywaarborgen bij de ontwikkeling van het landelijke Idensys (voorheen eID Stelsel), dat de toegang regelt tot de onlinediensten van zowel de overheid als het bedrijfsleven.

DigiD

Is de beveiliging van DigiD wel voldoende? De Autoriteit Persoonsgegevens vroeg in 2015 aandacht voor de beveiligingsrisico's rond de digitale handtekening waarmee burgers kunnen inloggen bij overheidsdiensten. Aanleiding was haar onderzoek naar de verwerking van DigiD-gegevens door het Brabantse reclamebureau Digi-D.

Reclamebureau Digi-D bleek van meer dan 8.500 DigiD-accounts zowel de gebruikersnamen als wachtwoorden te hebben opgeslagen nadat burgers onbedoeld hadden geprobeerd in te loggen op de website van het bureau. In reactie op het onderzoek van de Autoriteit Persoonsgegevens heeft het reclamebureau het loggen van de wachtwoorden gestaakt. De beheerder van DigiD, Logius, heeft de DigiD-inloggegevens die opgeslagen waren bij het reclamebureau verwijderd en de betrokken mensen hierover geïnformeerd. Door deze twee maatregelen is een einde gekomen aan de veiligheidsrisico's rond de DigiD-inloggegevens die het reclamebureau had ontvangen.

Naar aanleiding van het onderzoek signaleerde de Autoriteit Persoonsgegevens dat ook in andere situaties misbruik kan worden gemaakt van DigiD-inloggegevens. Het is niet ondenkbaar dat onbevoegden DigiD-inloggegevens achterhalen, bijvoorbeeld met phishing. Op die manier kunnen zij misbruik maken van allerlei gevoelige persoonsgegevens, bijvoorbeeld belastinggegevens of gemeentelijke toeslagen. Daarom is een verplichte extra veiligheidsvoorziening noodzakelijk voor instanties die zijn aangesloten bij DigiD. Denk daarbij aan het gebruik van een verificatiecode via sms bij het inloggen met gebruikersnaam en wachtwoord. De Autoriteit Persoonsgegevens heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties hierop gewezen.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/8

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Online solliciteren bij een gemeente, dat wil je goed beveiligd kunnen doen'

'We kregen een tip van een vrouw dat zij na het uploaden van haar cv en brief deze documenten kon terugvinden op de website van een gemeente. Het is natuurlijk niet de bedoeling dat iedereen deze vertrouwelijke informatie zomaar kan inzien! Daarom meldde ze dit bij de gemeente en die verwijderde – na enig aandringen – haar documenten van de site. Maar toen ze bij wijze van proef nogmaals solliciteerde, verschenen haar documenten opnieuw online. Ik heb gebeld met de gemeente over deze tip. De gemeente heeft het uitgezocht en ervoor gezorgd dat de online sollicitatieprocedure nu goed beveiligd is.'

Idensys

Voor dienstverlening van de overheid gebruiken we DigiD. Maar in het bedrijfsleven geldt nog geen standaard voor online identificatie. Het is de bedoeling dat Idensys (voorheen het eID Stelsel) een landelijk inlogsysteem realiseert waarmee Nederlandse consumenten en ondernemingen toegang kunnen krijgen tot de onlinediensten van zowel de overheid als het bedrijfsleven. In 2015 maakte de Autoriteit Persoonsgegevens een globale analyse van het Introductieplateau eID, de eerste fase van het stelsel.

Volgens de analyse van de Autoriteit Persoonsgegevens is in het Introductieplateau eID, waarin verschillende partijen zijn vertegenwoordigd, onduidelijk wie verantwoordelijk is voor de verwerking van welke persoonsgegevens. Dit staat op gespannen voet met het uitgangs-

punt van de Wet bescherming persoonsgegevens dat er één verantwoordelijke is voor de verwerking van persoonsgegevens. Vanwege de verdeelde verantwoordelijkheden ontbreekt bovendien het overzicht over het gehele stelsel. Hierdoor zijn beveiligingsincidenten moeilijk te ontdekken. Tot slot zijn er juridische beperkingen aan het gebruik van het burgerservicenummer (BSN). Het bedrijfsleven mag het BSN alleen verwerken als daarvoor een wettelijke grondslag bestaat, hetgeen bij het Introductieplateau eID (nog) niet het geval is.

Jeugdzorg

Sinds 1 januari 2015 is de nieuwe Jeugdwet van kracht. Hierdoor zijn gemeenten verantwoordelijk voor de ondersteuning van – en hulp aan – kinderen en hun ouders bij (dreigende) opgroei-, opvoedings- of psychiatrische problemen.

In 2015 onderzocht de Autoriteit Persoonsgegevens de gegevensverwerking bij twee Bureaus Jeugdzorg. Daarnaast publiceerde zij adviezen over de geheimhoudingsplicht binnen de Jeugdwet.

Bureaus Jeugdzorg

In 2015 constateerde de Autoriteit Persoonsgegevens tijdens onderzoek bij Bureaus Jeugdzorg in Noord-Holland en Limburg dat de organisaties onvoldoende maatregelen hadden getroffen om te waarborgen dat gegevensverwerking plaatsvindt in overeenstemming met de Wet bescherming persoonsgegevens. De toezichthouder heeft de situatie behalve bij de twee Bureaus Jeugdzorg ook bij Jeugdzorg Nederland aangekaart.

Uit het onderzoek bleek dat de werkwijzen van de Bureaus Jeugdzorg Noord-Holland en Limburg onvoldoende waren om de kwaliteit van de gegevens in hun dossiers te waarborgen. Dit kwam omdat bij de Bureaus Jeugdzorg onvoldoende was vastgelegd hoe persoonsgegevens worden geregistreerd en hoe onderscheid wordt gemaakt tussen feiten en 'zachte' gegevens (meningen, indrukken en vermoedens). Daarnaast ontbrak een standaardwerkwijze voor onder meer het weergeven van de herkomst van informatie, het actualiseren van informatie en het markeren van onjuistheden.

De Autoriteit Persoonsgegevens benadrukte het grote belang van juiste en nauwkeurige informatie voor de taakuitoefening van de Bureaus Jeugdzorg. Op basis van allerlei persoonsgegevens kunnen ingrijpende beslissingen worden genomen over bijvoorbeeld zorgverlening en

jeugdbeschermingsmaatregelen. De jongeren en hun ouders om wie het gaat, bevinden zich bovendien in een afhankelijke positie ten opzichte van de Bureaus Jeugdzorg.

In maart 2016 concludeerde de Autoriteit Persoonsgegevens dat beide Bureaus Jeugdzorg de overtredingen hebben beëindigd. Zij hebben richtlijnen geïmplementeerd waarin is beschreven hoe de medewerkers de gegevens moeten registreren. Ook is er in de organisatie controle en naleving van deze werkwijze.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/9

Geheimhoudingsplicht jeugdhulpverleners

Veel jeugdhulpverleners worstelen met vragen over de rechtmatigheid van het verstrekken van persoonsgegevens bij de betaling van jeugdhulp. De Autoriteit Persoonsgegevens adviseerde in 2015 over de wet- en regelgeving die in de toekomst de geheimhoudingsplicht van jeugdhulpverleners regelt.

De Autoriteit Persoonsgegevens adviseerde allereerst over de Veegwet VWS 2015. Het wetsvoorstel betreft een aanpassing van onder andere de Jeugdwet. Het is de bedoeling dat daarmee een wettelijke basis ontstaat voor de doorbreking van de geheimhoudingsplicht van jeugdhulpverleners, zodat zij gegevens van hun cliënten aan de gemeente kunnen doorgeven voor de betaling en controle van declaraties. Volgens de Autoriteit bieden de voorgestelde wijzigingen daarvoor onvoldoende basis. Daarnaast ontbreekt een wettelijke verankering van de aard en omvang van de verplichting van jeugdhulpverleners om persoonsgegevens aan gemeenten te verstrekken. Bovendien oordeelt de toezichthouder dat er een uitzondering nodig is voor cliënten in de geestelijke gezondheidszorg die bezwaar hebben tegen gegevensverstrekkingen. De Autoriteit Persoonsgegevens komt tot de conclusie dat het doorbreken van de geheimhoudingsplicht om persoonsgegevens te verstrekken voor de bekostiging van jeugdhulp in de Veegwet VWS 2015 niet goed is geregeld.

In 2015 gaf de Autoriteit Persoonsgegevens vervolgens ook advies over de Tijdelijke regeling persoonsgegevens op facturen Jeugdwet. Deze regeling zorgt – vooruitlopend op de wijziging van de Jeugdwet – dat jeugdhulpaanbieders bij de facturering van jeugdhulp gegevens aan gemeenten kunnen verstrekken. Omdat de regeling noodzakelijk wordt geacht voor de betaling en declaratie van jeugdhulp, heeft de Autoriteit Persoonsgegevens er geen bezwaar tegen gemaakt. Wel heeft de toezichthouder vijf strikte voorwaarden verbonden aan de regeling. Deze gaan onder andere over de mogelijkheid van een opt-out voor de jeugd-ggz en over het minimaliseren van de hoeveelheid gegevens die wordt uitgewisseld.

