Jaarverslag 2016

AUTORITEIT
PERSOONSGEGEVENS

Voorwoord

Beveiliging & meldplicht datalekken

Internet & telecom

Gezondheid

Overheid

Werk

Politie & justitie

Dit jaarverslag gaat over de belangrijkste werkzaamheden van de AP uit 2016. Alle feiten en cijfers staan in de bijlage.

Internationaal

Organisatie

Voorwoord

Mensen moeten in een vrij land vrij kunnen leven. Maar hoe vrij ben je nog als je wordt gevolgd bij bijna elke stap die je – letterlijk en figuurlijk – zet? Via bijvoorbeeld camera's, gps, cookies, apps en zelfs je televisie en het wifisignaal van je telefoon? Alles wordt in kaart gebracht: onze gedachten, voorkeuren, gedrag, bewegingen. De grenzen tussen ons hoofd, lijf, huis en de buitenwereld vervagen. Bedrijven en ook de overheid zitten mensen steeds dichter op de huid. Sommige werkgevers vragen hun zieke werknemers de hemd van het lijf. Of proberen zelfs het beweeg- en slaappatroon van hun werknemers te achterhalen door hen een *wearable* te laten dragen. De gemeente komt letterlijk aan de keuken-tafel zitten. Politie en justitie willen iedereen op de voet kunnen volgen.

Wat gebeurt er vervolgens met al die informatie over ons? Krijgen we te horen dat onze gegevens zijn verzameld en waarom? Hebben we hier iets over te zeggen? En wat betekent het voor de manier waarop we worden benaderd en behandeld? Dat zijn belangrijke vragen die alleen maar belangrijker worden. Bescherming van je privacy en persoonsgegevens is een grondrecht, dat nauw samenhangt met fundamentele waarden als vrijheid, solidariteit en gelijkheid. Dat betekent dat mensen nog steeds zélf keuzes moeten kunnen maken, niet dat zij – op basis van hun 'profiel' – een voorgesorteerd programma krijgen of zelfs worden gediscrimineerd. De Autoriteit Persoonsgegevens (AP) komt als privacytoezichthouder op voor de bescherming van deze fundamentele waarden.

Sinds 1 augustus 2016 ben ik voorzitter van de AP. Ik ben bij de AP gekomen in een spannende tijd: in 2016 is, na een traject van enkele jaren, nieuwe Europese privacywetgeving aangenomen. Die nieuwe wet, de Algemene verordening gegevensbescherming (AVG), geldt vanaf 25 mei 2018. In de tussentijd hebben organisaties én de AP de kans zich voor te bereiden op de AVG. Onder de AVG krijgen organisaties meer verantwoordelijkheden en betrokkenen – de mensen van wie persoonsgegevens worden verwerkt – meer rechten. Ook krijgen alle Europese privacytoezichthouders steviger bevoegdheden, zoals de mogelijkheid om boetes op te leggen tot 20 miljoen euro. Ik ben er trots op aan het hoofd te mogen staan van een AP die bondgenoot wordt van betrokkenen, die organisaties adviseert en op weg helpt, maar die óók stevig optreedt als het moet.

Het grondrecht op privacy komt steeds meer onder druk te staan door de gigantische vlucht die dataverzamelingen hebben genomen. Natuurlijk leveren technologische ontwikkelingen ook grote voordelen op, niet in de laatste plaats voor de bedrijven die er geld mee verdienen. Maar ook consumenten hebben baat bij handige nieuwe producten en diensten. De AP juicht innovatie dan ook van harte toe – maar houdt wel een vinger aan de pols bij de manier waarop. Wordt er bij de ontwikkeling van een dienst of product vanaf het begin goed nagedacht over de privacyaspecten, dan weet ik zeker dat er veel mogelijk is. Zolang de juiste toetsen en waarborgen er zijn, kan de AP zich prima vinden in nieuwe producten en diensten. Ik ben ervan overtuigd dat we zo de juiste balans vinden en daarmee ons fundamentele recht op privacy en onze vrijheid kunnen blijven beschermen.

Aleid Wolfsen
Voorzitter van de Autoriteit Persoonsgegevens

Beveiliging & meldplicht datalekken

Verantwoord omgaan met persoonsgegevens valt of staat met een adequate beveiliging van de gegevens. De meeste mensen komen in honderden tot zelfs duizenden databases voor. Zij moeten erop kunnen vertrouwen dat hun persoonsgegevens goed beveiligd zijn. Slechte beveiliging kan ertoe leiden dat gevoelige gegevens op straat komen te liggen en vervolgens worden misbruikt, bijvoorbeeld voor identiteitsfraude. Net als in voorgaande jaren stond het onderwerp beveiliging in 2016 dan ook hoog op de agenda van de AP – al helemaal omdat op 1 januari 2016 de meldplicht datalekken in werking trad.

De AP vroeg in 2016 bij verschillende onderwerpen aandacht voor beveiligingsaspecten. Zo zorgde de AP ervoor dat de beveiliging van Suwinet verbeterde, liet de AP weten dat bij de ontwikkeling van het eID-stelsel het beveiligingsniveau van de inlogmiddelen omhoog moet en adviseerde de AP fysiotherapeuten over de beveiliging van het contactformulier op hun website. Maar verreweg de meeste aandacht van de AP ging in dit jaar naar de meldplicht datalekken en alles wat daaruit voortkwam.

Datalek?

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Er is dus niet alleen sprake van een datalek als er gegevens zijn vrijgekomen (gelekt), maar ook als er (zonder dat dit de bedoeling is):

- toegang is geweest tot gegevens;
- gegevens zijn vernietigd;
- gegevens zijn gewijzigd.

Meldplicht datalekken

Organisaties die een ernstig datalek hebben, moeten dit melden bij de AP en soms ook aan de mensen van wie de gelekte gegevens zijn. De meldplicht datalekken heeft tot doel om het beveiligingsniveau te verhogen en de zelfredzaamheid van mensen te vergroten. De AP ontving in 2016, het eerste jaar van de meldplicht, bijna 5700 meldingen van datalekken.

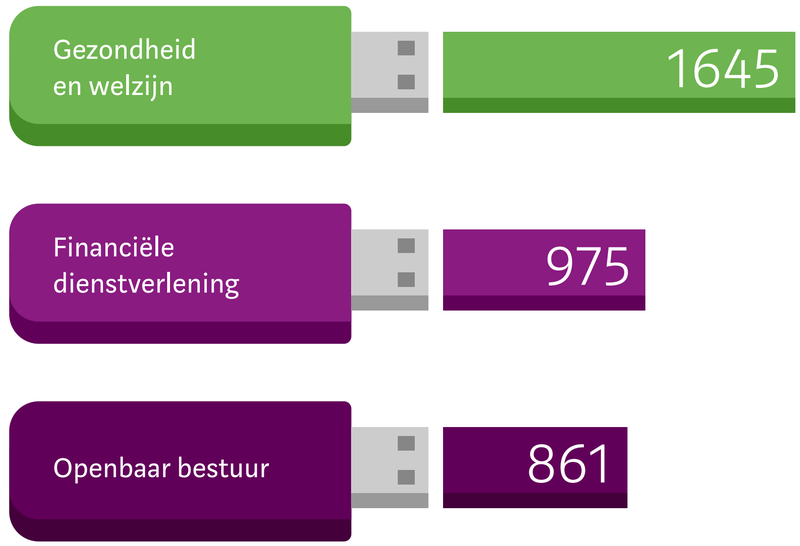
Het aantal mensen dat werd geraakt door een datalek varieerde per melding van één enkel persoon tot – in enkele gevallen – honderdduizenden betrokkenen.

Vaak voorkomende datalekken

- Een klant ziet in een klantportaal de gegevens van iemand anders.
- Iemand raakt een USB-stick of andere gegevensdrager kwijt waarop persoonsgegevens staan. De persoonsgegevens zijn dan vaak niet versleuteld.
- Een laptop of smartphone waar persoonsgegevens op staan wordt gestolen.
- Een poststuk met persoonsgegevens komt niet aan bij de ontvanger of komt geopend terug.
- Een e-mail met persoonsgegevens komt bij de verkeerde ontvanger terecht.

Meldingen van datalekken

Sector	Aantal	Perc.
Gezondheid en welzijn	1.645	28,9%
Financiële dienstverlening	975	17,1%
Openbaar bestuur	861	15,1%
Informatie en communicatie	662	11,6%
Vervoer	336	5,9%
Onderwijs	220	3,9%
Overige organisaties	191	3,4%
Specialistische zakelijke dienstverlening	176	3,1%
Overige zakelijke dienstverlening	139	2,4%
Energie	132	2,3%
Handel en autobranche	97	1,7%
Politie en justitie	72	1,3%
Industrie	69	1,2%
Onroerend goed	58	1,0%
Bouw	42	0,7%
Water en milieu	14	0,2%
Horeca	3	0,1%
Cultuur, sport en recreatie	1	0,0%
Totaal	**5.693**	**100%**



De meeste datalekken zijn gemeld vanuit de sectoren gezondheid en welzijn (28,9%), financiële dienstverlening (17,1%) en openbaar bestuur (15,1%). 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 burgerservicenummer (BSN). En dus moeten organisaties in deze sectoren – gezien de aard van de gegevens – eerder een melding doen.

Acties AP

Wat doet de AP met de datalekmeldingen?

De AP kan 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 om wijzen om de mensen van wie de gegevens zijn gelekt op de hoogte te stellen;
- (algemene) voorlichting geven naar aanleiding van een binnengekomen melding, bijvoorbeeld om andere organisaties bewust te maken van mogelijke beveiligingsrisico's.

Van de bijna 5700 meldingen heeft de AP in ruim vierduizend gevallen een eerste, oriënterend onderzoek gedaan. Ruim honderd organisaties kregen naar aanleiding hiervan een waarschuwing van de AP. In enkele andere tientallen gevallen is er sprake van een diepgaander onderzoek van de AP.

Datalek door ransomware

Wat te doen na een aanval met ransomware? Is dit een datalek? Moet ik het melden bij de AP? En de betrokkenen informeren? Wat kan ik verder doen? Deze vragen kreeg de AP geregeld. Daarom publiceerde de AP Q&A's over ransomware.

Bewustwording beveiliging

De bewustwording van het belang van beveiliging van persoonsgegevens is gegroeid. Steeds vaker ontvangt de AP vragen en tips over mogelijk onvoldoende beveiliging bij organisaties. Naar aanleiding hiervan heeft de AP in 2016 meer dan honderd organisaties waarschuwingen gegeven dat zij hun beveiliging op orde moeten brengen omdat er mogelijk een datalek kan ontstaan.

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Openbare computers goed beveiligen'

'Een verontruste klant van een bank belde ons. Hij had een van de publiekscomputers in zijn bankvestiging gebruikt om zijn jaaroverzicht te downloaden. Toen kwam hij erachter dat het pdf-bestand op de computer bleef staan, ook al had hij uitgelogd. Alle klanten die na hem de computer gebruikten, konden dus zijn jaaroverzicht inzien. Ik heb direct gebeld met het betreffende bankfiliaal en erop gewezen dat de bank beveiligingsmaatregelen moest nemen. De bank heeft het probleem meteen op landelijk niveau aangepakt. Alle openbare computers in alle vestigingen van de bank hebben nu een systeem dat automatisch alle gegevens verwijdert als de bezoeker een sessie beëindigt of als er langer dan een minuut geen activiteit is geweest op de computer.'

