NUMMER 41 / JULI 2022 / JAARGANG 12

DE COMPLIANCE OFFICER

PRIVACY

COLOFON

De Compliance Officer is het vakblad voor compliance officers en andere betrokkenen bij het complianceproces. De doelgroep bestaat uit compliance officers, bestuurders, toezichthouders, secretarissen van de vennootschap en bedrijfsjuristen die betrokken zijn bij het uitvoeren van compliancetaken.

REDACTIE:
Melissa Veen (eindredactie)
Bojana Huising (bureauredactie)
Tel. 088 99 88 100
E-mail: info@compliance-instituut.nl
AAN DEZE EDITIE WERKTEN VERDER MEE: Cecile Schut, Peter van den Bosch, Koen Versmissen, Caroline Poerbodipoero- van Gisbergen, Bart Peters, Hans Kooij, Edwin van Tongerlo, Niels Arends, Francis Joung Sander van de Molen, Joost Damen
FOTOGRAFIE: Wilco van Dijen
INTERVIEWS: Monique Hurkmans
VORMGEVING: Tangram Studio
DRUK: Platform P, Rotterdam
UITGEVER: Nederlands Compliance Instituut, Jan Leentvaarlaan 61-63 3065 DC Rotterdam

Nieuwsfeiten, ingezonden artikelen en personeelsmutaties kun je per e-mail doorgeven aan info@complianceofficer.nl.

Het abonnement is gratis voor de doelgroep. Abonnees buiten de doelgroep: € 50 per jaar.

Wil je je abonnement opzeggen, dan kun je je afmelden via info@complianceofficer.nl.

Oplage 4.100 exemplaren
ISSN 1878-7991

INHOUD

PRIVACY COMPLIANCE: WE DOEN ONS BEST, MAAR EENVOUDIG IS HET NIET!

Met trots presenteren wij hierbij de 41e editie van De Compliance Officer met als thema: Privacy. Een thema waar – met name sinds de komst van de Algemene Verordening Gegevensbescherming (AVG) – enorm veel aandacht voor is. Een compliance onderwerp waar organisaties speciale afdelingen met gespecialiseerde officers voor inrichten. Een ontzettend boeiend, maar ook veeleisend rechtsgebied waar voor organisaties een grote uitdaging in schuilt om compliant te zijn en te blijven.

Met de komst van de AVG werden namelijk niet alleen meer rechten voor burgers ten aanzien van de bescherming van hun persoonsgegevens geïntroduceerd, maar het bracht ten minste evenzoveel extra verplichtingen met zich mee voor de organisaties die die persoonsgegevens verwerken. En belangrijker nog, de mogelijkheid om het niet voldoen aan de verplichtingen te beboeten door toezichthouders, werd in het leven geroepen. Ondanks dat veel organisaties altijd al wel wisten dat zij zorgvuldig met de gegevens van hun klanten en medewerkers om moesten gaan – in Nederland hadden we immers al de Wet bescherming persoonsgegevens en was het melden van datalekken reeds een verplichting – was deze boetemogelijkheid (mogelijk) nog net een stukje extra motivatie om dit ook daadwerkelijk te gaan doen.

Maar voldoen aan de AVG is zo eenvoudig nog niet. De verordening staat namelijk bol van de open normen waaraan in de praktijk invulling gegeven dient te worden. En ondanks dat onder meer het Europees Parlement en de Raad van de Europese Unie hebben hier middels 173 overwegingen weliswaar enige duiding aan hebben proberen te geven, blijkt uit het steeds groter wordende aantal uitgedeelde boetes dat er nog een lange weg te gaan is voor vele organisaties.

Daarnaast volgen de ontwikkelingen op het gebied van privacy elkaar in rap tempo op. Neem bijvoorbeeld de uitwisseling van gegevens met een in Amerika gevestigde onderneming. Denk je als organisatie het juiste te doen door de samenwerking aan te gaan met een bij het Privacy Shield aangesloten onderneming, wordt dit framework nietig verklaard en blijk je je als organisatie ineens schuldig te maken aan illegale gegevensverwerking. Datzelfde lijkt nu waarschijnlijk ook het geval te gaan zijn als je als onderneming gebruik maakt van Google Analytics, privacyvriendelijk ingesteld of niet.

