AUTORITEIT
PERSOONSGEGEVENS

Agenda 2016

Het gebruik van gegevens is overal. Zo goed als alle bedrijven en overheden verwerken op grote schaal persoonsgegevens. Voortdurend zien nieuwe technologieën, diensten en gadgets het levenslicht. Dat brengt veel voordelen met zich mee, maar kan ook risico's opleveren voor de persoonlijke levenssfeer. Organisaties hebben de verantwoordelijkheid om zorgvuldig met persoonsgegevens om te gaan. Burgers op hun beurt moeten zich ervan bewust zijn dat hun gegevens op allerlei plekken worden verzameld, gekoppeld en gebruikt. Zij hebben het recht hierover goed te worden geïnformeerd.

De Autoriteit Persoonsgegevens – tot voor kort College bescherming persoonsgegevens - houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving. Zij maakt jaarlijks bekend op welke onderwerpen zij zich in het bijzonder richt. Om redenen van transparantie, maar ook om te bevorderen dat bedrijven en overheden zich aan de Wet bescherming persoonsgegevens (Wbp) en aanverwante wetten houden. De toezichthouder kan natuurlijk – bijvoorbeeld naar aanleiding van de actualiteit of aanhoudende tips – tevens optreden bij vermeende overtredingen op andere onderwerpen binnen haar toezichtsdomein.

Om ook op de langere termijn effectief te zijn, houdt de Autoriteit Persoonsgegevens in 2016 op hoofdlijnen dezelfde prioriteiten als de afgelopen jaren: beveiliging van persoonsgegevens, big data & profiling, medische gegevens, persoonsgegevens bij de (digitale) overheid en persoonsgegevens in de arbeidsrelatie. Wel worden naar aanleiding van maatschappelijke en technologische ontwikkelingen, zowel nationaal als internationaal, andere accenten gelegd. Bovendien krijgt de Autoriteit Persoonsgegevens er per 1 januari 2016 een nieuwe taak en een nieuwe bevoegdheid bij.

In 2016 treedt de meldplicht datalekken in werking. Ernstige datalekken moeten bij de Autoriteit Persoonsgegevens en in bepaalde gevallen ook aan de betrokkenen worden gemeld. De meldplicht ligt in het verlengde van een onderwerp dat al jaren hoog op de agenda van de toezichthouder staat, namelijk de beveiliging van persoonsgegevens. Vanaf 2016 heeft de Autoriteit Persoonsgegevens ook een extra sanctiemogelijkheid. Zij kan nu naast de last onder dwangsom ook een boete opleggen. Vooral vanwege de preventieve werking die ervan uitgaat, is de boete een belangrijke aanvulling op het sanctiearsenaal.

Beveiliging van persoonsgegevens

1

Databases met persoonsgegevens groeien exponentieel en de impact van een datalek kan zeer ingrijpend zijn. Bedrijven en overheden moeten op grond van de Wet bescherming persoonsgegevens (Wbp) technische en organisatorische maatregelen nemen om deze gegevens adequaat te beveiligen. Dit is een continu proces, dat al begint bij het ontwerp van een informatiesysteem. Op die wijze verkleinen organisaties de kans dat kwetsbaarheden leiden tot een datalek.

Meldplicht datalekken

Op 1 januari 2016 treedt de meldplicht datalekken in werking. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de meldplicht en heeft deze taak uiteraard hoog op haar agenda staan in 2016. De meldplicht heeft tot doel om het beveiligingsniveau te verhogen en de zelfredzaamheid van burgers te vergroten. Organisaties die een ernstig datalek hebben, moeten dit melden bij de Autoriteit Persoonsgegevens. In bepaalde gevallen is de organisatie ook verplicht de betrokkenen over het datalek te informeren.

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook de onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Meldplicht datalekken in werking

Big data en profiling

2

ICT biedt uitdagende kansen om innovatieve diensten te ontwikkelen en om problemen in de samenleving aan te pakken. Voor deze en voor andere doeleinden worden steeds meer en grotere databases aangelegd. Daarbij worden enorme hoeveelheden persoonsgegevens verzameld, gekoppeld en geanalyseerd, wat als 'big data' wordt aangeduid.