Internet & telecom

Tracking en tracing – als een postpakketje zijn mensen tegenwoordig overal te volgen. Dat websites tracking cookies plaatsen om hun bezoekers te volgen, is niet nieuw. Maar zelfs ziekenhuizen spelen gegevens van hun website-bezoekers door aan commerciële partijen, ontdekte de AP in 2016. Bovendien hoef je je niet op internet te bevinden om gevolgd te worden: ook door een winkelstraat lopen blijft niet onopgemerkt. En zit je thuis rustig tv te kijken, dan heb je kans dat je telecomprovider over je schouder meekijkt. Natuurlijk kan het ook voordelen opleveren als organisaties mensen beter leren kennen en hun aanbod daarop afstemmen. Maar mensen moeten wél weten dat dit gebeurt en zelf kunnen beslissen of ze dit willen.

Wifitracking

Verschillende organisaties maken gebruik van wifitracking. Hiermee kunnen zij mensen volgen via het wifisignaal van hun smartphone of tablet. Winkels gebruiken deze techniek om bedrijfseconomische informatie te genereren: hoeveel mensen passeren de winkel, hoeveel bezoekers gaan de winkel in en hoelang blijven zij op een bepaalde plaats in de winkel. Gemeenten en evenementenorganisatoren zetten wifitracking bijvoorbeeld in om loopstromen in kaart te brengen en bij te houden hoe lang bezoekers op een bepaalde plaats blijven.

Bluetrace

In juni 2016 legde de AP een last onder dwangsom op aan Bluetrace, een bedrijf dat de technologie voor wifitracking levert. Uit eerder onderzoek van de AP was namelijk gebleken dat Bluetrace locatiegegevens van winkelbezoekers en voorbijgangers verzamelde zonder hun hier goed over te informeren. Bovendien verzamelde en bewaarde Bluetrace meer gegevens dan noodzakelijk.

Bluetrace trof na het onderzoek maatregelen, maar die waren onvoldoende om de overtredingen te beëindigen. Inmiddels is Bluetrace gestopt met wifitracking in en rondom winkels. Daardoor zijn de resterende overtredingen beëindigd en hoeft Bluetrace geen dwangsom te betalen.

Brief

Daarnaast stuurde de AP in juni 2016 een brief aan Detailhandel Nederland en aan de VNG om winkels en gemeenten te wijzen op de wettelijke eisen voor wifitracking.

- AP legt wifi-tracker Bluetrace last onder dwangsom op
- AP wijst winkels en gemeenten op voorwaarden wifi-tracking
- Veelgestelde vragen over wifitracking

Voorwaarden wifitracking

In winkels

- De winkel informeert de klanten over de wifitracking.
- De wifitracking staat niet dag en nacht aan, maar alleen op bepaalde tijden.
- De winkel anonimiseert of vernietigt de verzamelde gegevens binnen 24 uur.

In de buurt van winkels

- De winkel anonimiseert of vernietigt de gegevens van mensen die langs de winkel lopen direct.
- De winkel verzamelt geen gegevens van mensen die naast, boven of tegenover de winkel wonen door de muren van hun woning heen.

Op straat door de gemeente

- De gemeente gebruikt wifitracking om een publieke taak uit te voeren en heeft een wettelijke bevoegdheid.
- De gemeente informeert het publiek over de wifitracking.
- De wifitracking staat niet altijd aan, maar alleen tijdens bijvoorbeeld grote evenementen.
- De gemeente anonimiseert of vernietigt de verzamelde gegevens direct.

Interactieve tv

XS4ALL en KPN, aanbieders van interactieve digitale televisie, beëindigden na onderzoek van de AP diverse overtredingen. De AP constateerde onder meer dat XS4ALL en KPN hun tv-klanten onvoldoende informeerden over het verzamelen en gebruiken van persoonsgegevens over het tv-kijkgedrag. KPN en XS4ALL stelden zonder toestemming van klanten kijkcijfers op over het tv-kijk-gedrag voor onder meer marktonderzoek, terwijl die gegevens nog herleidbaar waren. De AP concludeerde verder dat de bedrijven gegevens van klanten langer bewaarden dan noodzakelijk voor het doel.

XS4ALL en KPN hebben daarop hun systemen en de informatie in hun privacyverklaringen aangepast. Ook hebben de bedrijven de bewaartermijnen ingekort. Door de deels al tijdens het onderzoek genomen maatregelen zijn alle geconstateerde overtredingen beëindigd.

XS4ALL en KPN beëindigen privacyovertredingen interactieve tv

Cookies ziekenhuiswebsites

De AP onderzocht in 2016 de websites van alle Nederlandse zieken-huizen. Bij bijna de helft hiervan (39 van de 85) bleek via tracking cookies informatie van websitebezoekers doorgegeven te worden aan commerciële derde partijen. Wanneer mensen op de website

van een ziekenhuis informatie bekijken over specifieke aandoeningen of specialistische afdelingen, kan dit iets zeggen over hun gezondheid. Gegevens over iemands gezondheid verwerken mag in principe alleen met uitdrukkelijke toestemming van de persoon om wie het gaat.

De cookies werden op de apparatuur van de bezoekers van de ziekenhuiswebsites geplaatst zonder dat zij daarvoor toestemming hadden gegeven. Dat is dus in strijd met de wet. De AP heeft de 39 ziekenhuizen en de brancheorganisaties van de ziekenhuizen NVZ en NFU gewezen op de overtredingen. De AP is momenteel bezig om de websites van de ziekenhuizen opnieuw te controleren.

AP: ziekenhuiswebsites volgen in strijd met wet bezoekers via cookies

‘Als iemand de webpagina over de afdeling cardiologie bezoekt, mag hij vervolgens niet ongewild benaderd worden als mogelijk hartpatiënt.’

Wilbert Tomesen, vicevoorzitter van de Autoriteit Persoonsgegevens

Hardloop-app

Eind 2016 liet de AP weten dat Nike niet langer de wet overtreedt met de Nike+ Running app (tegenwoordig Nike+ Running Club). De AP stelde tijdens eerder onderzoek vast dat Nike de gebruikers van deze hardloop-app onvoldoende informeerde over de verwerking van hun gezondheidsgegevens. Nike kreeg daardoor niet de vereiste uitdrukkelijke toestemming van de appgebruikers. Nike had ook geen bewaartermijnen bepaald voor de gegevens.

Nike heeft tijdens en na het onderzoek maatregelen getroffen en daarmee de overtredingen beëindigd. Het bedrijf heeft nieuwe appversies uitgebracht waarin het toestemming vraagt voor het gebruik van gezondheidsgegevens. De informatie aan alle gebruikers is verbeterd en Nike heeft vaste bewaartermijnen ingevoerd.

Nike beëindigt overtredingen hardloop-app

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

‘Nieuw gsm-abonnement? Afgeschermde kopie van je paspoort!’

‘Een tipgever vertelde ons dat zij een nieuw gsm-abonnement had afgesloten. De koerier die haar simkaart kwam bezorgen, maakte een scan van haar paspoort. De vrouw had gehoord dat daarbij ter bescherming van haar privacy haar burgerservicenummer (BSN) en pasfoto zouden moeten worden afgeschermd. Maar de koerier weigerde om dat te doen. Ik heb contact opgenomen met de telecomaanbieder. Die mag, om telecomfraude tegen te gaan, een kopie of scan maken van het identiteitsbewijs van klanten. Maar daarbij moeten wél – precies zoals de vrouw dacht – het BSN en de foto worden afgeschermd. De telecomaanbieder heeft laten weten de koeriers nogmaals op de werkinstructie te wijzen, waarin dit juist staat vermeld.’

Beveiligingsprotocol

Begin maart maakte de AP bekend verscherpte aandacht te hebben voor het verouderde beveiligingsprotocol SSLv2. Aanleiding hiervoor was een lek in dit protocol. Door deze kwetsbaarheid kunnen kwaadwillenden toegang krijgen tot vertrouwelijke inhoud van het netwerkverkeer. De AP wees erop dat organisaties maatregelen moesten nemen, zoals het aanpassen van hun configuratie.

Verscherpte aandacht AP voor verouderd beveiligingsprotocol SSLv2

Google

In 2016 beëindigde Google de laatste van de privacyovertredingen die de AP eerder had geconstateerd. De AP eiste in 2015 maatregelen onder dreiging van een dwangsom. Google nam maatregelen waarmee een groot deel van de overtredingen al in 2015 werd beëindigd. In 2016 stelde de AP vast dat Google ondubbelzinnige toestemming vraagt van ál zijn gebruikers voor het gebruik van hun persoonsgegevens. Hierdoor is de resterende overtreding beëindigd en hoefde Google geen dwangsom te betalen.

Overtredingen Google beëindigd na optreden Autoriteit Persoonsgegevens

Gezondheid

Gegevens over iemands gezondheid behoren tot de gevoeligste persoonsgegevens die er zijn. Ze vallen dan ook onder de zogeheten bijzondere persoonsgegevens, die wettelijk extra zijn beschermd. En ook het medisch beroepsgeheim is er natuurlijk niet voor niets. Toch zijn er ontwikkelingen zichtbaar die de bescherming van gezondheidsgegevens onder druk zetten, zoals meer fraude-onderzoek in de zorg en de opkomst van online patiënten-portalen. Hoe legitiem het doel hiervan ook mag zijn, de strikte waarborgen voor het uitwisselen van gezondheidsgegevens mogen nooit uit het oog worden verloren. Zodat deze zeer persoonlijke gegevens niet terechtkomen bij mensen die er niets mee te maken hebben.

Privacyverklaring zorgverzekering

In februari 2016 heeft de AP een aantal grote zorgverzekeraars gevraagd of zij verwijsbrieven en behandelplannen opvragen van verzekerden met een privacyverklaring. Via een privacyverklaring kunnen ggz-patiënten regelen dat er op de declaratie aan hun zorgverzekeraar geen diagnosegegevens staan. Van de ondervraagde zorgverzekeraars bleek er één om een verwijsbrief te vragen. Dit is in strijd met de wet, omdat er zo diagnosegegevens naar de zorgverzekeraar gaan. Deze zorgverzekeraar is hier door het optreden van de AP mee gestopt.

De AP heeft daarna aan alle zorgverzekeraars in Nederland het juridisch kader gestuurd voor het opvragen van diagnose-informatie uit verwijsbrieven en behandelplannen van verzekerden met een privacyverklaring. Dit juridisch kader is afgestemd met de Nederlandse Zorgautoriteit, die toezicht houdt op de uitvoering van rechtmatigheidscontroles door zorgverzekeraars.

AP: opvragen verwijsbrief verzekerde met privacyverklaring mag niet

Juridisch kader in het kort

Formele controle (valt de declaratie onder het pakket van de verzekerde?)

- Zorgverzekeraars mogen niet vragen om een behandelplan of verwijsbrief.
- Ook medische adviseurs van zorgverzekeraars mogen dit niet.

Materiële controle (is de gedeclareerde behandeling uitgevoerd en was deze passend?)

- Zorgverzekeraars mogen vragen om een behandelplan of verwijsbrief, maar moeten hierbij strikte regels volgen.
- Zorgverzekeraars mogen zo'n controle niet uitvoeren alleen maar omdat iemand een privacyverklaring heeft.

Advies definitieve Regeling Jeugdwet

De AP adviseerde in juli 2016 over de definitieve Regeling Jeugdwet. Op grond van deze regeling mogen jeugdhulpverleners hun geheimhoudingsplicht doorbreken voor de bekostiging van de jeugdhulp. De regeling geeft regels voor de verwerking van persoonsgegevens door jeugdhulpverleners en gemeenten om

declaraties te betalen, controles uit te voeren en fraudeonderzoek te doen. De AP heeft er eerder (in 2015) op gewezen dat in de Jeugdwet het doorbreken van de geheimhoudingsplicht voor de bekostiging van jeugdhulp niet goed was geregeld. Dit advies van de AP heeft geleid tot aanpassing van de Jeugdwet en een tijdelijke ministeriële regeling. Die tijdelijke regeling is nu vervangen door de definitieve Regeling Jeugdwet.

