Jaarverslag 2017

AUTORITEIT
PERSOONSGEGEVENS

Inhoud

Dit jaarverslag gaat over de belangrijkste werkzaamheden van de AP uit 2017. Alle feiten en cijfers staan in de bijlage.

Voorwoord

Privacy gaat iedereen wat aan. Bij organisaties die persoonsgegevens gebruiken werken uiteindelijk ook maar mensen. Mensen die ambtenaar, docent, fraudeonderzoeker, marketingspecialist, winkelier of wat dan ook zijn. Maar ook gewoon mens. Ouders die niet willen dat de vakantiekiekjes van hun kinderen over internet zwerven. Patiënten die bang zijn dat hun medisch dossier op straat komt te liggen. Consumenten die er niet aan moeten denken dat banken hun betaalgegevens doorverkopen.

Bescherming van persoonsgegevens is dan ook niet voor niets een grondrecht. Het is belangrijk als op zichzelf staand recht, maar ook omdat het samenhangt met andere rechten. Het recht op non-discriminatie, op zelfontplooiing, om als volwassene niet achtervolgd te worden door iets wat je als kind op internet plaatste. Als je de privacy van mensen schendt, raak je de fundamenten van de rechtsorde. Het is het dus van fundamenteel belang om de persoonsgegevens van mensen goed te beschermen.

Maar hoe doe je dat in het digitale tijdperk? De tijd waarin grote databedrijven tot de machtigste bedrijven ter wereld behoren en handel in persoonsgegevens booming business is? Waarin we bepaalde zaken niet meer kunnen regelen als we dit niet digitaal willen doen? Waarin we feitelijk niet meer kunnen meedoen in de maatschappij zonder digitale identiteit?

De Europese privacyrichtlijn, waarop onze huidige Wet bescherming persoonsgegevens gebaseerd is, komt uit 1995. De tijd dat het internet nog in de kinderschoenen stond. Daarom is het de hoogste tijd voor een nieuwe wet. En die is in aantocht: per 25 mei 2018 gelden de Algemene verordening gegevensbescherming (AVG) en de Richtlijn voor gegevensverwerking door politie en justitie. De AVG versterkt de positie van mensen, doordat zij meer privacyrechten krijgen. Tegelijkertijd krijgen organisaties die persoonsgegevens verwerken meer verantwoordelijkheden en de privacytoezichthouders steviger bevoegdheden.

Voor de Autoriteit Persoonsgegevens (AP) draaide het in 2017 dan ook vooral om de voorbereiding op deze nieuwe wetgeving. Voorlichting geven stond bovenaan onze agenda, zodat organisaties weten wat ze straks moeten doen. We zorgden voor meer capaciteit bij onze publieksvoorlichting en trokken vaak het land in om te spreken bij congressen en bijeenkomsten. En omdat de AP er nieuwe taken en bevoegdheden bij krijgt, zijn we in 2017 gereorganiseerd. Zodat ook wij er op 25 mei 2018 klaar voor zijn. Bijvoorbeeld om klachten van mensen te behandelen over organisaties die hun persoonsgegevens verwerken.

Daarnaast ging het reguliere werk van de AP natuurlijk ook door. We deden in 2017 onderzoek naar diverse organisaties, variërend van relatief kleine organisaties tot de grote internationale spelers als Facebook en Microsoft. Ook brachten we, zoals elk jaar, tientallen adviezen uit over nieuwe wet- en regelgeving. De focus in ons werk lag dit jaar op het onderwerp bijzondere persoonsgegevens. Dat zijn gegevens die zo gevoelig zijn dat de verwerking ervan grote gevolgen kan hebben voor de privacy van mensen. Bijvoor-

beeld medische of strafrechtelijke gegevens. Hoewel het verwerken van bijzondere persoonsgegevens meestal verboden is, ziet de AP toch dat steeds meer organisaties deze gegevens gebruiken. Reden dus om een aantal
organisaties op de vingers te tikken en het onderwerp extra onder de aandacht te brengen.

En nu is het nog maar een maand te gaan totdat de nieuwe Europese privacyregels van toepassing zijn. De nieuwe wet en de bijbehorende nieuwe organisatie van de AP maken ons werk nog mooier, uitdagender en internationaler. Wij blijven ons inzetten voor de bescherming van het grondrecht op bescherming van persoonsgegevens en kunnen straks een nóg stevíger vuist maken. Voor u, voor uw familie en vrienden, buren, collega's, huisarts, wethouder of wie dan ook. Want privacy gaat iedereen wat aan.

Aleid Wolfsen
Voorzitter van de Autoriteit Persoonsgegevens

Nieuwe privacy-wetgeving

Het jaar 2017 was bijzonder voor de Autoriteit Persoonsgegevens (AP), omdat dit het laatste volledige jaar was van de Wet bescherming persoonsgegevens (Wbp). Vanaf 25 mei 2018 is nieuwe Europese privacywetgeving van toepassing: de Algemene verordening gegevensbescherming (AVG) en de richtlijn voor gegevensverwerking door politie en justitie. Hierover voorlichting geven stond daarom bovenaan de agenda van de AP, zodat organisaties weten wat ze straks moeten doen. En mensen zich bewust zijn van hun privacyrechten.

Ook de AP zelf bereidde zich in 2017 voor op de toekomstige situatie. Bijvoorbeeld door met de andere privacytoezichthouders in de EU gezamenlijke afspraken te maken over de uitleg van de nieuwe normen en taken. En door de organisatie van de AP opnieuw in te richten.

zie hoofdstuk Organisatie

Voorlichting over de AVG

In 2017 gaf de AP, voorafgaand aan de grote voorlichtingscampagne die in januari 2018 startte, al veel voorlichting over de AVG. Bijvoorbeeld door vaak het land in te gaan en presentaties te houden op congressen, bijeenkomsten en bij brancheorganisaties. En door een tienstappenplan te publiceren dat organisaties helpt bij de voorbereiding op de AVG.

Ook kwam in het speciale AVG-dossier op de website steeds meer informatie te staan, waaronder antwoorden op concrete vragen uit de praktijk. In mei 2017 riep de AP organisaties dan ook op hun vragen te mailen. Vervolgens gaf de AP op de website wekelijks antwoord op de drie meest gestelde vragen.

AVG-dossier

Veelgestelde vragen over de nieuwe wet

- Per wanneer moet ik aan de nieuwe privacyregels voldoen?
- Geldt de nieuwe Europese privacywetgeving ook voor kleine mkb'ers en zzp'ers?
- Wat moet een functionaris voor de gegevensbescherming (FG) weten en kunnen?
- Blijft het BSN straks een bijzonder persoonsgegeven?
- Welke verwerkingen van persoonsgegevens zijn volgens de AVG grootschalig?
- Mag ik onder de AVG gegevens van kinderen verwerken?

Telefoonteam

Organisaties en burgers kunnen ook telefonisch terecht bij de AP voor informatie over hun verplichtingen en rechten bij het verwerken van persoonsgegevens. Mede vanwege de grote hoeveelheid vragen over de AVG breidde de AP in 2017 de openingstijden van het telefonisch spreekuur uit. Op 24 mei 2017, een jaar voordat de AVG van toepassing wordt, konden mensen met vragen bellen met voorzitter Aleid Wolfsen. Wolfsen maakte die ochtend deel uit van het telefoonteam van de AP.

’Aan de telefoon hoor je waar het echt om gaat. Privacy is geen abstract begrip, maar gaat om het dagelijks leven van mensen. Mensen met soms schrijnende verhalen, bijvoorbeeld over het delen van medische gegevens.’

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens

Wat verandert er met de AVG?

- Mensen krijgen meer en sterkere privacyrechten.

- Organisaties die persoonsgegevens verwerken, krijgen meer verantwoordelijkheden.

- Privacytoezichthouders krijgen steviger bevoegdheden en gaan internationaal intensiever samenwerken.

AVG in een notendop

Guidelines

De gezamenlijke Europese privacytoezichthouders publiceerden in 2017 verschillende guidelines om bepaalde onderwerpen uit de AVG te verduidelijken. Dit geeft organisaties houvast bij de voorbereiding op en de naleving van de nieuwe privacywet. In 2018 volgen meer guidelines.
In 2017 zijn de volgende guidelines gepubliceerd:

Functionaris voor de gegevensbescherming (FG)
- Guidelines on Data Protection Officers ('DPOs')
- Nederlandse vertaling guidelines FG

Leidende toezichthouder
- Guidelines for identifying a controller or processor's lead supervisory authority
- Nederlandse vertaling guidelines leidende toezichthouder

Recht op dataportabiliteit
- Guidelines on the right to dataportability
- Nederlandse vertaling guidelines recht op dataportabiliteit

Data protection impact assessment (DPIA)
- Guidelines on Data Protection Impact Assessment (DPIA)
- Nederlandse vertaling guidelines DPIA

Administratieve boetes
- Guidelines on the application and setting of administrative fines
- Nederlandse vertaling guidelines administratieve boetes

Advisering over de AVG

De AP heeft in 2017 geadviseerd over de uitvoering van de nieuwe EU-wetgeving – de AVG en de Richtlijn gegevensbescherming politie en justitie – in Nederland.

Advies Uitvoeringswet AVG

Om de AVG in Nederland te kunnen uitvoeren, wordt de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) vastgesteld. Het doel van deze wet is om voor bepaalde onderwerpen nationale regels te maken en om de Wet bescherming persoonsgegevens (Wbp) in te trekken. Bepalingen in nationale wetgeving zijn vooral nodig voor de positie van de AP en onderwerpen waarbij ruimte is voor afwijking of aanvulling van de Europese regels. De AP heeft in april 2017 advies gegeven over het wetsvoorstel UAVG.

Onafhankelijke positie AP

De Europese wetgever en het Europese Hof hanteren strenge eisen om de onafhankelijke positie van de nationale toezichthouders te waarborgen. De AP constateerde dat haar onafhankelijke positie als toezichthouder nog onvoldoende gewaarborgd werd in het wetsvoorstel. De AP adviseerde deze positie te versterken door bijvoorbeeld haar begroting een afzonderlijk onderdeel te laten zijn van de Rijksbegroting.

Uitleg van normen AVG
Het idee achter de AVG is om het niveau van bescherming van persoonsgegevens in alle EU-lidstaten hetzelfde te laten zijn. De regels uit de AVG werken dan ook grotendeels rechtstreeks in de hele EU. Het is aan de Europese privacytoezichthouders om een definitieve interpretatie te geven van de rechtstreeks werkende normen uit de AVG, die de rechter vervolgens kan controleren. De AP adviseerde daarom om in de UAVG terughoudend te zijn bij het uitleggen van de normen uit de AVG.

Beleidsneutrale uitvoering
Ook adviseerde de AP om een beleidsneutrale uitvoering als uitgangspunt te hanteren in het wetsvoorstel. Dat betekent dat bestaande bepalingen van de Wet bescherming persoonsgegevens worden overgenomen in de UAVG. Bijvoorbeeld over bijzondere persoonsgegevens.

Het advies van de AP heeft tot verschillende aanpassingen geleid. De UAVG is inmiddels aangenomen door de Tweede Kamer.

Advies Uitvoeringswet AVG

Advies implementatie Richtlijn gegevensbescherming politie en justitie

In april 2017 adviseerde de AP over het wetsvoorstel Implementatie Richtlijn gegevensbescherming politie en justitie (Wijzigingswet). Het doel van dit wetsvoorstel is deze richtlijn om te zetten naar Nederlandse wetgeving. Hiervoor is het nodig om de huidige Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) aan te passen.

Toepassing Richtlijn
In het advies stelde de AP allereerst dat de voorgestelde wijzigingen in de Wpg en de Wjsg niet genoeg overeenkomen met de aanpassingen die nodig zijn en volgen uit de tekst van de Richtlijn. Het toepassingsgebied van de Richtlijn is volgens de AP breder dan het wetsvoorstel omschrijft. Een van de gevolgen hiervan is dat niet steeds duidelijk is voor welke toepassingen deze Richtlijn geldt en voor welke andere de AVG. Dit speelt bijvoorbeeld bij de hulpverleningstaak van de politie.

Boetebevoegdheid
De AP heeft geadviseerd de boetebepalingen in het voorstel meer in lijn te brengen met de boetemogelijkheden van de AVG. Er wordt in de Wpg namelijk maar één artikel voorgesteld waarbij oplegging van een boete mogelijk is en de hoogte daarvan is relatief laag. De AP vindt het verschil te groot met de bepalingen van de AVG, waarbij boetes kunnen worden opgelegd voor een groot aantal wetsovertredingen en waarbij de boetes voor overheidsorganisaties hoog kunnen oplopen.

