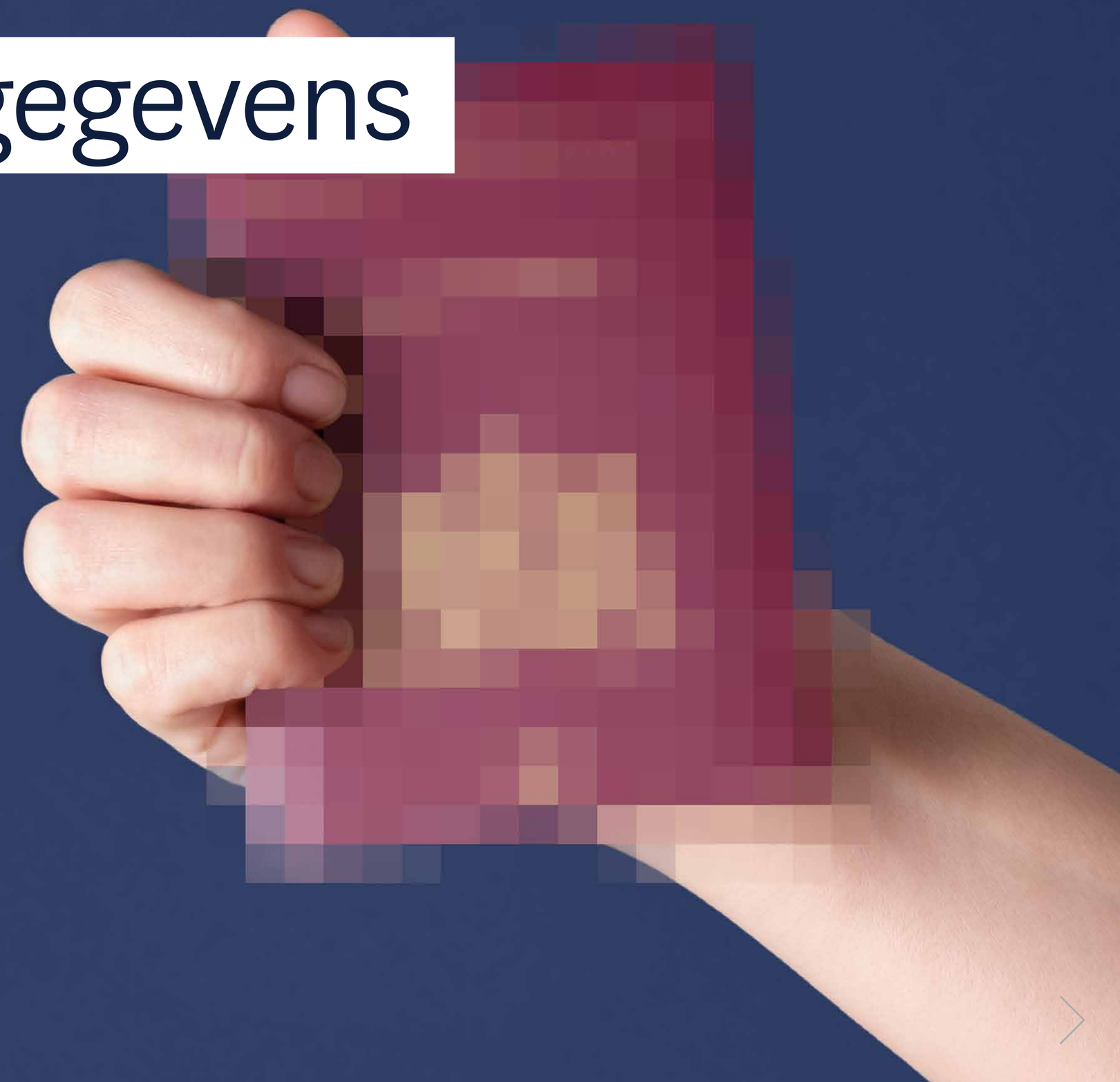
Grip op persoonsgegevens

Jaarverslag 2018



AUTORITEIT
PERSOONSGEGEVENS

Inhoud

Dit jaarverslag gaat over de belangrijkste werkzaamheden van de AP uit 2018. Alle feiten en cijfers staan in de bijlage. In de samenvatting vindt u ons werk chronologisch op een tijdlijn.

Voorwoord

Nederlanders maken zich zorgen over hun privacy. Uit onderzoek dat de Autoriteit Persoonsgegevens (AP) liet doen, bleek dat maar liefst 94% van de mensen zich zorgen maakt over de bescherming van hun persoonsgegevens. Vooral over misbruik van hun identiteitsbewijs, het volgen van hun online zoekgedrag en wifitracking. Bij uitstek situaties waarin mensen de grip op hun persoonsgegevens kwijt zijn. De nieuwe Europese privacywet die sinds 25 mei 2018 geldt, de Algemene verordening gegevensbescherming (AVG), kwam dan ook geen dag te laat. De AVG zorgt voor meer grip: voor de mensen van wie gegevens worden verwerkt, maar óók voor de organisaties die hun persoons-gegevens verwerken en voor de privacytoezichthouder.

Mensen hebben door de AVG meer en betere privacyrechten gekregen. Bijvoorbeeld het recht op heldere informatie over wat organisaties met hun gegevens doen. Een ellenlang privacystatement vol juridische termen, dat kan écht niet meer.
Ook kunnen mensen een privacyklacht indienen bij de AP als zij het niet eens zijn met hoe een organisatie met hun persoonsgegevens omgaat. Als AP behandelen wij elke klacht. In 2018 ontvingen we meteen ruim 11.000 klachten – nog een teken dat mensen hun privacy serieus nemen.

In de AVG is veel aandacht voor verantwoording ('accountability'). Dat houdt in dat organisaties moeten kunnen aantonen dat zij zich aan de privacywet houden. De AVG-regels dwingen organisaties om – al aan de tekentafel – goed na te denken over hoe zij persoonsgegevens verwerken en beschermen. Zodat zij grip krijgen op waar zij mee bezig zijn.
En daardoor een goed privacyverhaal hebben, zowel voor de mensen van wie zij gegevens verwerken als voor de toezichthouder. Natuurlijk is een nieuwe wet ook lastig. Wij hebben organisaties daarom zo veel mogelijk geholpen bij de voorbereiding, bijvoorbeeld met praktische hulpmiddelen.
Ook dat geeft grip.

Als toezichthouder hebben wij door de AVG steviger bevoegdheden gekregen. Zo kunnen we een boete opleggen van maximaal 20 miljoen euro. Het is nu menens. En dat is niet meer dan terecht, want de bescherming van persoonsgegevens is een grondrecht. Dat door de digitalisering feitelijk de hoeder is van alle andere grondrechten, zoals het recht op non-discriminatie, op godsdienstvrijheid en op briefgeheim. De uiting van deze rechten kan te vinden zijn in persoonsgegevens. Met deze gegevens moet dus uiterst zorgvuldig worden omgegaan, om niet alleen het recht op privacy maar ook de andere grondrechten te beschermen.

Eind 2018 ligt het eerste half jaar van de AVG achter ons. Voor de AP was 2018 een enerverend jaar. Dynamisch, maar ook met de nodige groeipijnen.
We kregen er nieuwe taken bij, onder meer op het gebied van Europese samenwerking, voorlichting en behandeling van privacyklachten. Dat vroeg om een ander soort organisatie. In 2018 zijn we daarom overgegaan naar een grotere organisatie met een andere structuur en rechtspersoonlijkheid en een nieuwe missie en toezichtkader. Op dit moment is de AP nog volop in ontwikkeling: we zijn bezig nieuwe medewerkers in te werken, de nieuwe structuur daalt in, werkprocessen voor nieuwe taken worden helder.

Ondanks deze grote veranderingen is 'de winkel open gebleven'. De AP heeft ook in 2018 toezicht gehouden op de naleving van de privacywetgeving, naast de voorbereidingen op de nieuwe wet en de nieuwe organisatie. Zo hebben wij bijna 27.000 mensen te woord gestaan tijdens onze telefonische spreekuren, ruim 11.000 privacyklachten, 4.000 tips en 21.000 datalekmeldingen ontvangen, meer dan 80 keer advies gegeven over nieuwe wet- en regelgeving, diverse grotere en kleinere onderzoeken gedaan en sancties opgelegd aan onder meer Uber, de Belastingdienst en het UWV.

Maar ook al zijn we gegroeid, we zijn nog steeds een relatief kleine toezichthouder. Dat betekent dat we niet overal tegelijk kunnen zijn. Daarom zijn wij heel blij met de 8000 functionarissen gegevensbescherming (FG's) die zich in 2018 bij ons hebben aangemeld. FG's spelen een grote rol bij de naleving van de privacyregels binnen organisaties. Ze zijn als het ware onze oren en ogen ter plaatse. Een belangrijke functie dus, waar wij als AP veel waardering voor hebben.

Tot slot zijn er ook ruim 17 miljoen kleine toezichthouders – mensen in Nederland die zich bewust zijn van hun privacyrechten en die zich niet alleen zorgen maken, maar die ook in actie komen. Die organisaties aanspreken op hoe zij met hun persoonsgegevens omgaan. Die waar nodig de hulp van de AP inschakelen. Zodat zij grip houden op hun persoonsgegevens, waar het uiteindelijk allemaal om draait.

Het bestuur van de Autoriteit Persoonsgegevens,

Aleid Wolfsen
Monique Verdier
Katja Mur

Nieuwe wet, nieuwe organisatie

Op 25 mei 2018 werd de nieuwe Europese privacywet van toepassing: de Algemene verordening gegevensbescherming (AVG). En even daarvoor, op 6 mei 2018, de aparte Richtlijn gegevensbescherming voor de rechtshandhaving. De kern van beide is: meer rechten, meer plichten, steviger toezicht en de oprichting van een nieuw Europees instituut, de European Data Protection Board (EDPB). De Autoriteit Persoonsgegevens (AP) kreeg er als toezichthouder nieuwe taken en bevoegdheden bij, onder meer op internationaal gebied. Dat vroeg om een ander soort organisatie. De nieuwe organisatie van de AP is groter en heeft een nieuwe structuur. Ook heeft de AP een nieuwe missie en een nieuw toezichtkader.

In dit deel van ons jaarverslag staan we kort stil bij de nieuwe wet, vervolgens komt de nieuwe organisatie aan bod en focussen we op ons nieuwe toezichtkader. We kijken hierbij terug op 2018: welke plannen uit ons toezichtkader hebben we in dit jaar uitgevoerd? Daarna gaan we in op de internationale aspecten van ons werk.

Nieuwe wet

De nieuwe privacywet is aangepast aan deze tijd en geeft mensen meer zeggenschap over hun persoonsgegevens. Bovendien gelden nu in de hele Europese Unie dezelfde privacyregels en is er een nieuw Europees privacy-instituut, de EDPB. Mensen hebben door de AVG meer privacyrechten gekregen en organisaties meer verplichtingen en verantwoordelijkheden. De privacytoezichthouders kregen steviger bevoegdheden.

Privacyrechten

Iedereen heeft privacyrechten. Zoals het recht om in te zien welke persoonsgegevens een organisatie van je heeft. Die rechten zijn nu uitgebreid met het recht op data-portabiliteit (het recht om je gegevens mee te nemen) en het recht op vergetelheid (organisaties moeten je persoonsgegevens wissen als je erom vraagt). Verder kunnen mensen een privacyklacht indienen bij de AP als zij het niet eens zijn met hoe een organisatie met hun persoonsgegevens omgaat. De AP behandelt elke klacht.

zie verder: webdossier Privacyrechten
zie verder: webdossier Privacyklacht indienen

Verantwoordelijkheden

Het uitgangspunt van de AVG is dat iedere verwerking van persoonsgegevens onrechtmatig is, tenzij een organisatie een grondslag heeft voor de verwerking. In de AVG is dan ook veel aandacht voor verantwoording (accountability). Dat houdt in dat organisaties moeten kunnen aantonen dat zij zich aan de privacywet houden. In de AVG staat daarom een aantal concrete verantwoordingsplichten, zoals een verwerkingsregister bijhouden. En sommige organisaties zijn bijvoorbeeld ook verplicht om een functionaris gegevensbescherming (FG) te benoemen. Daarnaast moeten organisaties al vanaf de tekentafel bezig zijn met de privacyrisico's. De AVG-regels dwingen organisaties dus om goed na te denken over hoe zij persoonsgegevens verwerken en beschermen.

zie verder: webdossier Verantwoordingsplicht
zie verder: webdossier Functionaris gegevensbescherming (FG)

Toezicht

De AVG heeft ook veranderingen meegebracht voor het toezicht en de toezichthouder. De AP heeft er nieuwe taken en bevoegdheden bij gekregen. Bijvoorbeeld op het gebied van Europese samenwerking, voorlichting aan mensen en organisaties en bij de behandeling van privacy-klachten. Ook kan de AP nu een boete opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde omzet als een organisatie de privacywet overtreedt.

Nieuwe organisatie

Om de nieuwe AVG-taken goed te kunnen uitvoeren, heeft de AP een nieuwe organisatiestructuur gekregen en een andere rechtspositie. Ook is het aantal medewerkers flink gegroeid. Verder heeft de AP een nieuwe vorm van toezicht geïntroduceerd: systeemtoezicht.

Organisatiestructuur
Vanwege de nieuwe taken en bevoegdheden en de grotere organisatie heeft de AP een nieuwe managementstructuur ingesteld, met vier directies.

Rechtspositie
De onafhankelijkheid van de AP is versterkt, doordat de AP sinds 1 januari 2019 eigen rechtspersoonlijkheid heeft gekregen.