De AP adviseerde in 2016 om op korte termijn ook te voorzien in regels voor de gegevens die jeugdhulpverleners en gemeenten mogen verwerken voor jeugdhulpvoorzieningen. Daarnaast adviseerde de AP om de toelichting op de definitieve Regeling Jeugdwet op een aantal punten aan te vullen en te verduidelijken.

AP adviseert over definitieve Regeling Jeugdwet

Beleidsregels machtigingsvereiste zorgpolis

De AP publiceerde in december 2016 de beleidsregels machtigingsvereiste zorgpolis. Deze beleidsregels geven zorgverzekeraars, zorgverleners en patiënten duidelijkheid over wat zorgverzekeraars wel en niet mogen bij het verwerken van persoonsgegevens voor het machtigingsvereiste. Dit vereiste houdt in dat een verzekerde vooraf toestemming van de zorgverzekeraar moet hebben voor de vergoeding van bepaalde behandelingen, geneesmiddelen, hulpmiddelen of zorgaanbieders.

Diagnosegegevens uit DIS

Informatie over diagnoses van patiënten in de ziekenhuiszorg, geestelijke gezondheidszorg en forensische zorg komt terecht in het landelijke Diagnose Informatie Systeem (DIS). Zorgverleners zijn wettelijk verplicht informatie aan het DIS te verstrekken over wat zij aan zorg hebben geleverd en gedeclareerd.

Het systeem wordt beheerd door de Nederlandse Zorgautoriteit (NZa). De informatie wordt – na pseudonimisering – gedeeld met verschillende derde partijen. De AP onderzocht in 2016 deze verstrekking van diagnosegegevens uit het DIS. De AP concludeerde dat niet alle partijen aan wie de NZa de gegevens verstrekte deze gegevens mogen ontvangen.

De NZa heeft daarop toegezegd geen DIS-informatie meer aan de betreffende partijen te geven.

AP: NZa mag diagnosegegevens uit DIS beperkt verstrekken

Conclusies DIS-onderzoek

- De NZa mag DIS-gegevens delen met verschillende in de wet genoemde partijen.
- De NZa mag geen DIS-gegevens delen met de minister van Volksgezondheid, Welzijn en Sport (VWS) en het Centraal Planbureau (CPB). Hiervoor bestaat geen wettelijke grondslag.
- DIS-gegevens zijn weliswaar gepseudonimiseerd, maar dit is niet hetzelfde als anonieme gegevens. DIS-gegevens zijn dus (bijzondere) persoonsgegevens.
- Daardoor zijn de regels van de Wet bescherming persoonsgegevens van toepassing.

Bescherming van patiëntgegevens

Begin 2016 vroeg de AP in een open brief aan raden van bestuur van zorginstellingen aandacht voor de bescherming van patiëntgegevens. De AP benadrukte in de brief dat zorgvuldig omgaan met patiëntgegevens integraal deel uitmaakt van goede patiëntenzorg. En dat een leidende rol van de raad van bestuur daarbij onmisbaar is.

Eerder deed de AP bij negen zorginstellingen (ziekenhuizen, ggz-instellingen en huisartsenposten) onderzoek naar de toegang tot patiëntgegevens. Deze zorginstellingen bleken er onvoldoende voor te zorgen dat uitsluitend bevoegde medewerkers toegang hadden tot digitale patiëntendossiers en andere medewerkers dus niet. Er waren vervolgens intensieve verbetertrajecten nodig om de overtredingen te beëindigen. In 2016 constateerde de AP dat de door de onderzochte zorginstellingen getroffen maatregelen aan de wettelijke eisen voldoen.

AP vraagt extra aandacht voor bescherming patiëntgegevens

Maatregelen toegang patiëntgegevens

- autorisaties (wie kan er bij de gegevens)
- logging (bijhouden wie wanneer welke gegevens inziet)
- controle van logging.

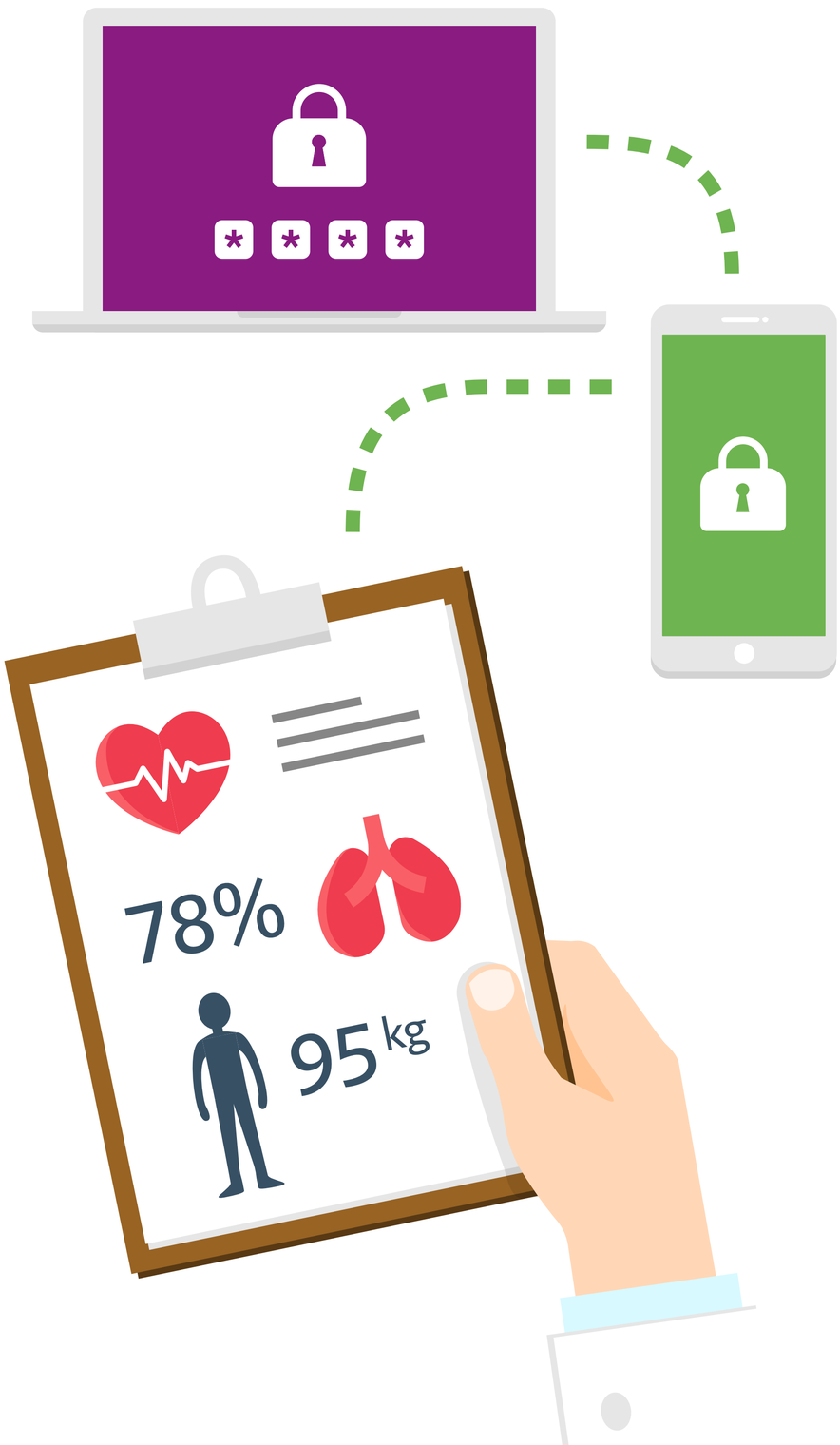
Patiëntenportalen ziekenhuizen

Steeds meer ziekenhuizen hebben een patiëntenportaal. Via zo'n portaal kunnen patiënten online hun (medische) gegevens inzien. Het is belangrijk dat alleen de patiënten zelf toegang kunnen krijgen tot hun gegevens en niemand anders. Ziekenhuizen moeten er daarom voor zorgen dat zij op een betrouwbare manier toegang geven tot het patiëntenportaal.

Dit doen zij door zogeheten tweefactorauthenticatie te gebruiken. Dat betekent dat het niet betrouwbaar genoeg is als patiënten inloggen met alleen een gebruikersnaam en een wachtwoord, maar dat er nog een verificatiemiddel nodig is. Bijvoorbeeld een token of een sms-code.

Eind 2016 stuurde de AP een brief aan de Nederlandse Vereniging van Ziekenhuizen (NVZ) om erop te wijzen dat ziekenhuizen hierin nu nog te vaak tekortschieten. Dat was namelijk uit een onderzoek van Nictiz gebleken. Daarnaast gaat de NVZ in 2017 ziekenhuizen stimuleren om een patiëntenportaal in te richten en hierbij ondersteuning bieden. Dit is voor de AP nóg een reden om het belang van tweefactorauthenticatie onder de aandacht te brengen.

AP: toegang tot patiëntenportalen ziekenhuizen betrouwbaar inrichten



Medewerker Frontoffice van de Autoriteit Persoonsgegevens

‘Niet iedereen mag bij je medisch dossier’

‘We kregen een tip dat bij een ggz-instelling alle hulpverleners toegang hadden tot de digitale dossiers van alle patiënten, óók van de patiënten die zij niet zelf behandelden. Dat mag niet. Alleen medewerkers binnen het behandelteam van een patiënt mogen zijn medisch dossier inkijken. Mensen moeten erop kunnen vertrouwen dat zorgvuldig wordt omgegaan met de gevoelige gegevens die zij toevertrouwen aan een hulpverlener. Ik heb daarom direct contact opgenomen met de ggz-instelling. Die heeft de toegangsautorisaties aangescherpt, waardoor nu alleen nog het behandelteam toegang heeft tot iemands dossier en andere hulpverleners dus niet.’

Contactformulier website

De AP kreeg van verschillende fysiotherapeuten vragen over het beveiligen van het contactformulier op hun website. Zij wilden vooral weten wanneer een beveiligde verbinding (https) nodig is. Daarom schreef de AP in maart 2016 een brief met uitleg aan de KNGF, de overkoepelende vereniging van fysiotherapeuten.

Het standpunt van de AP was toen dat fysiotherapeuten het contactformulier in ieder geval moesten beveiligen als zij hiermee bijzondere persoonsgegevens verwerkten, zoals gezondheidsgegevens en het burgerservicenummer (BSN) van hun patiënten. Maar inmiddels zijn de benodigde componenten voor een beveiligde verbinding gratis beschikbaar. Daarom stelt de AP nu dat fysiotherapeuten hun contactformulier altijd via https moeten aanbieden, ongeacht het soort persoonsgegevens dat zij via het formulier verwerken.

Verder moeten fysiotherapeuten als zij een website (laten) bouwen rekening houden met de NEN 7512:2015 norm en de NCSC ICT-Beveiligingsrichtlijnen voor webapplicaties (2015).