Internet of Things en profiling

Het verzamelen van persoonsgegevens vindt inmiddels op allerlei manieren plaats. Via mobiele telefoons, tablets, smart tv's, koelkasten, stofzuigers en energiemeters maar ook via zogeheten 'wearables' zoals smart watches. Dit fenomeen wordt het 'Internet of Things' genoemd. Gegevensverwerkingen dringen zo steeds meer binnen in de persoonlijke levenssfeer en de gegevens die hiermee worden gegenereerd zijn vaak van gevoelige aard. Een voorbeeld hiervan zijn de gezondheidsgegevens, die in sommige gevallen zelfs voortdurend worden verzameld via apps op een telefoon of smart watch.

Met deze gegevensverwerkingen kunnen organisaties profielen opstellen, op basis waarvan zij mensen verschillend kunnen behandelen (profiling). Sommige mensen vinden dit wenselijk, anderen niet. Het probleem is dat profiling vaak op onzichtbare manier gebeurt, waardoor de betrokkenen hier niet of moeilijk invloed op kunnen uitoefenen. En dat terwijl de kern van de bescherming van persoonsgegevens is dat mensen in beginsel zeggenschap hebben over hun persoonsgegevens en zo een weloverwogen keuze kunnen maken.

In de publieke sector worden profielen bijvoorbeeld gebruikt om fraude te bestrijden en de veiligheid in de openbare ruimte te vergroten. De Autoriteit Persoonsgegevens kijkt in 2016 onder meer of dergelijke gegevensverwerkingen in verhouding staan tot de inbreuk die zij maken op de persoonlijke levenssfeer. In de private sector worden profielen voornamelijk gebruikt voor commerciële doeleinden. De gegevens die voor profiling worden verzameld - bijvoorbeeld door 'tracking en tracing' van mobiele apparatuur of via gezondheidsapps – geven een steeds indringender beeld van een persoon. De Autoriteit persoonsgegevens zal op dit gebied handreikingen geven

en onderzoek doen, waarbij onder meer naar beveiligingsaspecten wordt gekeken.

Kinderen

Kinderen zijn steeds vaker het object van profiling. De huidige generatie kinderen krijgt als eerste generatie te maken met het fenomeen van 'life-logging'; grote hoeveelheden informatie over hun leven belanden in publieke en private databases. Dit fenomeen vraagt van kinderen zelf en hun ouders en verzorgers dat zij zich bewust zijn van de keuzes die zij hierin kunnen maken. De Autoriteit Persoonsgegevens richt in 2016 zijn onderzoek op apps voor kinderen en de privacy van kinderen in het onderwijs.

Medische gegevens

3

Medische gegevens zijn bijzondere persoonsgegevens. Ze zijn van gevoelige aard en mogen alleen onder strikte voorwaarden worden verzameld, bewaard en gebruikt. In de zorgsector worden medische gegevens steeds vaker in de cloud geplaatst, onder meer omdat zorgaanbieders de gegevens zo eenvoudiger kunnen delen. De gedachte hierachter is dat zo de effectiviteit en efficiëntie van de zorg kan worden vergroot en fouten kunnen worden verminderd. Hieraan zijn echter ook risico's verbonden, bijvoorbeeld het risico op datalekken.

E-health en wetenschap

Medische gegevens worden verzameld bij zorgaanbieders en patiënten, maar steeds vaker verzamelen bedrijven medische gegevens via gezondheids- en lifestyle apps op (mobiele) apparaten. Hierbij ontbreekt vaak de bescherming van het medisch beroepsgeheim. Bij wetenschappelijk onderzoek wordt ook in toenemende mate gebruik gemaakt van grote hoeveelheden medische gegevens.

Het plaatsen van medische gegevens in de cloud heeft in 2016 de nadrukkelijke aandacht van de Autoriteit Persoonsgegevens. Bijzondere aandacht zal daarbij uitgaan naar de bewustwording omtrent de risico's hiervan én naar het adequaat beveiligen van bijzondere persoonsgegevens. Ook zal de Autoriteit Persoonsgegevens handreikingen opstellen voor het gebruik van persoonsgegevens op het snijvlak van zorg en wetenschap.