Beveiliging
De AP merkte op dat de voorgestelde bepaling die de regels beschrijft voor de beveiliging van persoonsgegevens die politie en justitie verwerken, onvoldoende overeenkomt met de voorschriften voor informatiebeveiliging die de Richtlijn stelt.

Waarborgen
De AP heeft geadviseerd om betere waarborgen aan te brengen voor het verwerken van bijzondere persoonsgegevens. Ook zouden er volgens de AP betere waarborgen moeten zijn als politie of justitie, bijvoorbeeld door analyse van big data, geautomatiseerde besluiten neemt of profilering toepast.

Doorgifte van gegevens
Tot slot heeft de AP geadviseerd om de regels voor doorgifte van gegevens door politie of justitie buiten de EU aan te passen aan wat daarover in de Richtlijn staat.

Advies implementatie Richtlijn gegevensbescherming politie en justitie

Advies GEB Rijksdienst

De rijksoverheid is verplicht om bij de ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een privacy impact assessment (PIA), ook wel gegevensbeschermingseffectbeoordeling genoemd. Dit is een instrument om privacyrisico's in kaart te brengen en zo een goede afweging te maken over de impact die een bepaald voorstel heeft op de privacy van betrokkenen. En om maatregelen te nemen om risico's te voorkomen of verkleinen.

Met de AVG op komst heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een nieuw toetsmodel ontwikkeld, het toetsmodel Gegevensbeschermingseffectbeoordeling (GEB Rijksdienst). In juni 2017 adviseerde de AP over het concept-toetsmodel. De AP adviseerde onder meer de GEB Rijksdienst aan te vullen met voorbeelden van situaties waarin een GEB verplicht is. Ook gaf de AP in overweging om alle criteria waaraan een GEB moet voldoen op te nemen in het model. Tot slot raadde de AP aan om in het ontwerp op te nemen dat een uitgevoerde GEB onder omstandigheden na verloop van tijd geëvalueerd moet worden. En onder welke omstandigheden een GEB aan de AP moet worden voorgelegd.

Advies GEB Rijksdienst

Bijzondere persoonsgegevens

Niet alle persoonsgegevens zijn even gevoelig. In de wet is er daarom verschil gemaakt tussen 'gewone' persoonsgegevens en bijzondere persoonsgegevens. Dit zijn gegevens die zo gevoelig zijn – zoals medische gegevens – dat de verwerking ervan grote gevolgen kan hebben voor de privacy van mensen. Daarom gelden er extra strenge regels voor het verwerken van bijzondere persoonsgegevens.

In de Wet bescherming persoonsgegevens (Wbp) staan duidelijke regels voor de verwerking van bijzondere persoonsgegevens. Het is in beginsel verboden om bijzondere persoonsgegevens te verwerken. Tenzij er een wettelijke uitzondering is.

Toch ziet de Autoriteit Persoonsgegevens (AP) dat bijzondere persoonsgegevens steeds vaker worden verwerkt. Zo zijn bijzondere persoonsgegevens bijvoorbeeld vaker onderdeel van big data. Bedrijven en overheden verzamelen, koppelen, analyseren en gebruiken enorme hoeveelheden gegevens. Bijvoorbeeld om risicoprofielen te maken van mensen die een toeslag, lening of verzekering aanvragen.

We zien ook dat bijzondere persoonsgegevens voor andere doelen worden verwerkt dan waarvoor ze zijn verzameld. Bovendien zijn er steeds meer methoden en technieken beschikbaar om bijzondere gegevens te verwerken, zoals commerciële bloed- en DNA-tests.

Dit was voor de AP reden om in 2017 speciale aandacht te besteden aan het onderwerp bijzondere persoonsgegevens. Hierbij focuste de AP op de naleving van het verbod om bijzondere persoonsgegevens te verwerken. Ook was de AP alert op de juiste toepassing van de wettelijke waarborgen bij uitzonderingen op dit verbod.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens over iemands:

- gezondheid
- ras
- godsdienst
- politieke voorkeur
- seksuele leven
- lidmaatschap van een vakbond
- strafrechtelijk verleden.

Ook het burgerservicenummer (BSN) is een bijzonder persoonsgegeven, omdat dit een uniek en tot de persoon herleidbaar nummer is.

Gezondheidsgegevens

Gegevens over iemands gezondheid behoren tot de gevoeligste persoonsgegevens die er zijn. Gezondheidsgegevens zijn dan ook niet voor niets bijzondere persoonsgegevens. Het gaat hierbij niet alleen om medische gegevens die artsen vaststellen en vastleggen, maar om alle gegevens over iemands lichamelijke of geestelijke gezondheid.

Onderzoek alcohol- en drugscontrole werknemers

In februari 2017 publiceerde de AP een onderzoek naar het beleid van energiebedrijf Uniper om medewerkers te testen op alcohol- en drugsgebruik. Volgens dit beleid was Uniper van plan gegevens over de gezondheid van medewerkers te verwerken, zoals de uitkomsten van adem- en wangslijmtesten. Het doel hiervan was om onveilige situaties te voorkomen. Na onderzoek van de AP trok Uniper dit beleid in, omdat het in strijd bleek met de Wbp.

Werkgevers mogen over het algemeen geen alcohol- en drugstesten inzetten waarbij ze medische gegevens van werknemers verwerken. Dit mag in principe alleen als het in de wet is geregeld, zoals voor de luchtvaart. De gegevens kunnen in een arbeidsrelatie niet op grond van toestemming van de werknemer worden verwerkt. Werknemers zijn immers niet vrij in hun keuze om wel of niet mee te werken aan deze controles.

In het beleid van het energiebedrijf stond ook dat werknemers gevraagd zou worden hun leidinggevende te informeren over het gebruik van medicijnen die het beoordelingsvermogen of de reactiesnelheid beïnvloeden. Ook dit mag niet. Werkgevers mogen deze gegevens over de gezondheid van hun personeel niet zelf verwerken, dit mag alleen de bedrijfsarts.

Tot slot wilde Uniper in bepaalde gevallen drugshonden inzetten om te controleren of medewerkers drugs bij zich hadden. De noodzaak van zo'n vergaande en intimiderende beleidsmaatregel heeft het energiebedrijf niet aangetoond.

Uniper trekt alcohol- en drugscontrolebeleid in na onderzoek AP

Advies second opinion bedrijfsarts

In februari 2017 adviseerde de AP over de mogelijkheid voor werknemers om een second opinion aan te vragen bij een andere bedrijfsarts. Wanneer een werknemer dit doet, moet volgens het wetsvoorstel de eerste bedrijfsarts alle relevante informatie over de werknemer doorgeven aan de andere bedrijfsarts. Het gaat hierbij onder meer om gegevens over de gezondheid van de werknemer.

De AP adviseerde om duidelijk te maken op grond van welke wettelijke uitzondering de andere bedrijfsarts gezondheidsgegevens mag verwerken. Daarnaast adviseerde de AP om opnieuw af te wegen of doorbreking van de geheimhoudingsplicht gebaseerd kan zijn op veronderstelde toestemming van de werknemer. In het wetsvoorstel staat namelijk dat de eerste bedrijfsarts ervan uitgaat dat

de werknemer akkoord gaat met het verstrekken van zijn gegevens aan de andere bedrijfsarts, omdat de werknemer belang heeft bij de second opinion. De AP wees erop dat het bij een second opinion niet gaat om een doorverwijzing, maar om een herbeoordeling door een nieuwe arts. Er zou dus bijvoorbeeld verschil van mening kunnen zijn tussen de werknemer en de eerste arts over de juistheid van de te verstrekken persoonsgegevens.

Het advies van de AP heeft ervoor gezorgd dat het wetsvoorstel is aangepast. De belangrijkste aanpassing is dat de eerste bedrijfsarts alleen informatie over de werknemer mag doorgeven aan de andere bedrijfsarts als de werknemer daarvoor uitdrukkelijk toestemming heeft gegeven. De toestemming van de werknemer wordt dus niet meer verondersteld.

Advies second opinion bedrijfsarts

‘Niet zomaar vingerafdrukken van kinderen gebruiken’

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

‘Een tipgever maakte zich zorgen over de plannen van een jeugdsoos in haar woonplaats. De soos was van plan vingerafdrukken van kinderen en jongeren te gebruiken voor toegangscontrole. De soos vroeg hiervoor geen toestemming aan de ouders. De wettelijke regels zijn dat een organisatie alleen vingerafdrukken mag gebruiken als daarvoor een goede reden is. Bovendien moet de organisatie hiervoor toestemming vragen aan de mensen om wie het gaat. Bij een kind onder de 16 moeten de ouders toestemming geven. Daarnaast moet de organisatie altijd een alternatief bieden, bijvoorbeeld identificatie met een identiteitsbewijs of toegangspas. Tot slot moeten biometrische gegevens goed worden beveiligd. Ik heb contact opgenomen met de jeugdsoos. Dat heeft ervoor gezorgd dat de soos het plan om vingerafdrukken te gebruiken van kinderen onder de 16 jaar niet heeft uitgevoerd.’

Brief aan gemeenten over leerlingenvervoer

In oktober 2017 vroeg de AP bij de Vereniging van Nederlandse Gemeenten (VNG) aandacht voor de bescherming van persoonsgegevens van kinderen bij aanbestedingen voor leerlingenvervoer door gemeenten. De AP had tips ontvangen over publicatie van (bijzondere) persoonsgegevens van kinderen met een zorgvraag of beperkingen op de aanbestedingswebsite TenderNed. Het ging om namen, adresgegevens, telefoonnummers, geboortedata en schoollocaties, maar ook om heel gevoelige gegevens, zoals een aanduiding van de beperking(en) van de kinderen. Naar aanleiding van deze tips benaderde de AP enkele gemeenten, die de documenten met persoonsgegevens daarop lieten verwijderen.

De AP benadrukte vervolgens in een brief aan de VNG dat het verwerken – dus ook het publiceren – van persoonsgegevens noodzakelijk moet zijn voor het doel waarvoor ze worden gebruikt, in dit geval de aanbesteding. De vraag moet altijd zijn of het doel niet kan worden bereikt met minder gegevens of dat er een andere, minder ingrijpende manier is om hetzelfde doel te bereiken. Bijvoorbeeld door alleen niet-herleidbare gegevens te verwerken.

AP vraagt aandacht voor privacy bij aanbesteding leerlingenvervoer

Burgerservicenummer

Het burgerservicenummer (BSN) is een uniek en tot de persoon herleidbaar nummer. Daarom is het een bijzonder persoonsgegeven. Met het BSN kan gemakkelijk een koppeling worden gemaakt tussen informatie uit verschillende bestanden. Onzorgvuldig gebruik van het BSN brengt daarom privacyrisico's met zich mee, bijvoorbeeld misbruik van persoonsgegevens en identiteitsfraude. Organisaties buiten de overheid mogen het BSN alleen verwerken als dit in de wet staat.

Onderzoek btw-nummers zzp'ers

In juni 2017 liet de AP weten te onderzoeken of de Belastingdienst een wettelijke grondslag heeft voor het verwerken van het BSN in btw-identificatienummers van zelfstandigen zonder personeel (zzp'ers). De AP had in de maanden daarvoor verzoeken van zzp'ers gekregen om zich hier over uit te spreken.

Het BSN van zzp'ers is integraal opgenomen in hun btw-identificatienummer. Zzp'ers hebben de verplichting om hun btw-nummer aan (potentiële) klanten bekend te maken, bijvoorbeeld op hun website en op facturen. Het onderzoek van de AP is niet in 2017 afgerond.

AP onderzoekt verwerking BSN in btw-nummers zzp'ers

Onderzoek transportbedrijf

Transportbedrijf Nippon Express stopte met de onrechtmatige verwerking van het BSN van chauffeurs na onderzoek van de AP. In het onderzoeksrapport concludeerde de AP dat Nippon de identiteitsbewijzen van chauffeurs scande en daarbij onder meer het BSN verwerkte, terwijl dat niet mag. Ook bewaarde Nippon deze scans te lang en had het bedrijf de beveiliging niet op orde. Nippon nam maatregelen nadat de AP had laten weten een last onder dwangsom te gaan opleggen.

Scannen identiteitsbewijs

Om fraude te voorkomen, controleerde Nippon de identiteitsdocumenten van vrachtwagenchauffeurs die goederen komen laden. Zodat de juiste lading met de juiste chauffeur meegaat. Nippon maakte daarbij gebruik van scanapparatuur en diensten van een extern bedrijf. Op deze manier verwerkte Nippon het BSN zonder dat dit was toegestaan.