Scholen

Het gebruik van persoonsgegevens van leerlingen (en hun ouders) door scholen is aan regels gebonden.

De Autoriteit Persoonsgegevens wil de naleving van privacywetgeving door scholen bevorderen. In 2015 stonden onder andere anti-pestprogramma's in de schijnwerpers. Als daarbij gegevens worden gebruikt over bijvoorbeeld het ras, de godsdienst of de gezondheid van leerlingen, gelden op grond van de Wet bescherming persoonsgegevens extra strikte voorwaarden. De Autoriteit Persoonsgegevens vroeg nadrukkelijk aandacht voor deze regels.

Anti-pestprogramma's

Steeds meer scholen maken in de strijd tegen pesten gebruik van speciale anti-pest-programma's. Binnen de programma's is software beschikbaar om pestgedrag onder leerlingen te monitoren en te signaleren. Hierbij worden persoonsgegevens van leerlingen verwerkt. Scholen die met een anti-pestprogramma aan de slag gaan, krijgen dus te maken met de regels van de Wet bescherming persoonsgegevens. Om scholen te helpen, publiceerde de Autoriteit Persoonsgegevens in 2015 een uitgebreide Q&A op haar website.

Wie heeft er toegang tot gegevens van leerlingen die zijn verzameld binnen een anti-pest-programma? Hoe lang mogen gegevens worden bewaard? Welke beveiligingsmaatregelen zijn noodzakelijk? Op deze vragen geeft de Autoriteit Persoonsgegevens antwoorden.
Een bijzonder aandachtspunt betreft de verwerking van gevoelige gegevens, zoals informatie over de afkomst, godsdienst of seksuele voorkeur van leerlingen. Dit is in beginsel verboden, tenzij een uitzondering kan worden gevonden in de Wet bescherming persoonsgegevens.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/10

Toezicht op de verwerking van persoonsgegevens in de arbeidsrelatie behoorde in 2015 tot de speerpunten van de Autoriteit Persoonsgegevens. Werknemers zijn (financieel en maatschappelijk) afhankelijk van hun werkgever; een gebrekkige bescherming van persoonsgegevens maakt hen extra kwetsbaar. Bovendien ontvangt de toezichthouder jaarlijks veel vragen en tips over (potentiële) wetsovertredingen in de arbeidssector. Naar aanleiding hiervan voerde de toezichthouder in 2015 diverse onderzoeken uit. Daarnaast bleef de Autoriteit in gesprek met branche-verenigingen en vakbonden. Dit alles met als doel de naleving van de bescherming van persoonsgegevens op de werkplek te bevorderen.

Werk & inkomen

Zieke werknemers

Wat mag een werkgever weten over de gezondheid en medische behandeling van een zieke werknemer? Op grond van de Wet bescherming persoonsgegevens is die informatie beperkt tot gegevens die noodzakelijk zijn voor salarisbetalingen en re-integratie.

Het is een werkgever wettelijk niet toegestaan om bij een zieke werknemer te informeren naar de aard en oorzaak van de ziekte. Een arbodienst of bedrijfsarts mag dat wel.
Een belangrijk aandachtspunt hierbij is de beveiliging van ICT-systemen die werkgevers en arbodiensten gebruiken om verzuimgegevens te registreren. In 2015 richtte de Autoriteit Persoonsgegevens zich daarom onder meer op de bescherming van medische informatie via verzuimsystemen.

Humannet

Veel Nederlandse werkgevers en arbodiensten maken gebruik van het verzuimsysteem Humannet van ICT-bedrijf VCD voor het verwerken van medische gegevens van werknemers. In 2015 bleek uit onderzoek van de Autoriteit Persoonsgegevens dat de beveiliging van Humannet onvoldoende was.

Medische gegevens over werknemers, zoals die via de verzuimapplicatie Humannet worden verwerkt, behoren tot zogenoemde bijzondere persoonsgegevens. De Wet bescherming persoonsgegevens stelt extra eisen aan de verwerking hiervan. Daarom is het van belang dat aanbieders en beheerders van verzuimsystemen passende beveiligingsmaatregelen nemen om te voorkomen dat onbevoegden toegang krijgen tot deze gegevens. Uit het onderzoek van de Autoriteit Persoonsgegevens naar Humannet bleek dat de medische gegevens in de systemen niet goed waren beveiligd. Voor het inloggen was bijvoorbeeld uitsluitend een gebruikersnaam en wachtwoord nodig, terwijl uit de wet meerfactorauthenticatie volgt. Dat wil zeggen dat een systeem de identiteit van iemand die inlogt op meerdere manieren controleert. De Autoriteit Persoonsgegevens constateerde daarnaast dat VCD de beveiligingsrisico's van de verzuimapplicaties niet periodiek in kaart bracht en het bedrijf onvoldoende aandacht besteedde aan de kwetsbaarheden die uit verschillende audits naar voren kwamen.

Al tijdens het onderzoek introduceerde VCD verschillende vormen van meerfactorauthenticatie. Daarnaast stelde het bedrijf een plan van aanpak op, waaruit bleek dat ook andere overtredingen beëindigd zouden worden. De Autoriteit Persoonsgegevens heeft na

controle geconcludeerd dat Humannet daadwerkelijk een einde heeft gemaakt aan die overtredingen.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/11

Beheerders van verzuimsystemen

Weloverwogen inlogprocedures en regelmatige security scans. Het zijn maatregelen die noodzakelijk zijn om gegevens over zieke werknemers in verzuimsystemen passend te beveiligen. De Autoriteit Persoonsgegevens stuurde in 2015 een brief aan tientallen beheerders van verzuimsystemen om hen te wijzen op hun verantwoordelijkheid voor de beveiliging van software en applicaties.

Met verwijzing naar relevante wettelijke bepalingen, maakte de Autoriteit Persoonsgegevens beheerders van verzuimsystemen attent op concrete technische beveiligingsmaatregelen om privacyovertredingen te voorkomen en beveiligingsrisico's te verminderen. Daarnaast wees de toezichthouder op de eisen rond technische en organisatorische maatregelen uit de Wet bescherming persoonsgegevens. Het gaat dan bijvoorbeeld om autorisatieprocedures, anonimisering van patiënteninformatie en bescherming van inloggegevens.

De Autoriteit Persoonsgegevens benadrukte dat beheerders van verzuimregistraties verantwoordelijk zijn voor informatiebeveiliging en gegevensbescherming in hun systemen. Als zij niet aan de beveiligingsvereisten uit de Wet bescherming persoonsgegevens voldoen, kan de toezichthouder ook jegens hen handhavend optreden.

> Medische gegevens van werknemers zijn bijzondere persoonsgegevens, die wettelijk extra beschermd zijn.

Sociale zekerheid

Instanties zoals sociale diensten en het UWV hebben veel persoonsgegevens nodig om te kunnen beoordelen of mensen recht hebben op een uitkering. Vaak gaat het daarbij om gevoelige gegevens, zoals overzichten van de financiële situatie en het arbeidsverleden.

Adequate beveiliging van persoonlijke informatie van werkzoekenden is nodig in alle onderdelen van de keten van werk en inkomen. Net als in 2014 onderzocht de Autoriteit Persoonsgegevens in 2015 de beveiliging van Suwinet, het systeem waarmee onder meer gemeenten, het UWV en de Sociale Verzekeringsbank persoonsgegevens uitwisselen op het gebied van werk en inkomen.

Beveiliging van Suwinet

Niet meer dan 17 procent van de Nederlandse gemeenten voldoet aan de wettelijke normen voor de beveiliging van Suwinet. Dat constateerde de Inspectie Sociale Zaken en Werkgelegenheid in een onderzoek waarover de Autoriteit Persoonsgegevens in 2015 op de hoogte werd gebracht. Hoewel de gemeenten hiermee een verbetering lieten zien vergeleken met eerdere inspecties, waren de onderzoeksresultaten aanleiding voor de Autoriteit om het eigen onderzoek naar het gemeentelijke gebruik van Suwinet uit te breiden.

In Suwinet worden gevoelige gegevens verwerkt die volgens de Wet bescherming persoonsgegevens extra bescherming verdienen. Het is daarom van groot belang dat de gegevens in Suwinet goed beveiligd en alleen toegankelijk voor bevoegde medewerkers zijn. In 2014 concludeerde de Autoriteit Persoonsgegevens dat het UWV en de gemeente 's-Hertogenbosch de beveiliging niet goed op orde hadden. Begin 2016 concludeerde de Autoriteit dat deze gemeente inmiddels de geconstateerde overtredingen heeft beëindigd.

In Suwinet worden gevoelige gegevens verwerkt, zoals gegevens over iemands financiële situatie en werkverleden.

De Autoriteit startte in 2015 ook een onderzoek naar de werkwijze in vijf andere gemeenten. In reactie op het onderzoek van de Inspectie Sociale Zaken en Werkgelegenheid werden daar nog eens acht gemeenten aan toegevoegd.