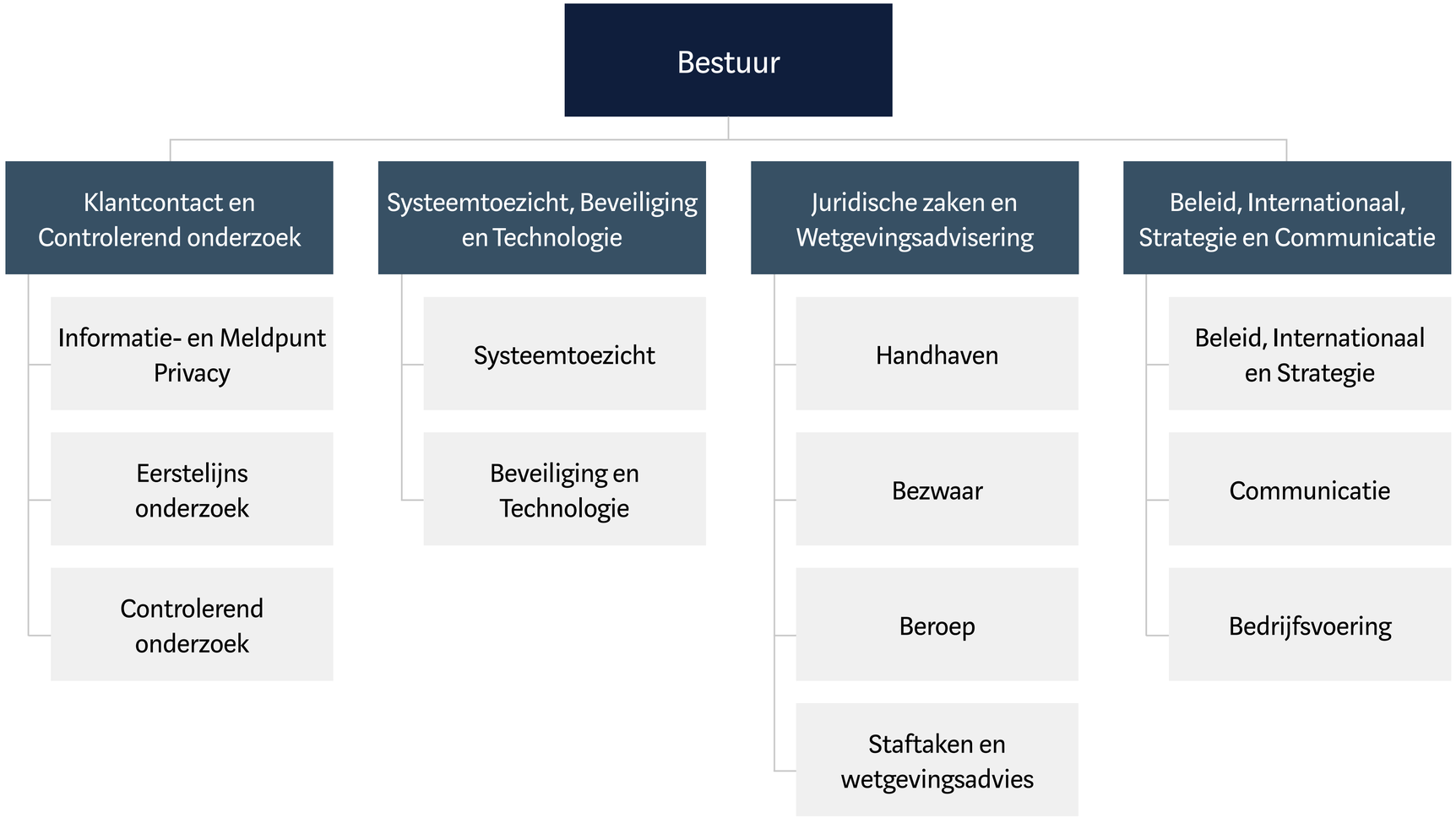
Personeel
Het aantal medewerkers van de AP is in de afgelopen twee jaar meer dan verdubbeld: van 75,7 fte begin 2017 naar 157,1 fte eind 2018. De grootste groei – met meer dan 60 fte – vond plaats in 2018. De verwachting is dat er in 2019 nog meer medewerkers bijkomen.

Systeemtoezicht
Een andere belangrijke wijziging is dat de AP in 2018 een nieuwe vorm van toezicht heeft geïntroduceerd: systeemtoezicht. Uitgangspunt hierbij is het bevorderen van de eigen verantwoordelijkheid van organisaties om aan de privacywetgeving te voldoen. Deze vorm van toezicht is een aanvulling op controlerende onderzoeken, handhaving en communicatie.

AVG-proof
De AP verwerkt zelf ook persoonsgegevens. Gegevens van en over burgers en medewerkers moeten bij de AP veilig zijn en de privacy van deze mensen moet zijn gewaarborgd. In 2018 heeft de AP een AVG-privacybeleid vastgesteld, het beveiligingsbeleid geactualiseerd, een verwerkingsregister opgesteld en alle werkprocessen en autorisaties getoetst en waar nodig aangepast aan de AVG.

Om belangenverstrengeling te voorkomen heeft de AP een externe FG aangesteld. De taken en de positie van de FG zijn uitgewerkt in het Statuut Functionaris gegevensbescherming. Daarnaast heeft de AP binnen iedere directie twee privacycontactpersonen aangewezen en voor directieoverstijgende aspecten een concern-privacycontactpersoon.

Organogram Autoriteit Persoonsgegevens



Bestuur

Het bestuur heeft de leiding over de AP-organisatie. Het bestuur bestond jarenlang uit twee leden. Uit de UAVG volgt dat het bestuur van de AP uit drie leden bestaat: een voorzitter en twee andere leden.

Vicevoorzitter Wilbert Tomesen verliet de AP en werd per 1 juli 2018 voorzitter van het Huis van de Klokkenluiders.

Sinds 1 februari 2019 is het bestuur van de AP compleet. De drie bestuursleden vormen een collegiaal bestuur. De voorzitter en de leden zijn betrokken bij alle werkzaamheden van de AP: toezicht, handhaving, klachtbehandeling, voorlichting en wetgevingsadvisering.

v.l.n.r.: Monique Verdier (vicevoorzitter), Aleid Wolfsen (voorzitter) en Katja Mur (bestuurslid).

Directies

De nieuwe organisatie van de AP bestaat uit vier directies. Onder de directies vallen verschillende afdelingen.

Directie Klantcontact en Controlerend onderzoek
De directie Klantcontact en Controlerend onderzoek bestaat uit het Informatie- en Meldpunt Privacy (IMP) en twee onderzoeksafdelingen. IMP is het eerste aanspreekpunt voor burgers en organisaties met vragen over de AVG. Ook behandelt IMP privacyklachten van mensen.

De afdeling Eerstelijns onderzoek beoordeelt alle meldingen van datalekken en doet beknopt onderzoek naar aanleiding van klachten of datalekmeldingen. De afdeling Controlerend onderzoek doet uitgebreider en complexer onderzoek naar mogelijke overtredingen.

Directie Systeemtoezicht, Beveiliging en Technologie
De directie Systeemtoezicht, Beveiliging en Technologie bestaat uit de afdeling Systeemtoezicht en de afdeling Beveiliging en Technologie.

De afdeling Systeemtoezicht houdt toezicht op de interne privacyprocessen van organisaties en is aanspreekpunt voor brancheorganisaties en FG's. Verder beoordeelt deze afdeling voorafgaande raadplegingen, vergunningaanvragen en privacy-instrumenten als gedragscodes en bindende bedrijfsvoorschriften.

Bij de afdeling Beveiliging en Technologie is de technologische privacy-expertise binnen de AP ondergebracht.

De afdeling levert bijdragen aan de onderzoeken die de andere directies doen.

Directie Juridische Zaken en Wetgevingsadvisering
De directie Juridische Zaken en Wetgevingsadvisering is verantwoordelijk voor de sancties die de AP oplegt. Verder behandelt de directie bezwaarzaken en vertegenwoordigt de directie de AP bij de nationale en Europese rechter.

Daarnaast geeft de directie gevraagd en ongevraagd advies over privacyaspecten van nieuwe wet- en regelgeving. Verder maakt de directie de juridische analyses die de AP nodig heeft om de AVG eenduidig uit te leggen. Tot slot vallen de juridische staftaken onder deze directie, zoals contracten, convenanten, besluiten en WOB-verzoeken.

AutPersoonsgegevens @toezicht_AP · 11 jul. 2018
Bij online streamen is geen sprake meer van beslotenheid van kerkgemeenschap. Omkijken naar mensen betekent ook zuinig zijn op hun privacy. In dat geval is er een grondslag zoals toestemming nodig. Wij zien ook veel misverstanden, soms wordt ten onrechte gemeld dat iets niet mag ‘vanwege de privacywet’. Kerk mag namen van zieken uit kerkgemeenschap natuurlijk in kerkblaadje/tijdens kerkdienst vermelden. Wordt kerkdienst online gestreamd? Dan kan hele wereld meekijken.

Directie Beleid, Internationaal, Strategie en Communicatie
De directie Beleid, Internationaal, Strategie en Communicatie ontwikkelt het beleid en de (middel)langetermijnstrategie van de AP. Ook is de directie op internationaal gebied onder meer verantwoordelijk voor de behandeling van internationale zaken en het (gezamenlijke) toezicht op Europese informatiesystemen.

Verder verzorgt de directie de interne en externe communicatie, onder andere via woordvoering en voorlichtingscampagnes. Tot slot zijn de AP-brede bedrijfsvoeringstaken bij deze directie ondergebracht, zoals ICT, administratie, financiën en het secretariaat.

Tussenstand toezicht 2018-2019

Er is vrijwel geen organisatie te bedenken die géén persoonsgegevens verwerkt, dus bijna iedereen moet zich aan nieuwe regels houden. De AP moet als toezichthouder bevorderen en bewaken dat alle organisaties die nieuwe regels ook echt naleven. In verhouding tot het aantal organisaties is de AP een kleine toezichthouder, die simpelweg niet overal tegelijk kan zijn. De AP heeft daarom een toezichtkader gemaakt, waarin staat wat we in 2018-2019 willen en kunnen doen en hoe we dat gaan doen.

Het toezichtkader geldt voor het halve jaar dus waarin de AVG nog relatief nieuw was, maar ook voor het jaar daarna – wanneer het eerste stof is neergedaald en we meer van organisaties verwachten.

"De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt." Dat is onze missie. In ons toezichtkader beschrijven we daarom eerst wat we doen om de naleving van de privacyregels te bevorderen en daarna wat we doen om de naleving te bewaken.

Als relatief kleine organisatie moet de AP keuzes maken. We bekijken in welke sectoren en bij welke soorten verwerkingen de grootste risico's zijn. En daar richten we ons dan vooral op. Dat noemen we risicogericht toezicht. In het toezichtkader geven wij aan wat onze focus is voor de periode 2018-2019.

In dit onderdeel van ons jaarverslag kijken we terug op 2018. Welke plannen uit ons toezichtkader hebben we ook daadwerkelijk uitgevoerd? Ook blikken we vooruit naar (de tweede helft van) 2019.

Naleving bevorderen

Naleving bevorderen is een net zo belangrijk onderdeel van ons toezicht als de naleving bewaken. De AP bevordert dat organisaties, maar ook mensen zelf, hun verantwoordelijkheid nemen om persoonsgegevens te beschermen. Dit doen wij door beide groepen te informeren over de regels en de risico's.

Zo leggen wij mensen uit wat hun rechten zijn en stimuleren wij organisaties om privacyvriendelijke systemen en processen toe te passen. Daarnaast adviseren wij de overheid – zowel gevraagd als ongevraagd – over nieuwe wet- en regelgeving die over de verwerking van persoonsgegevens gaat.

Voorlichting

De AP maakt zich sterk voor de bescherming van persoonsgegevens als vanzelfsprekende waarde in onze maatschappij. Daarom hebben wij in 2018 nadrukkelijk geïnvesteerd in voorlichting. Dit is een bewuste keuze geweest, naast dat het volgens de AVG expliciet onze taak is om voorlichting te geven.

Wij hebben bijna 27.000 mensen te woord gestaan tijdens onze telefonische spreekuren en 834 keer contact gehad met journalisten. Ook hebben we ruim 70 presentaties en workshops verzorgd voor diverse (branche)organisaties. En tientallen gesprekken gevoerd met stakeholders in uiteenlopende sectoren, om problemen en risico's te signaleren en samen naar oplossingen te zoeken.

Voorlichtingscampagne

Met de campagne 'Privacy gaat iedereen wat aan' hebben wij mensen bewuster gemaakt van hun privacyrechten en organisaties praktische hulp geboden om aan de AVG te voldoen. Bijvoorbeeld met een digitale 'regelhulp' waarmee organisaties snel in kaart konden brengen wat zij nog moesten doen voor 25 mei 2018. In 2019 volgt een nieuwe voorlichtingscampagne voor het algemeen publiek, het mkb en jongeren van 12, 13 en 14 jaar.