Het moge duidelijk zijn, privacy is een rechtsgebied dat volop in beweging is. Dat maakt het, als gezegd, niet alleen boeiend, maar ook uitdagend voor organisaties om te voldoen aan de vereisten die erop hen rusten, om compliant te zijn. Voor ons een reden om aan dit thema een editie van De Compliance Officer te wijden. Het doel van deze editie is niet alleen om te informeren over de verschillende – naar ons inzicht op dit moment de belangrijkste – privacy onderwerpen, maar ook om handvatten te geven die jullie kunnen meenemen in jullie eigen uitdagingen met betrekking tot de AVG. Om te leren. Te leren van organisaties die in hetzelfde spreekwoordelijke schuitje zitten en de visie die zij hebben op de invulling van de open normen van de AVG. Maar ook om te leren van de toezichthouder en de boetebesluiten die zij heeft uitgevaardigd. En om te leren van een organisatie waarop een vergrootglas ligt vanwege de nauwe banden met Amerika en als gevolg daarvan grote inspanningen moet leveren om aan te kunnen tonen te voldoen aan de AVG-verplichtingen.

Kortom, een editie ter leering ende vermaeck.
Veel leesplezier gewenst!

Melissa Veen

CECILE SCHUT:

“BESCHERMING PERSOONSGEGEVENS HOORT BIJ MAATSCHAPPELIJK VERANTWOORD ONDERNEMEN”

De Autoriteit Persoonsgegevens (AP) bevordert en bewaakt de bescherming van persoonsgegevens. Ze stimuleert bedrijven en overheden om zich aan de privacyregels te houden en controleert of ze dat ook echt doen. Zo nodig kan het worden afgedwongen. Welke speerpunten staan centraal? Hoe blijven beloning en bestraffing in balans? Wat is de strategie op handhaving? Een gesprek met Cecile Schut, directeur van de afdeling Systeemtoezicht, Beveiliging en Technologie.

'Sinds 2018 ben ik directeur bij de AP. De directie Systeemtoezicht, Beveiliging en Technologie houdt zich onder meer bezig met toezicht op de opzet, reikwijdte en werking van de privacyprocessen. Om ervoor te zorgen dat organisaties hun persoonsgegevens optimaal beschermen. We houden ons vooral bezig met de preventieve en compliance bevorderende kant van toezicht.

In de Algemene verordening gegevensbescherming (AVG) staan, naast allerlei verplichtingen voor mensen en organisaties die met persoonsgegevens werken, ook allerlei instrumenten die preventief kunnen werken. Bijvoorbeeld het gebruik van gedragscodes.

We geven voorlichting *(guidance)* en brengen knelpunten in kaart. Hoe en waarmee kunnen we vanuit de AP ondersteuning bieden? Dat doen we door contact te leggen met Functionarissen Gegevensbescherming, brancheorganisaties, de wetgever, de Vereniging van Nederlandse Gemeenten, et cetera.

We kijken bijvoorbeeld hoe een functionaris gegevensbescherming optimaal kan werken binnen een organisatie. Heeft hij de goede middelen? Passen zijn taken bij een goed en onafhankelijk toezicht? Bijten deze niet met andere werkzaamheden? Maar we richten ons ook op de inrichting van het systeem in de breedte. Als we zien dat organisaties moeite hebben met een bepaald onderdeel van de AVG, dan kan het al helpen om een goed gesprek te voeren.

Een voorbeeld: veel kleine bedrijven maken gebruik van softwaretoepassingen die ze inkopen. Stel je bent een fysiotherapeut en je software voldoet niet aan de AVG, zonder dat je dat weet. Dat kan een probleem zijn. Je bent immers zelf verantwoordelijk voor de bescherming van de persoonsgegevens van je cliënten. Hoe kunnen wij bevorderen dat dergelijke software voldoet? In dit voorbeeld heeft de AP de gedragscode van brancheorganisatie NLdigital goedgekeurd die gebruikt kan worden door IT-bedrijven die dit soort software aanbieden. Hierdoor weet je als ondernemer dat je verzekerd bent van een stuk compliance.