De Autoriteit constateerde in januari 2016 dat een deel van de dertien onderzochte gemeenten maatregelen heeft genomen om een einde te maken aan de geconstateerde overtredingen. Twee van de onderzochte gemeenten voldeden inmiddels aan de onderzochte wettelijke vereisten voor de beveiliging van Suwinet. De andere onderzochte gemeenten voldeden bij sluiting van het onderzoek niet aan deze vereisten. De Autoriteit Persoonsgegevens controleert of zij de overtredingen hebben beëindigd en kan zo nodig handhavende maatregelen inzetten. Begin 2016 kon zij in ieder geval over één van de resterende gemeenten concluderen dat deze inmiddels de geconstateerde overtreding heeft beëindigd.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/12

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Je baas mag je niet met camera's in de gaten houden'

'Winkeliers kunnen camera's ophangen om diefstal en geweld door klanten tegen te gaan. Maar wat als je in een winkel werkt en de baas je via de camera's in de gaten houdt? Een man belde ons dat zijn baas dagelijks de camerabeelden bekeek en bijvoorbeeld vroeg waarom iemand zo lang op het toilet was. Die man voelde zich in zijn privacy aangetast en vroeg zich af of dit wel mocht. Mijn antwoord hierop was: nee. Zijn baas mag de beelden alleen gebruiken voor het doel waarvoor ze zijn gemaakt en dus niet om zijn werknemers aan te spreken. Ik heb deze werkgever een brief gestuurd waarin ik schreef dat wat hij deed verboden is en dat hij hiermee moest stoppen.'

Screening van personeel

Werkgevers hebben er belang bij dat hun personeel betrouwbaar en integer is. Screening is daarvoor een veelgebruikt hulpmiddel.

Bij screening verzamelt een werkgever informatie over een sollicitant of werknemer, bijvoorbeeld via eerdere werkgevers of zwarte lijsten. Voor bepaalde functies (bijvoorbeeld in de kinderopvang) is screening wettelijk verplicht. In andere gevallen kan screening een inbreuk maken op de persoonlijke levenssfeer van sollicitanten en werknemers. Daarom is screening alleen onder strikte voorwaarden toegestaan. De Autoriteit Persoonsgegevens controleerde in 2015 de protocollen van twee uitzendbureaus.

Pre-employment screening door uitzendbureaus

Uitzendbureaus krijgen regelmatig te maken met opdrachtgevers die vragen om een pre-employment screening voordat zij een flexkracht inhuren. Bij zo'n screening wordt het (arbeids)verleden van de kandidaat doorgelicht. In veel gevallen komen daarbij strafrechtelijke gegevens en andere gevoelige gegevens aan bod. Organisaties mogen deze zogenoemde bijzondere persoonsgegevens volgens de wet alleen bij uitzondering verwerken. De Autoriteit Persoonsgegevens controleerde in 2015 bij twee grote uitzendbureaus het (privacy)protocol van de pre-employment screenings.

Zowel Randstad als Adecco ontwikkelden in 2015 (privacy)protocollen voor pre-employment screenings die volgens de Autoriteit Persoonsgegevens voldoende waarborgen bevatten voor de bescherming van persoonsgegevens. De toezichthouder keek daarbij vooral naar de mate waarin de uitzendbureaus zich konden beroepen op een gerechtvaardigd belang. Daarnaast bekeek de Autoriteit of de noodzaak van de screening voldoende was onderbouwd, dat wil zeggen of er geen ander, minder ingrijpend middel is om de risico's van onbetrouwbaar personeel te verminderen.

Bij screening van sollicitanten en werknemers komen vaak strafrechtelijke gegevens en andere gevoelige gegevens aan bod.

Bescherming van personeelsgegevens

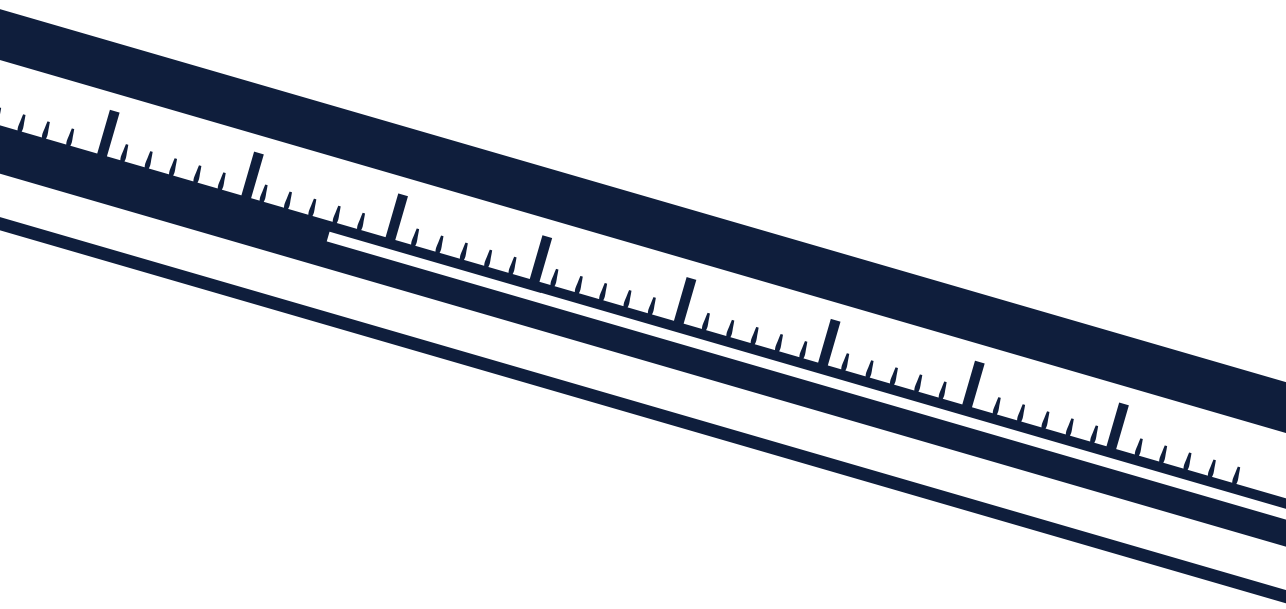
Het recht op bescherming van persoonsgegevens geldt ook op de werkvloer. Dat betekent onder andere dat werkgevers personeelsgegevens niet zomaar aan externe partijen mogen verstrekken.

Het verwerken van personeelsinformatie kan direct raken aan de persoonlijke levenssfeer van werknemers, vooral in combinatie met gevoelige gegevens als foto's. In 2015 deed de Autoriteit Persoonsgegevens onderzoek naar zo'n situatie.

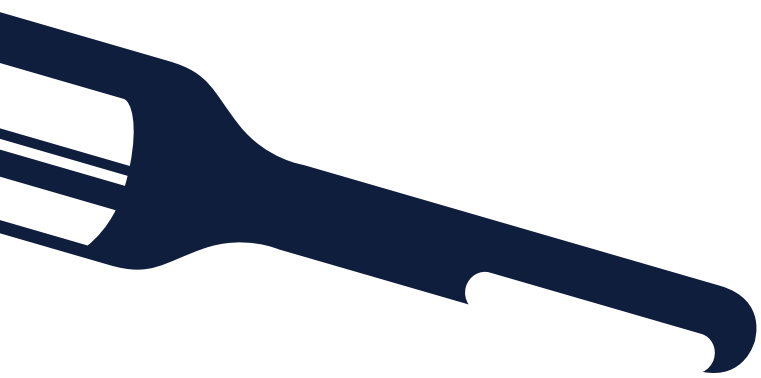
Pakketbezorgdienst

Na een bestelling in een webwinkel via een online portal zien waar de bezorger van het pakketje zich precies bevindt. Dat is handig voor klanten die willen inschatten wanneer ze hun bestelling kunnen verwachten. Maar door de volledige namen en locaties van de pakketbezorgers bekend te maken, handelde transportbedrijf NE DistriService B.V. (NDS) in strijd met de Wet bescherming persoonsgegevens. Dat constateerde de Autoriteit Persoonsgegevens in 2015 tijdens onderzoek naar de werkwijze van het bedrijf.

De Autoriteit constateerde dat NDS geen wettelijke grondslag had om de personeelsgegevens van pakketbezorgers te delen met klanten. Bovendien was NDS van plan om het online portal van de transportservice uit te breiden met foto's van de pakketbezorgers. Volgens de Autoriteit Persoonsgegevens zou de publicatie van de foto's, zeker in combinatie met de andere persoonsgegevens op het portal, leiden tot een grotere inbreuk op de persoonlijke levenssfeer van de betrokken werknemers. In reactie op het onderzoek van de Autoriteit Persoonsgegevens heeft NDS de werkwijze aangepast.



Gegevens over iemands gezondheid behoren tot de bijzondere persoonsgegevens. De Wet bescherming persoonsgegevens stelt extra strenge eisen aan de verwerking van deze gegevens. In 2015 behoorden bijzondere gegevens tot de thematische speerpunten van de Autoriteit Persoonsgegevens. Zo deed de toezichthouder diepgaand onderzoek bij negen zorginstellingen. Ook richtte de Autoriteit Persoons-gegevens het vizier op e-health: apparatuur waarmee mensen zelf hun gezondheid en levensstijl kunnen monitoren.