Beveiliging contactformulier op websites fysiotherapeuten

Advies Wet verplichte ggz

In februari 2016 adviseerde de AP over de tweede nota van wijziging van de Wet verplichte geestelijke gezondheidszorg (Wvggz). Deze wet vervangt de bestaande wetgeving over gedwongen opname in een psychiatrisch ziekenhuis. De rechter kan straks één zorgmachtiging afgeven met een keuze uit verschillende vormen van verplichte zorg voor mensen die door een psychische stoornis aanzienlijk risico lopen zichzelf of anderen schade te berokkenen.

De AP constateerde in haar advies dat met deze tweede nota van wijziging opnieuw grote wijzigingen zijn aangebracht in de verantwoordelijkheden bij de aanvraag en uitvoer van een zorgmachtiging. Die wijzigingen hebben gevolgen voor de verwerking van persoonsgegevens – en dus voor de privacy van de betrokkenen – bij de uitvoering van de Wvggz.

Verschillende partijen, zoals gemeenten, het openbaar ministerie en de ggz, wisselen dan namelijk (gevoelige) gegevens over iemand uit, zoals medische en strafrechtelijke gegevens. Op deze privacygevolgen gaat het wetsvoorstel niet in, aldus de AP. Daarom adviseerde de AP om de toelichting bij het wetsvoorstel op verschillende punten aan te vullen.

AP adviseert over wijziging Wet verplichte ggz

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

'Geen BSN in brief zorgverlener'

'We kregen een tip van een vrouw die haar ziekenhuisafspraak had verplaatst. Zij kreeg een schriftelijke bevestiging thuis gestuurd met de nieuwe datum. In deze brief stond haar burgerservicenummer (BSN) vermeld. Ze vroeg zich af of dit wel mag. Mijn antwoord was: nee. Zorgverleners mogen het BSN gebruiken om er zeker van te zijn dat het om de juiste patiënt gaat, bijvoorbeeld als zij onderling gegevens uitwisselen. Maar bij een brief aan de patiënt zelf is dat niet aan de orde. En mogen zij het BSN dus niet gebruiken. Ik heb contact opgenomen met het ziekenhuis, dat daarop de systemen heeft aangepast. Het BSN wordt nu niet meer vermeld in de correspondentie met patiënten.'

Overheid

De overheid is een van de grootste verwerkers van persoonsgegevens. Verschillende organisaties binnen de overheid delen gegevens met elkaar. Hoe meer er technisch mogelijk is, hoe groter de databases worden en hoe meer gegevens de overheid aan elkaar koppelt. Ook is er een tendens zichtbaar dat de overheid dichterbij komt: de gemeente is letterlijk aan de keukentafel komen zitten. Dit alles kan een betere dienstverlening opleveren. Maar de overheid moet zich ook bewust zijn van de privacyrisico's die het met zich meebrengt. Mensen moeten erop kunnen blijven vertrouwen dat hun persoonsgegevens bij de overheid in goede handen zijn.

Gemeenten

Gemeenten hebben sinds 1 januari 2015 nieuwe taken op het gebied van jeugdzorg, maatschappelijke ondersteuning en arbeidsparticipatie. Dit wordt het sociaal domein genoemd. Hierdoor zijn gemeenten meer persoonsgegevens van meer mensen gaan verwerken. Het ontbreekt hierbij aan een overkoepelende regeling voor gegevensuitwisseling. Dit maakt dat de uitvoeringspraktijk voor gemeenten ingewikkeld is.

Onderzoek sociaal domein

Uit onderzoek van de AP bij 41 gemeenten blijkt dat zij niet goed weten welke gegevens zij in het sociaal domein mogen verwerken en welke regels daarvoor gelden. Bovendien informeren gemeenten mensen niet goed over het gebruik van hun gegevens.

Gemeenten vragen mensen bijvoorbeeld om toestemming om hun gegevens te gebruiken. Maar voor situaties waarin gemeenten de gegevens eigenlijk niet mogen gebruiken, is dit géén goede oplossing. Mensen moeten namelijk vrij zijn om toestemming te weigeren, maar zijn dat niet als zij van de gemeente afhankelijk zijn voor hulp of ondersteuning.

De AP doet gemeenten een aantal aanbevelingen. De AP gaat ervan uit dat gemeenten deze aanbevelingen gebruiken om snel te zorgen voor meer duidelijkheid over de persoonsgegevens die zij in het sociaal domein verwerken. Ook verwacht de AP dat gemeenten op basis daarvan hun medewerkers beter ondersteunen en hun inwoners informeren.

Gemeenten onzorgvuldig bij uitwerking privacyregels sociaal domein

Sociaal domein - tips voor gemeenten

- Specificeer welke gegevens noodzakelijk zijn:
  - voor welke specifieke doelen;
  - op basis van welke grondslag.

- Vertaal dit in instructies voor de professionals op de werkvloer. Zodat zij weten wat zij met welke gegevens mogen doen.

- Informeer mensen zorgvuldig over de gegevens die de gemeente over hen verwerkt. En over wanneer en waarom de gemeente toestemming vraagt.

Advies experiment integraal pgb

In mei 2016 adviseerde de AP over het Besluit experiment integraal persoonsgebonden budget (i-pgb) 2016. Het doel van het besluit is om in de gemeenten Delft en Woerden een pilot uit te voeren met een i-pgb. Dat houdt in dat mensen die ondersteuning nodig hebben op verschillende leefgebieden gebruik kunnen maken van één flexibel budget. Bijvoorbeeld voor thuishulp, ondersteuning op het werk en vervoer naar school.

De AP vraagt in haar advies aandacht voor de werkwijze van de gemeente bij de aanvraag van een i-pgb en voor de wettelijke grondslagen voor de gegevensverwerking bij het i-pgb. Zo stelt de AP dat toestemming van de mensen die een i-pgb aanvragen om hun gegevens te verwerken géén geldige grondslag is. Deze mensen zijn namelijk afhankelijk van de gemeente en kunnen dus niet in vrijheid toestemming geven of weigeren.

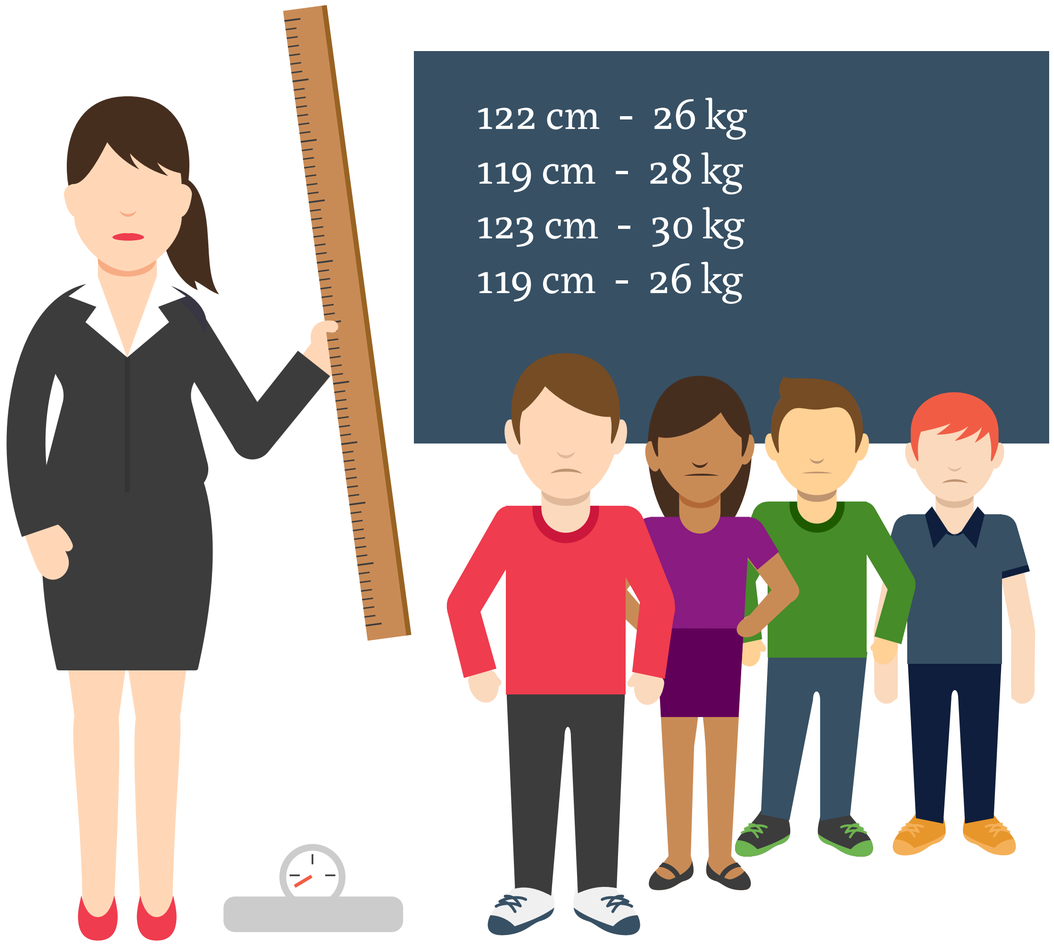
AP adviseert over experiment met persoonsgebonden budget

Gezondheidsprojecten kinderen en jongeren

De AP kreeg in 2016 een aantal vragen en tips over gezondheidsprojecten voor kinderen en jongeren. Gemeenten monitoren daarbij, met hulp van scholen, de gezondheid van leerlingen. Bijvoorbeeld om overgewicht tegen te gaan. Hierbij verzamelen de gemeenten gegevens over de gezondheid van de leerlingen, zoals gewicht, lengte en gegevens over motorische vaardigheden. Maar mag dat zomaar?

Het antwoord is: nee, niet zomaar. Gegevens over de gezondheid zijn zogeheten bijzondere persoonsgegevens. Dat zijn gevoelige gegevens. De regels voor het gebruik van deze gegevens zijn niet voor niets extra streng. Daarom moeten gemeenten zich aan een aantal voorwaarden houden als zij gezondheidsgegevens willen verzamelen. Dit geldt ook voor de scholen, afhankelijk van welke rol zij spelen in het project.

Gezondheidsproject voor kinderen en jongeren: wat mag wel en niet?



Belangrijkste regels gezondheidsproject

Informeren
Gemeenten moeten de ouders of de leerlingen goede informatie geven over wat zij met de gezondheidsgegevens doen. Op basis daarvan kunnen de ouders of de leerlingen zelf beslissen of zij willen meewerken.

Toestemming
Vervolgens moeten gemeenten om toestemming vragen om de gezondheidsgegevens te verwerken.

- Bij kinderen en jongeren onder de 16 jaar moeten de ouders toestemming geven, wie ouder is dan 16 jaar doet dit zelf.
- Alleen expliciete toestemming is geldig. Een brief waarin staat dat ouders of leerlingen die bezwaar hebben zich kunnen afmelden (‘wie zwijgt, stemt toe’), is niet genoeg.

Voorwaarden gemeente
Voorwaarden school

Advies Experimentenwet Gemeenten

In juli 2016 adviseerde de AP over de Experimentenwet Gemeenten. Dit wetsvoorstel stelt gemeenten in staat voor een bepaalde periode af te wijken van bestaande wettelijke bepalingen. Het doel hiervan is een innovatieve aanpak van maatschappelijke problemen mogelijk te maken.

Een concreet experiment op grond van het wetsvoorstel is dat Veilig Thuis (het advies- en meldpunt voor huiselijk geweld en kindermishandeling) in Midden-Brabant de mogelijkheid krijgt om vaker persoonsgegevens van vermoedelijke daders en slachtoffers te verwerken. Dit zou dan niet alleen bij een melding gebeuren, maar ook bij een adviesaanvraag. Deze registratie kan ervoor zorgen dat slachtoffers beter en eerder in beeld komen, aldus het wetsvoorstel. Bij de adviesaanvragen kan het gaan om professionals, zoals artsen, voor wie het medisch beroepsgeheim geldt.