Uitleg van de AVG
Wetteksten zijn niet voor iedereen makkelijk te begrijpen. En ook staat niet altijd letterlijk in de wet wat organisaties moeten doen. Daarom heeft de AP samen met de andere Europese privacytoezichthouders diverse *guidelines* gepubliceerd die bepaalde onderwerpen uit de AVG verduidelijken. Maar er zijn ook onderwerpen waarover nog geen *guidelines* bestaan. Om toch alvast duidelijkheid te bieden, heeft de AP in 2018 over diverse onderwerpen uitleg gegeven, zoals wifitracking, direct marketing en grootschalige gegevensverwerkingen in de zorg.

zie verder: AVG-guidelines

Voorlichting aan FG's
Volgens de AVG moeten bepaalde organisaties een FG – een interne toezichthouder – aanstellen en deze aanmelden bij de AP. Omdat FG's een grote rol spelen bij de naleving van de privacyregels binnen organisaties, vindt de AP het belangrijk om een goede relatie met hen te onderhouden. In 2018 zijn 8.000 FG's aangemeld bij de AP. Verder hebben wij zo'n 1.600 vragen van FG's beantwoord en de voorlichting aan FG's via onze website verbeterd.

zie verder: dossier Functionaris gegevensbescherming (FG)

Parlement
De Eerste en Tweede Kamer nodigen de AP met enige regelmaat uit om deel te nemen aan een hoorzitting, rondetafelgesprek of technische briefing. Zo nam de vicevoorzitter van de AP in mei 2018 deel aan een rondetafelgesprek over internetbedrijven en privacybescherming in de Tweede Kamer. De voorzitter nam in oktober 2018 deel aan een technische briefing in de Tweede Kamer over gegevensuitwisseling om ondermijnende criminaliteit te bestrijden. Verder bood de voorzitter in april 2018 de leden van de vaste commissie voor Justitie en Veiligheid van de Tweede Kamer het AP-jaarverslag 2017 aan, waarbij vooral het van toepassing worden van de AVG in mei 2018 onderwerp van gesprek was.

Behandeling van klachten
Iedereen die vermoedt dat een organisatie niet netjes omgaat met zijn of haar persoonsgegevens, kan een privacyklacht indienen bij de AP. Sinds de AVG neemt de AP elke klacht in behandeling die gaat over een mogelijke schending van de eigen persoonsgegevens. In 2018 hebben wij ruim 11.000 klachten ontvangen. De klachten gingen vooral over schending van privacyrechten, zoals het recht op inzage.

Omdat het aantal klachten zo groot was, richtten we ons op manieren om de klachten zo effectief en efficiënt mogelijk te behandelen. Zodat we toch zo veel mogelijk klachten op tijd konden afhandelen. We hebben onder meer uitleg gegeven over de regels, gesprekken gevoerd met organisaties en concrete tips gegeven om de problemen achter de klachten succesvol op te lossen.

De AP heeft zich in 2018 vooral gericht op het beëindigen van mogelijke overtredingen door aan te sturen op herstelmaatregelen door organisaties zelf. Klachten zullen in de toekomst vaker leiden tot onderzoek en sancties van de AP. Daarvoor zullen we meer medewerkers aanstellen.

zie verder: onderdeel 'Klachten en informatieverzoeken' in de bijlage bij het jaarverslag

Wetgevingsadvisering

De wetgever is verplicht om de AP te raadplegen over nieuwe wet- en regelgeving waarin de verwerking van persoonsgegevens aan de orde komt. Deze verplichting is sinds de AVG nog ruimer geworden en is bedoeld om ervoor te zorgen dat de nationale wetgeving in lijn is met de AVG. Ook kan de AP ongevraagd advies geven, niet alleen aan ministeries maar ook aan andere organisaties die betrokken zijn bij nieuwe wet- en regelgeving.

De wetgever is niet verplicht om het advies van de AP op te volgen. Een wetgevingsadvies is dus minder dwingend dan onze andere toezichts- en handhavingsbevoegdheden. Maar het heeft als voordeel dat hiermee al in een vroeg stadium inbreuken op de privacy van mogelijk grote groepen mensen voorkomen kunnen worden.

De AP vindt het dan ook belangrijk om de adviseringstaak nog verder te verbeteren en uit te breiden. Zeker nu de wetgever vaker verplicht is om advies te vragen en wijzelf als ambitie hebben om vaker ongevraagd advies te geven. In 2018 hebben wij daarom een aparte afdeling opgericht voor wetgevingsadvisering en extra adviseurs aangesteld. Verder hebben wij de adviesprocedure verbeterd in overleg met de ministeries. Wij hebben dit jaar prioriteit gegeven aan het op tijd afhandelen van de gevraagde adviezen. We kregen veel meer adviesaanvragen dan in voorgaande jaren (van rond de 30 naar meer dan 80), zodat vrijwel alle capaciteit van de nog nieuwe afdeling daarvoor nodig was.

Een terugkerend punt van aandacht in de wetgevingsadviezen waren de noodzaak, proportionaliteit (staat de privacyinbreuk in verhouding tot het doel?) en subsidiariteit (kan het doel niet op een andere, minder ingrijpende manier worden bereikt?) van voorgenomen gegevensverwerkingen. Daarnaast is van groot belang dat de AVG weliswaar op ruime schaal nationale wetgeving toelaat of vereist, maar dat aan die wetgeving wel eisen worden gesteld. Wetgeving moet vooral een waarborg zijn voor zorgvuldige afweging, niet een vrijbrief voor gegevensverwerking. Tot slot was een belangrijk thema, dat ook in 2019 nog aandacht zal vragen, uitwisseling van persoonsgegevens om ondermijnende criminaliteit tegen te gaan.

zie verder: onderdeel 'Adviesprojecten wetgeving 2018' in de bijlage bij dit jaarverslag

Naleving bewaken

De AP bewaakt dat organisaties zich aan de privacyregels houden door onafhankelijk onderzoek te doen naar (mogelijke) overtredingen. Als een overtreding wordt geconstateerd, treedt de AP handhavend op. Bijvoorbeeld door een boete op te leggen.

Wij werken samen met andere Europese privacytoezichthouders, want wij moeten reageren op nationale én internationale ontwikkelingen. Inherent daaraan is dat wij keuzes moeten maken. Keuzes over onze rol en over de meest effectieve aanpak per situatie.

Om een effectieve toezichthouder te kunnen zijn, past de AP uiteenlopende toezichts- en handhavingsinstrumenten toe. Een officieel onderzoek is bijvoorbeeld niet altijd nodig. Vaak is een waarschuwingsbrief of -gesprek al genoeg om een overtreding te beëindigen. Ons uitgangspunt is dat wij kiezen voor het instrument waarmee we het meeste effect bereiken. De wens van de klager is hierbij leidend.

Controle verantwoordingsplichten

In de AVG is veel aandacht voor verantwoording (*accountability*). Dat houdt in dat organisaties moeten kunnen aantonen dat zij zich aan de privacywet houden. In de AVG staat daarom een aantal concrete verantwoordingsplichten. Zoals een verwerkingsregister bijhouden en een FG aanstellen.

Dat een organisatie deze verantwoordingsplichten op orde heeft, wil niet per definitie zeggen dat de organisatie volledig voldoet aan de AVG. Maar het geeft wel een indicatie van de mate waarin de organisatie serieus werk heeft gemaakt van de implementatie van de AVG. En heeft nagedacht over belangrijke onderdelen uit de AVG, zoals grondslagen, doelbinding en beveiliging.

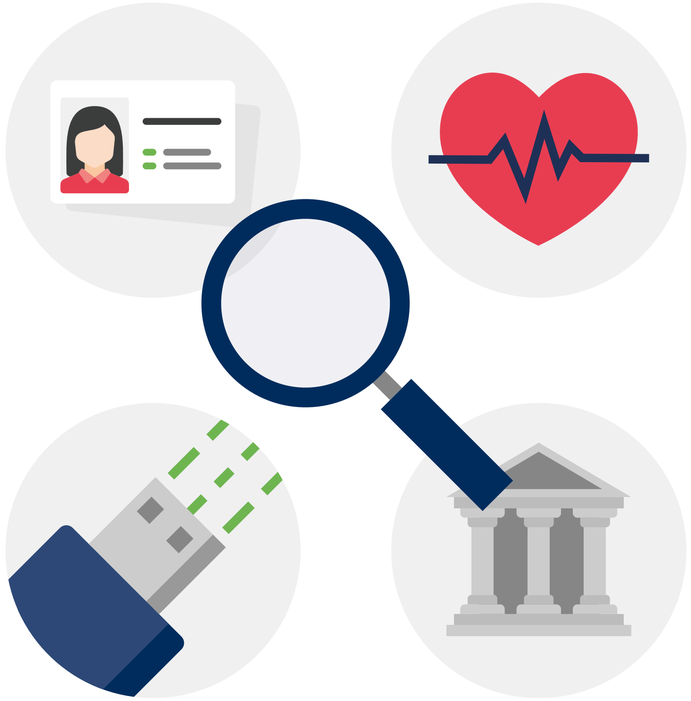
De AP heeft in 2018 in verschillende sectoren de naleving gecontroleerd van (een van de) verantwoordingsplichten uit de AVG: de FG bij de overheid, in de zorg, bij banken en bij verzekeraars; het privacybeleid in de zorg en bij politieke partijen; en tot slot het verwerkingsregister in de private sector.

Risicogericht toezicht

Omdat vrijwel iedere organisatie persoonsgegevens verwerkt, is het aantal organisaties waarop de AP toezicht houdt heel groot. Daarnaast heeft de AP er sinds de AVG geldt een aantal grote taken bij gekregen. Dit betekent dat wij keuzes moeten maken.

Daarbij stellen wij de mensen van wie gegevens worden verwerkt centraal, net als de AVG doet. Onze aanpak is risicogericht. Dat houdt in dat wij trends en privacyrisico's in kaart brengen, waarbij wij er speciaal op letten welke risico's voor grote groepen mensen gelden. Op basis van deze analyse bepalen wij per periode welke toezichtactiviteiten wij uitvoeren binnen welke aandachtsgebieden.

Aandachtsgebieden 2018-2019
In het toezichtkader 2018-2019 heeft de AP aangekondigd zich in deze periode vooral op de volgende sectoren en onderwerpen te richten: overheid, zorg, handel in persoonsgegevens en datalekken.



Overheid en zorg
Zowel overheidsorganisaties als zorginstellingen beschikken over grote hoeveelheden – vaak gevoelige – persoonsgegevens. Mensen zijn bovendien meestal verplicht om hun gegevens aan de overheid af te staan. En in de zorg gaat het vaak om medische gegevens, die tot de gevoeligste gegevens behoren die er zijn. Kortom: mensen moeten erop kunnen vertrouwen dat er zowel bij de overheid als in de zorg uiterst zorgvuldig met hun gegevens wordt omgegaan.

De AP deed in 2018 controles op de verantwoordingsplichten uit de AVG bij de overheid en in de zorg. De AP controleerde bij 400 overheidsorganisaties, 91 ziekenhuizen en 33 zorgverzekeraars of zij een FG hadden aangemeld. Bij de organisaties in de zorg keek de AP ook of zij de contactgegevens van hun FG op de goede manier vermeldden op hun website. Verder is de AP in december 2018 gestart met onderzoek naar het privacybeleid van een aantal IVF-klinieken en bloedbanken.

De AP zal in 2019 bij de overheid en in de zorg blijvende aandacht hebben voor zowel de beveiliging van persoonsgegevens als de vraag of de verwerking gebaseerd is op de juiste grondslag, vooral als de gegevens worden uitgewisseld.

zie verder: hoofdstuk 'Overheid'
zie verder: hoofdstuk 'Gezondheid'

Handel in persoonsgegevens
Datahandelaren verzamelen op grote schaal persoonsgegevens van consumenten via verschillende online en offline bronnen. Zij verwerken de gegevens tot profielen en verkopen deze door. Bijvoorbeeld aan organisaties die de gegevens gebruiken voor direct marketing of voor *creditscoring*. Mensen weten vaak niet om hoeveel gegevens het gaat en welke persoonsgegevens aan welke partijen met welk doel worden verstrekt. Ook zijn zij

meestal niet op de hoogte van profilering – tot het moment dat hun aanvraag voor een lening of abonnement wordt geweigerd. Een ander risico is dat sommige gegevens of opgestelde profielen onjuist zijn, wat grote gevolgen kan hebben. Mensen verliezen zo zeggenschap over hun gegevens.

De AP wil bevorderen dat organisaties die persoonsgegevens verkopen, dit alleen doen op basis van een juiste wettelijke grondslag. En dat zij mensen heldere informatie geven over wat er met hun gegevens gebeurt. Omdat het verhandelen van persoonsgegevens een complex proces is, heeft de AP zich in 2018 gericht op het in kaart brengen van dit proces en het ontwikkelen van een gefaseerde aanpak voor het toezicht op datahandel. Ook heeft de AP uitgebreide uitleg gegeven over wat er wel en niet mag bij direct marketing. Daarnaast is de AP in gesprek gegaan met de branche om de wettelijke regels toe te lichten.

zie verder: hoofdstuk 'Internet en telecom'

Datalekken
Verantwoord omgaan met persoonsgegevens valt of staat met een adequate beveiliging van de gegevens. Slechte beveiliging kan leiden tot een datalek, met alle gevolgen van dien. Een organisatie die een ernstig datalek heeft, moet dit melden aan de mensen van wie de gegevens zijn. Zodat zij bijvoorbeeld snel hun wachtwoord kunnen wijzigen. Ook moet de organisatie het datalek melden bij de AP, zodat de AP zich een beeld kan vormen van de feiten en kan ingrijpen als dat nodig is.

In 2018 werden er 20.881 datalekken gemeld bij de AP. Het aantal meldingen is meer dan verdubbeld vergeleken met 2017. De AP heeft sinds 25 mei 2018 de meeste datalekmeldingen ontvangen van alle Europese privacytoezichthouders. Omdat het aantal meldingen het eerder geschatte aantal fors overstijgt, zullen wij onze capaciteit uitbreiden om meer actie te kunnen ondernemen. Deze acties kunnen leiden tot meer handhavende maatregelen.

In 2018 heeft de AP bij 298 datalekmeldingen actief gehandeld richting de organisaties die het datalek meldden. Over het algemeen leidde dit tot een waarschuwing en gepaste acties van de organisaties. Hieronder vielen ook interventies naar mogelijke datalekken bij organisaties die het datalek níet hadden gemeld bij de AP. In 2019 gaan wij daar meer aandacht aan besteden.