Persoonsgegevens bij de (digitale) overheid

4

In het publieke domein groeien de toepassingen van ICT en de daaraan verbonden databases met persoonsgegevens. De overheid streeft ernaar haar taken effectiever en efficiënter uit te voeren. Dit leidt tot een toename van het gebruik van big data en profiling.

Sociale domein

In het sociale domein ontbreekt sinds de decentralisatie van overheidstaken naar gemeenten een overkoepelende regeling voor gegevensuitwisseling. Dit maakt dat de uitvoeringspraktijk voor gemeenten ingewikkeld is en dat het voor burgers lastig is hun rechten uit te oefenen. De Autoriteit Persoonsgegevens heeft permanent aandacht voor mogelijke risico's met betrekking tot het bovenmatig verwerken van gegevens, het gebruik van gegevens voor andere doelen dan waarvoor zij zijn verzameld en het risico op onvoldoende beveiliging van de gegevens. In de fraudebestrijding wordt steeds meer met ICT en gedragsanalyses gewerkt. De Autoriteit Persoonsgegevens zal dit in 2016 opnieuw onder de loep nemen, zowel om gemeenten heldere kaders aan te reiken als om op te treden tegen overtredingen.

Veiligheid

Binnen het veiligheidsdomein gelden strikte regels voor het verwerken van persoonsgegevens, zowel in nationaal als internationaal verband. Aandachtspunten van de Autoriteit Persoonsgegevens in dit domein zijn onder meer de verwerking van persoonsgegevens in grensoverschrijdende systemen en de trend om ten behoeve van de veiligheid (afwijkende) gedragspatronen te voorspellen.

Toename gebruik big data en profiling bij overheid

Persoonsgegevens in de arbeidsrelatie

5

De relatie tussen werkgever en werknemer wordt gekenmerkt door wederzijdse afhankelijkheid. Tegelijkertijd is sprake van een kwetsbare relatie, bijvoorbeeld omdat de werknemer financieel afhankelijk is van de werkgever. Hierdoor is het voor een werknemer lastig om niet te voldoen aan een verzoek van de werkgever, ook als dat verzoek raakt aan zijn persoonlijke levenssfeer

De Autoriteit Persoonsgegevens krijgt veel signalen van burgers en vakbonden over de controle van werknemers door werkgevers. Dergelijke controles worden intenser en kunnen hierdoor sneller een inbreuk vormen op de privacy van werknemers. Denk hierbij aan het gebruik van cameratoezicht, dat vaak primair een beveiligingsdoel heeft, maar ook wordt gebruikt om werknemers te controleren op hun functioneren. Ook op het terrein van de gezondheid van werknemers is vaak sprake van grote inmenging van werkgevers in de persoonlijke levenssfeer van werknemers. De Autoriteit Persoonsgegevens doet in 2016 ten aanzien van beide fenomenen onderzoek.

De Autoriteit Persoonsgegevens krijgt veel signalen over de controle van werknemers door werkgevers.

Nationale en internationale samenwerking

Nationaal

De Autoriteit Persoonsgegevens werkt op nationaal niveau samen met verschillende toezichthouders. Op bilaterale basis als er raakvlakken zijn in het werkterrein en daarnaast in het samenwerkingsverband van het Markttoezichthoudersberaad (MTB) waarin ook AFM, ACM, Commissariaat voor de Media, DNB, Ksa en NZa zitting hebben.

Internationaal

De Autoriteit Persoonsgegevens speelt traditioneel een belangrijke rol in zowel de Artikel 29-werkgroep van Europese privacytoezichthouders als in het mondiale platform van privacytoezichthouders en zal dat in 2016 ook doen.

Op het internationale speelveld van de gegevensbescherming is momenteel veel beweging. In het voorjaar van 2016 stemmen de Europese instituties naar verwachting over een EU-verordening inzake gegevensbescherming die in alle lidstaten rechtstreekse werking zal hebben. Daarnaast zal het arrest van het Europese Hof van Justitie van oktober 2015 over de Safe Harbour-overeenkomst gevolgen hebben voor de doorgifte van persoonsgegevens naar de Verenigde Staten en voor het toezicht daarop.