Gezondheid

E-health

Steeds vaker verzamelen niet alleen zorgaanbieders maar ook bedrijven medische gegevens, via gezondheids- en lifestyle apps op (mobiele) apparaten. Hierbij ontbreekt vaak de bescherming van het medisch beroepsgeheim.

Zonder toestemming van de gebruiker mogen bedrijven medische gegevens niet verwerken. En gebruikers horen goede informatie te krijgen over wat de bedrijven met hun gezondheidsgegevens doen.

Gezondheidsgegevens bij Nike

Een app die berekent hoeveel kilometer je hardloopt, op welke snelheid en met hoe grote passen. En die ook nog laat zien hoeveel calorieën je daarbij verbrandt. De Nike+ Running App, die wereldwijd miljoenen keren is gedownload, doet het allemaal. Na onderzoek van de Autoriteit Persoonsgegevens heeft Nike enkele maatregelen genomen om de verwerking van de gebruikersgegevens beter te regelen.

Gebruikers van de Nike+ Running App deelden gevoelige gegevens met Nike. Via de app verzamelde Nike namelijk gedurende langere tijd informatie over de sportieve prestaties van individuele hardlopers. Bijvoorbeeld over hoe vaak ze sporten, wat ze wegen en hoeveel calorieën ze verbranden. Dit zijn gevoelige persoonsgegevens die alleen mogen worden verwerkt na uitdrukkelijke toestemming. De Autoriteit Persoonsgegevens constateerde dat Nike de gebruikers onvoldoende informeerde over de verwerking van hun gezondheidsgegevens via de app. Daardoor was er geen sprake van geïnformeerde toestemming, zoals de Wet bescherming persoonsgegevens vereist. Ook liet Nike app-gebruikers niet weten dat er persoonsgegevens werden verwerkt voor analyse- en onderzoeksdoeleinden.

Gebruikers van lifestyle-apps moeten goede informatie krijgen over wat bedrijven met hun gezondheidsgegevens doen.

Naar aanleiding van het onderzoek van de Autoriteit Persoonsgegevens nam Nike in 2015 een aantal privacybeschermende maatregelen. Nieuwe gebruikers van de app zijn nu niet meer verplicht hun lengte en gewicht te registreren. Ook bevatten nieuwe versies van de app extra informatie over het verwerken van deze persoonsgegevens. Nike heeft bovendien toegezegd om álle gebruikers beter te informeren over de verwerking van gezondheidsgegevens. Daarnaast wordt aan bestaande gebruikers alsnog toestemming gevraagd voor de verwerking van hun medische informatie. De toezichthouder controleert of de maatregelen in overeenstemming zijn met de Wet bescherming persoonsgegevens.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/13

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Online een herhaalrecept aanvragen bij je huisarts kan heel handig zijn - mits het goed beveiligd gebeurt'

'We kregen een tip van een man dat hij geen slotje zag staan in de balk naast het adres van de site van zijn huisarts. Daarom durfde hij zijn herhaalrecept niet online aan te vragen. De website bleek inderdaad niet goed beveiligd. Deze man had dus groot gelijk dat hij zijn gevoelige medische gegevens niet via een onbeveiligde verbinding wilde versturen! De huisartsenpraktijk heeft na een gesprek met mij het formulier om herhaalrecepten aan te vragen direct van de website gehaald en pas terug gezet toen een beveiligde verbinding was geregeld.'

Gegevensverwerking in de zorgsector

Vertrouwelijke omgang met patiëntgegevens is in de gezondheidszorg essentieel.

Mensen hebben recht op bescherming van hun persoonsgegevens, ook in de gezondheidszorg. Onzorgvuldigheid hierbij zou mensen bovendien kunnen afschrikken om tijdig hulp te vragen. Het is daarom belangrijk dat patiëntgegevens, zoals gegevens over iemands diagnose, niet onder ogen van onbevoegden komen.

Toegang tot digitale patiëntendossiers

Alleen bevoegde medewerkers van ziekenhuizen, GGZ-instellingen of huisartsenposten mogen toegang hebben tot digitale patiëntendossiers en andere medewerkers dus niet. De Autoriteit Persoonsgegevens krijgt echter regelmatig vragen en tips over patiëntendossiers die onder ogen zouden zijn gekomen van medewerkers van zorginstellingen die daar niets mee te maken hadden. De toezichthouder deed naar aanleiding hiervan diepgaand onderzoek bij negen zorginstellingen. Hierbij kwam aan het licht dat geen van deze zorginstellingen aan de wet voldeed bij de toegang tot patiëntendossiers.

Het voorkomen van incidenten en het daadwerkelijk goed regelen van gecontroleerde toegang tot patiëntgegevens bleek een complexe, maar niet onmogelijke opgave. Er waren intensieve verbetertrajecten nodig om de overtredingen te beëindigen. In 2015 constateerde de Autoriteit Persoonsgegevens dat alle zorginstellingen inmiddels aan de wet voldeden. Hiermee kon de toezichthouder het onderzoek afsluiten.

In vervolg op het onderzoek vroeg de Autoriteit Persoonsgegevens in februari 2016 aandacht voor de bescherming van patiëntgegevens in een open brief aan raden van bestuur van zorginstellingen in Nederland. De Autoriteit benadrukte in deze brief dat het zorgvuldig omgaan met patiëntgegevens integraal deel uitmaakt van goede patiëntenzorg.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/14

Diagnose Informatie Systeem

Informatie over diagnoses van patiënten in de ziekenhuiszorg, geestelijke gezondheidszorg en forensische zorg komt terecht in het landelijke Diagnose Informatie Systeem (DIS). Zorgaanbieders verstrekken informatie aan het DIS, dat wordt beheerd door de Nederlandse Zorgautoriteit (NZa), over wat zij aan zorg hebben geleverd en gedeclareerd. De informatie wordt – na pseudonimisering – gedeeld met het ministerie van Volksgezondheid, Welzijn en Sport, het Zorginstituut Nederland, het CBS en de NZa. De Autoriteit Persoonsgegevens wees de NZa in 2015 op de noodzaak om bij verwerking van (bijzondere) persoonsgegevens te voldoen aan de eisen van de Wet bescherming persoonsgegevens.

Bij verwerking van patiëntgegevens in het Diagnose Informatie Systeem moet de NZa voldoen aan de eisen van de Wet bescherming persoonsgegevens.

In het DIS worden (bijzondere) persoonsgegevens verwerkt. Die mogen alleen onder strikte voorwaarden worden verwerkt. Door de pseudonimisering zijn de gegevens van patiënten in het DIS weliswaar beperkt herleidbaar tot individuen, maar er is geen sprake van een onomkeerbare anonimisering.

De Autoriteit Persoonsgegevens heeft in december 2015 gemeld een onderzoek te doen naar de naleving van de Wet bescherming persoonsgegevens door de beheerder van het DIS. De NZa heeft in reactie hierop toegezegd om voorlopig het leveren van gegevens aan derden te staken.

→ De verwerking van medische gegevens komt ook aan bod in de hoofdstukken 'Overheid' (jeugdzorg) en 'Werk en inkomen' (zieke werknemers).

Met het oog op opsporing en vervolging verwerken de politie en het Openbaar Ministerie bijzondere persoonsgegevens, zoals strafrechtelijke gegevens. Omdat het gevoelige informatie betreft, kunnen strafrechtelijke gegevens volgens de Wet bescherming persoonsgegevens alleen onder strikte voorwaarden worden verzameld, gebruikt en bewaard.
De publiek-private samenwerkingsverbanden die in het veiligheidsdomein steeds vaker ontwikkeld worden, roepen dan ook privacyvraagstukken op.
De Autoriteit Persoonsgegevens benadrukte in 2015 in verschillende wetgevingsadviezen de noodzaak om – ook binnen het veiligheidsdomein – de wettelijke eisen van gegevensbescherming serieus te nemen.

Politie & justitie

Cameratoezicht

Langs snelwegen, in winkelcentra en bij uitgaansgebieden. Op allerlei plekken houden bewakingscamera's van publieke en private partijen een oogje in het zeil. Maar met de miljoenen smartphones die in Nederland in gebruik zijn, hebben ook steeds meer burgers een camera onder handbereik.

De Autoriteit Persoonsgegevens vroeg in 2015 aandacht voor de wettelijke eisen rond het gebruik van camera's van particulieren en bedrijven voor de opsporing van strafbare feiten.

Camerabeelden voor opsporing

Met een wetswijziging wil de regering regelen dat particulieren en bedrijven zelfstandig camerabeelden van een diefstal of vernieling op internet mogen publiceren. De Autoriteit Persoonsgegevens oordeelde in 2015 dat het wetsvoorstel de noodzaak van een dergelijke privacygevoelige werkwijze onvoldoende aantoont.

De opsporing van verdachten van strafbare feiten is van oudsher een zaak van de politie en het Openbaar Ministerie. Daarbij gelden ook waarborgen voor de bescherming van de persoonlijke levenssfeer. Volgens de Autoriteit Persoonsgegevens zou het wetsvoorstel in feite leiden tot een legalisering van de publicatie van camerabeelden door iedereen voor het opsporen van diefstal en vernieling.

Publicatie van camerabeelden door burgers en bedrijven kan zeer ingrijpende gevolgen hebben voor de persoonlijke levenssfeer van individuen die op de beelden staan.