Het bedrijf maakt inmiddels gebruik van een afgeschermde scan, waardoor het BSN en de pasfoto van een chauffeur niet meer worden verwerkt. Direct na het vaststellen van de identiteit wordt de scan verwijderd. Alle scans van identiteitsbewijzen die waren opgeslagen, zijn verwijderd. Na controle van de identiteitsbewijzen blijft alleen een tekstdocument hiervan twintig dagen beschikbaar.

Beveiliging

In het onderzoeksrapport concludeerde de AP dat Nippon de opgeslagen scans van identiteitsbewijzen onvoldoende beveiligde. Dat is gevaarlijk, want met zulke scans kan identiteitsfraude worden gepleegd. Inmiddels heeft Nippon ervoor gezorgd dat alleen via het IP-adres van Nippon zelf toegang kan worden gekregen tot de opgeslagen tekstdocumenten. Hierdoor zijn deze documenten niet meer toegankelijk voor iedereen.

Vervoersbedrijf Nippon past werkwijze aan na optreden AP

Onderzoek Airbnb

Op aandringen van de AP stopte het Amerikaanse bedrijf Airbnb eind 2017 met het verwerken van het BSN. Airbnb verwijdert inmiddels automatisch het BSN uit alle digitale kopieën van identiteitsbewijzen en heeft alle BSN's van eerder verzamelde identiteitsbewijzen vernietigd. De AP ontving zo'n honderd tips van Nederlanders over het onrechtmatige gebruik van hun BSN door Airbnb en heeft samengewerkt met de Ierse privacytoezichthouder om de overtreding te laten beëindigen.

Airbnb is een bemiddelingsplatform voor het tijdelijk huren en verhuren van woningen. Om een woning te kunnen huren via Airbnb, moeten mensen via de website van het bedrijf een digitale kopie van hun paspoort of identiteitsbewijs uploaden. Deze identiteitsbewijzen bevatten het BSN.

AP: Airbnb beëindigt verwerking BSN

’Geen BSN bij aanmelding voor een tv-programma’

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

‘We kregen een tip van een man die graag eens bij een studio-opname van zijn favoriete tv-programma wilde zijn. Toen hij zich hiervoor aanmeldde, moest hij zijn BSN doorgeven. De man belde ons om te vragen of dit wel mocht. Ons antwoord was: nee. Organisaties buiten de overheid mogen het BSN namelijk alleen gebruiken als dit in de wet staat. En in deze situatie is dat niet zo. Ik heb daarom direct contact opgenomen met de producent van het tv-programma. Het resultaat is dat de producent nu niet meer naar het BSN vraagt. Ook heeft de producent alle aanmeldformulieren vernietigd waarop mensen hun BSN hadden ingevuld.’

Strafrechtelijke gegevens

Sommige verwerkingen van persoonsgegevens brengen bijzondere privacyrisico’s met zich mee. Zoals de verwerking van strafrechtelijke gegevens. Organisaties die van plan zijn zulke gegevens te verwerken, moeten eerst door de AP een voorafgaand onderzoek laten uitvoeren. De AP kijkt dan of de verwerking aan alle wettelijke eisen voldoet. Pas als de AP de verwerking heeft goedgekeurd, mag een organisatie hiermee beginnen.

SNA-keurmerk

In februari 2017 keurde de AP de verwerking van strafrechtelijke gegevens voor het SNA-keurmerk goed. De Stichting Normering Arbeid (SNA) geeft een keurmerk uit aan ondernemingen die arbeid ter beschikking stellen en/of werk aannemen. Het doel hiervan is het voorkomen van fraude en illegaliteit in de uitzendbranche en bij alle vormen van (onder)aanneming van werk. De SNA doet dit samen met geaccrediteerde inspectie-instellingen. Deze voeren inspecties uit om te beoordelen of ondernemingen voldoen aan de eisen van het keurmerk.

De SNA stelde in overleg met de inspectie-instellingen een protocol op voor de verwerking van strafrechtelijke gegevens voor het SNA-keurmerk. Dit protocol gaat over strafrechtelijke gegevens die de inspectie-instellingen aan de SNA verstrekken en die de SNA aan de Belastingdienst en de Inspectie SZW verstrekt. Het doel van deze verstrekkingen is om handhavend te kunnen optreden. De AP onderzocht het protocol en keurde dit goed.

Besluit SNA-keurmerk

Gegevens over politieke voorkeur en godsdienst

Onderzoek stemhulpen

De AP deed in februari 2017 onderzoek naar de beveiliging van de internetverbinding van 24 interactieve stemhulpen voor de verkiezingen in maart van dat jaar. Hieruit bleek dat 14 van de stemhulpen geen beveiligde verbinding hadden. Gebruikers van online stemhulpen vullen gedetailleerde vragen in over hun politieke voorkeur en soms ook over geloofsovertuiging. Dit zijn bijzondere persoonsgegevens. Er worden zware eisen gesteld aan de beveiliging van deze persoonsgegevens.

Kiesgeheim

Het is heel belangrijk dat gebruikers van online stemhulpen zich onbespied weten bij het invullen van vragen over hun politieke voorkeuren. En dat informatie hierover ook niet langer wordt bewaard dan strikt noodzakelijk. Dit raakt aan het kiesgeheim. Mensen moeten vrij gebruik kunnen maken van hun stemrecht. Op wie je verwacht te gaan stemmen moet ook geheim blijven, zodat je vrijuit je voorkeuren en wensen kunt aangeven.

De AP heeft de beheerders van de stemhulpen opgedragen de beveiliging binnen een week in orde te maken. Direct daarna zijn vier interactieve stemhulpen verwijderd. Alle andere aangeschreven stemhulpen hebben de beveiliging van hun internetverbinding verhoogd.

Tracking cookies

Samen met de Autoriteit Consument en Markt (ACM) trad de AP ook op tegen vijf stemhulpen die tracking cookies gebruikten, waaronder StemWijzer.nl. De stemhulpen verwijderden de tracking cookies direct.

- Toezichthouders ACM en AP treden op tegen StemWijzer.nl
- Stemhulpen verhogen beveiliging na optreden AP
- Stemhulpen passen werkwijze aan na optreden AP

Gegevens over seksueel leven

Registratie prostituees

Zowel de gemeente Den Haag als de gemeente Utrecht waren van plan om prostituees te registreren en daarmee bijzondere persoonsgegevens van hen vast te leggen. In Den Haag ging het om gegevens over het seksuele leven van prostituees en in Utrecht om gegevens over hun ras en gezondheid. In beide gevallen heeft de AP géén ontheffing verleend om deze bijzondere persoonsgegevens te mogen verwerken.

Den Haag

De gemeente Den Haag ziet registratie van prostituees als een belangrijke maatregel om mensenhandel te bestrijden. De AP oordeelde echter dat de gemeente Den Haag geen gegevens van prostituees in een apart register mag vastleggen. Omdat de gemeente uitsluitend gegevens van prostituees in een afzonderlijke database wilde vastleggen, zou er sprake zijn van gegevens over het seksuele

leven. Verwerking van persoonsgegevens over iemands seksuele leven is verboden, tenzij er sprake is van een uitzonderingsgrond.

De AP zag geen reden om de gemeente Den Haag een ontheffing te verlenen, onder meer omdat de gemeente niet aannemelijk kon maken dat het register noodzakelijk is voor het bestrijden van mensenhandel. De gemeente is hierop naar de rechter gegaan. De rechtbank Den Haag heeft het beroep van de gemeente in maart 2018 ongegrond verklaard.

AP: Den Haag mag persoonsgegevens prostituees niet registreren

Utrecht

De gemeente Utrecht was van plan om een registratieplicht in te voeren voor raamprostituees. Ook deze gemeente ziet dit als een belangrijke maatregel om mensenhandel te bestrijden. Voor de verwerking van bijzondere persoonsgegevens van raamprostituees, zoals rasgegevens en gezondheidsgegevens, deed de gemeente daarnaast een ontheffingsverzoek bij de AP.

De AP oordeelde dat de gemeente Utrecht geen wettelijke grondslag heeft om gegevens van prostituees in een register op te nemen. Daarnaast heeft de gemeente niet aannemelijk kunnen maken dat er toch sprake is van een algemeen zwaarwegend belang dat deze inbreuk op het privéleven van prostituees rechtvaardigt. Ook zag de AP geen reden om de gemeente een ontheffing te verlenen voor het verwerken van bijzondere persoonsgegevens van raamprostituees.

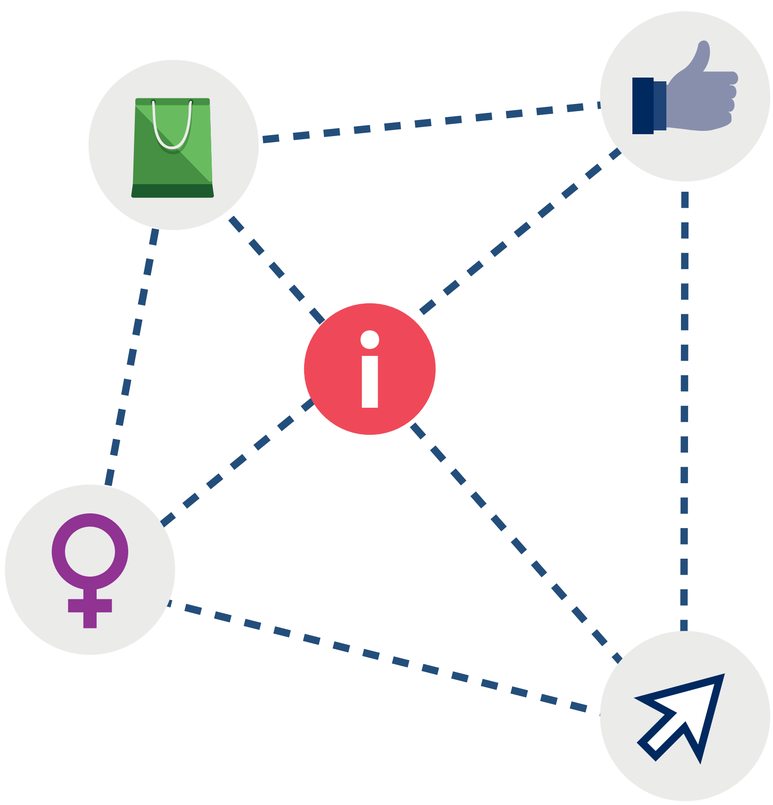
AP van plan registratie prostituees Utrecht onrechtmatig te verklaren

Internet & telecom

Het gebruik van internet- en telecomdiensten – zoals websites, apps, zoekmachines, smart tv's, maar ook besturingssystemen – kan op verschillende manieren de privacy van mensen aantasten. Natuurlijk door de grote bedrijven die over de schouder van mensen meekijken als zij op hun smartphone, achter hun computer of voor hun smart tv zitten. Maar ook kleinere organisaties, zoals scholen, kunnen inbreuk maken op iemands privacy als zij bijvoorbeeld zo-maar foto's van leerlingen op hun website zetten.

Big data en profiling

Organisaties kunnen door nieuwe technologie steeds makkelijker veel verschillende soorten gegevens verzamelen en deze aan elkaar koppelen. Ze gebruiken deze big data om bepaalde verbanden te vinden. Zo is het mogelijk mensen in groepen in te delen en hun gedrag te voorspellen. Dat heet profiling. Het risico bij het gebruik van big data is dat mensen de zeggenschap over hun gegevens kwijtraken. En ook organisaties kunnen het zicht verliezen op welke gegevens zij allemaal verwerken en waarvoor precies.



Onderzoek Facebook

De Autoriteit Persoonsgegevens (AP) deed in mei 2017 onderzoek naar de verwerking van persoonsgegevens van zo'n 9,6 miljoen Nederlandse Facebookgebruikers. Uit dat onderzoek bleek onder meer dat Facebook de gebruikers onvolledig informeerde over het gebruik van hun persoonsgegevens. Ook stelde de AP vast dat Facebook bijzondere persoonsgegevens gebruikte zonder uitdrukkelijke toestemming van de gebruikers. Zo gebruikte Facebook gegevens over seksuele geaardheid om op basis hiervan gerichte advertenties te tonen. Met dit laatste is Facebook inmiddels gestopt.