De AP adviseerde om de noodzaak van deze regeling meer inhoudelijk te motiveren. Dit geldt voor de verwerking van bijzondere persoonsgegevens, waarvoor strikte wettelijke eisen gelden, en voor de doorbreking van het (medisch) beroepsgeheim.

AP adviseert over Experimentenwet Gemeenten

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

’Voorzichtig omgaan met het BSN’

‘We kregen een tip van een man die met zijn gezin was verhuisd en zich online had ingeschreven bij hun nieuwe woonplaats. Dat ging via een beveiligd webformulier, dus daar maakte hij zich geen zorgen over. Maar dat deed hij wél toen hij vervolgens een onversleutelde bevestigingsmail ontving van de gemeente, met daarin het burgerservicenummer (BSN) van alle gezinsleden. Ik heb contact opgenomen met de gemeente en uitgelegd dat het BSN een zogeheten bijzonder persoonsgegeven is. Misbruik hiervan kan bijvoorbeeld leiden tot identiteitsfraude. Er gelden daarom extra strenge regels voor de beveiliging van het BSN. In de bevestigingsmail van de gemeente staat het BSN nu niet meer vermeld.’

Digitale overheid

De overheid is bezig om de dienstverlening aan zowel mensen als bedrijven steeds meer digitaal te laten verlopen. Zo werken de overheid en het bedrijfsleven samen aan een standaard voor online

identificatie, het eID-stelsel genoemd. Ook zijn er grote databases waarmee verschillende overheidsorganisaties achter de schermen gegevens uitwisselen, zoals het informatiesysteem Suwinet voor gegevens over werk & inkomen. Voor beide vormen van grootschalige digitale gegevensverwerking geldt dat de beveiliging goed geregeld moet zijn.

eID

In september 2016 schrijft de AP aan de minister van BZK dat er bij de ontwikkeling van het eID-stelsel meer aandacht moet zijn voor privacyaspecten. De beveiliging van de inlogmiddelen moet omhoog. Zo adviseert de AP om het beveiligingsniveau van DigiD (waarmee mensen kunnen inloggen) te verhogen naar minimaal tweefactorauthenticatie. Dat houdt in dat inloggen met alleen een gebruikersnaam en wachtwoord niet genoeg is, maar dat iemand ook nog op een andere manier zijn identiteit moet aantonen.

De minister van BZK heeft laten weten dat het beveiligingsniveau van DigiD inderdaad wordt verhoogd. Naar verwachting in de tweede helft van 2017 wordt het niveau verhoogd naar 'substantieel'. Mensen loggen dan in via DigiD door als extra (eenmalig) de chip van hun identiteitsbewijs te laten uitlezen. In 2018 komen er identiteitsbewijzen met een nieuwe chip. Door deze chip te laten uitlezen, kunnen mensen op een hoog betrouwbaarheidsniveau inloggen via DigiD.

AP: onvoldoende aandacht voor privacy bij eID

Advies AP over eID

Privacy by design

- Besteed bij de ontwikkeling van het eID-stelsel meer aandacht aan (technische) privacyaspecten, zoals logging.

Incidentbeheersing en toezicht

- Besteed meer aandacht aan het detecteren en afhandelen van beveiligingsincidenten.

Beveiliging

- Verhoog het beveiligingsniveau van DigiD (waarmee mensen kunnen inloggen) naar minimaal tweefactor-authenticatie. En ontwerp het eID-stelsel zo dat snel en eenvoudig nieuwe (technische) beveiligingsmaatregelen kunnen worden getroffen als dat nodig is.

Beveiliging Suwinet

De AP onderzocht in 2015 bij dertien gemeenten de beveiliging van persoonsgegevens die met Suwinet worden uitgewisseld. Het gaat hierbij bijvoorbeeld om gegevens over iemands arbeidsverleden, opleiding, alimentatie, uitkering of boetes. De AP constateerde toen dat meerdere gemeenten geen formele autorisatieprocedure hadden voor de toegangsrechten en geen beveiligingsplan specifiek voor Suwinet. In januari 2016 hadden twee van de dertien gemeenten de problemen al opgelost. In juli 2016 volgden de andere elf gemeenten.

Ook het UWV (beheerder Suwinet) en de gemeente 's-Hertogenbosch (afnemer Suwinet) beëindigden in 2016 de overtredingen die de AP eerder had geconstateerd. Zo hebben beide organisaties inmiddels een beveiligingsplan specifiek gericht op Suwinet. Ook zijn er procedures voor het analyseren en afwikkelen van incidenten.

Beveiliging Suwinet verbeterd na onderzoek Autoriteit Persoonsgegevens
AP: UWV en 's-Hertogenbosch beëindigen overtredingen Suwinet
AP: gemeenten beëindigen overtredingen beveiliging Suwinet

Top 3 beveiligingsnormen Suwinet

1. door het management goedgekeurd beveiligingsplan
2. toegangsrechten goed geregeld in formele procedure
3. controle op gebruik van Suwinet (logging)

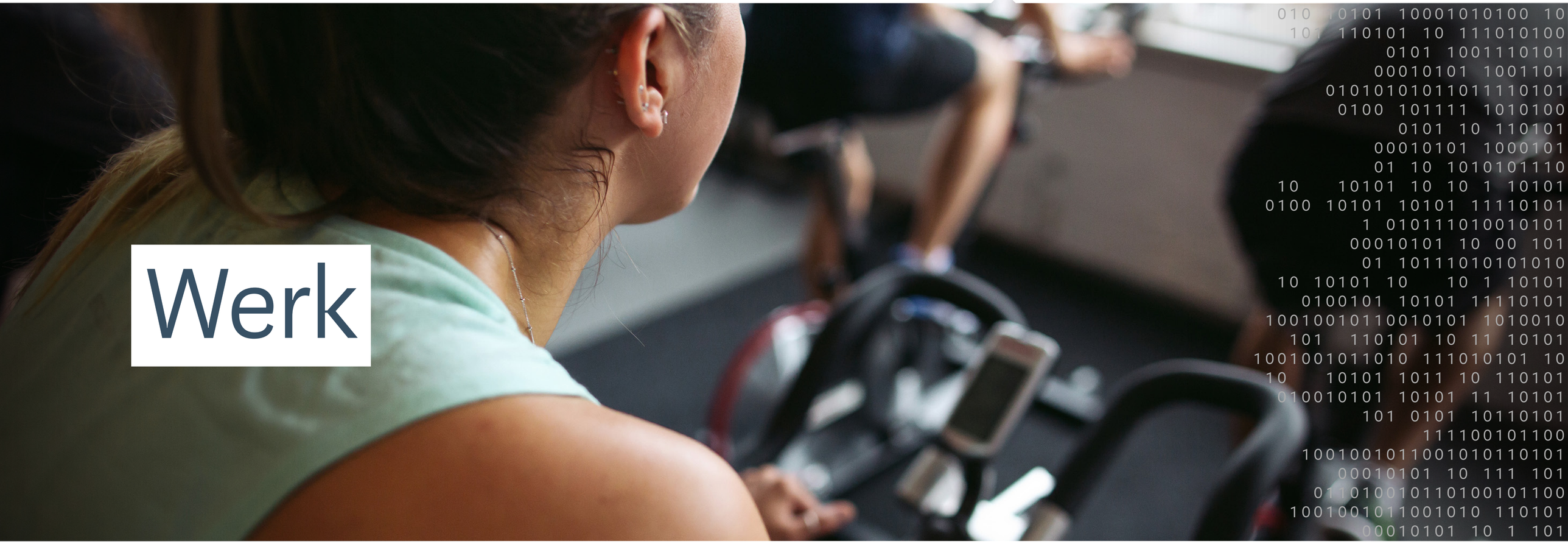
Belastingdienst Toeslagen

Tot mei 2016 kregen zowel de AP als de Nationale ombudsman regelmatig klachten van mensen die in hun toekenningsbrief van de Belastingdienst of in hun Toeslagen-portaal gegevens zagen van mensen die níet tot hun huishouden behoren, zogenoemde spookbewoners. Het ging daarbij om BSN, geboortedatum en inkomensgegevens.

De AP heeft de Belastingdienst opgedragen deze problemen op te lossen. De Belastingdienst heeft daarop verschillende maatregelen getroffen. Zo worden van het BSN alleen de laatste drie cijfers getoond, is er een team bij de Belastingdienst dat direct het probleem in het toeslagensysteem kan oppakken en koppelt de Belastingdienst de juiste gegevens terug naar de Basisregistratie Personen (BRP), zodat ook daar de gegevens worden aangepast. Het aantal klachten over de Belastingdienst Toeslagen is bij de AP en de Nationale ombudsman sinds de invoering van deze eerste maatregelen in mei 2016 sterk afgenomen.

Maar ondanks deze maatregelen kan het nog steeds voorkomen dat mensen op hun beschikking gegevens zien van een spookbewoner. Dat komt omdat de gegevens in de BRP niet altijd kloppen en de BRP het bronbestand is waar de Belastingdienst mee werkt. De Belastingdienst gaat de systemen aanpassen en zal de aanvrager van een toeslag voortaan direct laten controleren of zijn gegevens kloppen. Zo niet, dan neemt de Belastingdienst de aanvraag niet in behandeling en moet de aanvrager contact opnemen met de gemeente. Deze maatregel moet de Belastingdienst uiterlijk 1 juni 2017 hebben ingevoerd.

AP: Belastingdienst treft maatregelen persoonsgegevens toeslagen



Werk

Werkgevers die camera's ophangen om hun personeel in de gaten te houden. Die zieke werknemers het hemd van het lijf vragen. Die zelfs zó ver indringen in het privéleven van hun werknemers dat ze inzicht willen in hun beweeg- en slaappatroon. De werkgever lijkt de werknemer steeds dichter op de huid te gaan zitten. Natuurlijk is het voor werkgevers van groot belang om goed presterend personeel te hebben. Maar zij moeten daarbij wél rekening houden met de privacy van hun werknemers. Hun recht op privacy geldt namelijk net zo goed op de werkvloer als daarbuiten. Bovendien bevinden werknemers zich in een kwetsbare positie, omdat zij financieel afhankelijk zijn van hun werkgever. Alle reden dus voor de Autoriteit Persoonsgegevens (AP) om ook in 2016 speciale aandacht te besteden aan de arbeidsrelatie.

Filmen werknemers

De AP deed onderzoek bij het transportbedrijf De Rooy Transport BV. Dit bedrijf filmde zijn chauffeurs in de vrachtwagencabine tijdens hun ritten. De beelden werden vastgelegd en bewaard bij een plotselinge beweging van de vrachtwagen. Het bedrijf bleek deze camerabeelden te gebruiken om de chauffeurs aan te spreken op hun rijgedrag. Het doel was om het rijgedrag te verbeteren.

Het is voor dit doel echter niet proportioneel om de chauffeurs gedurende hun werktijd onafgebroken te filmen. De chauffeurs staan hierdoor continu onder toezicht. Dat maakt de inbreuk op de persoonlijke levenssfeer van de chauffeurs te groot. Het transportbedrijf handelde hierdoor in strijd met de wet. Door het onderzoek van de AP is het bedrijf gestopt met de video-opnames van zijn chauffeurs. Ook zijn de eerdere opnames gewist.