De AP startte 4 onderzoeken: 2 naar niet-gemelde datalekken en 2 naar gemelde datalekken die zijn veroorzaakt door ernstige tekortkomingen in de beveiliging. In november 2018 legde AP Uber een boete van 600.000 euro op voor het te laat melden van een datalek.

zie verder: hoofdstuk 'Beveiliging'

Actualiteit
De AP treedt ook op naar aanleiding van klachten of de actualiteit. In 2018 zijn wij 14 onderzoeken gestart nadat mensen een klacht bij ons hadden ingediend. Ook hebben wij bijvoorbeeld onderzoek gedaan naar camera's in sauna's, nadat er onrust was ontstaan in de media over

gelekte camerabeelden en wij in korte tijd een groot aantal vragen kregen van bezorgde mensen. En ophef over camera's in reclamezuilen was voor ons reden om de regels uit te leggen en daarover een brief te sturen aan de brancheverenigingen.

Sinds 2018 is de AP ook actief op Twitter. Op deze manier kunnen we snel op reageren op vragen en actualiteiten.

zie verder: hoofdstuk 'Cameratoezicht'
zie verder: AP op Twitter

Vooruitblik 2019

In 2018 heeft de AP de nadruk gelegd op het bevorderen van de naleving. Wij hebben daarom veel geïnvesteerd in voorlichting en advisering om organisaties en mensen te laten wennen aan de AVG. Dit is een bewuste keuze geweest, naast dat het volgens de AVG een expliciete taak is van de toezichthouder om voorlichting te geven.

We zijn vooralsnog terughoudend geweest met de inzet van 'zwaardere' middelen als onderzoeken en boetes. In plaats daarvan hebben wij vaker waarschuwingsbrieven aan organisaties gestuurd en gesprekken met hen gevoerd om te bevorderen dat zij zich aan de AVG houden.

Het effect hiervan is dat zowel organisaties als mensen de AVG beter kennen en de AP weten te vinden. En dat zij ons zien als gesprekspartner bij het signaleren en oplossen van privacy-issues. Wij zijn er trots op dat we dit – ondanks onze beperkte middelen – hebben weten te bereiken.

In 2019 gaan wij aan de slag om onze werkprocessen verder te verbeteren, onze risicogestuurde aanpak door te ontwikkelen en de focus van ons toezicht te verbreden van voornamelijk voorlichting naar meer handhaving.

Verbetering werkprocessen

De nieuwe organisatie van de AP heeft een nieuwe missie, een grotere omvang, een andere structuur en een nieuw toezichtkader. De AP is nog volop in ontwikkeling. Daarbij hebben wij het afgelopen jaar zeer veel klachten en datalekmeldingen ontvangen. Daarom gaan we in 2019 verder met het optimaliseren van onze werkprocessen.

AutPersoonsgegevens @toezicht_AP · 2 feb. 2018
Waarom komt er eigenlijk een nieuwe privacywet? We delen onze persoonsgegevens steeds vaker. De #AVG is aangepast aan het digitale tijdperk #privacygaatiedereenwataan autoriteitpersoonsgegevens.nl

Verder gaan we in 2019 meer programmatisch werken. Het doel hiervan is efficiënter te werken en meer effect te bereiken. We verwachten op deze manier onze expertise en instrumenten optimaal te kunnen inzetten. Een voorbeeld hiervan is de aanpak voor het toezicht op handel in persoonsgegevens.

Aanpassen ICT-systemen
Het aantal medewerkers van de AP is in 2018 fors gegroeid. Ook heeft de nieuwe organisatiestructuur nieuwe werkprocessen met zich meegebracht. Wij zijn bezig de ICT-systemen af te stemmen op de nieuwe omvang en processen.

Doorontwikkeling risicogestuurde aanpak
De AP brengt privacyontwikkelingen in kaart door trend- en risicoanalyses te maken. Wij gaan hiertoe onder meer in gesprek met verschillende sectoren, zoals de overheid, de zorg en de financiële sector. Op basis van de aard en omvang van de onderliggende problematiek kiezen wij de meest impactvolle aandachtsgebieden en kijken wij vervolgens welke interventie- en instrumentenmix daar het beste bij past. In 2019 richt de AP zich in ieder geval op niet-gemelde datalekken en handel in persoonsgegevens.

Van voorlichting naar handhaving
In 2019 brengt de AP de inzet van preventieve, correctieve en repressieve instrumenten in evenwicht. Concreet betekent dit: een balans tussen voorlichting, onderzoek en handhaving (zoals boetes). Wij hebben er in 2018 bewust voor gekozen om ons de eerste periode nadat de nieuwe privacywet ging gelden vooral te richten op voorlichting, normuitleg en normoverdracht. Wij vinden dat dit bij een redelijke toezichthouder past. In 2019 geven wij ook voorlichting om de naleving van de privacywetgeving te bevorderen, maar daarnaast gaan wij, vergeleken met 2018, meer onderzoeken doen en waar nodig handhaven.

Internationale samenwerking

Door de AVG gelden in de hele EU dezelfde privacyregels. Een belangrijke stap om de persoonsgegevens van alle EU-inwoners beter te beschermen. Maar minstens zo belangrijk is dat de AVG in alle EU-landen ook op dezelfde manier wordt uitgelegd en toegepast. Zodat iedereen daadwerkelijk dezelfde privacybescherming krijgt en er duidelijkheid is voor organisaties die in meerdere EU-lidstaten actief zijn.

European Data Protection Board

Op 25 mei 2018 is de EDPB opgericht. In de EDPB werken de privacytoezichthouders uit de EU samen bij hun toezicht op de AVG. De EDPB speelt een centrale rol in het zogeheten samenwerkings- en coherentiemechanisme. Dit mechanisme bestaat uit de verschillende instrumenten die de AVG biedt om ervoor te zorgen dat de wet in alle EU-lidstaten hetzelfde wordt geïnterpreteerd en toegepast.

De EDPB coördineert de samenwerking tussen de EU-privacytoezichthouders, neemt (bindende) besluiten en publiceert regelmatig uitleg over de toepassing van de AVG en andere privacykwesties. De AP is de Nederlandse toezichthouder in de EDPB.

In 2018 stond het internationale werk van de AP vooral in het teken van de EDPB. Het merendeel van de 90 internationale bijeenkomsten waaraan de AP deelnam, bestond uit vergaderingen van de EDPB, de bijbehorende subgroepen en verschillende werkgroepen. De AP speelde hierin een actieve rol, bijvoorbeeld door als (hoofd)rapporteur op te treden voor verschillende Europese projecten.

onderdeel 'Autoriteit Persoonsgegevens internationaal' in de bijlage bij dit jaarverslag

Een-loketmechanisme (onestopshop)

Wanneer organisaties in meerdere EU-lidstaten actief zijn – omdat ze vestigingen in meerdere lidstaten hebben of omdat hun activiteiten mensen in verschillende lidstaten raken – kregen ze voorheen te maken met meerdere privacytoezichthouders. Door de AVG is dit veranderd.

De AVG kent het een-loketmechanisme (ook wel 'onestopshop' genoemd). Dit houdt in dat organisaties die grensoverschrijdend gegevens verwerken, nog maar met één privacytoezichthouder zaken hoeven te doen. Die wordt de 'leidende toezichthouder' genoemd. Dit is vrijwel altijd de toezichthouder van het land waar de hoofdvestiging van de organisatie is gevestigd.

Het een-loketmechanisme heeft nog een voordeel. Heeft iemand een klacht over de verwerking van zijn gegevens door een internationale organisatie? Dan krijgt ook deze persoon nog maar met één privacytoezichthouder binnen de EU te maken, zelfs als de organisatie is gevestigd in een andere EU-lidstaat dan waar diegene woont. Zo krijgen alle EU-inwoners dezelfde privacybescherming.

De leidende toezichthouder werkt samen met de zogeheten betrokken toezichthouders. Dit zijn de toezichthouders van de lidstaten waarin ook mensen worden geraakt door de activiteiten van de internationale organisatie.

In 2018 heeft de AP in 69 internationale zaken opgetreden als leidende toezichthouder en in 342 zaken als betrokken toezichthouder.

zie verder: onderdeel 'Internationale zaken' in de bijlage bij dit jaarverslag

zie verder: webdossier Een-loketmechanisme (onestopshop)

Wederzijdse bijstand

De privacytoezichthouders in de EU kunnen elkaar volgens de AVG om wederzijdse bijstand vragen. Dit houdt in dat elke toezichthouder bijvoorbeeld informatie kan opvragen bij een andere toezichthouder of deze kan vragen om iets te doen. Het uitgangspunt is dat de toezichthouders meewerken en binnen 4 weken op zo'n verzoek reageren. In 2018 heeft de AP 15 keer een verzoek om wederzijdse bijstand gekregen en zelf 9 keer om wederzijdse bijstand gevraagd.

AutPersoonsgegevens @toezicht_AP · 6 dec 2018
Meer weten over wat @toezicht_AP op Europees gebied doet? Lees bijvoorbeeld hier wat er in de laatste vergadering van de @EU_EDPB is besproken en besloten:
@EU_EDPB
Read up on the EDPB's 5th plenary meeting here:
https://bit.ly/2zM17fA 07:10 - 6 dec. 2018

Gezamenlijke werkzaamheden

De AVG geeft de EU-privacytoezichthouders de mogelijkheid om in één team, dat bestaat uit medewerkers van verschillende toezichthouders, onderzoek te doen in een of meer EU-lidstaten. Dit worden gezamenlijke werkzaamheden genoemd. Bijvoorbeeld wanneer de leidende toezichthouder en de betrokken toezichthouders samen een onderzoek op locatie willen doen in een complexe, grensoverschrijdende zaak. In 2018 zijn er nog geen gezamenlijke werkzaamheden uitgevoerd.

Adviesprocedure EDPB

Is een van de EU-privacytoezichthouders van plan om een besluit te nemen dat gevolgen kan hebben voor andere EU-lidstaten? Dan moet deze toezichthouder in een specifiek aantal gevallen eerst advies vragen aan de EDPB. Bijvoorbeeld als de toezichthouder van plan is om een (transnationale) gedragscode goed te keuren of een lijst vast te stellen met verwerkingen waarvoor een data protection impact assessment (DPIA) verplicht is.

De privacytoezichthouders kunnen de EDPB ook uit zichzelf om advies vragen. Bijvoorbeeld als ze fundamentele vragen hebben over hoe de AVG moet worden uitgelegd en deze vragen van belang zijn voor (of gevolgen hebben in) meerdere EU-lidstaten. Via de adviesprocedure kunnen de toezichthouders gemeenschappelijke standpunten innemen over kwesties die voor meerdere EU-lidstaten van belang zijn. Hiermee is deze procedure een belangrijk middel voor duidelijke normuitleg en een hoog niveau van gegevensbescherming in de hele EU.

In 2018 heeft de AP 1 keer advies gevraagd aan de EDPB. Dat ging over de Nederlandse lijst van verwerkingen waarvoor een DPIA verplicht is. De EDPB heeft in 2018 27 adviezen vastgesteld.

Bindende besluiten EDPB

In de praktijk kan het voorkomen dat privacytoezichthouders het niet met elkaar eens zijn. Bijvoorbeeld over hoe de AVG op bepaalde punten moet worden uitgelegd.
Als dat gebeurt, leggen zij de vraag voor aan de EDPB. Vervolgens neemt de EDPB een bindend besluit, zodat er toch een duidelijke Europese normuitleg komt.
Alle privacytoezichthouders moeten deze uitleg vervolgens toepassen. In 2018 heeft de EDPB geen bindende besluiten vastgesteld.

Guidelines EDPB

De EDPB publiceert regelmatig guidelines over diverse onderwerpen uit de AVG en de Richtlijn gegevensbescherming voor de rechtshandhaving. Met deze guidelines laat de EDPB zien hoe bepaalde punten uit de nieuwe privacywetgeving moeten worden begrepen of toegepast.
Het doel hiervan is mensen inzicht te bieden in hun privacyrechten en organisaties duidelijk te maken wat zij moeten doen.

De voorloper van de EDPB, de Artikel 29-werkgroep, heeft in de aanloop naar 25 mei 2018 diverse guidelines voorbereid. De EDPB heeft deze 16 guidelines na 25 mei formeel overgenomen. Daarnaast heeft de EDPB in 2018 4 nieuwe guidelines opgesteld. De AP heeft regelmatig de

leiding genomen bij het opstellen van guidelines binnen de Artikel 29-werkgroep en de EDPB.

zie verder: AVG-guidelines
zie verder: onderdeel 'Autoriteit Persoonsgegevens Internationaal' in de bijlage bij het jaarverslag

Europees toezicht op politie en justitie

In 2018 heeft de AP, net als in voorgaande jaren, deelgenomen aan verschillende Europese toezichthoudende groepen op het gebied van politie, justitie en migratie. Het gaat onder meer om het toezicht op Europol, Eurojust en een aantal Europese informatiesystemen.

Nieuw toezichtplatform

De AP heeft in 2018 uitgebreid overleg gevoerd in de groep BTLE (Borders, Travel and Law Enforcement) en diverse andere toezichtgroepen om een nieuw toezichtplatform op te richten. Het doel van dit nieuwe platform is om al deze aparte toezichtgroepen op het gebied van politie, justitie en migratie te vervangen. Naar verwachting wordt dit nieuwe model van toezichthouden in de loop van 2019 vastgesteld.

SIS II

De AP heeft in 2018 meegedaan aan twee Schengen-evaluaties. Samen met de Europese Commissie controleren de EU-privacytoezichthouders hierbij of de lidstaten het Schengen Informatiesysteem (SIS II) volgens de regels gebruiken.

zie verder: webdossier Europese informatiesystemen
zie verder: onderdeel 'Autoriteit Persoongegevens Internationaal' in de bijlage bij het jaarverslag

Internationale doorgifte

De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld. Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag daarom alleen als een land voldoende bescherming biedt.