AP: Facebook handelt in strijd met de privacywetgeving

Onderzoek Microsoft

In oktober 2017 concludeerde de AP dat Microsoft in strijd met de wet persoonsgegevens verwerkte via het besturingssysteem Windows 10 Home en Pro. Uit onderzoek van de AP bleek dat Microsoft de gebruikers van dit systeem niet duidelijk informeerde over welke persoonsgegevens het bedrijf precies waarvoor gebruikte. Microsoft vertelde niet dat het bij de standaardinstellingen voortdurend gegevens verzamelde over het gebruik van apps en het surfgedrag van de gebruiker. Microsoft kreeg zo inzicht in het internetgedrag en computergebruik van de individuele Windows 10-gebruiker.

Dit gebrek aan informatie was een van de redenen dat Microsoft geen rechtsgeldige toestemming van gebruikers kon krijgen om hun gegevens te verwerken. Mensen kun-

nen namelijk alleen geldige toestemming geven wanneer zij volledig zijn geïnformeerd, precies weten waarvoor zij toestemming geven en ze de toestemming ook vrij kunnen geven. Ook kreeg Microsoft niet de vereiste ondubbelzinnige toestemming, omdat het bedrijf alleen een opt-out aanbood. Dat iemand de standaardprivacyinstellingen bij de installatie van Windows niet actief wijzigt, wil niet zeggen dat hij dús toestemming geeft voor het gebruik van zijn gegevens. Microsoft heeft aangegeven de overtredingen te willen beëindigen door in een update een herstelplan uit te voeren.

AP: Microsoft verwerkt gegevens Windowsgebruikers in strijd met wet

> ’Het bleek dat Microsofts besturingssysteem ongeveer iedere stap volgde die je op je computer zet. Dat levert een indringend beeld van jou op. Wat betekent dat? Weten mensen dat, willen ze dat? Microsoft moet mensen een eerlijke kans geven hier zelf over te beslissen.’
>
> Wilbert Tomesen, vicevoorzitter van de Autoriteit Persoonsgegevens

Reclame op smart tv’s

De AP heeft in januari 2017 TP Vision, een bedrijf dat televisies produceert en ontwikkelt, aangesproken op het plan om persoonlijke reclames te laten zien op smart tv’s van Philips. Het bedrijf gaf aan veel te weten van het kijkgedrag van mensen, bijvoorbeeld naar welke zenders ze kijken en welke apps ze gebruiken. Met deze gegevens wilde TP Vision reclames relevanter maken. De AP liet TP Vision weten dat het bedrijf alleen gegevens over het kijkgedrag van mensen mag verwerken als zij daar duidelijk en volledig over zijn geïnformeerd en er toestemming voor hebben gegeven. TP Vision verklaarde aan de AP op dat moment alleen nog intern te testen met persoonlijke reclames en dat er geen toestellen op de markt waren die op deze manier reclames toonden.

AP spreekt TP Vision aan op reclame op smart tv’s

Gebruik van big data en profiling

Zowel het bedrijfsleven als de overheid maken gebruik van big data en profiling.

Bedrijven kunnen dit doen voor verschillende commerciële doelen. Bijvoorbeeld om een specifieke winstgevende klantengroep te behouden of om gerichte advertenties te tonen op basis van voorspelde interesses. Of juist om ongewenste klanten te weren, zoals bij een aanvraag voor een lening.

De overheid kan bigdata-analyses bijvoorbeeld inzetten om epidemieën te bestrijden of fraudeurs op te sporen. Profiling bij de overheid kan ook een vorm van risicomanagement zijn, zoals bij grenscontroles.

Persoonsgegevens op internet

Veel mensen publiceren gegevens over zichzelf of over anderen op internet, zoals foto's op Facebook. Ook organisaties plaatsen persoonsgegevens op internet. De gevolgen hiervan kunnen groot zijn voor de mensen om wie het gaat. Onder meer omdat eenmaal op internet geplaatste gegevens jaren later nog vindbaar zijn. Dit kan bijvoorbeeld bij een sollicitatie nadelige gevolgen hebben.

Beeldmateriaal van leerlingen online

De AP krijgt regelmatig vragen over scholen die foto's van leerlingen online publiceren. Foto's en video's van leerlingen zijn persoonsgegevens, hiervoor gelden dus de regels uit de privacywet. Maar die zijn niet altijd bekend bij scholen. Of scholen zijn onzeker over hoe ze de regels moeten toepassen. De AP heeft in augustus 2017 in een brief aan de koepelorganisaties duidelijk gemaakt hoe scholen moeten omgaan met het publiceren van beeldmateriaal van leerlingen op een website of social media.

Willen scholen foto's of video's van leerlingen publiceren, dan hebben zij toestemming nodig van elke leerling die herkenbaar in beeld is. Is een leerling jonger dan 16 jaar, dan moeten de ouders toestemming geven. Die toestemming moeten leerlingen of ouders vrij en zonder druk kunnen geven. De school mag niet uitgaan van het principe 'wie zwijgt, stemt toe'. Bovendien geldt dat leerlingen of ouders toestemming moeten geven voor een specifiek doel en dat ze hun toestemming altijd weer kunnen intrekken. Scholen moeten gepubliceerde foto's van leerlin-

gen daarnaast goed beschermen, zodat ze niet in verkeerde handen terechtkomen. Dat kan bijvoorbeeld door een portal op de website te plaatsen waar alleen leerlingen en hun ouders met een persoonlijke inlognaam en wachtwoord kunnen inloggen.

AP roept scholen op zorgvuldig om te gaan met beeldmateriaal van leerlingen

Onderzoek voormijnkleinkind.nl

Op de website voormijnkleinkind.nl kunnen grootouders die tegen hun wil geen contact hebben met hun kleinkind berichten plaatsen voor dit kind. Uit onderzoek van de AP in 2016 bleek dat de Stichting Voor Mijn Kleinkind hiermee de privacyrechten schond van de kinderen om wie het ging en hun ouders. De berichten voor de kleinkinderen waren namelijk zichtbaar voor iedereen die via een zoekmachine op de site kwam. In september 2017 zag de AP af van handhavende maatregelen, omdat de stichting de website had aangepast. Via de website kan nu niet meer worden afgeleid dat een kleinkind door zijn of haar grootouder(s) wordt gezocht. Ook verschijnen de persoonsgegevens van de kleinkinderen niet langer in de zoekresultaten van Google. Hiermee werden de overtredingen beëindigd.

Voormijnkleinkind.nl past werkwijze aan na optreden AP

Standpunt publicatie WHOIS-gegevens

Het onbeperkt publiekelijk toegankelijk maken van WHOIS-gegevens van domeinnaamhouders (naam, adres, e-mailadres en telefoonnummer) door Nederlandse registries is in strijd met de Nederlandse privacywetgeving. Dit standpunt publiceerde de AP in oktober 2017 op verzoek van een Nederlandse registry, een beheerder van domeinnaamextensies (zoals .com of .nl).

Volgens de regels van de wereldwijde domeinnaambeheerder ICANN zijn registries verplicht om WHOIS-gegevens van alle domeinnaamhouders, zoals eigenaren van een website, onafgeschermd te publiceren. Maar het openbaar maken van deze persoonsgegevens voor iedereen is helemaal niet noodzakelijk, zo oordeelde de AP. Het is voldoende als toegang tot de gegevens mogelijk is als dat echt nodig is, bijvoorbeeld om technische redenen. Of voor partijen zoals justitie en politie, die daartoe wettelijk bevoegd zijn.

De gezamenlijke Europese privacytoezichthouders hebben in december 2017 een brief naar ICANN gestuurd om duidelijk te maken dat het onbeperkt publiekelijk toegankelijk maken van WHOIS-gegevens niet mag. ICANN heeft hierop aangegeven te onderzoeken hoe de publicatie van WHOIS-gegevens in overeenstemming met de nieuwe Europese privacywet kan worden gebracht.

AP: onafgeschermde publicatie van WHOIS-gegevens in strijd met de wet

Regels voor persoonsgegevens publiceren op internet

Niemand mag zomaar persoonsgegevens van een ander op internet publiceren, zoals foto's op Facebook. Dit mag in principe alleen als daarvoor een wettelijke grondslag is uit de privacywet, zoals toestemming van de mensen om wie het gaat. Maar publiceert iemand privé, dus niet namens een bedrijf? En niet (ook) voor professionele of commerciële doeleinden? Dan is er geen grondslag, zoals toestemming, nodig. Let op: de informatie mag daarbij alleen zichtbaar zijn voor een beperkte kring mensen en dus niet openbaar zijn voor iedereen (ook niet voor 'vrienden van vrienden' op Facebook) of gevonden worden door zoekmachines.

Advies PSD2

Innovatieve mobiele en internetbetalingsdiensten bevorderen en consumentenrechten versterken. Dat is het doel van de Europese richtlijn Payment Service Directment 2, beter bekend als PSD2. Hiermee krijgen nieuwe soorten dienstverleners de kans actief te worden op de betaalmarkt. De AP adviseerde in augustus 2017 over de Implementatiewet PSD2 en in december 2017 over het Implementatiebesluit. Beide wetsvoorstellen hebben als doel de Europese richtlijn om te zetten in Nederlandse wetgeving.

De nieuwe dienstverleners gebruiken betaalgegevens van consumenten, mits die consumenten daarvoor hun uitdrukkelijke toestemming geven. De dienstverleners moeten een vergunning krijgen van de Nederlandsche Bank (DNB). DNB beoordeelt onder meer of alles rond de benodigde toestemming goed geregeld is.

In het advies over de Implementatiewet adviseerde de AP om de verhouding tussen PSD2 en de AVG (de nieuwe Europese privacywet) te verduidelijken in het wetsvoorstel. Betaalgegevens van consumenten zijn persoonsgegevens en dus is de privacywetgeving van toepassing. Aanbieders van betalingsdiensten moeten vanaf 25 mei 2018 dus aan de AVG voldoen, maar in het wetsvoorstel voor PSD2 staan ook aparte regels voor privacybescherming. En dat werkt volgens de AP verwarrend. In het advies over het Implementatiebesluit adviseerde de AP ook om het gehele toezicht op de bescherming van persoonsgegevens onder te brengen bij één toezichthouder, namelijk de AP. En niet deels bij DNB.

Advies Implementatiewet PSD

Advies Implementatiebesluit PSD2

Privacyverklaring noodzakelijk

De AP heeft naar aanleiding van een tip vijf Nederlandse social media monitoring-bedrijven gewezen op het ontbreken van een openbaar toegankelijke privacyverklaring op hun website. Volgens de privacywetgeving moeten deze organisaties via een privacyverklaring in duidelijke taal communiceren welke persoonsgegevens zij verzamelen, hoe ze dit doen, met welk doel, hoe lang deze bewaard worden en hoe betrokkenen gebruik kunnen maken van hun rechten. Na het optreden van de AP hebben de vijf bedrijven hun privacybeleid aangepast. Zij hebben een toereikende privacyverklaring opgesteld en op hun website gepubliceerd.

Online auteursrechten

De AP heeft in december 2017 na voorafgaand onderzoek bepaald dat filmdistributeur Dutch FilmWorks B.V. persoonsgegevens, zoals IP-adressen en NAW-gegevens, mag verwerken van mensen die downloaden uit illegale bronnen. De filmdistributeur is van plan mensen die films en series illegaal downloaden een schikkingsvoorstel sturen, om zo inbreuk op auteursrechten tegen te gaan en illegaal downloaden te ontmoedigen.

De AP onderzocht of Dutch FilmWorks op een zorgvuldige manier met deze persoonsgegevens om kan gaan. Volgens de AP heeft het bedrijf voldoende waarborgen getroffen door een gedragsregeling en een informatiebeveiligingsbeleid op te stellen. De AP heeft haar besluit op 6 december 2017 gepubliceerd in de Staatscourant. Twee partijen hebben tegen dit besluit beroep ingesteld bij de rechtbank. Ten tijde van het opstellen van dit jaarverslag is hierover nog geen uitspraak gedaan.

AP geeft groen licht voor verwerking persoonsgegevens door Dutch FilmWorks

Beveiliging & meldplicht datalekken

Bij het verwerken van persoonsgegevens is de juiste beveiliging heel belangrijk. Mensen moeten erop kunnen vertrouwen dat organisaties ervoor zorgen dat deze gegevens niet op straat komen te liggen. Dit betekent dat de beveiliging van persoonsgegevens binnen een organisatie een blijvend punt van aandacht moet zijn. Als de beveiliging niet in orde is, kan dat leiden tot een datalek en vervolgens misbruik, zoals identiteitsfraude.