Transportbedrijf stopt filmen chauffeurs na onderzoek Autoriteit Persoonsgegevens

Cameratoezicht - checklist werkgever

- Heb ik een gerechtvaardigd belang? (bijvoorbeeld diefstal of fraude bestrijden)
- Is het cameratoezicht hiervoor noodzakelijk? Of kan ik mijn doel ook op een minder ingrijpende manier bereiken?
- Hoe zwaar wegen mijn belangen tegenover die van mijn personeel? (privacytoets)
- Wat vindt de ondernemingsraad ervan?

Dossier Cameratoezicht op de werkplek

Ziekteverzuim en preventie

Werkgevers mogen geen gegevens over de gezondheid van hun werknemers verwerken. Dit zijn zogeheten bijzondere persoonsgegevens, die niet voor niets extra beschermd moeten worden. Natuurlijk is het voor werkgevers van belang om zieke werknemers zo snel mogelijk weer aan het werk te krijgen. En zal elke werkgever ziekteverzuim het liefst zo veel mogelijk voorkomen. Maar werkgevers hebben zich daarbij aan strenge wettelijk regels te houden. Zo mogen zij niet informeren naar de aard en oorzaak van de ziekte van hun werknemers. Alleen de arbodienst of bedrijfsarts mag deze medische gegevens verwerken.

Onderzoek ziekmelding

Stichting Abrona handelde bij ziekmelding van werknemers in strijd met de Wet bescherming persoonsgegevens. Dat was de conclusie van de AP na onderzoek. In oktober 2016 legde de AP een last onder dwangsom op aan Abrona. Inmiddels heeft Abrona voldoende maatregelen getroffen om de overtredingen te beëindigen. Daardoor hoefde Abrona geen dwangsommen te betalen.

Abrona is gespecialiseerd in dienstverlening aan mensen met een verstandelijke beperking in de provincie Utrecht. Er werken 1300 werknemers en 800 vrijwilligers. De organisatie bleek bij ziekmelding aard en oorzaak van de ziekte van de zieke werknemer te registeren. Bijvoorbeeld of het ging om psychische klachten of om fysieke beperkingen. Dat mag niet. Werkgevers mogen alleen gegevens vragen die noodzakelijk zijn om te bepalen of zij loon moeten doorbetalen en om te bepalen hoe het verder moet met de werkzaamheden van de zieke.

Abrona gaf aan het – ondanks de door de stichting genomen maatregelen – niet eens te zijn met het dwangsombesluit en stelde bezwaar in. De AP heeft het bezwaar van Abrona afgewezen. De termijn om tegen het besluit van de AP in beroep te gaan is inmiddels verstreken. Het besluit op bezwaar van de AP is hierdoor onherroepelijk.

AP: Abrona beëindigt overtredingen met gegevens zieke werknemers
AP controleert maatregelen Abrona na dwangsom over zieke werknemers
AP: Abrona verwerkt in strijd met wet medische gegevens medewerkers

Verzuimsysteem

In welk verzuimsysteem mag ik als bedrijfsarts of arbodienst medische dossiers van werknemers opslaan? Mag dat het systeem van mijn opdrachtgever (de werkgever) zelf zijn? Of een extern verzuimsysteem dat de werkgever heeft uitgekozen? De AP kreeg regelmatig vragen over het opslaan van medische dossiers in verzuimsystemen. En zette daarom in november 2016 de do's & don'ts op een rijtje.

Medische dossiers opslaan in verzuimsystemen: wat mag wel en niet?

Medische gegevens in verzuimsystemen

Een bedrijfsarts of arbodienst mag de medische dossiers van werknemers…

- … niet opslaan in een verzuimsysteem dat de werkgever zelf gebruikt én beheert.
- … wel opslaan in een door de werkgever uitgekozen verzuimsysteem, bijvoorbeeld het (extern beheerde) verzuimsysteem dat hij zelf ook gebruikt.
  Let op: de bedrijfsarts of arbodienst moet dan een bewerkersovereenkomst afsluiten met de beheerder van het verzuimsysteem.

Beleidsregels ‘De zieke werknemer’

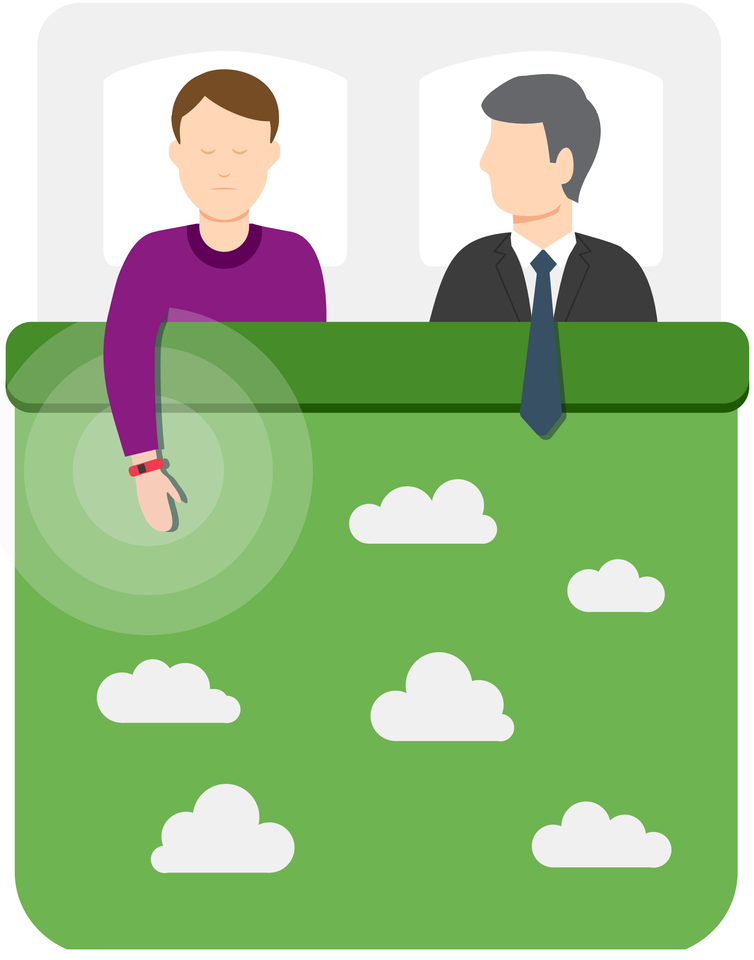
De AP publiceerde in april 2016 de beleidsregels ‘De zieke werknemer’. Deze beleidsregels geven werkgevers, werknemers en andere betrokken partijen (zoals de bedrijfsarts en het UWV) duidelijkheid over wie welke gegevens over de gezondheid van (zieke) werknemers mag verwerken. Daarnaast zijn de normen in de beleidsregels het uitgangspunt voor de AP bij onderzoek. De beleidsregels zijn een geactualiseerde versie van een eerdere AP-publicatie over zieke werknemers.

Onderzoek wearables

Twee bedrijven zijn na onderzoek van de AP gestopt met het verwerken van gezondheidsgegevens van hun werknemers via wearables. Beide bedrijven hadden hun werknemers een armband gegeven waarmee de werkgever inzicht kreeg in de hoeveelheid beweging van de werknemers. Een van de werkgevers had ook inzicht in het slaappatroon.

Gegevens over beweging en slaappatroon zijn gevoelige persoonsgegevens die iets zeggen over de gezondheid. Voor deze bijzondere persoonsgegevens gelden strenge wettelijk eisen. Werkgevers mogen deze gegevens niet verwerken. Dit mag overigens óók niet als een werknemer hiervoor toestemming zou geven. In een arbeidsverhouding, waarin de werknemer financieel afhankelijk is van de werkgever, is over het algemeen namelijk geen sprake van de wettelijk vereiste ’vrije’ toestemming.

AP: verwerking gezondheidsgegevens wearables door werkgevers mag niet



Wearable van de werkgever

Wat mag wel

- De werkgever geeft werknemers een wearable cadeau, zodat zij zelf aan de slag kunnen om hun fitheid te verbeteren.
- De werknemers kiezen er zelf voor om hun gegevens al dan niet te delen met de leverancier (door een account aan te maken).
- De werknemers kiezen er zelf voor om hun gegevens al dan niet te delen met vrienden of collega's (via de portal van de leverancier).

Wat mag niet

- De werkgever mag geen gezondheidsgegevens van de werknemer inzien.
- De werkgever mag de werknemer niet dwingen om gegevens te delen met collega's of de leverancier van de wearable.
- De leverancier mag géén gegevens aan de werkgever verstrekken.

BMI

De AP kreeg een tip van een OR-lid over een werkgever die de *body mass index* (BMI) van zijn werknemers wilde gaan registreren om hen te stimuleren om af te vallen. Wie meedeed, zou een theaterbon krijgen. De werkgever dacht dat hij dit mocht, omdat zijn medewerkers er toestemming voor hadden gegeven.

De AP liet hierop aan het OR-lid weten dat toestemming binnen de arbeidsrelatie niet geldig is, omdat werknemers deze niet in vrijheid kunnen geven. En dat de werkgever dus geen gezondheidsgegevens – zoals de BMI – van zijn medewerkers mag verzamelen. Hierop paste de werkgever zijn werkwijze aan. De werkgever betaalt nog wel een traject voor mensen die willen afvallen, maar hij krijgt geen toegang tot de gegevens.

Medewerker Frontoffice van de Autoriteit Persoonsgegevens

‘Werkgever mag personeel niet bespioneren’

‘Een supermarktmedewerkster schreef ons dat er op haar werk beveiligingscamera’s hangen om criminaliteit tegen te gaan. Maar leidinggevenden van verschillende afdelingen zouden die camera’s in de praktijk óók gebruiken om hun personeel in de gaten te houden. Via een oortje krijgen de medewerkers het direct te horen als ze volgens hun chef iets verkeerd doen. Dat mag niet. Werkgevers mogen weliswaar camera’s ophangen om hun personeel en eigendommen te beschermen, maar ze mogen de beelden niet voor een ander doel gebruiken. Ik heb de supermarkt een waarschuwingsbrief gestuurd.’

Screening

Het bedrijfsrecherchebureau Hoffmann BV heeft na onderzoek van de AP zijn werkwijze bij het screenen van sollicitanten en werknemers gewijzigd. De AP constateerde aan het begin van het onderzoek dat het bedrijf op verschillende punten de Wet bescherming persoonsgegevens overtrad.

Het bedrijfsrecherchebureau voerde onder meer screenings uit op basis van toestemming van de sollicitanten en werknemers. Toestemming als wettelijke grondslag is in deze situatie echter verboden. Ook maakte het bedrijf integrale kopieën van identiteitsbewijzen. Daardoor verwerkte het bedrijf het BSN en rasgegevens terwijl dat niet mocht. Het bedrijfsrecherchebureau bleek ook het socialemediaprofiel van betrokkenen aan het dossier toe te voegen. Hierin stond irrelevante informatie voor de betreffende functie en dat is in strijd met de wet.

Recherchebureau Hoffmann beëindigt overtredingen na onderzoek AP

Belangrijkste voorwaarden screening

Gerechtvaardigd belang

- De werkgever moet een zogeheten gerechtvaardigd belang hebben. Dat is bij een screening meestal dat hij erop moet kunnen vertrouwen dat zijn (toekomstig) personeel integer en betrouwbaar is.

Noodzakelijkheid

- De screening moet noodzakelijk zijn. Dit houdt onder meer in dat de werkgever zijn doel niet met een ander, minder ingrijpend middel dan screening mag kunnen bereiken.