Om gegevens te mogen doorgeven buiten de Europese Economische Ruimte (EER), kunnen internationaal opererende organisaties bindende bedrijfsvoorschriften (binding corporate rules, BCR's) opstellen of een modelcontract van de Europese Commissie gebruiken.

De AP beoordeelt, samen met de andere EU-privacytoezichthouders, of BCR's en modelcontracten voldoende waarborgen hebben om de doorgifte van persoonsgegevens buiten de EER veilig te laten zijn. In 2018 heeft de AP 6 nieuwe modelcontracten afgehandeld. Verder zijn er 32 nieuwe BCR's bij de AP ingediend en 5 gewijzigde modelcontracten.

Overheid

Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige – persoonsgegevens. Mensen zijn meestal verplicht om hun persoonsgegevens af te geven aan de overheid. Daarom moet iedereen erop kunnen vertrouwen dat de overheid zorgvuldig met deze gegevens omgaat. En dat de overheid dus bijvoorbeeld altijd een wettelijke basis heeft om gegevens te verwerken, niet meer persoonsgegevens verwerkt dan noodzakelijk en de gegevens goed beveiligt.

NL 123456789 B01

btw-nummer

Het BSN van zzp'ers is deel van hun btw-nummer. Dat maakt hen kwetsbaar voor identiteitsfraude. De AP legde een verwerkingsverbod op aan de Belastingdienst. Dit betekent dat het BSN geen deel meer mag zijn van het btw-nummer.

400

organisaties

De AP controleerde bij ruim 400 overheidsorganisaties of zij een FG hadden aangemeld. De FG is de interne privacytoezichthouder van een organisatie.

1-1-19

nieuwe richtlijn

Naast de nieuwe privacywet, de AVG, is er de aparte Richtlijn gegevensbescherming voor de rechtshandhaving. In Nederland is deze richtlijn per 1 januari 2019 geïmplementeerd. De AP hielp de sector politie en justitie bij de voorbereiding op deze implementatie.

Onderzoek btw-nummer

Het burgerservicenummer (BSN) van zzp'ers is deel van hun btw-nummer. Omdat zij wettelijk verplicht zijn om dit nummer op hun facturen te vermelden en soms ook op hun website, is hun BSN breed bekend. Dat maakt hen kwetsbaar voor identiteitsfraude.

De Autoriteit Persoonsgegevens (AP) heeft daarom in december 2018 een verwerkingsverbod opgelegd aan de Belastingdienst. Dit gebeurde nadat de AP eerder dat jaar na onderzoek concludeerde dat de Belastingdienst geen wettelijke basis heeft om het BSN te gebruiken in het btw-identificatienummer.

Het verwerkingsverbod gaat per 1 januari 2020 in. Vóór die tijd moet de Belastingdienst dus maatregelen hebben genomen die ervoor zorgen dat het BSN niet langer deel is van het btw-nummer. De Belastingdienst heeft de AP laten weten welke maatregelen genomen zullen worden. Op papier lijken deze maatregelen voldoende, maar ze moeten eerst nog worden uitgevoerd voordat de AP kan beoordelen of de overtreding daarmee is beëindigd.

Belastingdienst mag BSN niet meer gebruiken in btw-identificatienummer

'Het BSN van zelfstandigen moet gewoon goed beschermd worden.'

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens

Controle FG's overheid

Sinds de Algemene verordening gegevensbescherming (AVG) geldt, moeten alle overheidsorganisaties een functionaris gegevensbescherming (FG) hebben. De FG is, kort gezegd, de interne privacytoezichthouder van een organisatie. Organisaties moeten aan de AP laten weten wie hun FG is.

In 2018 onderzocht de AP in meerdere sectoren of organisaties een FG hadden aangemeld. De AP startte met deze controles bij de overheid: bij ruim 400 overheidsorganisaties, waaronder gemeenten, provincies, waterschappen, ministeries en een aantal zelfstandige bestuursorganen.

De meeste van deze organisaties bleken al te voldoen aan de eis om een FG aan te stellen. De AP liet de overige organisaties weten dat zij alsnog een FG moesten aanmelden, omdat zij anders een sanctie konden krijgen. Bij de afronding van het onderzoek hadden alle gecontroleerde overheidsorganisaties een FG aangemeld.

AP rondt controle af op functionaris gegevensbescherming overheid

AutPersoonsgegevens @toezicht_AP · 13 nov. 2018

Euh? Natuurlijk heeft de brandweer het hele adres nodig om snel ter plaatse te zijn! Privacywet staat dit niet in de weg. De brandweer mag gegevens verwerken ‘als dat noodzakelijk is voor de vervulling van hun taak in het algemeen belang’
(zie ook autoriteitpersoonsgegevens.nl) ^PG

Onderzoek gemeenten

Gemeenten verzamelen meer persoonsgegevens dan noodzakelijk is om te beoordelen welke zorg mensen nodig hebben. Dat concludeerde de AP begin 2018 na onderzoek. De AP onderzocht bij twee gemeenten de manier waarop zij persoonsgegevens verwerkten in een zelfredzaamheidsmatrix (ZRM). Met dit onderzoek liet de AP zien hoe alle gemeenten die een ZRM gebruiken, dit zorgvuldig en volgens de privacywet kunnen doen.

De ZRM is een instrument waarmee wordt gemeten hoe zelfredzaam mensen zijn. Bij de uitvoering van de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet gebruiken veel gemeenten de ZRM als leidraad bij contacten met burgers. Bijvoorbeeld tijdens keukentafelgesprekken. Met een ZRM verzamelt de gemeente persoonsgegevens op veel verschillende gebieden, zoals lichamelijke en psychische gezondheid, financiën en justitie.

Uit het onderzoek van de AP bleek dat de twee gemeenten bij het gebruik van een ZRM ook persoonsgegevens van mensen verzamelden die niet relevant waren voor hun hulpvraag. Dat mag niet volgens de privacywet. Gemeenten die een ZRM gebruiken, moeten hun werkwijze hierop aanpassen.

De AP kwam er ook achter dat de gemeenten geen goede instructies gaven aan hun medewerkers over wat zij mensen wel en niet mogen vragen. Terwijl gemeenten verplicht zijn om ervoor te zorgen dat medewerkers hun werk goed kunnen doen, bijvoorbeeld door opleidingen te organiseren en goede handleidingen te maken.

Gemeenten verzamelen te veel persoonsgegevens bij uitvoering Wmo en Jeugdwet

Advies wijziging Wet Bibob

De minister van Justitie en Veiligheid wil de wet Bibob op een aantal punten aanpassen. Zo zouden overheden de wet Bibob vaker kunnen toepassen. In september 2018 adviseerde de AP kritisch over dit wetsvoorstel. De AP adviseerde om het voorstel niet in deze vorm door te zetten, maar het eerst beter te onderbouwen. Bijvoorbeeld door bij diverse onderdelen te motiveren waarom er sprake is van een *pressing social need*, die wettelijk vereist is om de grotere privacyinbreuk te rechtvaardigen.
En als deze onderbouwing niet mogelijk blijkt,
van de wetswijziging af te zien.

De wet Bibob staat voor de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur. Met deze wet in handen kunnen overheden optreden als het gevaar dreigt dat een vergunning wordt misbruikt voor criminele activiteiten. Overheden kunnen (laten) onderzoeken of de aanvrager van de vergunning betrouwbaar is en zo niet, de vergunning weigeren of een al afgegeven vergunning intrekken.

Het wetsvoorstel is op het moment van publicatie van dit jaarverslag nog in behandeling.

> ‘De AP onderschrijft uiteraard het belang om criminele activiteiten aan te pakken. De voorgestelde wijzigingen kunnen echter te grote gevolgen hebben voor de privacy van betrokkenen.’
>
> Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens

Advies wijziging Wet Bibob

Onderzoek politie

In december 2018 legde de AP voor de tweede keer een last onder dwangsom op aan de Nationale Politie voor een voortdurende overtreding. De Nationale Politie moest betere maatregelen treffen om politiegegevens goed te beveiligen tegen onbevoegde inzage door politiemedewerkers. Eind februari 2019 constateerde de AP dat er inmiddels voldoende maatregelen waren genomen, waardoor de Nationale Politie aan de last voldoet.

De overtreding betrof de beveiliging van het N.SIS II-systeem. In dit systeem staat informatie over signaleringen binnen het Schengengebied, zoals gegevens over gezochte of vermiste personen of over gestolen voertuigen. Niet alle medewerkers van de Nationale Politie die toegang hebben tot dit systeem mogen ongelimiteerd alle politiegegevens inzien. Daarom moet de Nationale Politie regelmatig en proactief controleren wie welke informatie heeft ingezien.

Begin 2017 legde de AP een last onder dwangsom op aan de Nationale Politie vanwege onvoldoende controle op logbestanden van N.SIS II. Daarna heeft de Nationale Politie een dwangsom van 40.000 euro betaald, omdat de overtreding niet was beëindigd. In november 2018 legde de AP een tweede last onder dwangsom op, omdat de AP de tot dan toe getroffen maatregelen onvoldoende vond. De Nationale Politie heeft bezwaar gemaakt tegen de last onder dwangsom. Deze procedure loopt nog.

Nationale Politie voldoet aan last onder dwangsom

Implementatie Richtlijn gegevensbescherming voor de rechtshandhaving

Naast de nieuwe privacywet, de AVG, is er de aparte Richtlijn gegevensbescherming voor de rechtshandhaving. Deze richtlijn werd op 6 mei 2018 van toepassing en had op die datum ook omgezet moeten zijn in nationale wetgeving. In Nederland is de richtlijn per 1 januari 2019 geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

De AP heeft in het najaar van 2018 de sector politie en justitie benaderd bij de voorbereiding op deze implementatie. Zo heeft de AP een bijeenkomst georganiseerd voor de FG's van organisaties die te maken hebben met de Wpg en Wjsg, zoals de Nationale Politie, het Openbaar Ministerie en de bijzondere opsporingsdiensten.

Aparte richtlijn voor rechtshandhaving

De AVG geldt niet voor alle autoriteiten die als taak hebben om strafbare feiten op te sporen en te vervolgen, straffen uit te voeren en de openbare veiligheid te beschermen. Zoals de politie en het Openbaar Ministerie.

Daarvoor geldt de Richtlijn gegevensbescherming voor de rechtshandhaving. Deze speciale regels zijn er omdat deze autoriteiten speciale bevoegdheden nodig hebben om deze taken te kunnen uitvoeren.

Voor hun andere taken is de AVG wel van toepassing. Bijvoorbeeld bij de verwerking van personeelsgegevens.

Gezondheid

Gegevens over iemands gezondheid behoren tot de gevoeligste persoonsgegevens die er zijn. Daarom zijn het bijzondere persoonsgegevens, die wettelijk extra zijn beschermd. Dat betekent dat er strengere regels gelden voor het verwerken van deze gegevens. Bijvoorbeeld door zorginstellingen, die over grote hoeveelheden medische persoonsgegevens beschikken. Het is dan ook essentieel dat zorginstellingen zich aan de privacywet houden, vooral bij speciale verplichtingen als een functionaris gegevensbescherming (FG) aanstellen en een privacybeleid hebben.

124

organisaties

De AP controleerde bij 124 organisaties in de zorg (91 ziekenhuizen en 33 zorgverzekeraars) of zij een FG hadden aangemeld. En of zij de contactgegevens van de FG op hun website vermeldden. De FG is de interne privacytoezichthouder van een organisatie.

10.000

patiënten

Organisaties die als kerntaak op grote schaal bijzondere persoonsgegevens verwerken, hebben een aantal verplichtingen. Maar wanneer is een verwerking grootschalig? Volgens de AP altijd bij ziekenhuizen, huisartsenposten en zorggroepen; daarbuiten als het gaat om meer dan 10.000 patiënten in één informatiesysteem.

BrainCompass

Uit onderzoek van de AP bleek dat assessmentbureau BrainCompass de privacywet overtrad bij de verwerking van gegevens over onder meer gezondheid en ras. In 2018 liet de AP weten dat de overtredingen waren beëindigd.

Controle FG's

Sinds de nieuwe privacywet geldt, moeten onder meer alle ziekenhuizen en zorgverzekeraars een functionaris gegevensbescherming (FG) hebben. De FG is, kort gezegd, de interne privacytoezichthouder van een organisatie.

Vervolgens moeten deze organisaties aan de Autoriteit Persoonsgegevens (AP) laten weten wie hun FG is. En de contactgegevens van hun FG (direct telefoonnummer, e-mailadres, postadres en/of direct contactformulier) op hun website publiceren. Zodat iedereen die dat wil, snel en in vertrouwen contact kan opnemen met de FG over privacy-issues.

De FG's vervullen bij grotere zorgorganisaties een belangrijke functie om de medische gegevens van mensen te beschermen en om de privacywetgeving na te leven.

De AP controleerde bij 91 ziekenhuizen en 33 zorgverzekeraars of zij een FG hadden aangemeld en de contactgegevens hadden gepubliceerd. Uit een eerste controle bleek dat 2 ziekenhuizen nog geen FG hadden aangemeld bij de AP. En dat 17 ziekenhuizen en 2 zorgverzekeraars nog geen directe contactgegevens op hun website hadden geplaatst. Van de organisaties die wel contactgegevens op hun website vermeldden, vond de AP aanvankelijk bij 3 ziekenhuizen en 1 zorgverzekeraar geen direct e-mailadres of doorkiesnummer.

Inmiddels hebben, door toedoen van de AP, alle gecontroleerde ziekenhuizen en zorgverzekeraars een FG aangemeld. Ook vermelden zij nu allemaal op een goede manier de contactgegevens van hun FG's.

AP rondt controle ziekenhuizen en zorgverzekeraars af

Uitleg begrip 'grootschalig'

De Algemene verordening gegevensverwerking (AVG) bevat een aantal verplichtingen voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken en dit als kerntaak hebben. Deze organisaties moeten een FG aanstellen en in bepaalde gevallen een *data protection impact assessment* (DPIA) doen.