Focusdocument en meerjarenplan

In 2019 heeft de AP een focusdocument opgesteld voor de periode 2020-2023. Hierbij richten we ons op drie speerpunten: digitale overheid, datahandel en algoritmes en Artificial Intelligence (AI). Uiteraard zitten hier ook allerlei dwarsverbanden tussen. Op dit moment zijn we bezig met een nieuw meerjarenplan. Ik verwacht dat bovengenoemde speerpunten ook de komende jaren relevant zullen blijven. De digitalisering schrijdt immers voort, ontwikkelingen op het gebied van AI gaan razendsnel. Er komt nieuwe Europese AI-wetgeving aan en de handel in persoonsgegevens zal ook punt van aandacht blijven.

Er komen heel veel klachten en signalen bij ons binnen. Dat gebeurt rechtstreeks, via de pers of vanuit eigen waarneming. Daarnaast worden er zo'n 25.000 datalekken per jaar bij ons gemeld. Onze capaciteit is echter beperkt. Het tekort aan mankracht heeft impact op ons hele werkterrein. We kunnen lang niet alle klachten afhandelen en de wachttijd is erg lang. Losse tips en signalen kunnen slechts beperkt worden opgepakt. We kunnen slechts een klein deel van de datalekken goed onderzoeken en de verlening van vergunningen kan lang duren.

Daarom proberen we onze middelen zo doelmatig mogelijk in te zetten. Vervolgens moeten we risicogericht te werk gaan. Geen enkele toezichthouder kan alle "boeven" vangen. Stel dat een ondernemer een inzageverzoek weigert. Dat lossen we meestal op door een telefoontje te plegen. Dat werkt heel goed. Gaat het om een klacht tegen een grotere organisatie?

Dan moet de klager zich eerst bij de functionaris gegevensbescherming melden. Op die manier lost het probleem zich vaak vanzelf op. Soms moeten we een verkenning doen, omdat we niet goed weten wat er aan de hand is. Daar kan bijvoorbeeld een berisping of een verwerkingsverbod van persoonsgegevens uit volgen.

Gaat het om grote kwesties, veel betrokkenen of gevoelige data? Dan kan het tot een grootschalig onderzoek komen. Eerst worden de feiten onderzocht en doet de organisatie aan hoor en wederhoor. Vervolgens gaan we juridisch kijken of er sprake is van een overtreding. Daarna volgt een handhavingstraject op basis waarvan we de strafmaat bepalen. Dat kan een boete, een dwangsom of een verwerkingsverbod zijn. We hebben een heel scala aan mogelijkheden.

De burger staat altijd centraal. We proberen door zijn bril te kijken. Hoeveel burgers zijn erbij betrokken? Wat is het effect en het gevolg van de overtreding? Dat kan soms echt ernstig zijn. Iemand wordt uitgesloten van bepaalde diensten of heeft geen grip meer op de opgeslagen data. Terwijl op grond daarvan wel besluiten worden genomen. Soms komen signalen ook uit een brancheverenigingen of van ondernemers.

Geld en mankracht

Eind 2020 heeft KPMG onderzoek gedaan naar de taken en het werk van de AP. Hieruit kwam dat we fors zouden moeten groeien. Ter illustratie, een brede toezichthouder telt al gauw tussen de 600 en 2.500 fte. De AP heeft nu zo'n 170 fte. Ook in het nieuwe coalitieakkoord is meer budget beschikbaar gesteld. Daar zijn we blij mee. Door de toenemende digitalisering en AI neemt ons werk alleen maar toe. En veel grote bedrijven hebben een hoofdvestiging in Nederland. Er wordt steeds meer gedaan met data, er komt steeds meer Europese wetgeving gelieerd aan de AVG. Maar met meer geld en mankracht zullen we niet alle knelpunten kunnen oplossen.

Het is nodig dat we nog meer aandacht kunnen besteden aan behandeling van de klachtenstroom bij de AP. Mensen moet nu veel te lang wachten voordat we überhaupt in actie komen.

Ook een verkorting van de wachttijd voor bedrijfsvergunningen is wenselijk. Uiteraard is het enorm belangrijk dat we blijven investeren in onze eigen kennis. Juist omdat de ontwikkeling van technologie zo snel gaat.

We moeten uitbreiden op het gebied van goede *guidance* van bedrijven die iets nieuws willen. Wat zijn de gevolgen voor de burger én het imago van je bedrijf? Dus meer tijd voor de bevordering van compliance, meer aandacht voor *awareness* en de risico's van niet goed omgaan met privacy. Ook willen we graag meer *best practices* delen.