In haar wetgevingsadvies wijst de Autoriteit Persoonsgegevens erop dat publicatie van camerabeelden door burgers en bedrijven zeer ingrijpende gevolgen kan hebben voor de persoonlijke levenssfeer van individuen die op de beelden staan. Bijvoorbeeld met stigmatisering en represailles tot gevolg. Bovendien kunnen onschuldige burgers ten onrechte als verdachten te boek komen te staan. Voor deze risico's heeft het wetsvoorstel te weinig oog. Verder oordeelt de toezichthouder dat het beoogde doel van opsporing ook

bereikt kan worden met minder ingrijpende middelen. Bovendien zijn de noodzaak en proportionaliteit van de voorgestelde werkwijze onvoldoende onderbouwd.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/15

Fraudebestrijding

In de strijd tegen fraude wordt veelvuldig gebruik gemaakt van bijzondere persoonsgegevens, zoals strafrechtelijke gegevens. Dit kan voor de betrokkenen grote financiële en maatschappelijke gevolgen hebben, zoals discriminatie en uitsluiting.

De Autoriteit Persoonsgegevens benadrukte in 2015 bij haar adviestaken het belang van privacybescherming in de aanpak van fraude.

Gegevensuitwisseling voor fraudebestrijding

Met de Verkenning kaderwet gegevensuitwisseling wil het kabinet enkele knelpunten bij de fraudeaanpak vanuit samenwerkingsverbanden wegnemen. In een eerste reactie op het plan pleitte de Autoriteit Persoonsgegevens voor terughoudendheid bij de introductie van nieuwe regels en bevoegdheden. En voor een betere benutting van de bestaande wettelijke mogelijkheden voor publiek-private fraudebestrijding.

Om de knelpunten bij de gegevensuitwisseling voor fraudebestrijding weg te nemen, zouden samenwerkingsverbanden de mogelijkheden die bestaande wetgeving biedt in kaart moeten brengen en benutten.

De Verkenning kaderwet gegevensuitwisseling benoemt vijf knelpunten bij de gegevensuitwisseling voor fraudebestrijding. Bijvoorbeeld de geheimhoudingsplicht van professionals, de vorderingsplicht van politie en OM en de informatieplicht ten aanzien van betrokkenen. Volgens de Autoriteit Persoonsgegevens kan een groot deel van deze problemen worden weggenomen als samenwerkingsverbanden de mogelijkheden die

bestaande wetgeving biedt in kaart brengen en benutten. Daarom is er volgens de toezichthouder geen aanleiding om nieuwe wetgeving in te voeren.

Als er toch nieuwe wettelijke grondslagen voor gegevensverwerkingen binnen samenwerkingsverbanden moeten worden gecreëerd, zou deze regeling onderdeel moeten worden van de Wet bescherming persoonsgegevens. Een dergelijke wetswijziging moet voldoen aan de eisen van proportionaliteit en subsidiariteit. Daarnaast moet worden aangegeven van wie gegevens worden opgeslagen en hoe lang deze worden bewaard. Volgens de Autoriteit Persoonsgegevens staat de keuze voor de voorgestelde brede grondslag voor gegevensuitwisseling op gespannen voet met deze vereisten.

Kansspelen

Fraude en criminaliteit tegengaan en gokverslaving voorkomen zijn enkele doelen van de wijziging van de Wet op de kansspelen in verband met de modernisering van het speelcasinoregime. In haar advies over het wetsvoorstel benadrukte de Autoriteit Persoonsgegevens de noodzaak van een belangenafweging tussen de beoogde maatschappelijke doelen en de bescherming van persoonsgegevens van betrokkenen.

> Een belangenafweging tussen de beoogde maatschappelijke doelen en de bescherming van persoonsgegevens van betrokkenen ontbreekt in de voorgestelde wijziging van de Wet op de kansspelen.

De voorgestelde wet voorziet in een stelsel waarin de Kansspelautoriteit vergunningen kan verlenen om een casino te runnen. De toelichting op het wetsvoorstel benoemt de maatschappelijke noodzaak van zo'n systeem. Maar volgens de Autoriteit Persoonsgegevens ontbreekt een belangenafweging, die duidelijk maakt hoe de voorgestelde werkwijze voldoet aan de eisen van proportionaliteit en subsidiariteit. Daarnaast adviseerde de toezichthouder om in de toelichting op de wetswijziging aandacht te geven aan de resultaten van het *privacy impact assessment* dat is uitgevoerd.

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'De politie mag alleen noodzakelijke gegevens opvragen'

'De politie in een bepaalde regio vroeg dagelijks aan vijf hotels een lijst met de gegevens van alle gasten, liet een tipgever ons weten. Maar die gegevens heeft de politie lang niet altijd nodig. Het is in strijd met de wet om gegevens te verwerken die niet noodzakelijk zijn. Bovendien levert dit het risico op van bijvoorbeeld verlies van de gegevens of identiteitsfraude. Na tussenkomst van de Autoriteit Persoonsgegevens vraagt de politie nu alleen nog de gegevens op die echt nodig zijn om bijvoorbeeld gevaar te voorkomen of opsporingsonderzoek te doen.'

→ De verwerking van strafrechtelijke gegevens komt ook aan bod in de hoofdstukken 'Werk en inkomen' (pre-employment screening) en 'Internationaal' (toezicht op Europese informatiesystemen).

In een geglobaliseerde samenleving is internationale samenwerking tussen privacytoezichthouders belangrijker dan ooit. De Autoriteit Persoonsgegevens werkt dan ook intensief samen met collega-toezichthouders in Europa en daarbuiten. Bijvoorbeeld om gezamenlijk op te treden tegen wetsovertredingen. En om internationale toezichtstrategieën te ontwikkelen.
Daarnaast deelt de toezichthouder kennis, ervaringen en onderzoeksmethodes met buitenlandse collega's.
In 2015 stonden in internationaal verband onder andere profiling en het nieuwe Europese privacykader sterk in de belangstelling. Daarnaast presenteerde de Autoriteit Persoonsgegevens, als initiatiefnemer van het internationale Privacy Bridges Project, tijdens haar grote internationale conferentie in Amsterdam tien praktische voorstellen om trans-Atlantisch het niveau van gegevensbescherming te verhogen.

Internationaal

Profiling

Het verzamelen van grote hoeveelheden persoonsgegevens voor profiling overstijgt de landsgrenzen. Internationale opsporingsinstanties, samenwerkende inlichtingendiensten en multinationals spelen een actieve rol in internationale gegevensuitwisseling.

In samenwerking met andere privacytoezichthouders in Europa (en daarbuiten) monitort de Autoriteit Persoonsgegevens de naleving van privacywetgeving bij profiling en big data. In 2015 stond onder andere de verwerking van medische gegevens bij nieuwe consumententechnologie in de schijnwerpers.

Internationale onderzoeken

Apparaten en apps waarmee we zelf onze gezondheid en (on)gezonde levensstijl kunnen monitoren, verwerken allerlei gevoelige gegevens. Van locatiegegevens tot data over hartslag, bloeddruk, gewicht, eet- en beweegpatronen, alcoholconsumptie, rookgedrag en sportschoolbezoek. De Europese privacytoezichthouders, verzameld in de Artikel 29-werkgroep, publiceerden in 2015 een advies over de verwerking van medische gegevens bij gezondheidsapps en -apparaten.

Gezondheidsgegevens zijn gevoelige gegevens en kunnen daarom in de privacywet op extra bescherming rekenen. Dat betekent onder andere dat dergelijke gegevensverwerkingen in beginsel alleen zijn toegestaan als mensen hiervoor uitdrukkelijke toestemming hebben gegeven. De Europese privacytoezichthouders benadrukken dan ook het belang van begrijpelijke informatie over de verzameling en het gebruik van gezondheidsgegevens. Alleen op die manier kunnen mensen rechtsgeldige toestemming geven. Daarnaast bepleit de Artikel 29-werkgroep dat app-ontwikkelaars de gezondheidsgegevens zoveel mogelijk anonimiseren en in de ontwerpfase al rekening houden met privacybescherming (*privacy by design*).

De Europese privacytoezichthouders benadrukken het belang van begrijpelijke informatie over de verzameling en het gebruik van gezondheidsgegevens.

Internationale samenwerking

De huidige Europese richtlijn voor bescherming van persoonsgegevens vormt een stevige basis voor samenwerking tussen de privacytoezichthouders in de lidstaten.

De Autoriteit Persoonsgegevens werkt samen met diverse partijen binnen en buiten Europa, bijvoorbeeld op het gebied van onderzoek, advies en harmonisatie van regels. De internationale privacyconferentie in Amsterdam en de presentatie van tien voorstellen voor trans-Atlantische gegevensbescherming behoorden tot de kernresultaten van 2015.

