AUTORITEIT
PERSOONSGEGEVENS

Agenda 2017

Door voortschrijdende digitalisering en andere technologische innovaties nemen de mogelijkheden voor het verzamelen en gebruiken van persoonsgegevens in een razend tempo toe. Persoonsgegevens verwerken is makkelijker en goedkoper dan ooit. Dit zorgt voor kansen en mogelijkheden. Bijvoorbeeld om handige nieuwe producten en diensten te ontwikkelen waarvan mensen veel baat hebben. Tegelijkertijd houden bedrijven en overheden bij deze ontwikkeling lang niet altijd rekening met de privacywetgeving. Dit kan leiden tot overtredingen van de wet en daarmee tot negatieve gevolgen voor mensen.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving. De AP maakt jaarlijks bekend op welke onderwerpen zij zich in het bijzonder richt. Om transparant te zijn, maar ook om te bevorderen dat bedrijven en overheden zich aan privacywetgeving houden. De AP kan natuurlijk ook in actie komen bij onderwerpen die niet op deze Agenda staan, maar die bijvoorbeeld in het nieuws zijn of waarover veel tips binnenkomen.

Het jaar 2017 is een bijzonder jaar. Natuurlijk is de Wet bescherming persoonsgegevens (Wbp) nog van kracht. Maar bedrijven en overheden zijn ook bezig zich voor te bereiden op de wetgeving die vanaf 25 mei 2018 van toepassing is: de nieuwe Europese verordening voor de bescherming van persoonsgegevens en de nieuwe Europese richtlijn voor gegevensverwerking door politie en justitie. Ook de AP bereidt zich in 2017 voor op de toekomstige situatie. Dat doen we allereerst door met de andere privacytoezichthouders in de EU gezamenlijke afspraken te maken over de uitleg van de nieuwe normen en taken. Daarnaast geven we extra voorlichting. We informeren mensen over de nieuwe wetgeving, zodat zij zich bewust zijn van hun rechten. En we vertellen bedrijven en overheden wat zij moeten weten om straks aan de nieuwe wetgeving te voldoen. Dit alles betekent dat voorlichting en advisering over de nieuwe Europese privacywetgeving in 2017 bovenaan de agenda van de AP staan.

Het reguliere werk van de AP gaat ondertussen ook door. De toezichthouder zal niet aarzelen ernstige overtredingen van de Wbp te onderzoeken en zo nodig handhavende maatregelen te nemen. De belangrijkste thema's voor de AP in 2017 zijn naast de nieuwe EU-wetgeving over gegevensbescherming: profilering, bijzondere persoonsgegevens en beveiliging van persoonsgegevens.

Nieuwe EU-wetgeving gegevensbescherming

Als de algemene verordening gegevensbescherming (AVG) op 25 mei 2018 van toepassing is, ontstaat binnen de EU een gelijk speelveld voor organisaties die persoonsgegevens verwerken. De verplichtingen voor organisaties veranderen op een aantal punten. Zo hoeven organisaties vanaf die datum niet meer alle verwerkingen van persoonsgegevens te melden bij de AP. Zij moeten zich wel kunnen verantwoorden voor hun werkwijze. Organisaties moeten met documentatie kunnen aantonen dat zij passende organisatorische en technische maatregelen hebben getroffen om aan de eisen te voldoen. Daarnaast zijn organisaties in bepaalde gevallen verplicht om een *privacy impact assessment* (PIA) uit te voeren en een functionaris voor de gegevensbescherming (FG) aan te stellen.

De AP adviseert overheden en bedrijven om nu te onderzoeken of zij hun processen, diensten en producten moeten aanpassen om aan de vereisten van de AVG te voldoen. Via de website van de toezichthouder kunnen organisaties bijvoorbeeld nagaan of zij straks een FG moeten aanstellen. Ook vinden zij daar informatie over de 'leidende autoriteit' en de onestopshop-regel. Dit houdt in dat bedrijven met vestigingen in meerdere EU-lidstaten straks nog maar met één privacytoezichthouder te maken krijgen. De website biedt verder informatie over het recht op dataportabiliteit (overdraagbaarheid van persoonsgegevens). Dit is het recht van mensen om de persoonsgegevens te ontvangen die een organisatie van hen heeft.

De Autoriteit Persoonsgegevens intensiveert in 2017 de voorlichting en advisering over de nieuwe EU-wetgeving, zodat mensen weten wat hun rechten zijn en die ook kunnen uitoefenen en zodat organisaties weten hoe zij onder de nieuwe verordening en nieuwe richtlijn de wet moeten naleven.