We doen ongeveer twintig grote onderzoeken per jaar. Functionarissen gegevensbescherming zeggen regelmatig dat het prettig is om te kunnen verwijzen naar een boete van de AP. Dat kan *awareness* creëren binnen een organisatie. Ook heeft de uitslag van een onderzoek impact binnen de betrokken branche.

Organisaties die we met een klacht benaderen, zijn over het algemeen bereid om ernaar te kijken. We merken dat Functionarissen Gegevensbescherming steeds beter in hun rol komen. Hun kennis en vaardigheden nemen toe. Ze worden

> Kunnen verwijzen naar een boete van de AP kan awareness creëren binnen een organisatie.

bekender binnen de organisatie. Overigens is het niet zo dat elke onderneming de AVG bewust overtreedt. Sommigen schrikken echt als we bellen. Ze waren zich er niet van bewust en passen hun werkwijze daarna snel aan.

Als het tot een groter onderzoek komt, is er weinig ruimte voor dialoog tussen de organisatie en de AP. Vergelijk het met een snelheidsovertreding opgelegd door de politie. Soms is het lastig dat we zowel preventief als ook bestraffend acteren. Organisaties vragen zich af met welke kant ze te maken hebben. Met de voorlichtende of de berispende kant? We proberen helder te zijn met welke pet op we binnenkomen. Dat moet overigens ook vanuit de Algemene wet bestuursrecht (Awb).

Het is lastig te meten in hoeverre een verplichte, aangepaste werkwijze wordt opgevolgd. We volgen het in de contacten met brancheverenigingen. We sturen *guidance*-brieven of bieden extra informatie op onze website. Ook in Europees verband. Samen met andere autoriteiten persoonsgegevens in Europa brengen we allerlei voorlichtingsdocumenten uit.

Implementatie AVG en borging

Sinds 2018 hebben de meeste organisaties aandacht besteed aan de AVG. De grotere bedrijven met veel persoonsgegevens hebben vaak forse implementatietrajecten achter de rug. Het is aan het landen in een vaste structuur. Er is periodieke controle: *plan, do, check, act.*

Soms is er veel energie in de implementatie gestoken, maar is het daarna te weinig onderdeel van het continue proces. Of komt het sowieso in het gedrang. We moeten naar een stuk borging toe. Dat gaat niet overal even goed. Als er geen functionaris gegevensbescherming is, dan kan een compliance officer of accountant daarop letten. Staan alle puntjes (nog) op de i? Dat moet je jaarlijks nagaan.

Zodra je persoonsgegevens wilt gaan verwerken, krijg je te maken met *privacy by design*. Een verplichting vanuit de AVG. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy. Dat begint al bij het ontwerp. Een app, een database voor patiënten, een smartphone. Probeer alleen die data te verzamelen die echt nodig zijn voor je doel. Als iemand een boek of kledingstuk online bestelt, is het bijvoorbeeld niet nodig om zijn geboortedatum te weten.

> Verzamel alleen data die echt nodig zijn: als iemand een boek of kledingstuk bestelt, is het niet nodig om zijn geboortedatum te weten.

Mensen zeggen wel eens dat privacy de innovatie remt. Als je goed aan *privacy by design* doet, hoeft het elkaar niet in de weg te staan. Bij hele nieuwe technologieën is er altijd de verplichting om vooraf een *Data protection impact assessment* (DPIA) te doen. Hoe ontwerp ik de processen en systemen? Welke risico's levert het op? Kan het ook privacyvriendelijker? Een DPIA is een goede manier om privacyrisico's te beschrijven. Maar het is ook een waardevol proces om te kijken wat je wilt gaan doen en hoe.

Twijfel je aan het eind van de rit of alle risico's zijn weggenomen? Je kun het ook altijd aan de AP voorleggen in de vorm van een voorafgaande raadpleging. Daar zit een termijn van minimaal acht weken aan vast. Er wordt relatief weinig gebruik van gemaakt. Terwijl het toch vooraf een stuk zekerheid kan geven.

Overigens moeten bedrijven niet alleen zorgvuldig omgaan met data van hun klanten en medewerkers, maar ook met de producten die ze maken en verkopen. Denk aan apparaten die verbinding maken met het internet. Er wordt immers informatie gedeeld tussen het apparaat, de gebruiker en de ontvanger. Dat is bij steeds meer producten het geval.