De Autoriteit Persoonsgegevens zet zich in om de uitkomsten van de internationale conferentie van privacytoezichthouders die in oktober 2015 in Amsterdam plaatsvond in 2016 een stap verder te brengen. Het centrale thema van deze conferentie was het bouwen van pragmatische 'bruggen' tussen de privacybescherming in de VS en de EU. Toezichthouders, overheden, wetenschappers en bedrijfsleven geven in 2016 nadere invulling aan deze bruggen en streven ernaar ze ook daadwerkelijk te implementeren.

Werkwijze Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens een mix van instrumenten in op het gebied van toezicht, handhaving en communicatie.

Toezicht

De Autoriteit Persoonsgegevens doet onderzoek bij het vermoeden van ernstige overtredingen van de wet die structureel van aard zijn, veel mensen treffen en waarbij de toezichthouder verschil kan maken. Op basis van tips die via de website en het telefonisch spreekuur binnenkomen en op grond van kennis van het toezichtsdomein bepaalt zij waarnaar zij onderzoek doet. In bepaalde gevallen start de Autoriteit Persoonsgegevens geen onderzoek, maar stuurt zij een brief aan organisaties of voert zij een gesprek. Dit is meestal al voldoende om de overtreding te laten beëindigen. De Autoriteit Persoonsgegevens geeft ook handreikingen aan bedrijven en instellingen door het uitbrengen van beleidsregels waarin zij een toelichting geeft op de geldende regels.

Handhaving

De Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens ook een boete opleggen. Vooral vanwege de preventieve werking die ervan uitgaat, is de boete een belangrijke aanvulling op het sanctiearsenaal.

Communicatie

Externe communicatie is voor de Autoriteit Persoonsgegevens een belangrijk instrument om haar doelen te bereiken. Zij communiceert met burgers, media, bedrijven, overheden en andere stakeholders. Dit doet de Autoriteit Persoonsgegevens om te informeren, te waarschuwen en burgers handvatten te geven om zelf hun rechten uit te oefenen. Ook legt zij hiermee verantwoording af over haar keuzes. Externe communicatie is ook een belangrijk instrument om naleving van de privacywetgeving te bevorderen. Dit doet de Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens spreken regelmatig op conferenties en nemen deel aan paneldiscussies. Ook voeren zij gesprekken met branche-organisaties en gaan zij de dialoog aan met 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 Autoriteit Persoonsgegevens ervaren.

Onze missie

De Autoriteit Persoonsgegevens staat voor het grondrecht op bescherming van persoonsgegevens. Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Onze visie

Het grondrecht op bescherming van persoonsgegevens is fundamenteel voor de werking van de rechtsstaat.

De Autoriteit Persoonsgegevens beschermt dit grondrecht door:

- overtredingen van de wet aan te pakken;
- over nieuwe regelgeving te adviseren;
- op de hoogte te zijn van de dilemma's die in de samenleving spelen op het gebied van privacy;
- overheid, bedrijfsleven en andere maatschappelijke organisaties alert te maken op hun verantwoordelijkheid bij de bescherming van persoonsgegevens;
- informatie te verstrekken waarmee mensen hun recht kunnen uitoefenen;
- resultaten van toezicht en handhaving openbaar te maken;
- nationaal en internationaal samenwerking te zoeken ten behoeve van de bescherming van persoonsgegevens.

Onze kernwaarden

De Autoriteit Persoonsgegevens is **onafhankelijk.** Dat betekent dat wij binnen de kaders van de wet onze eigen koers bepalen. Wij kiezen prioriteiten op basis van de ernst en de omvang van overtredingen.

Deskundigheid staat bij de Autoriteit Persoonsgegevens hoog in het vaandel. Wij zetten ons dan ook volledig in om hoogwaardig werk af te leveren.

De Autoriteit Persoonsgegevens is **transparant** over haar resultaten en keuzes, creëert draagvlak voor haar werk en nodigt uit tot dialoog. Wij zijn open, eerlijk en zichtbaar.

De Autoriteit Persoonsgegevens werkt aan de bescherming van een grondrecht. Daar zijn wij trots op. Wij zijn **betrokken** bij ons werk en staan met beide benen in de samenleving.