Gelijk speelveld in de EU

Van verzamelen tot profileren

Het verzamelen van persoonsgegevens heeft dankzij slimme algoritmes en digitale platformen een nieuwe dimensie gekregen. Big data-analyses worden in vele sectoren toegepast en onder meer losgelaten op persoonsgegevens van gevoelige aard, zoals internetgedrag, locatiegegevens en communicatiegedrag. Er ontstaan daarnaast steeds meer omvangrijke, complexe gegevensknooppunten, waar uiteenlopende partijen persoonsgegevens uitwisselen. Daarbij wordt het ook mogelijk dat gegevens die in de offline wereld worden verzameld een koppeling krijgen met online data. De gegevensverzamelingen die ontstaan met deze knooppunten, kunnen worden gebruikt voor profiling.

Organisaties kunnen profielen opstellen op basis waarvan zij mensen verschillend kunnen behandelen. Sommige mensen vinden dit wenselijk, andere niet. Het probleem is dat profiling vaak onzichtbaar is, waardoor de betrokkenen – de mensen om wie het gaat – hier niet of moeilijk invloed op kunnen uitoefenen. En dat terwijl de kern van de bescherming van persoonsgegevens is dat mensen zeggenschap hebben over hun persoonsgegevens en zo een weloverwogen keuze kunnen maken.

In de private sector is sprake van een toenemend gebruik van slimme technologieën, zoals wifi-tracking. Ook ziet de AP dat bij fusies van bedrijven enorme gegevensverzamelingen ontstaan die nieuwe koppelingen mogelijk maken. Daarbij ontstaat het risico dat persoonsgegevens die voor een bepaald doel zijn verzameld, ook voor andere doeleinden worden gebruikt. Daarnaast signaleren we dat nieuwe spelers toetreden tot de financiële markten wat nieuwe ontwikkelingen in de samenleving met zich meebrengt.

In de publieke sector zien we het gebruik van big data bijvoorbeeld bij fraudebestrijding. Daarnaast verzamelen overheden – zowel op rijksniveau als bij gemeenten – steeds meer persoonsgegevens, vaak zelfs voor verschillende overheidstaken. Deze instanties verzamelen ook steeds vaker strafrechtelijke gegevens.

Door de ontwikkelingen in profiling zijn overheden en bedrijven in staat om allerlei nieuwe – vaak geautomati-

seerde – conclusies te trekken over mensen. Dit kan ingrijpende gevolgen hebben voor hun mogelijkheden om zelf keuzes te maken en om zich in vrijheid te ontwikkelen.

De AP legt in 2017 binnen het thema profiling de focus op transparantie. Het is immers van groot belang dat mensen goed worden geïnformeerd over welke gegevens van hen worden verwerkt, wat daarmee gebeurt en met welk doel. Dit is niet alleen een kernprincipe in de nu geldende Wbp, maar ook in de EU-verordening die vanaf 25 mei 2018 van toepassing is.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over gezondheid, ras, godsdienst, seksuele leven, politieke voorkeur en strafrechtelijk verleden. Ook het burgerservicenummer (BSN) is een bijzonder persoonsgegeven. Deze gegevens zijn van gevoelige aard en moeten daarom extra worden beschermd. De Wbp bevat duidelijke regels over de verwerking van bijzondere persoonsgegevens. In beginsel geldt er een verbod op de verwerking, tenzij er in de wet een uitzondering voor is. Toch spelen bijzondere persoonsgegevens een steeds belangrijkere rol in hedendaagse datapraktijken.

De AP signaleert de trend dat bijzondere persoonsgegevens onderdeel worden van big data-toepassingen. Overheden en bedrijven verzamelen, koppelen, analyseren en gebruiken enorme hoeveelheden gegevens. Bijvoorbeeld om risicoprofielen te maken van mensen die een toeslag, lening of verzekering aanvragen.

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

De AP legt bij het onderwerp bijzondere persoonsgegevens de focus op de naleving van het verbod op verwerking van bijzondere persoonsgegevens. Ook is de AP alert op de juiste toepassing van de wettelijke waarborgen bij uitzonderingen op dit verbod.

Beveiliging van persoonsgegevens

Nieuwe technologieën brengen prachtige nieuwe mogelijkheden met zich mee. De uitdaging is om deze technologische mogelijkheden óók in te zetten voor de bescherming van persoonsgegevens. Bijvoorbeeld door al bij het ontwerpen van nieuwe producten en diensten rekening te houden met gegevensbescherming (*privacy by design*). Adequate beveiliging is hierbij een kernpunt. Daarmee kan worden voorkomen dat mensen (financiële) schade ondervinden als hun persoonsgegevens op straat komen te liggen.