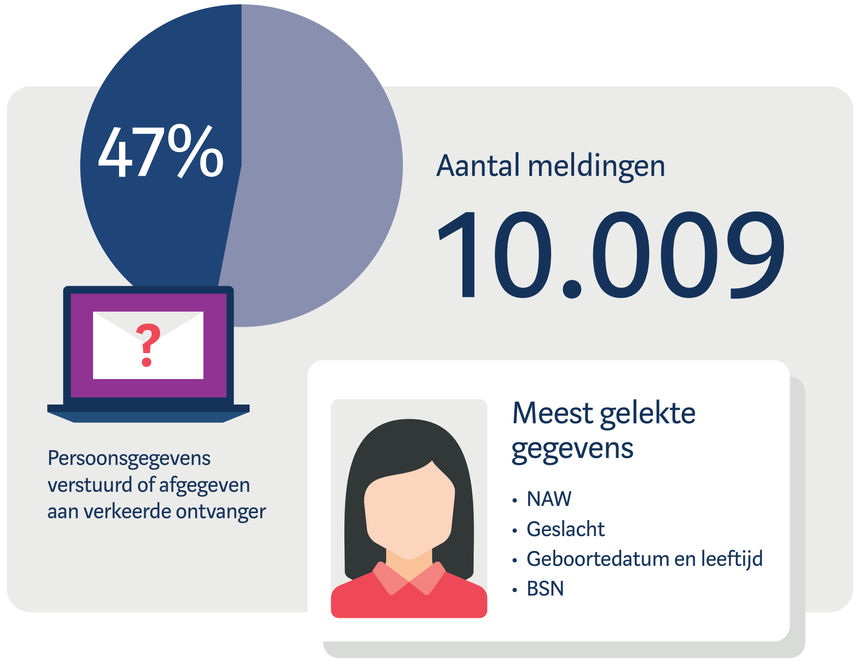
Meldplicht datalekken

Organisaties die een ernstig datalek hebben, moeten dit melden bij de Autoriteit Persoonsgegevens (AP) en soms ook aan de mensen van wie de gelekte gegevens zijn. De meldplicht datalekken heeft tot doel het beveiligingsniveau te verhogen en de zelfredzaamheid van mensen te vergroten. Krijgen mensen een melding dat hun gegevens zijn gelekt, dan kunnen zij snel in actie komen, bijvoorbeeld door een wachtwoord te wijzigen.

Datalekken 2017

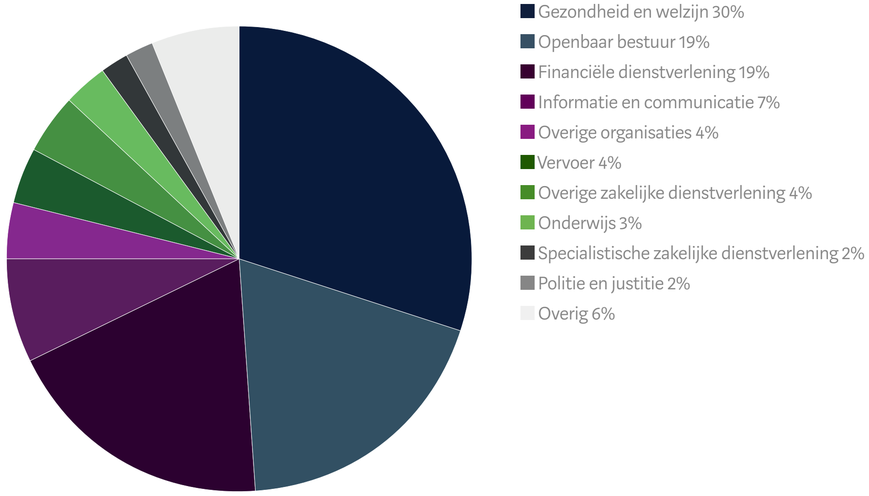
De AP ontving in 2017 iets meer dan 10.000 meldingen van datalekken. In 2016, het eerste jaar van de meldplicht, ontving de AP bijna 5700 meldingen van datalekken.

Het meest voorkomende type datalek in 2017 was dat persoonsgegevens aan de verkeerde ontvanger waren verstuurd of afgegeven (47%). Daarna werd er het meest gemeld over kwijtgeraakte of gestolen apparaten of papieren met daarop persoonsgegevens (14%). De meest gelekte gegevens waren NAW-gegevens (naam, adres, postcode en woonplaats), geslacht, geboortedatum en leeftijd en het burgerservicenummer (BSN). Het aantal mensen dat werd geraakt door een datalek varieerde per melding van één enkel persoon tot – in enkele gevallen – honderdduizenden betrokkenen.



Sectoren

De meeste datalekken zijn gemeld vanuit de sectoren gezondheid en welzijn (30%), financiële dienstverlening (19%) en openbaar bestuur (19%). Dat wil niet automatisch zeggen dat zich hier de ergste overtreders bevinden. In deze sectoren worden veel persoonsgegevens verwerkt. Vaak gaat het daarbij om gevoelige persoonsgegevens zoals gezondheidsgegevens, financiële gegevens en/of het BSN. En dus moeten organisaties in deze sectoren – gezien de aard van de gegevens – eerder een melding doen. Het aantal datalekken in een sector zegt nog niets over de impact ervan op de persoonlijke levenssfeer van mensen. Dat is onder meer afhankelijk van het aantal mensen van wie persoonsgegevens zijn gelekt en de gevoeligheid van de gegevens.



Acties AP

Bij een datalekmelding kan de AP onder meer:

- contact opnemen met een organisatie om de informatie in een melding te verifiëren en zo nodig aan te vullen;
- een eerste of nader onderzoek instellen;
- een sanctie opleggen;
- een organisatie op de plicht te wijzen de mensen van wie de gegevens zijn gelekt op de hoogte te stellen;
- (algemene) voorlichting geven naar aanleiding van patronen in meldingen, bijvoorbeeld om andere organisaties bewust te maken van mogelijke beveiligingsrisico's.

In 8.495 gevallen was er aanleiding voor de AP om de melding te controleren. In 2017 startte de AP in totaal 635 onderzoeken naar de beveiliging en naar mogelijke datalekken bij organisaties. In vrijwel alle gevallen gaf de AP de organisatie een waarschuwing en over het algemeen leidde dat tot beëindiging van de overtreding.

10.000 datalekken gemeld in 2017

Cyberaanval WannaCry

In mei 2017 vond de wereldwijde cyberaanval WannaCry plaats, die talloze computersystemen platlegde. Het ging om ransomware, kwaadaardige software, die een computer of bestanden gijzelt. Meestal wordt daarna betaling geëist, bijvoorbeeld via prepaidkaarten of Bitcoin, om de bestanden weer vrij te geven. Getroffen Nederlandse organisaties bleken vaak vragen te hebben over wat zij moesten doen. Is een aanval met ransomware een datalek? En moeten we dat melden bij de AP?

Als ransomware bestanden heeft versleuteld die persoonsgegevens bevatten, is dit een datalek. Dit betekent dat een organisatie het datalek bij de AP moet melden als het lek zorgt voor ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als een aanzienlijke kans bestaat dat dit gebeurt. Ook moet de organisatie de betrokkenen, de mensen van wie de persoonsgegevens zijn, meteen informeren als er (mogelijk) gevoelige gegevens zijn gelekt. Tenzij uit een technisch onderzoek blijkt dat het onwaarschijnlijk is dat er ongunstige gevolgen zijn voor de privacy van de betrokkenen. In dat geval hoeft de organisatie hen niet te informeren. De AP publiceerde kort na de berichtgeving over WannaCry vragen en antwoorden over ransomware op haar website.

Besmetting met ransomware door WannaCry

Datalek Uber

In november 2017 kwam een grootschalig datalek aan het licht bij taxibedrijf Uber. Hackers stalen al in 2016 persoonsgegevens van 57 miljoen klanten en 600.000 chauffeurs, waaronder die van ongeveer 174.000 Nederlandse passagiers en chauffeurs. Het gaat onder meer om namen, e-mailadressen, telefoonnummers en rijbewijsnummers. Volgens het taxibedrijf zijn er geen creditcardgegevens, bankrekeningnummers, geboortedata en ritlocatiegeschiedenissen gelekt. Privacytoezichthouders uit België, Duitsland, Frankrijk, Italië, Nederland, Spanje en het Verenigd Koninkrijk hebben een taskforce gevormd en onderzoeken het datalek bij Uber. De AP leidt deze taskforce.

AP leidt taskforce bij onderzoeken datalek Uber

Beveiliging

Organisaties zijn wettelijk verplicht om passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen. Dat betekent dat ze moderne techniek moeten gebruiken voor de beveiliging. Daarnaast moeten ze kijken naar hoe ze als organisatie met persoonsgegevens omgaan. Wie heeft er bijvoorbeeld toegang tot welke gegevens?

Onderzoek UWV

De AP stelde in november 2017 vast dat het UWV de wet overtrad bij de beveiliging van zijn online werkgeversportaal en bij verzuimbeheer. Het werkgeversportaal, waar werkgevers en arbodiensten ziekteverzuimgegevens van werknemers invoeren en bekijken, bleek onvoldoende beveiligd. Het UWV is verplicht om dit portaal goed te beveiligen met meerfactorauthenticicatie. Dat betekent dat de gebruiker zich op minimaal twee manieren moet authentiseren om toegang te krijgen. Bijvoorbeeld met een wachtwoord in combinatie met een pincode.

Het UWV verwerkt veel gevoelige persoonsgegevens van cliënten, zoals gegevens over hun gezondheid. Hiervoor gelden extra strenge regels. Uit onderzoek van de AP bleek dat de UWV-medewerkers die ziekmeldingen behandelen, daarvoor niet bevoegd zijn. Deze medewerkers vroegen aan werknemers die zich ziek meldden gegevens over hun gezondheid om de uitkeringsclaim te kunnen beoordelen. Dat mag alleen onder de verantwoordelijkheid van een arts en dat is bij het UWV niet het geval.

Het UWV is na deze conclusie een traject gestart om zijn werkwijze aan te passen. Het UWV heeft de AP ook toegezegd de beveiliging van het werkgeversportaal aan te passen. En dat de medewerkers verzuimbeheersing onder supervisie van een verzekeringsarts gaan werken.

UWV overtreedt wet bij verzuimbeheer en toegangsbeveiliging werkgeversportaal

Advies Cybersecuritywet

De AP adviseerde in oktober 2017 over het wetsvoorstel voor de Cybersecuritywet. Deze wet, die voortkomt uit Europese regelgeving, heeft als doel Nederland digitaal veiliger maken. In het wetsvoorstel staan bijvoorbeeld de digitale veiligheidseisen waar aanbieders van essentiële diensten aan moeten voldoen. Dat zijn diensten waar de maatschappij niet meer zonder kan, zoals drinkwater, energie en betalingsverkeer. Ook noemt het wetsvoorstel een meldplicht voor ICT-incidenten bij een daarvoor aangewezen Computer Security Incident Response Team (CSIRT).

De AP merkte op dat een ICT-incident ook een datalek kan zijn. En volgens de AVG moet een ernstig datalek bij de AP gemeld worden. De AP benadrukte dat bij zo'n incident de samenwerking tussen de AP, het betrokken CSIRT en de bevoegde autoriteit belangrijk is. Ook adviseerde de AP om andere partijen, zoals DigiD en MijnOverheid, onder het wetsvoorstel te laten vallen om zo te zorgen voor een landelijke dekking bij incidenten. Het voorstel voor de Cybersecuritywet is in februari van 2018 ingediend bij de Tweede Kamer. Het advies van de AP is grotendeels, in de vorm van intenties, opgenomen in de toelichting bij het voorstel.