Artikel 29-werkgroep

De Artikel 29-werkgroep is het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders, waaronder de Autoriteit Persoonsgegevens. De werkgroep speelt een belangrijke rol in de totstandkoming van Europees beleid voor de bescherming van persoonsgegevens. Van 2010 tot 2014 bekleedde Jacob Kohnstamm, voorzitter van de Autoriteit Persoonsgegevens, het voorzitterschap van de werkgroep. In 2015 leverde de Nederlandse privacywaakhond via de Artikel 29-werkgroep onder andere een actieve bijdrage aan de discussie over privacybescherming in het licht van terroristische dreigingen en over doorgifte van persoonsgegevens vanuit Europa naar de Verenigde Staten.

De Artikel 29-werkgroep reageerde in het voorjaar van 2015 op de roep om een Europees Passenger Name Record systeem (PNR-systeem). Het maatschappelijke draagvlak voor een dergelijk systeem, waarin persoonlijke reisinformatie uit computerreserveringssystemen wordt opgeslagen, groeide aanzienlijk na de aanslagen op Charlie Hebdo in januari 2015. De Artikel 29-werkgroep deed geen uitspraken over de (on)wenselijkheid van een PNR-systeem, maar benadrukte wel de serieuze privacyrisico's. In de zoektocht naar verdachte personen worden namelijk grote hoeveelheden persoonsgegevens over alle reizigers verzameld. De privacytoezichthouders oordelen dan ook dat een Europabreed PNR-systeem alleen zou mogen worden ingesteld als de noodzaak en proportionaliteit daarvan zijn aangetoond.

Een tweede kernactiviteit van de Artikel 29-werkgroep volgde op de uitspraak van het Europees Hof van Justitie, dat in oktober 2015 de Safe Harbour-overeenkomst tussen Europese landen en de Verenigde Staten ongeldig verklaarde. De Europese Commissie heeft de overeenkomst in 2000 opgesteld omdat in de Verenigde Staten geen algemene wetgeving bestaat voor de bescherming van persoonsgegevens. Dit betekende dat Europe-

se bedrijven en organisaties alleen persoonsgegevens kunnen doorgeven aan partijen in de Verenigde Staten die zich houden aan de zogenoemde Safe Harbour Principles. Met de uitspraak van het Hof van Justitie kwam deze juridische basis voor doorgifte van persoonsgegevens aan de Verenigde Staten te vervallen. De Artikel 29-werkgroep onderzocht in 2015 de gevolgen van het besluit van het Hof, waarbij de toezichthouders de betrokken partijen tot januari 2016 de tijd gaven om een oplossing te vinden. Begin februari 2016 werd bekend dat de Verenigde Staten en de Europese Unie tot afspraken zijn gekomen over een 'EU-VS privacyschild'. De Europese privacytoezichthouders zullen beoordelen of het nieuwe akkoord voldoet aan de eisen van het Europees Hof.

Internationale privacyconferentie in Amsterdam

De 37e editie van de Internationale Conferentie van Toezichthouders voor Gegevensbescherming en Privacy vond in oktober 2015 plaats in Amsterdam. Als gastheer verwelkomde de Autoriteit Persoonsgegevens naast collega-privacytoezichthouders ook vele vertegenwoordigers van bedrijven, universiteiten, maatschappelijke organisaties en overheden. Met ruim zevenhonderd deelnemers uit de hele wereld fungeerde de conferentie als een multidisciplinair platform om ervaringen uit te wisselen, kennis te delen en gezamenlijke plannen te maken.

Tijdens de conferentie in Amsterdam werden de eindresultaten gepresenteerd van het Privacy Bridges Project. Het project werd in 2014 gelanceerd door het Instituut voor Informatierecht van de Universiteit van Amsterdam en het Massachusetts Institute of Technology, op initiatief van de voorzitter van de Autoriteit Persoonsgegevens. Negentien Europese en Amerikaanse privacydeskundigen onderzochten manieren om de trans-Atlantische verschillen in gegevensbescherming te overbruggen. Die verschillen hangen samen met de verankering van de bescherming van persoonsgegevens in een grondrecht (binnen de Europese Unie) en in het consumentenrecht (in de Verenigde Staten). Volgens de Autoriteit Persoonsgegevens is het van essentieel belang deze kloof te verkleinen, om wereldwijd een hoger niveau van privacybescherming te bereiken. De tien voorstellen die de Europese en Amerikaanse privacyexperts presenteerden in het eindrapport van het Privacy Bridges Project ondersteunen deze ambitie.

Diverse deelnemers aan de Internationale Conferentie hebben toegezegd om voorstellen uit het Privacy Bridges Project te gaan oppakken en uitbouwen. De Nederlandse minister van Veiligheid en Justitie noemde in zijn speech tijdens de conferentie onder andere zijn ambitie om de verschillende procedures voor het melden van datalekken te standaardiseren en om de regelgeving op het gebied van drones te bespreken in Europees verband. Daarmee staan deze onderwerpen op de agenda van het Nederlandse voorzitterschap van de Europese Unie in de eerste helft van 2016.

Voorstellen uit het Privacy Bridges Project

Regie over eigen persoonsgegevens

Een van de belangrijke voorstellen is het verder ontwikkelen van een techniek om internetgebruikers weer 'in control' te laten zijn over hun persoonsgegevens. Bedrijven moeten de techniek kunnen gebruiken om hun internetdienst zo in te richten dat er aan de verschillende regels in de VS en de EU wordt voldaan bij het verzamelen en gebruiken van persoonsgegevens.

Standaardisatie meldproces datalekken

Datalekken hebben niet alleen binnen landsgrenzen maar ook wereldwijd impact. Op dit moment gelden er tientallen verschillende wetten voor het melden van datalekken met grote verschillen in de definitie van een datalek en de termijn waarop een lek moet worden gemeld. Het voorstel is te komen tot standaardisatie van het meldproces, zonder nu de wetten te moeten veranderen.

Samenwerking overheden

Beleidsmakers in de VS en de EU werken aan dezelfde privacyvraagstukken. Zij doen dat niet met elkaar, maar naast elkaar. Het zou efficiënt én effectief zijn als er op meer structurele basis informatie-uitwisseling, kennisdeling en samenwerking tussen overheden is bij deze maatschappelijke vraagstukken.

→ Lees meer: autoriteitpersoonsgegevens.nl/15/16

Federal Trade Commission

In 2014 tekende de Autoriteit Persoonsgegevens al een samenwerkingsovereenkomst met de privacytoezichthouder van Canada. In 2015 kwam daar nog een overeenkomst met de Amerikaanse Federal Trade Commission bij. Het zogenoemde Memorandum of Understanding heeft als doel om samenwerking tussen beide toezichthouders te faciliteren en om gezamenlijke onderzoeken uit te voeren. Zo maakt de samenwerkingsovereenkomst het mogelijk dat de partijen op vertrouwelijke basis informatie uitwisselen.

Global Privacy Enforcement Network

De Autoriteit Persoonsgegevens meldde zich in 2015 aan als deelnemer van het GPEN Alert System, een informatiesysteem van het Global Privacy Enforcement Network dat de Federal Trade Commission (FTC) initieerde. Het doel: de internationale samenwerking op het gebied van privacytoezicht verder bevorderen.

Via het GPEN Alert System delen privacytoezichthouders wereldwijd onderling informatie over toezichtzaken als er sprake is van grensoverschrijdende kwesties. Het kan gaan om informatie over onderzoeken, maar ook om signalen van burgers die voor andere toezichthouders relevant kunnen zijn. Naast de FTC en de Autoriteit Persoonsgegevens hebben privacytoezichthouders uit Australië, Canada, Ierland, Nieuw Zeeland, Noorwegen en het Verenigd Koninkrijk in 2015 de samenwerkingsovereenkomst voor het GPEN Alert Systeem ondertekend. Volgens de Autoriteit Persoonsgegevens en de FTC is GPEN daarmee een belangrijk samenwerkingshulpmiddel geworden dat privacyautoriteiten praktisch helpt om persoonsgegevens effectiever te beschermen.

Herziening Europese privacyregelgeving

Ook in 2015 volgde de Autoriteit Persoonsgegevens de ontwikkelingen rond de nieuwe Europese privacyregelgeving op de voet. Eind 2015 werden de Europese instellingen het inhoudelijk eens over een nieuwe EU-privacyverordening, die de huidige privacyrichtlijn uit 1995 zal vervangen. Naar verwachting zullen de instellingen de nieuwe regelgeving in het voorjaar van 2016 aanvaarden.

Positie Europees Parlement en Raad van Ministers

De Europese huidige privacyrichtlijn (‘Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in

verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens') is vastgesteld in een tijdperk waarin internet nog in de kinderschoenen stond. De Europese Commissie presenteerde in 2012 voorstellen voor een herziening van de Europese privacyregelgeving, die bestaat uit een algemene verordening over gegevensbescherming en een richtlijn over gegevensbescherming bij opsporing en vervolging. Het Europees Parlement heeft in 2014 zijn standpunt over de verordening en richtlijn vastgesteld.

Eind 2015 werden de Europese instellingen het inhoudelijk eens over een nieuwe EU-privacyverordening.

In de zomer van 2015 heeft de Raad van Ministers overeenstemming bereikt over de volledige teksten van de voorgestelde Europese verordening en richtlijn. Hiermee werd een belangrijke fase ingeluid in de ontwikkeling van het nieuwe Europese privacykader. Onder de noemer van de zogeheten triloog onderhandelden de Raad van Ministers, de Europese Commissie en het Europese Parlement over de definitieve wetteksten.