Dossier Screening

Politie & justitie

Door de terroristische aanslagen van de laatste jaren zijn veiligheid en privacy op gespannen voet met elkaar komen te staan. Natuurlijk is het goed dat er nagedacht wordt over hoe politie, justitie en de veiligheidsdiensten hun werk nog beter kunnen doen. Maar als er nieuwe bevoegdheden worden voorgesteld die een ernstige inbreuk maken op de privacy, moet daarbij altijd een zorgvuldige afweging worden gemaakt. Politie en justitie werken immers met gevoelige informatie. Ook kan het niet de bedoeling zijn dat zij iedereen – dus ook onschuldige mensen – op de voet volgen.

Wetsvoorstel inlichtingen- en veiligheidsdiensten

In december 2016 reageerde de AP op het wetsvoorstel voor vernieuwing van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Dit voorstel regelt dat de diensten grote hoeveelheden persoonsgegevens van mensen in bulk mogen onderscheppen en analyseren. Ook mogen de diensten apparatuur van mensen hacken om zo toegang te krijgen tot apparatuur van concrete doelwitten. Daarnaast biedt het wetsvoorstel de diensten ruime mogelijkheden om onderschepte gegevens uit te wisselen met andere partijen, zoals buitenlandse inlichtingen- en veiligheidsdiensten.

Het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) is direct van toepassing op de inlichtingen- en veiligheidsdiensten. Uit het EVRM vloeien de voorwaarden voort waaraan het wetsvoorstel moet voldoen. De AP is van mening dat belangrijke onderdelen van het wetsvoorstel nog niet aan deze voorwaarden voldoen:

- de noodzaak van de voorgestelde bevoegdheden is onvoldoende onderbouwd;
- de voorgestelde nieuwe bevoegdheden zijn onvoldoende kenbaar en voorzienbaar voor mensen;
- de inzet van de voorgestelde nieuwe bevoegdheden is met onvoldoende waarborgen omkleed om de rechten van mensen te beschermen;
- er is nog geen sprake van daadwerkelijk effectief en onafhankelijk toezicht op de diensten.

Autoriteit Persoonsgegevens reageert op wetsvoorstel inlichtingen- en veiligheidsdiensten

Schengen Informatiesysteem II

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, wisselen deze gegevens uit via verschillende informatiesystemen. Een daarvan is het Schengen Informatiesysteem II (SIS II).

SIS II bevat 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 aangesloten zijn op SIS II zich moeten houden. De AP is de toezichthouder op het Nederlandse deel van het systeem (N.SIS II).

Onderzoek Politie

In 2016 deed de AP een verplicht periodiek onderzoek naar hoe de Politie met de signaleringen in N.SIS II omgaat. De AP constateerde dat de Politie hierop onvoldoende zicht heeft. De Politie blijkt onder meer vastgelegde werkprocessen en procedures niet na te komen. De Politie moet daarom betere maatregelen nemen om de politiegegevens in N.SIS II juist en nauwkeurig te verwerken, aldus de AP.

AP: Politie heeft onvoldoende zicht op signaleringen Schengenlanden

Onderzoek KMar en IND

Eind 2016 concludeerde de AP dat de Koninklijke Marechaussee (KMar) en de Immigratie- en Naturalisatiedienst (IND) niet langer de regels overtreden met SIS II. Eerder constateerde de AP dat de KMar onvoldoende organisatorische maatregelen had genomen om N.SIS II te beveiligen. En dat de IND signaleringen over vreemdelingen niet altijd conform de regels in N.SIS II verwerkte.

AP: Koninklijke Marechaussee en IND beëindigen overtredingen SIS

Onjuiste signalering in SIS II kan verstrekkende gevolgen hebben, bijvoorbeeld dat iemand onterecht wordt aangehouden bij de grens of zelfs langere tijd het Schengengebied niet in of uit kan.

Controle hotelregisters

Hotels zijn verplicht een nachtregistratie bij te houden met een aantal gegevens van gasten. De politie mag deze overnachtingsgegevens gericht opvragen voor bijvoorbeeld opsporingsonderzoek. Maar de politie-eenheid Oost vroeg en kreeg dagelijks lijsten met de gegevens van alle gasten van vijf hotels, bleek uit onderzoek van de AP. Het is voor de politie lang niet altijd noodzakelijk al deze gegevens te krijgen. Het verwerken van niet-noodzakelijke gegevens is in strijd met de wet. Bovendien levert dit risico's op, zoals verlies van gegevens of identiteitsfraude. Door het onderzoek van de AP vraagt de politie nu alleen die gegevens op die echt nodig zijn.

Politie vraagt nachtregisters hotels niet meer standaard op

Internationaal

De verwerking van persoonsgegevens houdt niet op bij de Nederlandse grens. Persoonsgegevens worden steeds meer wereldwijd verwerkt, voor uiteenlopende doelen. Bijvoorbeeld door grote internet- en telecombedrijven. Hoe pak je deze 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 zo multinationals dicht op de huid te blijven zitten. En natuurlijk ook om van elkaar te leren.

Het zwaartepunt van de internationale werkzaamheden van de AP ligt in Europa. De AP maakt deel uit van de Artikel 29-werkgroep, in het Engels Working Party 29 (WP29) geheten. Dit is het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders. WP29 speelt een belangrijke rol in de totstandkoming van Europees beleid voor de bescherming van persoonsgegevens. In 2016 was een belangrijk onderwerp voor WP29 de nieuwe Europese privacywetgeving, die na een voorbereidend traject van jaren – waarbij WP29 ook nauw betrokken was – in 2016 werd aangenomen.

Nieuwe EU-privacywetgeving

Vanaf mei 2018 geldt dezelfde privacywetgeving in de hele EU, in plaats van 28 verschillende nationale wetten. De nieuwe wet zorgt onder meer voor versterking en uitbreiding van privacyrechten van burgers, meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken en steviger bevoegdheden voor alle Europese privacytoezichthouders.

Op 4 mei 2016 is de Algemene verordening gegevensbescherming (AVG) gepubliceerd in het Publicatieblad van de Europese Unie en twintig dagen daarna is deze in werking getreden. Maar de AVG is pas vanaf 25 mei 2018 van toepassing. Deze tussenperiode van twee jaar is nodig om organisaties en toezichthouders zich goed te laten voorbereiden.

In 10 stappen voorbereid op de AVG

1. Bewustwording
Begin op tijd met de implementatie van de nieuwe privacyregels.

2. Rechten van betrokkenen
Zorg ervoor dat mensen hun privacyrechten goed kunnen uitoefenen.

3. Overzicht verwerkingen
Breng uw gegevensverwerkingen in kaart.

4. Privacy impact assessment (PIA)
Beoordeel of u straks PIA's moet uitvoeren en hoe u dit dan aanpakt.

5. Privacy by design & privacy by default
Hou al aan de tekentafel rekening met privacy.

6. Functionaris voor de gegevensbescherming
Stel, als dat moet, tijdig een FG (interne toezichthouder) aan.

7. Meldplicht datalekken
Evalueer uw procedure voor het registreren en melden van datalekken.

8. Bewerkersovereenkomsten
Beoordeel of de contracten met uw bewerkers voldoen aan de AVG.

9. Leidende toezichthouder
In meerdere EU-lidstaten actief? Bepaal onder welke toezichthouder u valt.

10. Toestemming
Evalueer hoe u van mensen toestemming vraagt, krijgt en registreert.

In 10 stappen voorbereid op de AVG (volledige versie)

Guidelines WP29

In december 2016 heeft WP29 de eerste *guidelines* en FAQ's gepubliceerd om organisaties te helpen bij deze voorbereiding. De AP heeft de guidelines laten vertalen in het Nederlands en heeft Nederlandstalige vragen en antwoorden opgesteld. In de loop van de tijd volgen nog meer guidelines.

Guidelines over de AVG

- Functionaris voor de gegevensbescherming (FG)
  Onder de AVG kunnen organisaties verplicht zijn een FG – een interne privacytoezichthouder – aan te stellen. De guidelines geven aan wanneer dit moet en wat de rol van de FG is. Ook gaan de guidelines in op het aannemen van een FG, de functie van de FG en zijn taken.
- Recht op dataportabiliteit
  De AVG geeft mensen een nieuw recht: het recht op dataportabiliteit. Dit houdt in dat zij het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. De guidelines geven meer duidelijkheid over welke persoonsgegevens organisaties moeten verstrekken en hoe zij dit moeten doen.
- Leidende toezichthouder
  De AVG gaat uit van de zogeheten onestopshop-regel. Heeft een organisatie meerdere vestigingen in de EU? Of hebben de gegevensverwerkingen van deze organisatie in meerdere EU-lidstaten impact? Dan hoeft die organisatie nog maar met één privacytoezichthouder zaken te doen. Dit wordt de 'leidende toezichthouder' genoemd. De guidelines gaan in op dit systeem en helpen organisaties om te bepalen wie in hun geval de leidende toezichthouder is.

Privacytoezichthouders publiceren richtlijnen Europese privacywet

’Met de nieuwe EU-wetgeving komt er ook een nieuwe AP. We gaan meer voorlichting geven aan burgers en aan organisaties. Zodat burgers weten welke rechten zij hebben en hoe zij hun recht kunnen halen. En bedrijven en overheden weten aan welke verplichtingen zij moeten voldoen.’

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens

EU-VS privacy shield

Op 12 juli 2016 nam de Europese Commissie (EC) het EU-VS privacy shield (privacyschild) aan, een regeling voor doorgifte van persoonsgegevens aan de Verenigde Staten (VS). Het privacy shield vervangt de Safe Harbour-overeenkomst, die het Europees Hof van Justitie op 6 oktober 2015 ongeldig verklaarde.

Advies WP29

De EC vroeg WP29 in april 2016 om advies over de conceptversie van het privacy shield. WP29 liet toen weten een aantal zorgpunten te hebben, onder meer over het ongericht verzamelen van persoonsgegevens uit de EU door Amerikaanse inlichtingendiensten. Ook vroeg WP29 de EC een aantal zaken te verduidelijken, zoals de definities van een aantal belangrijke privacyprincipes.

Standpunt WP29

De EC nam deze punten deels over en sloot vervolgens een akkoord met de VS over het definitieve privacyschild. WP29 stelde hierop vast dat het definitieve privacy shield verbeteringen kent, maar had nog steeds enkele punten van kritiek. Zo biedt het privacy shield nog steeds geen uitsluitsel over de inlichtingendiensten, aldus WP29. Tijdens de eerste jaarlijkse gezamenlijke controle van de afspraken in de tweede helft van 2017 beoordeelt WP29 of de kritiekpunten in de praktijk zijn opgelost.

Privacytoezichthouders kritisch over privacyschild
Toezichthouders houden zorgen over privacyschild

WhatsApp

In augustus 2016 werd bekend dat Whatsapp de persoonsgegevens van gebruikers toch gaat delen met Facebook, ondanks een eerdere toezegging om dit niet te doen.

WP29 vroeg daarop in een brief van 27 oktober 2016 om opheldering bij WhatsApp. In reactie op de vragen van de privacytoezichthouders maakte WhatsApp bekend te zijn gestopt met het delen van gegevens van Europese WhatsAppgebruikers voor verbeteringen van Facebookdiensten en advertentiedoeleinden. In een nieuwe brief van 19 december 2016 drong WP29 er onder andere op aan dat WhatsApp meer uitleg geeft over het delen van gegevens van Europese WhatsAppgebruikers. De zorg bestaat namelijk bij WP29 dat WhatsApp wél gegevens deelt met Facebook voor andere doeleinden.