Advies Cybersecuritywet

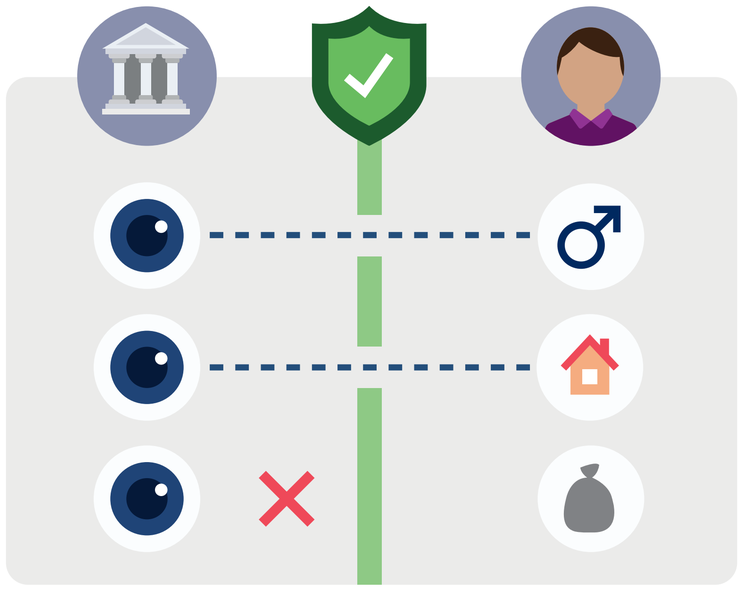
Overheid

Overheden vallen onder de grootste verwerkers van persoonsgegevens. Natuurlijk hebben overheidsinstanties – zoals gemeenten – persoonsgegevens nodig om hun taken te kunnen uitvoeren. Bijvoorbeeld om de inwoners te belasten voor afval, een rijbewijs te geven of huishoudelijke hulp toe te wijzen. Maar gemeenten moeten zich hierbij wel aan de privacywetgeving houden. En dus bijvoorbeeld niet meer persoonsgegevens verwerken dan noodzakelijk. Vaak zijn inwoners ook verplicht om hun persoonsgegevens aan de gemeente af te geven. Daarom moet iedereen erop kunnen vertrouwen dat gemeenten zorgvuldig met deze gegevens omgaan.

Onderzoek afvalpas

De Autoriteit Persoonsgegevens (AP) stelde in april 2017 na onderzoek vast dat de gemeente Arnhem via de afvalpas persoonsgegevens van inwoners verwerkte zonder dat dit noodzakelijk was voor de publiekrechtelijke taak van de gemeente. Een gemeente mag in het algemeen een afvalpassensysteem gebruiken voor ondergrondse afvalcontainers voor huishoudelijk afval. Maar een gemeente moet hiervoor wel een duidelijk doel hebben, zoals inwoners per hoeveelheid afval laten betalen.

De gemeente Arnhem wilde per 1 januari 2018 een nieuw afvalsysteem invoeren naar het principe 'de vervuiler betaalt'. Voor dit systeem is het noodzakelijk om persoonsgegevens te verwerken: om de kosten te berekenen moet de gemeente weten wie er wanneer afval aanbiedt. Met ingang van dit systeem zou de gemeente niet langer in strijd met de wet handelen. De AP zag daarom af van verdere handhaving.



In augustus 2017 kwam de AP terug op dat besluit. De gemeente maakte namelijk bekend dat er nog geen definitief besluit was genomen over het nieuwe systeem. De AP kon dus niet vaststellen dat de gemeente Arnhem op korte termijn niet langer de wet zou overtreden. De AP legde daarom een last onder dwangsom op. Als de gemeente Arnhem de overtreding niet zou beëindigen, dan kon de dwangsom oplopen tot 50.000 euro. De gemeente besloot hierna de afvalcontainers open te stellen en de persoonsgegevens te wissen.

AP legt gemeente Arnhem last onder dwangsom op voor gebruik afvalpas

Advies elektronisch aanvragen rijbewijs

In mei 2017 adviseerde de AP over een experiment met de elektronische aanvraag van rijbewijzen. Het experiment houdt in dat in een paar gemeenten mensen hun rijbewijs digitaal kunnen verlengen. Tot nu toe moeten mensen daarvoor naar het gemeentehuis gaan. Met het experiment wordt gekeken of dit sneller en makkelijker kan.

In het ontwerpbesluit voor het experiment stond onder meer dat een erkende fotograaf persoonsgegevens gaat verwerken, namelijk pasfoto's en handtekeningen. De AP stelde dat een fotograaf niet zomaar verantwoordelijk kan zijn voor die gegevensverwerking. Ook vroeg de AP te onderbouwen hoe de persoonsgegevens nauwkeurig verwerkt worden zonder een fysieke check van een medewerker van de gemeente. Hoe controleert de gemeente dat de aanvrager ook echt recht heeft op het rijbewijs?

De AP adviseerde bovendien een privacy impact assessment (PIA) te doen om de privacyrisico's duidelijk te krijgen.

Door het advies van de AP is het ontwerpbesluit op verschillende punten aangepast. Zo is onder meer duidelijk gemaakt wie de verantwoordelijke is voor de gegevensverwerking (de RDW) en wie de verwerker (de fotograaf), is onderbouwd dat de aanvrager wordt geïdentificeerd zonder een fysieke check bij de aanvraag, is de grondslag voor de gegevensverwerking aangepast en is een PIA uitgevoerd. Het kabinet heeft in september 2017 ingestemd met het voorstel voor het experiment.

Advies experiment elektronische aanvraag rijbewijzen

Brief over publicatie door gemeenten

De AP ontvangt regelmatig vragen en tips van mensen over de publicatie van hun persoonsgegevens door gemeenten. De gemeenten maken deze gegevens openbaar via besluitenlijsten, raadstukken, aanvragen en bezwaarschriften. Inwoners vinden dat de gemeente hun gegevens onterecht openbaar maakt.

Publicatie van persoonsgegevens, bijvoorbeeld op internet of in een dagblad, is een vorm van verwerking. Dat mag alleen als het noodzakelijk is om een wettelijke verplichting na te komen of om een publiekrechtelijke taak goed uit te voeren. Bovendien moet de gemeente nagaan of het doel ook met minder ingrijpende middelen kan worden bereikt.

In oktober 2017 stuurde de AP daarom een brief aan de Vereniging Nederlandse Gemeenten (VNG). In de brief maakte de AP duidelijk wat wel en niet mag bij het actief publiceren van persoonsgegevens. De AP verzocht de VNG om gemeenten hierover te informeren.

AP wijst gemeenten op privacyregels bij publicatie persoonsgegevens burgers

'Kosten inzage eigen dossier liggen vast'

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Een tipgever vertelde ons dat haar gemeente veel geld vroeg voor inzage in haar eigen dossier. Zij kon haar dossier alleen inzien door ter plekke te komen kijken. De gemeente bracht de kosten van de aanwezige ambtenaar in rekening (76 euro per uur), plus bijkomende kosten voor eventuele kopieën. Dat mag niet. Voor inzage mogen organisaties van de wet een vergoeding vragen van € 0,23 per kopie met een maximum van € 5,-. Tenzij het om bijvoorbeeld een heel groot dossier gaat, dan is het maximumbedrag € 22,50. Per 25 mei 2018, als de nieuwe Europese privacywet geldt, mogen organisaties zelfs helemaal geen kosten meer rekenen. Ik heb contact opgenomen met de gemeente. Die heeft, vooruitlopend op de nieuwe wet, besloten om geen geld meer te vragen voor inzage.'

Politie & justitie

Politie en justitie werken vaak met gevoelige informatie om de veiligheid te bevorderen. Door het uitwisselen van persoonsgegevens, ook internationaal, kunnen ze hun werk nog beter doen. Maar voordat ze nieuwe bevoegdheden krijgen die een ernstige inbreuk maken op de privacy, moet dat zorgvuldig worden afgewogen. En ook moet worden gecontroleerd of ze de afspraken over het werken met gevoelige informatie naleven. Het kan niet zo zijn dat mensen ten onrechte in een systeem komen te staan waardoor ze bijvoorbeeld worden aangehouden bij de grens. Of dat het onduidelijk is wat er met passagiersgegevens wordt gedaan bij terrorismebestrijding.

Onderzoek SIRENE

De EU-lidstaten wisselen (persoons)gegevens uit om de grenzen van het Schengengebied te bewaken en justitiële taken uit te voeren. De bevoegde autoriteiten in de lidstaten, zoals politie en justitie, delen deze gegevens via verschillende informatiesystemen. Een van die systemen is het Schengen Informatiesysteem II (SIS II). In SIS II staat informatie over bijvoorbeeld gezochte of vermiste personen of gestolen voertuigen. Op basis van deze signaleringen kunnen personen en goederen bij de grens van het Schengengebied worden tegengehouden.

Op Europees niveau is een aantal afspraken gemaakt waaraan de partijen die SIS II gebruiken zich moeten houden. Verkeerde signalering in SIS II kan namelijk grote gevolgen hebben, bijvoorbeeld dat iemand onterecht wordt aangehouden bij de grens of zelfs langere tijd het Schengengebied niet in of uit kan. Het is daarom heel belangrijk dat er zorgvuldig wordt geregistreerd in het systeem. Mensen mogen niet ten onrechte in het systeem staan, hun gegevens moeten kloppen en signaleringen moeten op tijd worden verwijderd. De Autoriteit Persoonsgegevens (AP) controleert periodiek of de partijen die in Nederland SIS II gebruiken de afspraken voor zorgvuldigheid nakomen.

In februari 2017 publiceerde de AP onderzoek naar het SIRENE-bureau van de politie. Dit bureau is verantwoordelijk voor de gegevensuitwisseling met de EU-lidstaten over signaleringen in SIS II. De AP constateerde dat de politie onvoldoende zicht heeft op deze signaleringen. De politie bleek onder meer vastgelegde werkprocessen en procedures niet na te komen.

De politie heeft na het onderzoek van de AP verschillende maatregelen genomen om de politiegegevens in SIS II juist en nauwkeurig te verwerken. Zo worden onder meer de signaleringen beter gecontroleerd. Verder delen mensen uit verschillende politie-eenheden die met het systeem werken hun kennis, ontwikkelingen en best practices.
Tot slot doet de politie in 2018 een kwaliteitscontrole en neemt daarbij de bevindingen van de AP mee. Door deze verbeteringen zag de AP geen aanleiding om op te treden.

AP: Politie heeft onvoldoende zicht op signaleringen Schengenlanden

Advies passagiersgegevens

De minister van Veiligheid en Justitie vroeg de AP begin 2017 te adviseren over het wetsvoorstel Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven. In dat voorstel staan regels die luchtvaartmaatschappijen verplichten persoonsgegevens van passagiers (PNR-gegevens) aan een speciale passagiersinformatie-eenheid door te geven. Deze eenheid verwerkt de PNR-gegevens voor instanties die bevoegd zijn om terrorisme en criminaliteit te bestrijden.

De AP concludeerde dat het wetsvoorstel voorbarig was en adviseerde de minister het niet in deze vorm in te dienen. Het voorstel was namelijk nog niet aangepast aan de nieuwe Europese privacyregelgeving die per 25 mei 2018 geldt. Daarnaast moest er nog een uitspraak worden afgewacht van het Hof van Justitie van de EU over het PNR-verdrag tussen de EU en Canada.

De AP gaf ook aan dat het uitwisselen van passagiersgegevens voor vluchten binnen Europa onvoldoende werd onderbouwd in het voorstel en dat de verwerking van bijzondere persoonsgegevens niet goed was geregeld. Ook was het onduidelijk wat die speciale passagiersinformatie-eenheid wel en niet doet bij het verwerken van persoonsgegevens.

Advies Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven (implementatie PNR-richtlijn)

Advies ANPR-gegevens politie

Met ANPR (Automatic Number Plate Recognition) scant een camera kentekens van voorbijrijdende voertuigen. Deze kentekens worden vergeleken met een lijst kentekens van personen die door de politie worden gezocht of die bijvoorbeeld boetes hebben open staan. De AP gaf in mei 2017 advies over het ontwerpbesluit vastleggen en bewaren kentekengegevens door de politie. In dat ontwerpbesluit staan regels over bijvoorbeeld de inzet en afstelling van de ANPR-camera's, toegestane foutmarges, toegang tot de ANPR-gegevens, vastlegging (logging) van de raadpleging, automatische vernietiging en beveiliging van gegevens. In het besluit staan ook voorwaarden waaronder de politie ANPR-gegevens aan het buitenland mag geven.

De AP adviseerde een aantal punten in het ontwerpbesluit te verduidelijken. Bijvoorbeeld waarom de regels voor het doorgeven van gegevens aan derden anders zijn dan voor verstrekking aan het buitenland of de BES-eilanden. Daarnaast adviseerde de AP om de regels voor de beveiliging van de ANPR-gegevens uit te breiden. En meer informatie op te nemen over bijvoorbeeld persoonsgebonden authenticatie en de begrippen 'wissen' versus 'vernietigen'. Als gevolg van het advies van de AP is een aantal bepalingen van het ontwerpbesluit duidelijker gemaakt, zoals de beveiligingseisen en de regels voor doorgifte van ANPR-gegevens aan het buitenland.

Advies ontwerpbesluit ANPR

Advies VOG politiegegevens

De AP adviseerde in september 2017 over het wetsvoorstel VOG politiegegevens. Het doel van dit voorstel is om mensen die solliciteren op bepaalde overheidsfuncties een verklaring omtrent het gedrag (VOG) te kunnen weigeren op basis van relevante politiegegevens. Het gaat dan om functies die zo'n hoge mate van integriteit vereisen dat de sollicitant van onbesproken gedrag moet zijn. Vooralsnog is het alleen mogelijk om een VOG te weigeren als er óók relevante justitiële gegevens over de aanvrager bekend zijn.