AutPersoonsgegevens @toezicht_AP · 17 aug. 2018
Er is veel te doen over kinderdagverblijven en vaccinaties. Wat zegt de privacywet daar eigenlijk over? Mag een kinderdagverblijf deze gegevens van kinderen zomaar registreren? autoriteitpersoonsgegevens.nl

In de zorg hebben organisaties vrijwel altijd als kerntaak het verwerken van bijzondere persoonsgegevens, omdat zij medische gegevens verwerken. Maar wanneer is de verwerking grootschalig? In de AVG staat niet precies uitgelegd wat 'grootschalig' inhoudt. De AP kreeg hierover veel vragen van zorgverleners. Daarom besloot de AP uitleg te geven.

Uitleg AP

De verwerking van persoonsgegevens door ziekenhuizen, huisartsenposten en zorggroepen interpreteert de AP altijd als grootschalig. Voor alle overige zorgaanbieders (zoals huisartsenpraktijken, verpleeg- en verzorgingstehuizen, ggz-instellingen en instellingen voor medisch-specialistische zorg, die geen ziekenhuis zijn) geldt dat zij grootschalig persoonsgegevens verwerken als zij van meer dan 10.000 patiënten gegevens verwerken in één informatiesysteem.

Apothekers

Verwerkingen van persoonsgegevens door apothekers ziet de AP al gauw als grootschalig, omdat apotheken gemiddeld genomen veel patiënten bedienen en met veel andere zorgaanbieders gegevens uitwisselen. Het zou dus goed zijn als apotheken een FG hebben. Maar als er minder dan 10.000 patiënten in het systeem van de apotheek zijn ingeschreven, ziet de AP dat – net als bij de andere zorgaanbieders – niet als grootschalig.

Tips van de AP

- Geen grootschalige verwerking? Een FG kan nog steeds nuttig zijn!
- Een FG kan worden 'gedeeld' met andere zorgaanbieders.
- Een FG kan extern (voor een beperkt aantal uren) worden ingehuurd.

Uitleg begrip 'grootschalig' verduidelijkt voor alle zorgaanbieders

Privacybeleid zorginstellingen

In december 2018 heeft de AP het privacybeleid opgevraagd van een aantal zorginstellingen en politieke partijen. Dit zijn voorbeelden van organisaties die op grond van de privacywet een privacybeleid moeten hebben. Deze organisaties verwerken namelijk bijzondere persoonsgegevens over gezondheid en politieke voorkeur, die extra goed beschermd moeten worden. Hebben deze organisaties geen privacybeleid of voldoet dit niet aan de eisen, dan overtreden zij de privacywet.

De AP heeft bij in totaal 53 bloedbanken, IVF-klinieken en de politieke partijen van 3 gemeenten het privacybeleid opgevraagd. De AP is bezig te beoordelen of het beleid voldoet aan de wettelijke eisen. Zo moet bijvoorbeeld helder zijn welke categorieën persoonsgegevens worden verwerkt, met welk doel, hoe de gegevens worden beveiligd, welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen.

Controle op privacybeleid bij zorginstellingen en politieke partijen

Privacybeleid

- Met een privacybeleid brengen organisaties in kaart welke maatregelen zij hebben genomen om de persoonsgegevens van bijvoorbeeld hun klanten, patiënten of cliënten te beschermen.
- Daarnaast kunnen organisaties hiermee aan zowel de doelgroep als aan de AP laten zien dat zij voldoen aan de privacywet.
- Let op: een privacybeleid is iets anders dan een privacyverklaring. Alle organisaties die persoonsgegevens verwerken, moeten mensen heldere informatie geven over de persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij dit doen. Bij voorkeur in een online privacyverklaring.

AutPersoonsgegevens @toezicht_AP · 6 apr. 2018

AutPersoonsgegevens heeft geretweet EenVandaag

Iedere patiënt heeft recht op een goede bescherming van zijn persoonsgegevens. Of je nu een BN'er of de buurvrouw bent. #privacygaatiedereenwataan

Onderzoek BrainCompass

Assessment-platform BrainCompass verwerkt niet langer persoonsgegevens over gezondheid en ras in strijd met de privacywet. De privacy van deelnemers is daardoor beter gewaarborgd. Dat liet de AP in oktober 2018 weten.

BrainCompass is een specifiek soort assessmentbureau. De basis voor hun rapportage is een persoonlijk en een biologisch profiel. Hiervoor worden gegevens verzameld en met elkaar in verband gebracht zoals het ras van de deelnemer, gewicht en lengte, DNA-gegevens en psychologische gegevens.

In 2017 concludeerde de AP na onderzoek dat BrainCompass niet op de juiste manier toestemming vroeg aan deelnemers voor de verwerking van hun gegevens. Ook het beveiligingsbeleid was niet op orde. BrainCompass heeft daarop verbeteringen doorgevoerd, zodat de overtredingen zijn beëindigd.

Een deel van de mensen die bij BrainCompass een assessment ondergaat, doet dit binnen een arbeidsrelatie. In zo'n relatie, waarin de werknemer (financieel) afhankelijk is van de werkgever, is over het algemeen geen sprake van 'vrije' toestemming. BrainCompass heeft ervoor gezorgd dat de toestemming aan BrainCompass voldoende vrij is, bijvoorbeeld door geen informatie over de deelnemer meer te delen met de werkgever en de assessments niet meer in groepssessies af te nemen.

Ook is er een BrainCompass-variant ontwikkeld waarbij in het geheel geen bijzondere persoonsgegevens worden verwerkt en informeert BrainCompass klanten op de juiste manier bij het vragen om toestemming. Tot slot heeft BrainCompass een beveiligingsbeleid opgesteld.

BrainCompass past werkwijze aan na onderzoek AP

Advies Besluit forensische zorg

Het medisch beroepsgeheim is de kern van de privacybescherming in de gezondheidszorg. De AP vindt dan ook dat de overheid uiterst terughoudend moet zijn met wettelijke regelingen die het medisch beroepsgeheim doorbreken. Dit is een van de redenen dat de AP in juni 2018 kritisch adviseerde over het voorgestelde Besluit forensische zorg.

Mensen die in aanraking komen met politie en justitie, kunnen een stoornis of een verstandelijke beperking hebben. Als onderdeel van hun straf of maatregel kunnen zij forensische zorg opgelegd krijgen.

De Wet forensische zorg (Wfz) en het bijbehorende Besluit forensische zorg, dat de wet op een aantal punten verder uitwerkt, hebben als doel de forensische zorg op verschillende punten te verbeteren. Onderdeel daarvan is dat er vaker gegevens van forensische patiënten worden uitgewisseld.

Noodzaak
De AP mist echter bij diverse onderdelen van het conceptbesluit de motivering waarom er een noodzaak zou zijn om gegevens uit te wisselen. Bijvoorbeeld als er wordt gesteld dat het noodzakelijk is dat de zorgaanbieder gegevens krijgt over de rechtszaak, de uitvoer van de straf of de reclassering, maar niet wordt uitgelegd waarom dat zo is.

Ook mist de AP op meerdere plekken de onderbouwing dat de gegevensverwerkingen voldoen aan de wettelijke beginselen van proportionaliteit (staat de privacyinbreuk in verhouding tot het doel?) en subsidiariteit (kan het doel niet op een andere, minder ingrijpende manier worden bereikt?).

Medisch beroepsgeheim
De zorgaanbieder moet volgens de Wfz en het conceptbesluit gegevens over de behandeltrouw van de forensische patiënt aan het Openbaar Ministerie (OM) of de reclassering verstrekken. Hierdoor wordt het medisch beroepsgeheim van de zorgaanbieder doorbroken.

De AP adviseert om in het conceptbesluit op te nemen dat de zorgaanbieder per geval beoordeelt of het noodzakelijk is om de gegevens door te geven aan het OM of de reclassering. Ook vindt de AP de bepaling over het verstrekken van de gegevens te ruim en adviseert de AP om deze in te perken.

Advies Besluit forensische zorg

Internet & telecom

Via internet- en telecomdiensten – zoals websites, apps, zoekmachines, maar ook besturingssystemen en het wifisignaal van mobiele telefoons – kunnen organisaties mensen op de voet volgen. Vaak worden de verzamelde persoonsgegevens gebruikt voor commerciële doelen. Bijvoorbeeld om mensen gerichte advertenties te laten zien. Het kan voordelen opleveren als organisaties mensen beter leren kennen en hun aanbod daarop afstemmen. Maar dan moeten mensen wél weten dat dit gebeurt en zelf kunnen beslissen of ze dit willen.

4 miljoen

apparaten

In Nederland zijn ruim 4 miljoen actieve apparaten met Microsoft Windows 10 Home en Pro. Maar na onderzoek van de AP bleek de privacy van Windows 10-gebruikers niet goed beschermd. Microsoft beloofde met de Windows 10-update van april 2018 herstelmaatregelen door te voeren.

9,6 miljoen

mensen

Zo'n 9,6 miljoen mensen in Nederland gebruiken Facebook. Maar Facebook informeerde deze mensen niet goed over het gebruik van hun gegevens, bleek uit onderzoek van de AP. Hierop kwam Facebook in april 2018 met een aangepast privacybeleid.

wifitracking

Mogen bedrijven mensen volgen op straat, in winkelcentra of op stations via hun mobiele telefoon? Meestal niet, liet de AP weten na vragen over dit onderwerp. Wifitracking is namelijk slechts onder zeer strikte voorwaarden toegestaan.

Onderzoek Windows

In Nederland zijn er meer dan 4 miljoen actieve apparaten met Microsoft Windows 10 Home en Pro. Van deze grote groep mensen die Windows 10 gebruikt, was de privacy niet goed beschermd. Dat bleek in oktober 2017 uit onderzoek van de Autoriteit Persoonsgegevens (AP). Microsoft beloofde hierop herstelmaatregelen, die met de Windows 10-update van april 2018 zouden worden doorgevoerd – niet alleen in Nederland maar in de hele Europese Unie, zoals de AP had geëist.

Microsoft verzamelt continu technische prestatie- en gebruiksgegevens van Windowsgebruikers. Bijvoorbeeld welke apps de gebruiker heeft geïnstalleerd en, afhankelijk van de privacy-instellingen, hoe vaak de apps worden gebruikt en welke sites de gebruiker bezoekt. Deze gegevens worden telemetriegegevens genoemd.

Microsoft informeerde de gebruikers hier niet goed over. Daardoor hadden zij onvoldoende controle over hun gegevens. Ze wisten niet welke gegevens waarvoor werden gebruikt. Ook wisten zij niet dat zij gepersonaliseerde advertenties en aanbevelingen konden krijgen als zij dit niet hadden uitgeschakeld.

De AP heeft na de Windows 10-update een nacontrole uitgevoerd om te bekijken of de beloofde herstelmaatregelen inderdaad zijn doorgevoerd. De AP is nog bezig met het verwerken van de resultaten van de nacontrole.

Privacy van Windows-gebruikers sterk verbeterd na onderzoek AP

Onderzoek Facebook

Zo'n 9,6 miljoen mensen in Nederland gebruiken Facebook. De AP deed in 2017 onderzoek naar hoe Facebook omging met de privacy van deze grote groep mensen. De AP constateerde toen dat het bedrijf in strijd handelde met de Nederlandse privacywetgeving. Bijvoorbeeld omdat Facebook mensen niet duidelijk informeerde over het gebruik van hun gegevens voor gerichte advertenties. Hierop kwam Facebook in april 2018 met een aangepast privacybeleid.

AutPersoonsgegevens @toezicht_AP · 16 nov. 2018
Wij krijgen regelmatig vragen van mensen die hun gegevens willen laten verwijderen uit de zoekresultaten van een zoekmachine. Moet een zoekmachine meewerken? Wanneer hoeft een zoekmachine niet aan een verwijderverzoek te voldoen? Lees het in onze Q&A's autoriteitpersoonsgegevens.nl

Gebruikers van Facebook kregen daarmee uitgebreidere informatie over wat voor gegevens Facebook verwerkt, waarvoor dit gebeurt, met wie en hoe Facebook gegevens deelt en op basis van welke rechtsgronden het bedrijf persoonsgegevens verwerkt.

Of Facebook voldoet aan de nieuwe Europese privacywet, die sinds 25 mei 2018 geldt, zal moeten worden onderzocht in Europees verband. Bij zo'n onderzoek heeft de Ierse privacytoezichthouder de leiding, omdat de hoofdvestiging van Facebook in Ierland staat.

Facebook past beleid aan na onderzoek AP

Aanpak social media

Hoe komen socialmediaplatformen eigenlijk aan hun gegevens? En hoe voorkomen ze dat deze gegevens in handen komen van mensen die er niets mee te maken hebben? Met deze vragen gaat een speciale privacywerkgroep zich bezighouden.

Dat lieten de samenwerkende Europese privacytoezichthouders, waaronder de AP, in april 2018 weten. Aanleiding voor het instellen van de werkgroep is de manier waarop Facebook persoonsgegevens heeft gedeeld met Cambridge Analytica en andere apps.

De werkgroep ontwikkelt een langetermijnstrategie voor het gebruik van persoonsgegevens door social media. Uitgangspunt is de bescherming van persoonsgegevens tegen onrechtmatig gebruik op socialmediaplatformen. De werkgroep kijkt niet alleen naar social media maar ook naar andere partijen, zoals datahandelaren en app-ontwikkelaars.

Europese privacytoezichthouders trekken samen op in aanpak social media

Uitleg direct marketing

Veel mensen maken zich zorgen over direct marketing, merkt de AP aan de hoeveelheid vragen over dit onderwerp. Mensen vragen zich vooral af hoe bedrijven aan hun gegevens zijn gekomen. Voor de AP is de handel in data dan ook een van de speerpunten in het toezichtkader voor 2018 en 2019. Maar ook vanuit de branche zelf kwamen er in de aanloop naar de nieuwe privacywet, de Algemene verordening gegevensbescherming (AVG), regelmatig vragen bij de AP binnen.