Brief Europese privacytoezichthouders aan WhatsApp

Internationale samenwerking

De AP nam in 2016 deel aan:

- Artikel 29-werkgroep (WP29)
- Internationale Conferentie van Privacy- en Dataprotectietoezichthouders
- Europese Conferentie van Privacy- en Dataprotectie-toezichthouders
- Gemeenschappelijk toezicht op Europol en Eurojust
- Gemeenschappelijk toezicht op Europese informatie-systemen
- Global Privacy Enforcement Network

Voor meer informatie, zie: Bijlage jaarverslag 2016

Organisatie

Per 1 januari 2016 mag het College bescherming persoonsgegevens (CBP) zich Autoriteit Persoonsgegevens (AP) noemen. Ook kreeg de AP vanaf dat moment de bevoegdheid om boetes op te leggen. En trad de meldplicht datalekken in werking. Tot slot kwam er per 1 augustus 2016 een nieuwe voorzitter. Kortom, het jaar 2016 bracht de AP veel nieuws.

Nieuwe naam en nieuw logo

'Bij de positie van stevige handhavende toezichthouder past niet langer een College, maar een Autoriteit. De nieuwe bevoegdheden en nieuwe naam vroegen om een logo dat uitdrukt waar de Autoriteit Persoonsgegevens voor staat'. Aldus Jacob Kohnstamm, de toenmalige voorzitter van de AP, bij de onthulling van het nieuwe logo van de AP.

AUTORITEIT
PERSOONSGEGEVENS

Het logo visualiseert een gezicht, een profiel dat is opgebouwd uit voorwerpen die de beleidsthema's van de AP illustreren. Dit maakt duidelijk dat de bescherming van persoonsgegevens met vrijwel alle facetten van het leven is verbonden.

Autoriteit Persoonsgegevens: nieuwe taken en nieuw logo

Boetebevoegdheid

De AP kan sinds 1 januari 2016 organisaties een boete opleggen als zij de Wet bescherming persoonsgegevens overtreden. De maximale boete is 820.000 euro. Voor een telecombedrijf dat een datalek niet meldt aan de AP, is de boete maximaal 900.000 euro. Met de boetebeleidsregels geeft de AP inzicht in hoe de hoogte van een bestuurlijke boete wordt bepaald. De AP heeft in 2016 nog geen boete opgelegd.

Nieuwe voorzitter

Mr. A. (Aleid) Wolfsen werd in 2016 benoemd tot voorzitter van de AP. Voor zijn benoeming heeft hij zowel in de politiek gewerkt als binnen de rechterlijke macht. Hij was onder meer rechter, vicepresident van de rechtbank, Tweede Kamerlid en burgemeester van Utrecht. Wolfsen was als lid van de raad van advies eerder betrokken bij de AP (toen nog CBP).

De AP nam afscheid van Jacob Kohnstamm, die sinds 2004 voorzitter was. Op 1 augustus 2016 liep zijn tweede en laatste benoemingstermijn af. Ter gelegenheid van zijn afscheid werd Kohnstamm benoemd tot Officier in de Orde van Oranje-Nassau. Hij ontving de Koninklijke onderscheiding voor zijn bijzondere verdiensten voor de bescherming van persoonsgegevens in Nederland, Europa en wereldwijd.

Koninklijke onderscheiding voor Jacob Kohnstamm

Organisatiecijfers

In 2016 was het budget van de AP 8,1 miljoen euro. De bezetting bedroeg gemiddeld 72.57 fte, waarmee de gemiddelde bezetting nagenoeg gelijk bleef aan die van 2015 (72.50 fte). Een groot deel van de capaciteit gebruikt de AP om onderzoek te doen naar de naleving van de wet. In 2016 rondde de AP 197 onderzoeken af, inclusief onderzoeken naar datalekken. Daarnaast heeft de AP in 2016 303 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 regelgeving. In 2016 bracht de AP 33 keer advies uit.

Bijlage jaarverslag 2016 voor alle organisatiecijfers uit 2016

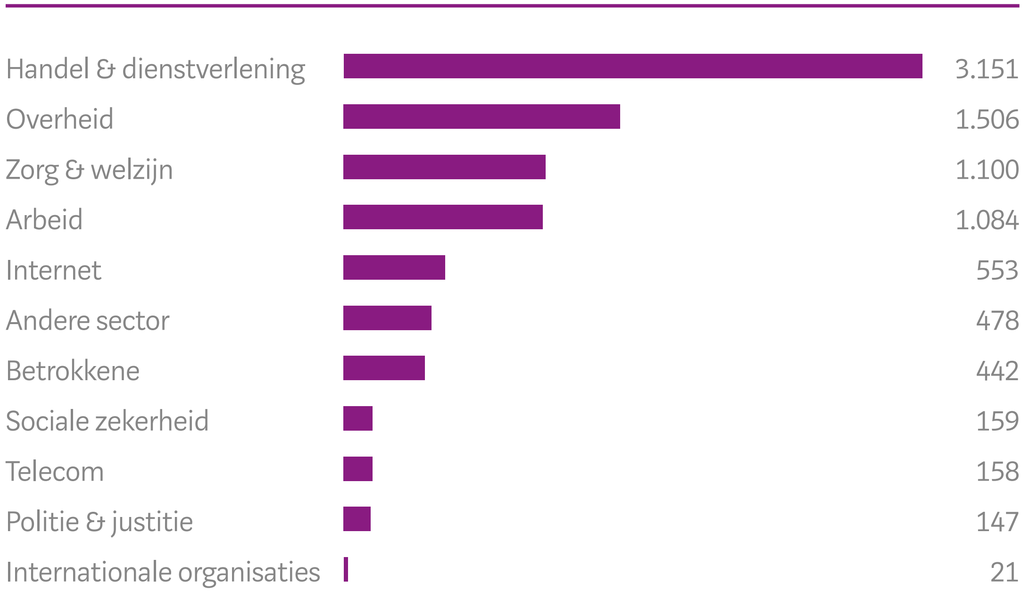
Voorlichting en communicatie

Door voorlichting aan bedrijven en overheidsorganisaties zorgt de AP dat zij de wettelijke privacyregels (beter) naleven. De AP staat tegelijkertijd dagelijks mensen te woord zodat zij weten wat hun rechten zijn op dit gebied en zij zelf in actie kunnen komen als hun privacy geschonden wordt. De AP zoekt ook geregeld zelf actief contact met de pers en maatschappelijke organisaties.

Publieksvoorlichting

De afdeling Frontoffice van de AP beantwoordt vragen en behandelt tips over (mogelijke) overtredingen van de privacywetgeving. In 2016 kreeg de AP 8.799 vragen en tips, een toename van bijna 30 procent ten opzichte van 2015. Het grootste deel van de vragen en tips kwam binnen via het telefonisch spreekuur en het speciale tipformulier op de website van de AP.

Veruit de meeste vragen en tips – ruim een derde van het totaal – gingen over de sector handel & dienstverlening. Ook waren er veel vragen en tips over de sectoren overheid (vooral over gemeenten), zorg & welzijn (vooral over medische zorg) en arbeid (vooral over werkgevers). 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.



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 (voor de criteria om onderzoek te doen, zie de Beleidsregels handhaving). De AP kan er ook voor kiezen niet direct een officieel onderzoek te starten, maar een zogeheten alternatieve interventie in te zetten. Zo kunnen waarschuwingsbrieven en/of gesprekken met organisaties al genoeg zijn om overtredingen te laten beëindigen.

In 2016 heeft Frontoffice 303 zaken alternatief behandeld. De meeste waarschuwingsbrieven gingen over datalekken, over het kopiëren van identiteitsbewijzen en gebruik van het BSN en over cameratoezicht door de werkgever. De gesprekken gingen vooral over beveiliging en over het kopiëren van identiteitsbewijzen en gebruik van het BSN.

Bijlage jaarverslag 2016 voor meer informatie over de vragen en tips aan de AP in 2016

Persvoorlichting

De AP heeft in 2016 797 keer contact gehad met de media. Dat is een stijging van 29 procent ten opzichte van 2015. Het ging hierbij onder meer om het beantwoorden van persvragen, interviews en radio- en televisieoptredens. Datalekken, de nieuwe EU-privacywetgeving, gebruik van gezondheidsgegevens en verwerkingen van persoonsgegevens op websites en via apps waren de onderwerpen die vaak voorkwamen.

Landelijke radio en televisie	295
Landelijke dagbladen	131
(Vak)bladen	96
Overig	79
Online-media	75
Regionale dagbladen	56
Persbureaus	38
Regionale radio en televisie	22
Internationale dagbladen	5
Totaal	**797**

Externe optredens

In 2016 bestond een belangrijk deel van de werkzaamheden uit externe optredens. De voorzitter, de vicevoorzitter en medewerkers van de AP hielden (keynote)speeches tijdens conferenties, namen deel aan debatten en gaven interviews aan zowel (inter)nationale radio en televisie als geschreven pers.

Speeches en presentaties
De AP hield in 2016 een groot aantal speeches en presentaties. De belangrijkste onderwerpen waren hierbij de meldplicht datalekken, de nieuwe EU-privacywetgeving en big data. Ook gingen presentaties over de bescherming van persoonsgegevens in de zorg, bij gemeenten, bij de Politie en in de arbeidsrelatie.

Tweede Kamer

- In februari 2016 sprak de voorzitter van de AP tijdens een hoorzitting in de Tweede Kamer over een wetswijziging ter versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III).
- In april 2016 boden de voorzitter en vicevoorzitter de leden van de vaste Kamercommissie voor Veiligheid en Justitie het Jaarverslag 2015 aan. Zij hadden ook een gesprek met de leden, met een terugblik op 2015 en een vooruitblik naar 2016. Daarbij kwam onder meer de meldplicht datalekken aan de orde.
- In december 2016 nam de vicevoorzitter deel aan een hoorzitting in de Tweede Kamer over het wetsvoorstel 'Wet inlichtingen en veiligheidsdiensten 20..'.

Markttoezichthoudersberaad

De AP nam ook in 2016 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 en Markt (ACM), Autoriteit Financiële Markten (AFM), Commissariaat voor de Media, De Nederlandsche Bank (DNB), Kansspelautoriteit en Nederlandse Zorgautoriteit (NZa).

Het MTB organiseerde in 2016 twee goed bezochte seminars voor bestuurders en medewerkers van de leden van het MTB. De bijeenkomst in juni ging over toezicht & communicatie en werd georganiseerd door het Commissariaat van de Media. In november 2016 organiseerde de AP een seminar over toezicht & innovatie.

Leden van de Autoriteit en directeur

Autoriteit

Mr. A. Wolfsen
Voorzitter
(vanaf 1 augustus 2016)

Mr. W.B.M. Tomesen
Vicevoorzitter

Mr. J. Kohnstamm was voorzitter tot 1 augustus 2016

Directeur

Drs. P.J.J. Frencken
Directeur

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 2016 waren de leden van de raad van advies:

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

De heer J.J. van Aartsen
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
Lid 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 drs. L.A.M. van Halder
Voorzitter raad van bestuur Radboudumc.

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.

Mevrouw mr. C.E. Passchier
Vicevoorzitter FNV.

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

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, mei 2017

Ontwerp - Teldesign, Rotterdam
Fotografie - Emilie Hudig (foto's leden Autoriteit en directeur), Stocksy United

Autoriteit Persoonsgegevens

Bezoekadres
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Postadres
Postbus 93374
2509 AJ DEN HAAG

Telefoon
070 8888 500

Fax
070 8888 501

autoriteitpersoonsgegevens.nl

Telefonisch spreekuur
maandag t/m vrijdag
09.30 - 12.30 uur:
0900 2001 201 (5 ct p/m)