Omgekeerd geldt dat ook voor de afnemer. Hoe zit een product in elkaar? Hoe werkt een beveiligingscamerasysteem? Zorg dat je je goed informeert via de producent of leverancier. Het is belangrijk hier aandacht voor te hebben en verantwoordelijkheid voor te nemen.

Compliance officer en persoonsgegevens

Ik zie paralellen tussen een functionaris gegevensbescherming en een compliance officer. Ik kan me voorstellen dat een compliance officer ook naar het systeem van het bedrijf kijkt. Is de bescherming van persoonsgegevens goed geborgd?

Bescherming van persoonsgegevens hoort bij maatschappelijk verantwoord ondernemen. Net als diversiteit en duurzaamheid. Hiermee kun je je als bedrijf onderscheiden. Het kan zaken voorkomen. Zo is een datalek een hele vervelende gebeurtenis voor een bedrijf. Ongeacht of het is ontstaan door een menselijke fout of doordat medewerkers bewust data hebben gestolen en doorverkocht. In de meeste gevallen blijkt de beveiliging toch niet goed op orde te zijn geweest.

Soms gaat het om data die eigenlijk al weggegooid hadden moeten worden. Ik zeg altijd: "Wat je weggooit, kun je ook niet kwijtraken." Daar moet je op toezien. En uiteraard of het systeem van plan, do, check, act ook voor gegevensbescherming op orde is. Klanten zullen het positief waarderen als je bedrijf goed en zorgvuldig met gevoelige data omgaat. We merken dat de aandacht voor privacy enorm is toegenomen. Zowel bij burgers als bij bedrijven.'

Cecile Schut is directeur Systeemtoezicht, Beveiliging en Technologie bij de Autoriteit Persoonsgegevens.

Na haar studie toegepaste wiskunde werkte ze eerst bij KPN Research en daarna 20 jaar bij het CBS. Bij het CBS was ze als directeur beleid en strategie onder andere verantwoordelijk voor de implementatie van de AVG.

Schut is wiskundig ingenieur en behaalde haar Master in Public Administration aan de Nederlandse School voor Openbaar Bestuur.

COMPLIANT EN TOCH DE SJAAK...

Bart Peters

Bart Peters was in het verleden lange tijd verbonden aan het Nederlands Compliance Instituut en is sinds 2016 werkzaam als Compliance Consultant in Nieuw-Zeeland.

Compliance officers verdienen er hun geld mee, maar toch: wetgeving is een beetje saai tot tenenkrommend saai. Privacy-wetgeving is daar geen uitzondering op. Die is meestal recht toe recht aan – in Europa maar ook daarbuiten zoals hier in Nieuw-Zeeland. Het komt erop neer dat je een aantal procedures moet hebben die regelen wat voor informatie je mag verzamelen, hoe je die veilig bewaart, in welke gevallen je die mag delen met anderen en wanneer je die informatie weer vernietigt. Zorg er ook nog voor dat je cliënt hiervoor tekent en dat je je personeel traint, en voila, *tick that box!*

Was het maar zo simpel. Ook het omgaan met privacygevoelige informatie is mensenwerk. Slordige of frauduleuze medewerkers, systeemfouten en op de loer liggende criminelen zijn altijd een risico geweest. Toch waren die risico's tot pakweg 30-40 jaar geleden te overzien. Cliëntdossiers waren meestal nog op papier, computerbestanden stonden nog niet op megaservers of in de cloud, criminelen net zo digibeet als de gemiddelde gebruiker en als er al wat misging was de reikwijdte daarom beperkt. Misschien dat een medewerker eens een dossier stal of dat er een doos met cliëntdossiers bij het huisvuil werd gezet, maar de gevolgen waren te overzien.

Hoe anders is dat in de huidige wereld. Ik hoef niet uit te leggen dat er zich grote veranderingen hebben voorgedaan in de laatste decennia. Ondanks mijn leeftijd is "alles was vroeger beter" niet mijn lijfspreuk, maar kijkend naar privacy zijn er veel factoren – technologisch en sociologisch – die de risico's op dit gebied enorm vergroot hebben, ook voor organisaties die hun best hebben gedaan om de privacywetgeving zo goed mogelijk in te vullen.