Positie Europese privacytoezichthouders

De Artikel 29-werkgroep van de gezamenlijke Europese privacytoezichthouders heeft ook in 2015 op verschillende manieren bijgedragen aan de discussies over het nieuwe wettelijke kader voor gegevensbescherming binnen de Europese Unie. Zo publiceerde de werkgroep opinies en aanbevelingen over kernthema's in de voorgestelde verordening en richtlijn. De Artikel 29-werkgroep adviseerde de deelnemers aan de triloog over zaken als de rechten van de betrokkenen en de bevoegdheden van toezichthouders.

Europol en Eurojust

Europol en Eurojust hebben als taak om ernstige vormen van grensoverschrijdende georganiseerde misdaad in de EU te bestrijden, zoals terrorisme, drugshandel, mensenhandel, fraude en cybercrime.

Europol en Eurojust hebben geen uitvoerende taken, maar ondersteunen het werk van politie en justitie in de EU-lidstaten. Europol en Eurojust verzamelen en analyseren

daarbij grote hoeveelheden informatie, vaak van persoonlijke aard, over verdachten, veroordeelden, getuigen en slachtoffers van misdaad. Op deze verwerking van persoonsgegevens bestaat onafhankelijk toezicht. De Autoriteit Persoonsgegevens levert een bijdrage aan dit toezicht. De vicevoorzitter van de Autoriteit Persoonsgegevens is vicevoorzitter van de Joint Supervisory Body Europol en voorzitter van de Joint Supervisory Body Eurojust.

Europese informatiesystemen

Om de grenzen van het Schengengebied te bewaken en justitiële taken uit te voeren, wisselen Europese lidstaten onderling persoonsgegevens uit. Bijvoorbeeld bij visumaanvragen en asielverzoeken.

De bevoegde autoriteiten (zoals inlichtingendiensten, douane en politie) gebruiken de volgende informatiesystemen om persoonsgegevens uit te wisselen: Eurodac, Schengen Informatiesysteem, Visum Informatiesysteem en Douane Informatiesysteem. Deze systemen staan onder onafhankelijk toezicht. De Autoriteit Persoonsgegevens levert een bijdrage aan dit toezicht. In 2015 deed de toezichthouder onderzoek naar het Nederlandse deel van het Schengen Informatiesysteem (SIS II).

De Europese informatiesystemen staan onder onafhankelijk toezicht, waaraan ook de Autoriteit Persoonsgegevens een bijdrage levert.

Schengen Informatie Systeem

Het SIS II is ingericht voor de controle op inkomend en uitgaand personen- en goederenverkeer in het Schengengebied. Op Europees niveau zijn voorschriften vastgelegd voor de partijen die zijn aangesloten op het informatiesysteem. De Autoriteit Persoonsgegevens controleert periodiek of deze voorschriften binnen het Nederlandse deel van het Schengen Informatiesysteem (N.SIS II) worden nageleefd. Uit het onderzoek dat plaatsvond in 2015 blijkt dat de organisatorische beveiligingsmaatregelen ontoereikend zijn. Dit creëert het risico dat onbevoegden toegang krijgen tot het systeem.

In Nederland heeft de politie de centrale verantwoordelijkheid voor N.SIS II. Als beheerder van het systeem moet de politie beschikken over onder meer personeelsprofielen waarin de taken en verantwoordelijkheden staan van de personen die bevoegd zijn om toegang te krijgen tot N.SIS II. Uit het onderzoek van de Autoriteit Persoonsgegevens blijkt dat deze personeelsprofielen er niet zijn. Bovendien worden de organisatorische beveiligingsmaatregelen voor N.SIS II onvoldoende nageleefd. Zo ontbreken een beveiligingsplan en een autorisatieprocedure die beschrijft welke medewerkers toegang hebben tot N.SIS II. Daarnaast worden toegekende autorisaties niet regelmatig gecontroleerd.

Ook de Koninklijke Marechaussee had onvoldoende organisatorische maatregelen genomen om N.SIS II te beveiligen. Er was bijvoorbeeld geen adequate autorisatieprocedure. De Autoriteit Persoonsgegevens constateerde dan ook dat een aantal medewerkers ten onrechte toegang kon krijgen tot het systeem. Bovendien informeerde de Koninklijke Marechaussee geregistreerde personen niet over de controle van hun gegevens en over hun rechten, terwijl zij daar wel toe verplicht is. De Koninklijke Marechaussee heeft al tijdens het onderzoek actie ondernomen om dit te verbeteren.

In 2015 bereidde de Autoriteit Persoonsgegevens zich voor op de uitbreiding van haar boetebevoegdheden en op de nieuwe taken vanuit de meldplicht datalekken. Daarnaast trof de organisatie voorbereidingen voor de naamsverandering die op 1 januari 2016 plaatsvond.

Het budget van de Autoriteit Persoonsgegevens was in 2015 € 8.188.000. De bezetting bedroeg gemiddeld 72,5 fte, een daling van bijna 2 fte ten opzichte van 2014.

Een groot deel van de capaciteit gebruikt de Autoriteit Persoonsgegevens om onderzoek te doen naar de naleving van de wet. In 2015 rondde de toezichthouder 43 onderzoeken af. Daarnaast heeft de Autoriteit Persoonsgegevens in 2015 226 zaken op een 'lichtere' manier afgehandeld, door niet direct een onderzoek te starten maar eerst een gesprek met een organisatie te voeren of een brief te sturen.

Een andere belangrijke taak van de Autoriteit Persoonsgegevens is adviseren over nieuwe regelgeving. In 2015 bracht de toezichthouder 27 keer advies uit.

Organisatie

Publieks- en persvoorlichting

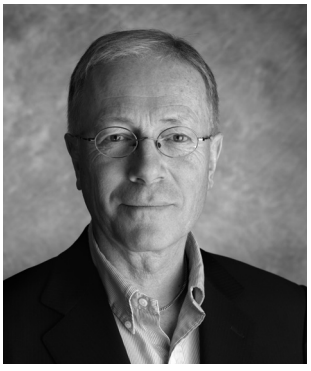
De Autoriteit Persoonsgegevens beantwoordt vragen en behandelt tips over (mogelijke) overtredingen van de privacywetgeving. Daarnaast zoekt de Autoriteit Persoonsgegevens actief contact met de pers en maatschappelijke organisaties. Ook weten de media de toezichthouder goed te vinden.

In 2015 ontving de Autoriteit Persoonsgegevens 6.778 vragen en tips. Veruit de meeste vragen en tips – ruim een derde van het totaal – gingen over de sector handel & dienstverlening.

Het aantal perscontacten in 2015 was 617. De Autoriteit Persoonsgegevens werd om een reactie gevraagd over uiteenlopende onderwerpen, variërend van datalekken tot medische apps.

Leden en directie van de Autoriteit Persoonsgegevens

Autoriteit



Mr. J. Kohnstamm
Voorzitter

Mr. W.B.M. Tomesen
Vicevoorzitter

Directie

Drs. P.J.J. Frencken
Directeur

Externe optredens voorzitter en vicevoorzitter

Privacy en meer specifiek de bescherming van persoonsgegevens konden in 2015 weer rekenen op veel maatschappelijke aandacht en publiciteit.

De voorzitter en de vicevoorzitter van de Autoriteit Persoonsgegevens hebben het afgelopen jaar veelvuldig het werk van de toezichthouder in binnen- en buitenland over het voetlicht gebracht.

De Autoriteit Persoonsgegevens zocht vele malen zelf actief contact met de pers en maatschappelijke organisaties. Belangrijk hierbij was de wijziging van de Wet bescherming persoonsgegevens per 1 januari 2016. Deze wetswijziging heeft drie belangrijke wijzigingen in het leven geroepen: een nieuwe naam, een boetebevoegdheid en een meldplicht voor organisaties die te maken hebben met een datalek. Tegelijkertijd wisten de media de Autoriteit Persoonsgegevens zelf goed te vinden over de meest uiteenlopende onderwerpen. Ook kreeg de Autoriteit Persoonsgegevens veel uitnodigingen om toespraken te houden op congressen.

In 2015 bestond een belangrijk deel van de werkzaamheden van voorzitter en de vicevoorzitter dan ook uit externe optredens. Zij hielden (keynote)speeches tijdens conferenties, namen deel aan debatten en gaven interviews aan zowel nationale en internationale radio en televisie als geschreven pers.

Een selectie uit de externe werkzaamheden van de voorzitter en de vicevoorzitter in 2015:

Datalekken

Er was in 2015 veel aandacht in de media voor datalekken. Journalisten namen hierover geregeld contact op met de Autoriteit Persoonsgegevens. Bijvoorbeeld om een reactie te vragen op een datalek, zoals bij de kinderspeelgoedfabrikant waarbij gegevens van meer dan 100.000 Nederlandse kinderen waren gestolen, een Amerikaanse datingsite waarvan de klantgegevens op straat lagen en een ziekenhuis waar medische dossiers waren gelekt.