Daarom publiceerde de AP uitgebreide informatie over de spelregels voor direct marketing. De belangrijkste regel is dat bedrijven meestal alleen iemands persoonsgegevens mogen gebruiken voor direct marketing als diegene hiervoor toestemming heeft gegeven. Tenzij het gaat om direct marketing voor soortgelijke producten naar bestaande klanten en, bij direct marketing per post,

het marketingdoel verenigbaar is met het doel waarvoor de gegevens zijn verkregen. Bovendien stelt de AVG strengere eisen aan de benodigde toestemming dan de vorige privacywet. En ook aan de kwaliteit en begrijpelijkheid van de informatie die bedrijven geven over hun direct marketing.

zie verder: dossier Direct marketing

Uitleg wifitracking

Mogen bedrijven mensen volgen op straat, in winkelcentra of op stations via hun mobiele telefoon? Meestal niet, liet de AP in november 2018 weten na vragen over dit onderwerp. Wifitracking, en ook andere digitale middelen om personen te volgen, zijn namelijk slechts onder zeer strikte voorwaarden toegestaan.

Omdat er bij wifitracking vrijwel altijd persoonsgegevens worden verwerkt, valt deze volgmethode onder de privacywet, de AVG. Ook als de gegevens gepseudonimiseerd worden verwerkt en bewaard, is de AVG van toepassing.

De AVG bepaalt dat organisaties die persoonsgegevens verwerken, een goede grondslag moeten hebben voor die verwerking. Bij wifitracking zou het bijvoorbeeld kunnen gaan om het uitvoeren van een contract of om het handhaven van de veiligheid. In beide gevallen is het dan altijd de vraag of tracking noodzakelijk is, omdat er ook minder ingrijpende alternatieven zijn. Het vragen van toestemming aan mensen die in het gebied lopen is in theorie een laatste mogelijkheid, maar is in de praktijk vooralsnog niet uitvoerbaar.

Bedrijven mogen mensen alleen bij hoge uitzondering met wifitracking volgen

> ‘Er zijn vrijwel geen redenen die het volgen van winkelend publiek of reizigers rechtmatig maken’
>
> Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens

Beveiliging

Verantwoord omgaan met persoonsgegevens valt of staat met de beveiliging van de gegevens. Mensen moeten erop kunnen vertrouwen dat hun gegevens niet op straat komen te liggen. Dit betekent dat de beveiliging van persoonsgegevens binnen organisaties een blijvend punt van aandacht moet zijn. Als de beveiliging niet in orde is, kan dat leiden tot een datalek. Met alle mogelijke gevolgen van dien, zoals misbruik van de gegevens voor identiteitsfraude.

20.881

meldingen

In 2018 kreeg de AP 20.881 meldingen van datalekken. Het aantal is meer dan verdubbeld vergeleken met 2017.

600.000

euro

De AP gaf Uber een boete van 600.000 euro. De reden hiervoor was dat Uber een groot datalek niet op tijd had gemeld. Door het lek werden 57 miljoen Uber-gebruikers getroffen.

50.000

leerlingen

Na onderzoek van de AP verbeterden drie grote onderwijsorganisaties de toegangsbeveiliging van hun leerlingvolgsysteem. Hierdoor zijn de gegevens van meer dan 50.000 leerlingen – zoals studieresultaten en gegevens over hun gezondheid – nu goed beschermd.

Meldplicht datalekken

In 2018 werden er 20.881 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP). Het aantal meldingen is meer dan verdubbeld vergeleken met 2017. De meeste datalekken werden gemeld door organisaties uit de sectoren zorg en welzijn (29%), financiële dienstverlening (26%) en openbaar bestuur (17%). Het aantal meldingen overstijgt het eerder geschatte aantal fors. De AP breidt daarom de capaciteit uit om meer actie te kunnen ondernemen, wat kan leiden tot meer handhavende maatregelen.

In ruim twee derde (63%) van de datalekken die in 2018 zijn gemeld, gaat het om persoonsgegevens die aan een verkeerde ontvanger zijn gestuurd. De overige 37% bestaat uit onder meer kwijtgeraakte persoonsgegevens door bijvoorbeeld een verloren of gestolen laptop of usb-stick, hacking, phishing of malware. Het gaat in de meeste gevallen om naw-gegevens, gegevens over geslacht, medische gegevens en BSN.

Phishing
Uit de meldingen valt op dat datalekken door hacking en phishing vooral voorkomen in de zorg. Bij phishing kan het gaan om nep e-mails die afkomstig lijken van een betrouwbare partij. Wanneer iemand op de link klikt of een bijlage opent, kan een virus worden geïnstalleerd. Bijvoorbeeld ransomware, een type malware dat gegevens versleutelt en ervoor zorgt dat deze niet meer toegankelijk zijn.

Acties 2018
De AP kan op verschillende manieren actie ondernemen bij gemelde (en niet-gemelde) datalekken. In 2018 heeft de AP in veel gevallen uitleg gegeven aan organisaties over te nemen beveiligingsmaatregelen, heeft de AP gevraagd om aanvullende informatie over het datalek, zijn brieven met normuitleg gestuurd en normoverdragende gesprekken gevoerd met organisaties.

In 2018 heeft de AP bij 298 datalekmeldingen actie ondernomen richting organisaties die een datalek gemeld hadden. Een deel van deze interventies loopt nog. Over het algemeen leidden deze acties tot een waarschuwing en beëindiging van de overtreding. Hieronder vielen ook interventies naar mogelijke datalekken bij organisaties die dit níet hebben gemeld bij de AP. In 2019 besteedt de AP daar meer aandacht aan. In november 2018 heeft de AP vervoersdienst Uber een boete van 600.000 euro opgelegd voor het te laat melden van een datalek aan betrokkenen en aan de AP.

Meldplicht datalekken

Een organisatie die een ernstig datalek heeft, moet dit melden aan de mensen van wie de gelekte gegevens zijn. Zodat zij bijvoorbeeld snel hun wachtwoord kunnen wijzigen. Ook moet de organisatie het datalek melden bij de AP, zodat de AP zich een beeld kan vormen van de feiten en kan ingrijpen als dat nodig is.

AP ontvangt bijna 21.000 datalekken in 2018

Boete voor Uber

In november 2018 legde de AP een boete van 600.000 euro op aan Uber voor het te laat melden van een groot datalek aan de betrokkenen (de mensen van wie de gegevens gelekt zijn) en aan de AP. Wereldwijd werden ruim 57 miljoen Uber-gebruikers getroffen door dit datalek, onder wie ongeveer 174.000 Nederlanders. Het ging om persoonsgegevens zoals namen, e-mailadressen en telefoonnummers van klanten en chauffeurs.

Het datalek vond al plaats in 2016, maar Uber meldde dit pas in november 2017 bij de AP. Terwijl organisaties met een ernstig datalek wettelijk verplicht zijn om dit binnen 72 uur te melden aan de betrokkenen en aan de AP.

De AP heeft als leidende toezichthouder een internationale taskforce aangestuurd, bestaande uit privacytoezichthouders uit België, Duitsland, Frankrijk, Nederland, Italië, Spanje en het Verenigd Koninkrijk. De taskforce coördineerde de onderzoeken van de verschillende toezichthouders naar het datalek.

De onderzoeken hebben uiteindelijk geleid tot het besluit van de AP om Uber een boete op te leggen van 600.000 euro. De top van het Uber-concern wist al eerder van het datalek, maar meldde dit niet op tijd aan de betrokkenen en bij de AP. De AP rekent dit Uber aan als ernstig verwijtbare nalatigheid, wat van invloed is geweest op de hoogte van de boete. Het besluit van de AP om een boete op te leggen is onherroepelijk.

AP legt Uber boete op voor te laat melden datalek

AutPersoonsgegevens @toezicht_AP · 19 jul. 2018
Vingerafdrukken of gezichtsafbeeldingen: mag u deze biometrische persoonsgegevens wel of niet gebruiken voor toegangscontrole? Lees hier het antwoord: autoriteitpersoonsgegevens.nl #avg #privacy #biometrie

Onderzoek UWV

In oktober 2018 legde de AP het Uitvoeringsinstituut Werknemersverzekeringen (UWV) een last onder dwangsom op. Heeft het UWV na 31 oktober 2019 het beveiligingsniveau van het werkgeversportaal niet op orde? Dan moet het UWV een dwangsom van 150.000 euro per maand betalen, met een maximum van 900.000 euro.

Omdat het UWV geen meerfactorauthenticatie toepast bij de toegangsverlening tot het online werkgeversportaal, is de beveiliging onvoldoende. Via het werkgeversportaal kunnen werkgevers en arbodiensten ziekteverzuimgegevens van werknemers in een verzuimsysteem invoeren en bekijken. Het gaat hier om gezondheidsgegevens van werknemers. Het UWV is daarom als aanbieder én beheerder van dit verzuimsysteem verplicht om de toegang tot dit portaal voldoende te beveiligen door minimaal meerfactorauthenticatie toe te passen.

Het UWV heeft eerder aangegeven meerfactorauthenticatie te willen implementeren door aan te sluiten op eHerkenning. Daarnaast heeft het UWV al wel andere maatregelen getroffen om toegang door onbevoegden tot het werkgeversportaal tegen te gaan, maar deze gaan niet over de authenticatie en zijn daardoor niet passend.

Meerfactorauthenticatie

Meerfactorauthenticatie is een vorm van (toegangs)beveiliging waarbij iemand alleen toegang krijgt tot een computer, (besturings)systeem of applicatie wanneer diegene zich op minstens twee verschillende manieren kan identificeren. Bijvoorbeeld met een wachtwoord in combinatie met een sms-code. Er zijn combinaties mogelijk tussen bijvoorbeeld:

- Iets wat de gebruiker weet. Zoals een wachtwoord, een pincode of het antwoord op een beveiligingsvraag.
- Iets wat de gebruiker heeft. Zoals een telefoon of een token.
- Iets wat de gebruiker is. Bijvoorbeeld een biometrisch gegeven zoals een vingerafdruk, spraakherkenning of gezichtsherkenning.

AP dwingt UWV met sanctie gegevens beter te beveiligen

Onderzoek leerling-volgsystemen

Gegevens van meer dan 50.000 leerlingen, zoals contactgegevens, BSN, verzuimgegevens, studieresultaten en gegevens over hun gezondheid en welzijn – die moeten goed beveiligd zijn, zodat onbevoegden hier geen toegang toe kunnen krijgen. Maar precies daar ging het mis bij drie grote onderwijsorganisaties die niet goed omgingen met hun leerlingvolgsystemen, concludeerde de AP na onderzoek.

In maart 2018 liet de AP weten dat onderwijsorganisaties ASKO, BOOR en MOVARE hun werkwijze hadden aangepast, waardoor zij voldeden aan de (toenmalige) privacywet. Na technische aanpassingen in het leerlingvolgsysteem hebben medewerkers nu alleen nog toegang tot persoonsgegevens van leerlingen die zij voor de uitvoering van hun taken nodig hebben. En niet meer tot de persoonsgegevens van alle leerlingen van de school. De drie onderzochte onderwijsorganisaties hebben daarnaast de beveiliging van de persoonsgegevens verbeterd door bij te houden welke bestanden van welke leerlingen zijn gelezen of aangepast.

Onderwijsorganisaties passen werkwijze met leerlingvolgsysteem aan na onderzoek AP

Financiën

Financiële gegevens zijn gevoelige gegevens, die veel kunnen zeggen over iemands privéleven. Bijvoorbeeld hoeveel iemand verdient, of diegene schulden heeft en waar deze persoon zijn geld aan uitgeeft. Financiële ondernemingen als banken en verzekeraars moeten er dan ook voor zorgen dat de privacy van hun klanten gewaarborgd is. Privacybescherming is ook een belangrijk onderdeel van de nieuwe Europese wet PSD2, waarbij mensen andere partijen dan hun bank toegang kunnen geven tot hun betaalgegevens.

138

organisaties

De AP controleerde bij 138 financiële instellingen (45 banken en 93 verzekeraars) of zij een FG hadden aangemeld. En of zij de contactgegevens van de FG op hun website vermeldden. De FG is de interne privacytoezichthouder van een organisatie.

48.000

euro

De AP vorderde 48.000 euro aan dwangsommen in bij Theodoor Gilissen Bankiers. De reden hiervoor was dat de bank weigerde een klant inzage te geven in zijn persoonsgegevens.

toestemming

Betaaldienstverleners mogen alleen inzage krijgen in iemands bankrekening als diegene daarvoor uitdrukkelijke toestemming heeft gegeven. Dat staat in de nieuwe betaalrichtlijn PSD2. De AP verduidelijkte waaraan deze toestemming moet voldoen.

FG's bij banken en verzekeraars

Sinds de nieuwe privacywet geldt, moeten onder meer alle financiële instellingen – zoals banken en verzekeraars – een functionaris gegevensbescherming (FG) hebben. De FG is, kort gezegd, de interne privacytoezichthouder van een organisatie.

Vervolgens moeten deze organisaties aan de Autoriteit Persoonsgegevens (AP) laten weten wie hun FG is. En de contactgegevens van hun FG (direct telefoonnummer, e-mailadres, postadres en/of direct contactformulier) op hun website publiceren. Zodat iedereen die dat wil, snel en in vertrouwen contact kan opnemen met de FG over privacy-issues.

De AP controleerde bij 45 banken en 93 verzekeraars of zij een FG hadden aangemeld en de contactgegevens hadden gepubliceerd. Uit een eerste controle bleek dat 6 banken en 9 verzekeraars nog geen FG hadden aangemeld bij de AP. En dat 7 banken en 14 verzekeraars nog geen directe contactgegevens op hun website hadden geplaatst.