Technologische factoren die veel invloed hebben, zijn bijvoorbeeld de verregaande digitalisering – met enorm grote en gekoppelde bestanden – opslag in de cloud of op servers die gehackt kunnen worden, mail en social media die ook voor criminele doeleinden gebruikt kunnen worden en het gedigitaliseerde geldverkeer. Stuk voor stuk doelwitten voor misdadigers die tegenwoordig een veelheid aan *cybercrimes* onder de knie hebben. Een recent voorbeeld daarvan is doxing, het verspreiden van bijvoorbeeld een woonadres of telefoonnummer om een bekend persoon (en zijn gezin) in de problemen te brengen of angst aan te jagen.

Daarnaast is er een aantal sociologische factoren die veel invloed hebben. Het Internet heeft uiteraard veel invloed gehad; mensen hebben via social media contact met bekenden, maar ook met dorpsgenoten, landgenoten en mensen aan de andere kant van de wereld. De verspreiding van informatie (goedbedoeld of juist niet) gaat daarom razendsnel en de rol van de publieke opinie is daarom tegenwoordig veel groter dan voorheen. Je kunt je afvragen of echte privacy nog bestaat. Dit heeft natuurlijk voordelen (mis-standen komen bijvoorbeeld sneller aan het licht), maar er is ook een keerzijde. Elk vermeend incident wordt in no time opgeblazen tot een schandaal, waarbij de betreffende organisatie in het nauw komt tussen de publicitaire druk en de verplichting om bepaalde informatie geheim te houden op grond van de privacywetgeving. Bijvoorbeeld juicekanalen, de MeToo-beweging of belangen-groeperingen kunnen met wisselende motieven deze publicitaire druk vergroten, waarbij de betrokken organisatie soms voor een duivels dilemma komt te staan en een keus moet maken tussen het naleven van de wetgeving of het toegeven aan deze druk.

Last but not least: soms kan een organisatie druk voelen om een zaak die zijn oorsprong vindt binnen de organisatie – bijvoorbeeld een melding van een klokkenluider of een interne of externe klacht – openbaar te maken, ook al staat dat op gespannen voet met de privacywetgeving.

De conclusie is dat ook de organisatie die naar eer en geweten de privacywetgeving naleeft absoluut niet gevrijwaard is van problemen op dit gebied. Dit is echter geen vrijbrief om die wetgeving niet na te leven, maar wel een opdracht aan het bestuur om zich voor te bereiden op dergelijke gebeurtenissen en dilemma's.

Kia Ora!

Bart Peters

TRACKING COOKIES
IS MIJN ORGANISATIE COMPLIANT?

Caroline Poerbodipoero- van Gisbergen

Vrijwel iedere website of app maakt gebruik van cookies. Dit zijn kleine tekst-bestandjes die op de computer, tablet of smartphone van de websitebezoeker of app-gebruiker worden geplaatst. Deze bestandjes kunnen informatie opslaan en verzamelen. Cookies kunnen niet alleen worden gebruikt om een website of app goed te laten functioneren of om het gebruik ervan te verbeteren. Ze kunnen ook worden geplaatst voor marketingdoeleinden. Cookies zorgen er dan voor dat bezoekers van apps of websites gerichte advertenties te zien krijgen die aansluiten bij hun profiel. Het gebruik van deze tracking cookies ligt al geruime tijd onder vuur, omdat ze een behoorlijke privacy-impact hebben. Ook wordt de bezoeker niet altijd goed geïnformeerd of wordt op een onjuiste manier om toestemming gevraagd.

Als Compliance Officer of Functionaris voor Gegevens-bescherming is het daarom raadzaam periodiek het gebruik van cookies en de informatievoorziening over cookies te monitoren en eventueel het gesprek daarover aan te gaan in de organisatie.

Dit artikel is bedoeld als leidraad daarbij. Het geeft je uitleg over de verschillende soorten cookies, de werking van cookies voor marketingdoeleinden in combinatie met *Real Time Bidding* (RTB) en de regels voor het plaatsen van dergelijke cookies. Ook wordt een aantal belangrijke recente ontwikkelingen besproken, zoals een verbod op het gebruik van het *Transparency and Consent Framework* van IAB Europe en een mogelijk verbod op Google Analytics. Tot slot wordt uitgelegd hoe je kunt achterhalen welke cookies de website van jouw organisatie gebruikt, zodat je kunt bepalen wat deze ontwikkelingen voor jouw organisatie betekenen.