De Autoriteit Persoonsgegevens heeft zelf ook veel aandacht gevraagd voor het risico op datalekken en het belang van een adequate beveiliging in verband met de meldplicht datalekken die per 1 januari 2016 in werking is getreden. Deze meldplicht houdt in dat

organisaties die te maken hebben met een datalek dit moeten melden aan de Autoriteit Persoonsgegevens en in sommige gevallen ook aan de betrokkenen om wiens persoonsgegevens het gaat. De Autoriteit Persoonsgegevens heeft in het laatste kwartaal van 2015 veel voorlichting gegeven over de meldplicht datalekken door toespraken te houden op diverse congressen en interviews te geven aan landelijke dagbladen, vakbladen, radio en televisie.

Naamswijziging en boetebevoegdheid

De wijziging van de Wbp per 1 januari 2016 hield voor de organisatie ook een nieuwe naam en een boetebevoegdheid in. Al in 2015 hebben de voorzitter en de vicevoorzitter tijdens externe optredens de nieuwe naam, Autoriteit Persoonsgegevens, veelvuldig laten vallen om het grotere publiek hiermee bekend te maken. Over de bevoegdheid van de Autoriteit Persoonsgegevens om boetes uit te delen hebben de voorzitter en de vicevoorzitter zowel tijdens media-optredens als tijdens toespraken op congressen voor privacyprofessionals voorlichting gegeven.

Nieuwe Europese Privacyverordening

In 2015 liepen de onderhandelingen over de toekomstige Europese privacyregelgeving. Zowel de nationale als internationale media hebben ons in 2015 regelmatig benaderd met vragen over de veranderingen voor burgers en organisaties als de verordening in werking is getreden.

Gezondheidsgegevens/e-health

Een van de prioriteiten van de Autoriteit Persoonsgegevens in 2015 was de bescherming van gegevens over gezondheid. Dit zijn bijzondere gegevens die extra beschermd moeten worden. De aandacht van de Autoriteit ging onder meer uit naar bedrijven die apparatuur produceren waarmee mensen zelf hun gezondheid en levensstijl kunnen monitoren.

In november 2015 publiceerde de Autoriteit Persoonsgegevens een onderzoek naar de Nike+ hardloopapp. Hieruit bleek dat Nike de gebruikers van de Nike+ Running app onvoldoende informeert over de verwerking van hun gezondheidsgegevens. Nike verkrijgt daardoor ook niet de vereiste uitdrukkelijke toestemming van de app-gebruikers. Er was veel media-aandacht voor dit onderwerp, onder meer van sites die gespecialiseerd zijn in nieuws over technologische ontwikkelingen en gadgets. Vicevoorzitter Tomesen gaf een interview aan BNR.

Voorzitter Kohnstamm gaf in februari een groot interview aan het Financieel Dagblad over e-health. Hij ging hierbij onder meer in op de rol van technologiebedrijven en de verwerking van gezondheidsgegevens. Begin december bracht tv-programma Zembla een twee-

luik over gezondheidsgegevens en apps. In beide uitzendingen kwam de voorzitter aan het woord. Hij wees onder meer op de voorwaarden waaronder gezondheidsgegevens mogen worden verwerkt. Daarbij heeft hij ook het Nike-onderzoek als voorbeeld genoemd.

Tracking & tracing

Er was in 2015 veel media-aandacht voor het volgen van mensen via hun telefoon, op internet en via hun tv-kijkgedrag. De vicevoorzitter gaf onder meer aan RTL-Nieuws een interview over het onderzoek bij Ziggo, dat klanten onvoldoende bleek te informeren en geen ondubbelzinnige toestemming vroeg voor het verzamelen en gebruiken van persoonsgegevens over het tv-kijkgedrag. Ziggo had al tijdens het onderzoek maatregelen genomen en de overtredingen beëindigd.

Ook het volgen van mensen in en rond winkels via de wifi-signalen van hun mobiele apparaten kreeg veel aandacht in de media. "Deze gegevens kunnen worden gebruikt om mensen anders te behandelen of mensen te confronteren met hun afgelegde route. Dat gaat veel te ver, zeker als dat stiekem en op de openbare weg gebeurt", aldus de vicevoorzitter tegen onder meer BNR en NOS.

Privacy Bridges - Internationale Privacyconferentie in Amsterdam

De Autoriteit Persoonsgegevens heeft veel contact met de media gehad over de Internationale Privacyconferentie die zij in oktober 2015 organiseerde. De contacten spitsten zich vooral toe op het Privacy Bridges-rapport dat kort voor de conferentie werd gepresenteerd en tijdens de conferentie werd besproken. Negentien toonaangevende privacyexperts uit de VS en Europa hebben in dit project tien praktische voorstellen ontwikkeld om trans-Atlantisch het beschermingsniveau van persoonsgegevens te verhogen. De meeste voorstellen kunnen binnen de bestaande wetgeving ter hand genomen worden en wereldwijd worden geïmplementeerd. Het gaat om pragmatische bruggen waarvan mensen, bedrijven, overheden en toezichthouders voordeel gaan hebben.

Voorafgaand aan de conferentie heeft de voorzitter in verschillende interviews de internationale pers al een voorproefje van de Privacy Bridges gegeven. Een week voorafgaand aan de conferentie is het integrale Privacy Bridges-rapport gepubliceerd. New York Times heeft de voorzitter, initiator van het Privacy Bridges Project, hierover geïnterviewd en een uitgebreid artikel gepubliceerd. Ook Trouw publiceerde een interview met de voorzitter en de NOS bracht zowel een radio- als tv-item over de voorgestelde bruggen. Tijdens de conferentie waren veertien nationale en internationale journalisten aanwezig die over de conferentie en de privacybruggen hebben bericht, onder meer Politico, BNA International, RTL nieuws, BNR en Trouw.

Tweede Kamer en Eerste Kamer

In 2015 werd de Autoriteit Persoonsgegevens meerdere keren uitgenodigd deel te nemen aan rondetafelgesprekken in het parlement. De voorzitter nam in januari 2015 op uitnodiging van de vaste commissie voor Veiligheid en Justitie van de Tweede Kamer deel aan het rondetafelgesprek over de evaluatie van de Wet bewaarplicht telecommunicatiegegevens en de kabinetsreactie op de ongeldigverklaring van de EU-richtlijn over deze bewaarplicht.

De vicevoorzitter nam in april 2015 op uitnodiging van de commissie van Onderwijs, Cultuur en Wetenschappen in de Tweede Kamer deel aan het rondetafelgesprek over digitale leermiddelen in het onderwijs. In mei 2015 nam hij op uitnodiging van de commissie voor Veiligheid en Justitie in de Tweede Kamer deel aan het rondetafelgesprek over 'slimme grenzen'.

In december 2015 nam de voorzitter deel aan het rondetafelgesprek in de Tweede Kamer naar aanleiding van de uitspraak van het Europees Hof van Justitie waarin het Hof de Safe Harbour-overeenkomst, de regeling van de Europese Commissie voor doorgifte van gegevens naar de Verenigde Staten, onrechtmatig verklaarde.

De vicevoorzitter sprak in april 2015 tijdens een deskundigenbijeenkomst in de Eerste Kamer over het onderwerp cliëntenrechten in de zorg.

Markttoezichthoudersberaad

De voorzitter en vicevoorzitter van de Autoriteit Persoonsgegevens namen ook in 2015 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).

Het MTB organiseerde in 2015 wederom twee seminars voor de bestuurders en medewerkers van de leden van het MTB. De bijeenkomst in juni ging over internationale samenwerking tussen toezichthouders en op de bijeenkomst in oktober spraken de deelnemers over het zoeken van een goede balans tussen formeel en informeel toezicht.

Raad van advies

De raad van advies heeft als taak de Autoriteit te adviseren over de hoofdlijnen van het beleid van de Autoriteit Persoonsgegevens. De leden van de raad van advies waren in 2015:

Mevrouw drs. T.A. Maas-de Brouwer (voorzitter)
Lid raad van commissarissen van onder meer PEN, Schiphol Groep, Arbo Unie en Van Leer Group Foundation. Voormalig senator PvdA.

De heer J.J. van Aartsen (vanaf 1 november 2015)
Burgemeester van 's-Gravenhage.

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

De heer H.W. Broeders (tot 1 november 2015)
Adviseur/bestuurder. Voormalig lid van de raad van bestuur van Capgemini S.A.

De heer drs. B.R. Combée
Directeur Consumentenbond.

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

Mevrouw prof. dr. M.M.M. van Eechoud
Hoogleraar Informatierecht, Universiteit van Amsterdam/Instituut voor Informatierecht.

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

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

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

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

De heer mr. A.A. Westerlaken (tot 4 november 2015)
Voorzitter raad van bestuur Maasstadziekenhuis.

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

De heer mr. A. Wolfsen (tot 1 november 2015)
Voormalig burgemeester van Utrecht.

Colofon

Autoriteit Persoonsgegevens
Den Haag, april 2016

Tekst: Leene Communicatie, Gouda
Ontwerp: Teldesign, Rotterdam
Fotografie: Mark Kohn
Druk: Xerox/OBT, Den Haag

De Autoriteit Persoonsgegevens staat voor het grondrecht op bescherming van persoonsgegevens.

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens 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. De Autoriteit Persoonsgegevens 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.