Van 2 banken en 2 verzekeraars kreeg de AP nadere informatie waaruit bleek dat zij niet verplicht zijn om een FG aan te stellen, omdat zij niet op grote schaal persoonsgegevens verwerken. De andere banken en verzekeraars bleken wel een FG te hebben aangesteld, maar deze nog niet bij de AP te hebben aangemeld. Zij hebben dit alsnog gedaan. Verder vermelden alle gecontroleerde banken en verzekeraars inmiddels op een goede manier de contactgegevens van hun FG's.

Banken en verzekeraars voldoen aan FG-verplichtingen na controle AP

Banken en verzekeraars verwerken veel (gevoelige) persoonsgegevens van hun klanten, zoals identificatiegegevens, financiële gegevens, transactiegegevens en medische gegevens. De FG's vervullen daarom een belangrijke functie om de gegevens van klanten te beschermen.

Last onder dwangsom ingevorderd

In augustus 2018 maakte de AP bekend een dwangsom ingevorderd te hebben van 48.000 euro bij Theodoor Gilissen Bankiers (inmiddels InsingerGilissen Bankiers).

Deze bank gaf in eerste instantie geen gehoor aan een verzoek van een klant om inzage in zijn persoonsgegevens. De klant wilde een overzicht van de persoonsgegevens die de bank van hem had, wat de herkomst was van de gegevens en met wie ze werden gedeeld. Dat de bank geen inzage wilde geven, is in strijd met de privacywetgeving. De AP legde de bank hiervoor een last onder dwangsom

op. Omdat de bank vervolgens nog steeds niet volledig voldeed aan het inzageverzoek, vorderde de AP eind 2017 dwangsommen in. Uiteindelijk heeft de klant inzage gekregen in zijn persoonsgegevens.

TGB betaalt dwangsom na niet voldoen aan inzageverzoek

AutPersoonsgegevens @toezicht_AP · 12 dec. 2018
Wij hebben diverse klachten over BKR en recht op inzage in behandeling. Privacywet AVG heeft duidelijke regels rond het recht op inzage en de vergoeding daarvoor. Meer weten over het recht op inzage?
Zie autoriteitpersoonsgegevens.nl

Nieuwe wet PSD2

Betaalgegevens zijn gevoelige financiële persoonsgegevens, die veel kunnen zeggen over iemands privéleven. Daarom is de bescherming van de privacy van consumenten een belangrijk onderdeel van de nieuwe Europese wet voor het betalingsverkeer (PSD2). Deze wet regelt onder meer dat niet alleen banken, maar ook andere partijen nieuwe betaal- en rekeningdiensten mogen aanbieden. Bijvoorbeeld een dienst die helpt overzicht te houden over afzonderlijke bankrekeningen. Vanwege de privacyaspecten van PSD2 heeft de AP zich in 2018 intensief bezighouden met de implementatie van deze nieuwe wet.

Toezicht
Het toezicht op PSD2 is verdeeld over verschillende toezichthouders. Naast de AP zijn dit de DNB, ACM en AFM. Een belangrijk aandachtspunt voor de AP in 2018 was afstemming met deze andere toezichthouders en het ministerie van Financiën, om de samenwerking bij de uitvoering van het toezicht te bevorderen. Verder heeft de AP zich ingespannen om het toezicht op de privacyaspecten van PSD2 zo veel mogelijk bij de AP belegd te krijgen.

Overleg
De AP heeft in 2018 niet alleen veelvuldig overlegd met de andere toezichthouders op PSD2, maar ook met bijvoorbeeld seniorenorganisaties, de Consumentenbond en de Betaalvereniging Nederland. Verder heeft de AP in november 2018 een workshop over PDS2 en privacy verzorgd tijdens de conferentie 'Fintech Meets the Regulators'.

Toestemming
PSD2 bepaalt dat betaaldienstverleners alleen toegang mogen krijgen tot de persoonsgegevens van een consument als diegene daarvoor uitdrukkelijke toestemming heeft gegeven. De consument beslist dus zelf of een betaaldienstverlener inzage mag hebben in zijn of haar bankrekening en betaalgedrag.

De AP vindt het belangrijk dat de inhoudelijke invulling van de privacyaspecten van PSD2 zo veel mogelijk aansluit bij de terminologie van de privacywet, de AVG. Dit geldt vooral voor het begrip 'uitdrukkelijke toestemming'. Het wetgevingsadvies van de AP over het toestemmingsbegrip onder PSD2 heeft ertoe geleid dat de wetgever de implementatiewetgeving heeft aangepast.

Verder heeft de AP in 2018 een nieuw dossier Betaaldiensten aan de website toegevoegd. Hiermee geeft de AP voorlichting over PSD2 aan marktpartijen en consumenten. Bijvoorbeeld over waar 'uitdrukkelijke toestemming' precies aan moet voldoen.

Advies verwijzingsportaal bankgegevens

Verschillende overheidsinstanties houden zich bezig met het bestrijden van witwassen, terrorismefinanciering en fraude. Daarvoor hebben zij gegevens nodig van cliënten van banken en andere betaaldienstverleners. Momenteel vorderen zij deze gegevens meestal handmatig en op individuele basis. De minister van Financiën wil dit proces automatiseren door een centraal elektronisch systeem op te richten, het verwijzingsportaal bankgegevens.

In november 2018 adviseerde de AP over de Wet verwijzingsportaal bankgegevens. De AP wees hierbij op de vraag wie de verwerkingsverantwoordelijke is voor het portaal. Hierin worden grote hoeveelheden persoonsgegevens verwerkt. Deze gegevens worden verstrekt door private partijen en gebruikt door veel overheidsdiensten, die onder verschillende ministeries vallen. Bij een zo groot aantal publieke en private partijen is het cruciaal dat helder is wie de verwerkingsverantwoordelijke is, aldus de AP.

Advies verwijzingsportaal bankgegevens

Verwerkingsverantwoordelijke en verwerker

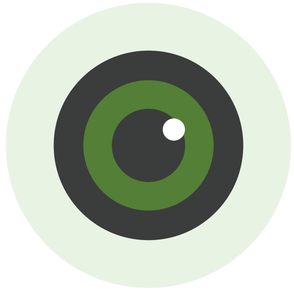
De verwerkingsverantwoordelijke is een persoon of organisatie die bepaalt waarvoor er persoonsgegevens worden verwerkt en hoe dat gebeurt. Een verwerker is een persoon of organisatie waaraan de verwerkingsverantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor.

De verwerkingsverantwoordelijke moet afspraken maken met de verwerker over het hoe en wat van de gegevensverwerking. En deze afspraken vastleggen in een verwerkersovereenkomst.

Cameratoezicht

Cameratoezicht kan helpen om personen en eigendommen te beschermen. Maar de inbreuk op de privacy van de personen die worden gefilmd is groot. Daarom mogen organisaties en particulieren alleen camera's ophangen als zij aan een aantal voorwaarden voldoen en ervoor zorgen dat de privacyinbreuk zo klein mogelijk is. Verborgen camera's zijn maar zelden toegestaan. En een camera in ruimtes waar mensen naakt in beeld kunnen komen, gaat altijd te ver.

130



tips

De AP kreeg 130 tips van verontruste saunabezoekers, omdat er op internet beelden te zien waren van blote mensen in de sauna. Daarop deed de AP een steekproef bij 11 sauna's om te kijken of zij verboden camera's hadden hangen.

camera in reclamezuil

De AP kreeg veel tips van bezorgde voorbijgangers over verborgen camera's in reclamezuilen, bijvoorbeeld op treinstations. De AP besloot daarop duidelijkheid te geven over de privacyregels voor het adverteren via digitale billboards.

Camera's in sauna's

In het voorjaar van 2018 was er veel aandacht in de media voor gelekte beelden op internet van blote mensen in de sauna. De Autoriteit Persoonsgegevens (AP) kreeg hierop 130 signalen van bezorgde saunabezoekers, die vreesden ontkleed gefilmd te worden. Dat was voor de AP aanleiding voor onderzoek. Cameratoezicht in ruimtes waar mensen ontkleed zijn, is volgens de privacywetgeving namelijk verboden.

De AP deed een steekproef en ging bij elf sauna's onaangekondigd op bezoek. De AP controleerde hierbij of er camera's waren in ruimtes waar bezoekers ontkleed zijn, zoals kleedkamers, doucheruimtes, toiletten, zwem- en bubbelbaden, de sauna's en eventuele buitenruimtes.

Bij negen van de elf sauna's werd geen enkele werkende camera aangetroffen op een plaats waar bezoekers ontkleed zijn. Veel saunaeigenaren gaven aan camera's weggehaald te hebben na een waarschuwingsbrief van de AP uit 2016 of na de recente commotie over de gelekte beelden op internet.

Bij één sauna vond de AP een niet goed werkende camera, die alleen vage contouren van mensen filmde. Een andere camera gaf alleen in een klein gedeelte van het beeld mogelijk zicht op blote bezoekers. De sauna-eigenaren hebben daarop deze camera's verwijderd of juist afgesteld.

Dummy's
De AP constateerde dat er soms nep-camera's (dummy's) of uitgeschakelde camera's hangen in ruimtes waar bezoekers ontkleed zijn. Dit is niet in strijd met de wet, omdat hiermee geen persoonsgegevens worden verwerkt. Saunaeigenaren gaven aan dat dit preventief werkt, om diefstal en (on)gewenste intimiteiten tegen te gaan. Ook zag de AP geregeld andere apparatuur hangen, zoals rook- en temperatuurmelders, die mogelijk kunnen worden aangezien voor camera's.

Camera's in andere ruimtes
Vaak hingen er wel werkende camera's bij de receptie, in het restaurant en in rustruimtes waar het dragen van badjassen of kleding verplicht is. De AP adviseerde de saunaeigenaren om bezoekers duidelijk te informeren over waar het dragen van een badjas verplicht is en waar er eventueel cameratoezicht is.

Gesprek met branche
De AP heeft de resultaten van het onderzoek besproken met VNSW, de brancheorganisatie voor sauna- en wellnessbedrijven.

AP constateert geen misstanden met camera's in onderzochte sauna's

Camera's in reclamezuilen

Een treinreiziger ontdekte een camera in een reclamezuil op een station en vroeg de NS om opheldering. Dat zorgde voor grote ophef op social media. Ook de AP kreeg veel tips van bezorgde voorbijgangers over deze verborgen camera's. De AP besloot daarop duidelijkheid te geven over de privacyregels voor het adverteren via digitale billboards.

Beeldscherm-exploitanten gebruiken camera's in billboards om mensen te tellen of om advertenties af te stemmen op kenmerken van de voorbijganger. Maar mag je zomaar mensen observeren zonder dat zij dat weten? Nee, liet de AP in juni 2018 duidelijk weten aan de branche van beeldscherm-exploitanten. Hiervoor is vrijwel altijd toestemming van de voorbijganger nodig.

Als mensen herkenbaar in beeld komen, is er sprake van een verwerking van persoonsgegevens. Dat betekent dat de privacywet, de Algemene verordening gegevensbescherming (AVG), van toepassing is. Een exploitant moet een grondslag hebben om deze gegevens te mogen verwerken. Uitzonderingen daargelaten, is de grondslag 'toestemming' volgens de normuitleg van de AP in dit geval de meest kansrijke.

Toestemming
Dat betekent in de praktijk dat een beeldscherm-exploitant toestemming moet hebben van elke voorbijganger om zijn of haar gegevens te mogen verwerken. Die toestemming moet volgens de AVG aan een aantal voorwaarden voldoen. Toestemming moet bijvoorbeeld vrij gegeven worden en specifiek zijn. Het moet duidelijk zijn voor welke gegevens iemand toestemming geeft en voor welk specifieke doel de gegevens worden gebruikt door de adverteerder. Een beeldscherm-exploitant kan dit bijvoorbeeld doen door een voorbijganger via een tussenstap met een QR-code of een app toestemming te vragen.

AP informeert branche over norm camera's in reclamezuilen

Camera's voor beveiliging

Mag iemand camera's ophangen om zijn eigendommen te beveiligen als hij hiermee ook andere mensen filmt? En dit dus de privacy van deze personen kan schaden? In november 2018 besliste de AP in een zaak tussen de eigenaar van bedrijfspanden en omwonenden dat de eigenaar zijn eigendommen mag beveiligen met camera's. Tegen dit besluit van de AP loopt nog een beroepsprocedure.

De zaak geeft meer inzicht in de normen voor cameratoezicht en in de beoordeling van de grondslag van het gerechtvaardigd belang bij cameratoezicht. De AP woog de belangen van de omwonenden af tegen de belangen van de eigenaar van de bedrijfspanden. In dit geval bleek dat de eigenaar zich kan beroepen op een gerechtvaardigd belang, namelijk de bescherming van zijn eigendommen.

AP geeft inzicht in gebruik camera's voor beveiligen eigendom

AutPersoonsgegevens @toezicht_AP · 26 jun. 2018
Mag je zomaar gefilmd worden door een camera in een reclamezuil of billboard? Antwoord: nee, je moet hier als voorbijganger bijna altijd eerst toestemming voor geven. De AP heeft de norm uitgewerkt en informeert vandaag de branche hierover autoriteitpersoonsgegevens.nl

Colofon

Autoriteit Persoonsgegevens, Den Haag, april 2018

Ontwerp

Teldesign, Rotterdam

Contactgegevens

Autoriteit Persoonsgegevens
Bezuidenhoutseweg 30
Postbus 93374
2509 AJ DEN HAAG
autoriteitpersoonsgegevens.nl

T 070 8888 500
F 070 8888 501
Telefonisch spreekuur 088-1805 250
(maandag t/m vrijdag van 9.00 tot 17.00 uur)