De AP adviseerde onder meer om de noodzaak van het wetsvoorstel verder te onderbouwen, daarbij te beargumenteren waarom de bestaande screening van overheidspersoneel niet zou voldoen en om duidelijker te maken voor welke functies het voorstel geldt. De AP adviseerde bovendien een privacy impact assessment (PIA) te doen om de voor- en nadelen en de privacyrisico's van het wetsvoorstel duidelijk te maken. En om zo een gedegen beoordelingskader te kunnen opstellen om te bepalen of de politiegegevens relevant zijn voor de functie waarvoor de VOG is aangevraagd. Naar aanleiding van het advies van de AP is een PIA uitgevoerd.

Advies VOG politiegegevens

Advies implementatie Richtlijn gegevensbescherming politie en justitie

In april 2017 adviseerde de AP over het wetsvoorstel dat de Europese Richtlijn gegevensbescherming politie en justitie omzet naar Nederlandse wetgeving. Met dit voorstel worden de huidige Wet politiegegevens (Wpg) en Wet justitiële en strafvorderlijke gegevens (Wjsg) aangepast.

Toepassing Richtlijn

Allereerst vindt de AP dat de voorgestelde wijzigingen in de Wpg en de Wjsg niet genoeg overeenkomen met de aanpassingen die nodig zijn en volgen uit de tekst van de Richtlijn. Het toepassingsgebied van de Richtlijn is volgens de AP breder dan het wetsvoorstel omschrijft. Een van de gevolgen hiervan is dat niet steeds duidelijk is voor welke toepassingen, zoals de hulpverleningstaak van de politie, deze Richtlijn geldt en voor welke andere de Algemene verordening gegevensbescherming (AVG).

Boetebevoegdheid

De AP heeft geadviseerd de boetebepalingen in het voorstel meer in lijn te brengen met de boetemogelijkheden van de AVG. Er wordt in de Wpg namelijk maar één artikel voorgesteld waarbij oplegging van een boete mogelijk is en de hoogte daarvan is relatief laag. De AP vindt het verschil te groot met de bepalingen van de AVG, waarbij boetes kunnen worden opgelegd voor een groot aantal overtredingen van de wet en de boetes voor overheidsorganisaties hoog kunnen oplopen.

Beveiliging

De AP vindt dat de voorgestelde bepaling die de regels voor de beveiliging van persoonsgegevens die politie en justitie verwerken beschrijft, onvoldoende overeenkomt met de voorschriften voor informatiebeveiliging die de Richtlijn stelt.

Waarborgen
De AP heeft geadviseerd om betere waarborgen aan te brengen voor het verwerken van bijzondere persoonsgegevens. Ook zouden er volgens de AP betere waarborgen moeten zijn als politie of justitie, bijvoorbeeld door analyse van big data, geautomatiseerde besluiten neemt of profilering toepast.

Doorgifte van gegevens
Tot slot heeft de AP geadviseerd om de regels voor doorgifte van gegevens door politie of justitie buiten de EU aan te passen aan wat daarover in de Richtlijn staat.

Toezicht Europol

Om criminaliteit en terrorisme te bestrijden verwerkt Europol persoonsgegevens. Per 1 mei 2017 is het toezicht op de verwerking van persoonsgegevens door Europol veranderd. Het toezicht is sinds deze datum in handen van de European Data Protection Supervisor (EDPS). Dat is de onafhankelijke privacytoezichthouder van de EU. Voorheen hield de Joint Supervisory Body (JSB) Europol toezicht. De JSB Europol bestond uit leden van de nationale privacytoezichthouders van de EU-lidstaten, waaronder de AP.
De nationale toezichthouders houden sinds 1 mei 2017 alleen nog rechtstreeks toezicht op de gegevensuitwisseling tussen de nationale opsporingsdienst (in Nederland is dat de politie) en Europol. Verder hebben de toezichthouders een adviserende rol.

Gewijzigd toezicht op Europol door nieuwe Europolverordening

Internationaal

De verwerking van persoonsgegevens houdt niet op bij de Nederlandse grens. Het is daarom belangrijk dat alle EU-lidstaten de privacywetgeving op een gelijke manier toepassen. En dat persoonsgegevens die wereldwijd uitgewisseld worden, bijvoorbeeld met de Verenigde Staten, even goed beschermd zijn als binnen de EU. Hoe pak je internationale bedrijven aan als zij de privacywetten overtreden? De Autoriteit Persoonsgegevens (AP) doet eigen onderzoek, maar werkt ook nauw samen met collega-toezichthouders van over de hele wereld. Omdat het soms krachtiger is om samen een vuist te maken. En natuurlijk ook om van elkaar te leren.

Europese samenwerking

De AP nam ook in 2017 deel aan het overlegorgaan van Europese privacytoezichthouders, de Artikel 29-werkgroep (Working Party 29, afgekort WP29). WP29 speelt een grote rol in de totstandkoming van Europees beleid voor de bescherming van persoonsgegevens. Een van de belangrijkste taken van WP29 is ervoor te zorgen dat de EU-privacywetgeving in alle EU-lidstaten hetzelfde wordt uitgelegd. Ook doet WP29 onderzoek en adviseert de werkgroep de Europese Commissie (EC) over de bescherming van persoonsgegevens.

Opinie ePrivacyverordening

Naast de nieuwe Europese privacywet, de Algemene verordening gegevensbescherming (AVG), bestaat er een Europese e-privacyrichtlijn. Die is specifiek bedoeld voor de verwerking van persoonsgegevens voor elektronische communicatiediensten. Voorbeelden hiervan zijn telemarketing (telefonische verkoop) en online marketing via e-mails of met cookies. De Europese Commissie wil de e-privacywetgeving herzien, omdat elektronische communicatie de afgelopen jaren enorm is ontwikkeld en gegroeid.

WP29 heeft het voorstel voor een nieuwe ePrivacyverordening van de EC in 2017 beoordeeld en gevraagd om het voorstel op een aantal punten aan te passen. Bijvoorbeeld als het gaat om cookiemuren, die gebruikers dwingen om toestemming te geven om gevolgd te worden als ze toegang willen krijgen tot een bepaalde dienst. De ePrivacyverordening zou volgens WP29 cookiemuren moeten verbieden.

Europese privacytoezichthouders publiceren opinie ePrivacyverordening

EU-VS privacyschild

Sinds juli 2016 bestaat het EU-VS privacyschild (Privacy Shield). Het doel hiervan is dat persoonsgegevens die uitgewisseld worden met de Verenigde Staten (VS) op hetzelfde niveau worden beschermd als binnen de EU. De Europese Commissie controleerde in het najaar van 2017 of dit privacyschild goed werkt. WP29 had bij deze

controle een aantal punten van kritiek. Bijvoorbeeld over het ongericht verzamelen van gegevens door Amerikaanse inlichtingendiensten en over de bevoegdheden van de ombudspersoon.

Deze kritiekpunten zijn doorgegeven aan de VS. Verder hebben alle Europese privacytoezichthouders klachtenformulieren op hun websites gepubliceerd waarmee burgers eventuele klachten kunnen indienen over het gebruik van hun persoonsgegevens door Amerikaanse bedrijven of organisaties.

Privacytoezichthouders bereiden eerste jaarlijkse controle EU-VS privacyschild voor

Opinie privacyrechten werknemers

Met alle nieuwe technische mogelijkheden kunnen werkgevers het gedrag van hun medewerkers steeds gemakkelijker systematisch volgen. Voorbeelden hiervan zijn technologie om internetverkeer te beveiligen, het gebruik van wearables en het gebruik van persoonsgegevens uit sociale media van (toekomstige) werknemers. WP29 vindt dat er meer balans moet komen tussen de legitieme belangen van de werkgever enerzijds en de bescherming van de privacy van werknemers anderzijds.

WP29 gaf in juli 2017 in een opinie aan hoe werkgevers nieuwe technologie op een privacyvriendelijke manier kunnen inzetten. De Europese toezichthouders benadrukten dat werkgevers zich zelden of nooit kunnen beroepen op de toestemming van medewerkers om hun persoonsgegevens te verwerken. Dit komt omdat werknemers afhankelijk zijn van hun werkgever en daarom meestal geen vrije toestemming kunnen geven.

Werkgevers zullen voor monitoringtechnologieën meestal aangewezen zijn op de grondslag van de noodzaak van 'de behartiging van hun gerechtvaardigd belang'. Werkgevers mogen bij deze grondslag het gedrag van medewerkers alleen volgen als dit noodzakelijk is, ze het doel niet op een andere manier kunnen bereiken en de verwerking proportioneel is. Daarnaast moeten werkgevers hun werknemers goed informeren.

Opinie Europese privacytoezichthouders over privacyrechten werknemers

Wereldwijde samenwerking

Privacytoezichthouders uit de hele wereld hebben in september 2017 tijdens een internationale privacyconferentie in Hong Kong afspraken gemaakt om effectiever te gaan samenwerken bij handhaving. Op initiatief van de AP en de Britse privacytoezichthouder Information Commissioner's Office (ICO) is een bestaande internationale overeenkomst over handhavingssamenwerking zo aangepast dat de toezichthouders zelf bepalen welke gegevens zij internationaal willen delen. De privacytoezichthouders werden het ook eens over een aantal uitgangspunten om samenwerking makkelijker te maken. De AP gaat samen met de

Britse en Canadese toezichthouders onderzoek doen naar de haalbaarheid van een internationaal kaderverdrag. De eerste bevindingen worden in oktober 2018 tijdens de volgende internationale conferentie voor privacytoezichthouders bekendgemaakt.

Privacytoezichthouders wereldwijd versterken samenwerking bij handhaving

‘Toezichthouders kijken wereldwijd over grenzen heen. In deze tijd van groeiend internationaal dataverkeer is een zo sterk mogelijk verbond van privacytoezichthouders onmisbaar.’

Wilbert Tomesen, vicevoorzitter van de AP

Internationale doorgifte persoonsgegevens

Internationale organisaties of multinationals geven persoonsgegevens door tussen verschillende vestigingen. Soms zijn dat vestigingen buiten de EU, die persoonsgegevens niet op hetzelfde niveau beschermen als in de EU. Om toch persoonsgegevens uit te kunnen wisselen, moeten organisaties interne gedragscodes opstellen voor het gegevensverkeer binnen de eigen organisatie. Dit worden binding corporate rules (BCR’s) genoemd. In BCR’s legt een organisatie vast hoe het deze persoonsgegevens beschermt bij het doorgeven naar landen zonder passend beschermingsniveau. BCR’s moeten in overeenstemming zijn met de Europese privacywetgeving. De Europese privacytoezichthouders moeten de BCR’s goedkeuren.

De AP beoordeelt de BCR’s wanneer de hoofdvestiging van een bedrijf in Nederland staat en ook juridisch aansprakelijk is bij inbreuk op de privacy. De AP keurde in 2017 vijf BCR’s goed: van Koninklijke Vopak, Arcadis N.V., TNT Express, Univar en Cisco Systems.

Organisatie

In 2017 bereidde de Autoriteit Persoonsgegevens (AP) zich intensief voor op de nieuwe Europese privacywetgeving die per 25 mei 2018 geldt: de Algemene verordening gegevensbescherming (AVG) en de Richtlijn voor gegevensverwerking door politie en justitie. Door deze wetgeving krijgt de AP er nieuwe taken en bevoegdheden bij. De AP is daarom in 2017 gereorganiseerd. Een belangrijke taak in 2017 was voorlichting geven over de nieuwe wet. Daarnaast ging het reguliere werk van de AP natuurlijk gewoon door.

Nieuwe privacyregels vragen om nieuwe organisatie

De nieuwe Europese privacywetgeving brengt niet alleen ingrijpende veranderingen mee voor de bescherming van persoonsgegevens, maar ook voor het toezicht en de toezichthouder. De AP krijgt er nieuwe taken en bevoegdheden bij, onder meer op het gebied van Europese samenwerking met haar collegatoezichthouders en de behandeling van klachten van burgers.

Wanneer de AVG en de Richtlijn voor politie en justitie in 2018 van toepassing worden, zal de Wet bescherming persoonsgegevens (Wbp) worden ingetrokken. Hierdoor wordt de bestaande organisatie van de AP opgeheven en gaan de medewerkers van rechtswege over naar de nieuwe organisatie. De nieuwe organisatie heeft een grotere omvang en een andere vorm.