De AP constateert dat steeds meer organisaties 'klantportalen' inrichten. Dit zijn websitepagina's waarop mensen hun gegevens kunnen inzien of aanpassen. Deze portalen hebben voordelen, maar kunnen ook risico's creëren. Bijvoorbeeld als mensen onbedoeld persoonsgegevens van anderen te zien krijgen. Het is van belang dat organisaties dit soort portalen goed beveiligen en – als dat nodig is – alleen toegang te verlenen tot gegevens door middel van tweefactorauthenticatie.

De meldplicht datalekken, die van kracht is sinds 1 januari 2016, verplicht organisaties om een ernstig datalek te melden bij de AP. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. De AP houdt toezicht op de naleving van de meldplicht en heeft deze taak ook in 2017 hoog op de agenda staan. Daarnaast blijft de AP zich richten op situaties waarin de beveiliging overduidelijk niet op orde is.

Privacy aan de tekentafel

Werkwijze Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving. Om naleving van de wet te bevorderen, zet de AP een mix van instrumenten in op het gebied van toezicht, handhaving en communicatie.

Toezicht

De AP doet onderzoek bij het vermoeden van ernstige overtredingen van de wet die structureel van aard zijn, die veel mensen treffen en waarbij de AP verschil kan maken. Op basis van kennis van het toezichtsdomein en van tips die via de website en het telefonisch spreekuur binnenkomen, bepaalt zij waarnaar zij onderzoek doet. In bepaalde gevallen start de AP geen onderzoek, maar stuurt een brief aan organisaties of voert een gesprek. Dit is meestal al voldoende om de overtreding te laten beëindigen.

Handhaving

De AP heeft de bevoegdheid om organisaties die de wet overtreden, een last onder dwangsom op te leggen. Zij krijgen dan een bepaalde periode om de overtredingen te beëindigen en als dit niet gebeurt, moeten zij een dwangsom betalen. Sinds 1 januari 2016 kan de AP ook een boete opleggen. De boetebevoegdheid is een belangrijke aanvulling op het sanctiearsenaal, vooral van belang vanwege de preventieve werking die ervan uitgaat.

Communicatie

Externe communicatie is voor de AP een belangrijk instrument om haar doelen te bereiken. Zij communiceert met het brede publiek, media, bedrijven, overheden en andere stakeholders. Om te informeren, te waarschuwen en om mensen handvatten te geven om zelf hun rechten uit te oefenen. Externe communicatie is ook een belangrijk instrument om naleving van de privacywetgeving te bevorderen. Dit doet de AP onder meer door onderzoeksbevindingen en sancties openbaar te maken, door haar jaarlijkse prioriteiten te publiceren en door te reageren op ontwikkelingen in de actualiteit. Vertegenwoordigers van de AP spreken regelmatig op conferenties en voeren gesprekken met brancheorganisaties en andere stakeholders. Om de contacten met hen te onderhouden, te vernemen tegen welke problemen zij aanlopen in de praktijk en te horen hoe zij het optreden van de AP ervaren.

Nationale en internationale samenwerking

Nationale samenwerking

De AP werkt binnen Nederland samen met verschillende andere toezichthouders. Bijvoorbeeld als er raakvlakken zijn in het werkterrein. Ook neemt de AP deel aan het samenwerkingsverband van het Markttoezichthoudersberaad (MTB). Daarin zijn ook Autoriteit Financiële Markten (AFM), Autoriteit Consument en Markt (ACM), Commissariaat voor de Media, De Nederlandsche Bank (DNB), Kansspelautoriteit en Nederlandse Zorgautoriteit (NZa) vertegenwoordigd. In 2017 zal de Autoriteit Persoonsgegevens met de DNB, AFM en ACM afspraken maken over samenwerking op het gebied van fintech, de technologische innovaties van financiële diensten.

Internationale samenwerking

De AP speelt al jarenlang een belangrijke rol in zowel de Artikel 29-werkgroep van Europese privacytoezichthouders als in het wereldwijde platform van privacytoezichthouders. Vanwege de nieuwe EU-wetgeving is internationale samenwerking voor de AP in 2017 zeer belangrijk. De AP werkt nauw samen met de Europese privacytoezichthouders aan bijvoorbeeld richtlijnen, veelgestelde vragen en handreikingen om zowel mensen als organisaties een heldere toelichting te geven op begrippen en eisen uit de nieuwe wetgeving.