De AP is daarom in 2017 gereorganiseerd, zodat zij op 1 januari 2018 al zo veel mogelijk is ingericht voor de nieuwe uitvoeringspraktijk. De AP heeft onder meer een nieuwe managementstructuur gekregen, met vier directies. Ook introduceert de AP een nieuwe vorm van toezicht: systeemtoezicht. Dit is toezicht op de manier waarop organisaties hun interne toezicht op de naleving van de privacyregels hebben geregeld. Deze vorm van toezicht is een aanvulling op controlerende onderzoeken, handhaving en communicatie.

Organogram van de nieuwe AP

Groei AP

Het onafhankelijke bureau Andersson Elffers Felix (AEF) onderzocht in 2017 hoeveel mankracht en middelen de AP nodig heeft om in de toekomst goed toezicht te kunnen houden. Het adviesbureau berekende aan de hand van drie mogelijke scenario's een groei van bijna 2,5 tot 3,5 keer de huidige formatie van de AP. Het onderzoeksrapport over de toekomstige organisatie van de AP is in juni 2017 aan de Tweede Kamer gestuurd.

Nieuwe Europese privacywetgeving vereist groei Autoriteit Persoonsgegevens

Organisatiecijfers

In 2017 was het budget van de AP 10,5 miljoen euro. Dat is ruim 2 miljoen euro meer dan het budget van 2016 (8,1 miljoen euro). Dat heeft onder meer te maken met de voorbereidingen op de nieuwe privacywetgeving. Het ministerie van Justitie en Veiligheid heeft de AP hiervoor 1 miljoen euro extra budget toegekend. Gedurende het jaar is het budget extra opgehoogd, onder meer vanwege hogere loonkosten door de cao-verhoging. De uitgaven van de AP hebben het budget desondanks overschreden met 3,6%. De oorzaak daarvan ligt in de uitbreiding van werkzaamheden en de voorbereidingen op de AVG.

De bezetting eind 2017 was 102,69 fte. Eind 2016 was dat 73,10 fte. Ook deze toename is een gevolg van de voorbereidingen op de nieuwe privacywetten. Deze groei is in lijn met de afspraken met het ministerie van Justitie en Veiligheid.

De AP gebruikt een groot deel van haar capaciteit om onderzoek te doen naar de naleving van de wet. In 2017 rondde de AP 200 onderzoeken af, inclusief onderzoeken naar datalekken. De AP heeft 217 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 AP is adviseren over nieuwe wet- en regelgeving. In 2017 bracht de AP 28 keer advies uit.

Bijlage jaarverslag 2017 voor alle organisatiecijfers uit 2017

Publieksvoorlichting

De afdeling Frontoffice van de AP beantwoordt vragen en behandelt tips over (mogelijke) overtredingen van de privacywetgeving. In 2017 kreeg de AP 9.501 vragen en tips. Dit aantal is met bijna 8% toegenomen ten opzichte van 2016.

De meeste vragen en tips gingen, net als in 2016, over de sector handel & dienstverlening (32,2%). En dan vooral over financiële dienstverlening en detailhandel. Ook waren er veel vragen en tips over de sectoren overheid (15,0%), met name over gemeenten. Tips en vragen over de sector zorg & welzijn (13,3%) gingen vooral over medische zorg. En bij de sector arbeid (10,7%), ging het vooral over werkgevers. De minste vragen en tips kwamen binnen over internationale organisaties (0,8%).

Voorlichting en communicatie

Door voorlichting aan bedrijven en overheidsorganisaties bevordert de AP dat zij de wettelijke privacyregels (beter) naleven. Een belangrijke taak in 2017 was het informeren over de nieuwe Europese privacywetgeving, waarover begrijpelijkerwijs veel organisaties vragen hadden. Tegelijkertijd staat de AP dagelijks mensen te woord, zodat zij weten wat hun rechten zijn en zij zelf in actie kunnen komen. Ook zoekt de AP geregeld actief contact met de pers en maatschappelijke organisaties.

Zie ook: hoofdstuk 1. Nieuwe Europese privacywetgeving

Top 3 sectoren onder vragen en tips

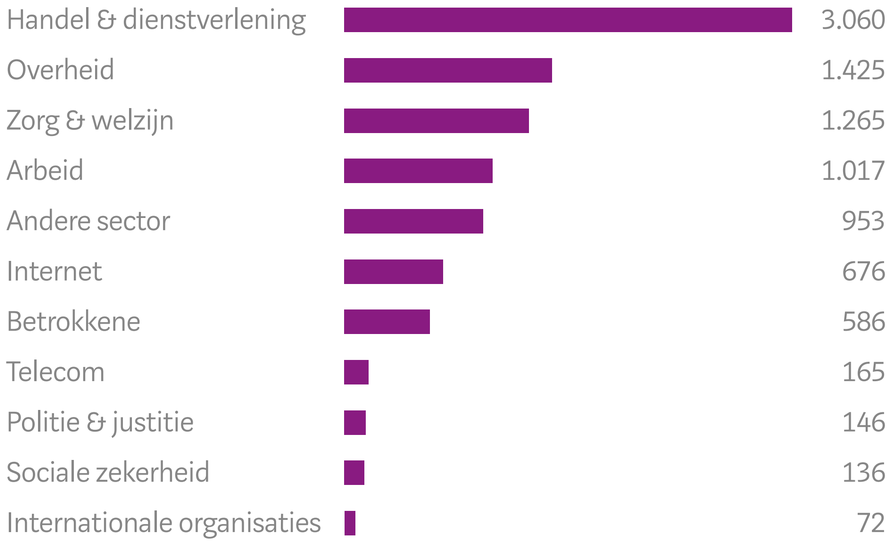
32,2%
Dienstverlening

15%
Overheid

13,3%
Medische zorg

De meest voorkomende onderwerpen waren identificatie en/of de registratie van het burgerservicenummer (BSN), derdenverstrekking (organisaties die persoonsgegevens aan andere organisaties doorgeven), datalekken, beveiliging en internet.

Vragen en tips 2017



Wat doet de AP met tips?
Frontoffice analyseert alle binnengekomen tips en geeft vervolgens de tips over (waarschijnlijke) overtredingen door aan de afdelingen Toezicht. Deze tips kunnen reden zijn om een onderzoek te starten. De AP kan er ook voor kiezen om niet direct een officieel onderzoek te starten, maar eerst een alternatieve interventie in te zetten. Zo kunnen waarschuwingsbrieven en/of gesprekken met bedrijven of organisaties al genoeg zijn om overtredingen te laten beëindigen.

In 2017 heeft Frontoffice 217 zaken alternatief behandeld. Frontoffice verstuurde in verschillende situaties waarschuwingsbrieven, vooral over (1) identiteitsbewijzen kopiëren en het BSN verwerken, (2) zaken binnen de arbeidsrelatie en (3) beveiliging. Daarnaast heeft Frontoffice in 2017 verschillende waarschuwingsgesprekken gevoerd, waarvan veruit de meeste gingen over het onrechtmatig kopiëren van identiteitsbewijzen en verwerken van het BSN.

Bijlage jaarverslag 2017 voor meer informatie over de vragen en tips aan de AP in 2017

Persvoorlichting

De AP heeft in 2017 658 keer contact gehad met de media. Het ging hierbij onder meer om het beantwoorden van persvragen, interviews en radio- en televisieoptredens. Vooral de nieuwe EU-privacywetgeving was onderwerp van gesprek. Maar ook gezondheidsgegevens, websites en apps – en dan vooral de beveiliging hiervan – waren onderwerpen die vaak voorkwamen.

Aantal perscontacten in 2017

Landelijke radio en televisie	238
Landelijke dagbladen	144
Overig	72
(Vak)bladen	52
Online-media	50
Regionale dagbladen	36
Persbureaus	34
Regionale radio en televisie	24
Internationale dagbladen	8
Totaal	**658**

Externe optredens

In 2017 bestond een belangrijk deel van de werkzaamheden uit externe optredens. De voorzitter, de vicevoorzitter, managers en medewerkers van de AP hielden een groot aantal (keynote)speeches en presentaties. Het belangrijkste onderwerp was hierbij de nieuwe EU-privacywetgeving. Ook gingen presentaties over de bescherming van persoonsgegevens in de zorg, bij gemeenten en in de arbeidsrelatie. Daarnaast gaven de voorzitter en vicevoorzitter interviews aan zowel (inter)nationale radio en televisie als geschreven pers.

Eerste Kamer en Tweede Kamer

De vicevoorzitter sprak in januari 2017 tijdens een rondetafelgesprek in de Tweede Kamer over antidopingbeleid. In mei bood de voorzitter de leden van de vaste Kamercommissie voor Veiligheid en Justitie het Jaarverslag 2016 aan. Hij had daarbij ook een gesprek met de leden, met een terugblik op 2016 en een vooruitblik naar 2017. De voorzitter nam in juni deel aan een hoorzitting in de Eerste Kamer over het wetsvoorstel computercriminaliteit-III. In november sprak de voorzitter tijdens een hoorzitting in de Tweede Kamer over PSD2.

Markttoezichthoudersberaad

De AP nam ook in 2017 zowel op bestuurlijk als ambtelijk niveau actief deel aan het Markttoezichthoudersberaad (MTB), een samenwerkingsverband van Nederlandse toezichthouders. Het MTB bestaat, naast de AP, uit de Autoriteit Consument & Markt (ACM), Autoriteit Financiële Markten (AFM), Commissariaat voor de Media (CvdM), De Nederlandsche Bank (DNB), Kansspelautoriteit en Nederlandse Zorgautoriteit (NZa).

Leden van de Autoriteit en directeur

Mr. A. (Aleid) Wolfsen
Voorzitter

Mr. W.B.M. (Wilbert) Tomesen
Vicevoorzitter

Drs. B.D. (Bas) den Hollander
Algemeen directeur (a.i.)
(per 15 augustus 2017)

Raad van advies

De raad van advies van de AP adviseert over de hoofdlijnen van het beleid van de AP en andere algemene aspecten van de bescherming van persoonsgegevens. De leden zijn afkomstige uit verschillende maatschappelijke sectoren.

Leden raad van advies

In 2017 waren de leden van de raad van advies:

Mevrouw drs. T.A. Maas-de Brouwer (voorzitter)
Voorzitter Utrecht Development Board. Voorzitter Alliantie Medezeggenschap en Governance. Lid bestuur SIDN fonds. Lid Accreditatie Commissie NVZD. Lid bestuur stichting Vrienden Anne Frank Huis.

De heer J.J. van Aartsen
Waarnemend burgemeester van Amsterdam. Waarnemend commissaris van de Koning van de provincie Drenthe. Oud-burgemeester van 's-Gravenhage.

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

De heer mr. G.W. van der Burg
Voorzitter van het College van procureurs-generaal.

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

Mevrouw prof. dr. H.M. Dupuis
Emeritus hoogleraar medische ethiek, Universiteit van Leiden. Voorzitter raad van toezicht Woonzorgcentra Haaglanden. Voorzitter Vereniging Gehandicaptenzorg Nederland. Lid Adviescommissie Pakket van het Zorginstituut Nederland.

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 de Veiligheid. Voorzitter Raad van Toezicht Rijksuniversiteit Groningen. Voormalig Nationaal Coördinator Terrorismebestrijding.

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

Mevrouw mr. C.E. Passchier
Vicevoorzitter International Labour Organization (ILO). Werknemersvoorzitter ILO. Lid Nationaal Contact Punt. Voormalig vicevoorzitter FNV.

Mevrouw ir. W.A.A. Peek-Vissers
Algemeen directeur Dell Nederland.

Mevrouw drs. M. Sint
Voorzitter Samenwerkende Topklinische opleidings Ziekenhuizen (STZ). Voorzitter Transitie Autoriteit Jeugd (TAJ).

De heer drs. L.J.E. Smits
Oud-directeur PBLQ

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

Colofon

Autoriteit Persoonsgegevens, Den Haag, april 2018

Ontwerp

Teldesign, Rotterdam

Fotografie

Leden Autoriteit: Emilie Hudig
Titelpagina's: Shutterstock

Autoriteit Persoonsgegevens

Bezoekadres:
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Postadres:
Postbus 93374
2509 AJ DEN HAAG

T 070 8888 500
F 070 8888 501

autoriteitpersoonsgegevens.nl

Telefonisch spreekuur:
maandag t/m vrijdag
09.00 - 17.00 uur:
0900 2001 201 (5 ct p/m)
m.i.v. 1 mei 2018: 088 1805 250