Soorten cookies

Functionele en technische cookies
Functionele en technische cookies zorgen voor een goed werkende website of app. Je kunt daarbij denken aan cookies die ervoor zorgen dat je ingelogd blijft of die de items in je winkelmandje onthouden.

Analytische cookies
Analytische of statistische cookies verzamelen informatie over het gebruik van een website of app, waarmee die website of app kan worden verbeterd.

Tracking cookies
Tracking cookies kunnen het surfgedrag van de bezoeker volgen. Hieruit kunnen de interesses van de bezoeker worden afgeleid, waarmee een profiel wordt opgebouwd. Deze vorm van profilering maakt het voor adverteerders mogelijk om de bezoeker op de website of app en daarbuiten advertenties te laten zien die aansluiten bij zijn interesses.

Tracking Cookies en Real Time Bidding

Real Time Bidding (RTB), waarbij advertentieruimte online wordt geveild, is een techniek voor het aanbieden van gepersonaliseerde online advertenties *(targeted advertising)*. Dagelijks worden via RTB miljarden advertenties geveild. RTB vindt plaats via *Supply-Side Platforms/Sell-Side Platforms* (SSPs) (hier wordt advertentieruimte aangeboden) en *Demand-Side Platforms* (DSPs) (hier zoeken adverteerders naar de beste advertentieruimte voor hun advertenties). Daartussen bevinden zich de *Ad Exchanges*, die ervoor zorgen dat vraag en aanbod worden samengebracht en deze partijen automatisch met elkaar communiceren.

Wanneer een bezoeker een website of app bezoekt, laat het SSP waar de website/app bij is aangesloten weten dat er kan worden geboden op een advertentie. Het profiel van de bezoeker wordt via een *Ad Exchange* doorgespeeld aan de DSPs. Op basis van deze gegevens kan via software en algoritmen worden bepaald in hoeverre dit profiel aansluit bij de doelgroep van de duizenden adverteerders die zijn aangesloten bij de DSPs. Aan de hand daarvan wordt de hoogte van het bod berekend en brengen de DSPs een bod uit. Dit veilingproces vindt geautomatiseerd en in *real time* plaats. De advertentie van de winnende adverteerder wordt binnen enkele milliseconden ingeladen. Dit kan verklaren waarom je bijvoorbeeld ineens veel advertenties voor zonnebrillen ziet als je je op het internet hebt georiënteerd op een zonvakantie.

In het samenstellen van bezoekersprofielen spelen Data *Management Platforms* (DMPs) een belangrijke rol. Deze platforms verzamelen enorm veel gegevens over bezoekers via verschillende bronnen, waaronder cookies, toestellen, pixels en online surfgedrag. Ook verkrijgen ze informatie via databrokers, zoals bijvoorbeeld Verisk, Acxiom, Oracle Data Cloud, Epsilon, Experian en Equifax. Deze gegevens worden vervolgens geanalyseerd. Via een DMP kan een adverteerder zijn eigen gegevens over een potentiële klant/websitebezoeker verrijken om zo een nog nauwkeuriger profiel van zijn doelgroep op te bouwen. Op die manier kan gericht op aangeboden advertentieruimte worden geboden.[1]

1 De impact van tracking cookies en de rol van data brokers is onlangs op ludieke wijze belicht in de online terug te kijken uitzending: *Data Brokers: Last Week Tonight with John Oliver*, HBO, 10 april 2022.

Behavioral advertising levert de aanbieder slechts ongeveer 4% meer op dan de traditionele manier van adverteren.

RTB biedt uiteraard marketingvoordelen, omdat alleen wordt betaald voor advertenties die de doelgroep bereiken. Het heeft echter ook nadelen, omdat de profielen van bezoekers worden gedeeld met talloze partijen die deelnemen aan het veiling-proces. Bovendien ontstaan zogenaamde *data lakes;* de gegevens van de enorme hoeveelheden bezoekers van al deze websites en apps vormen een meer van persoonsgegevens, waar maar weinig zicht op is. Het gaat daarbij ook om gevoelige gegevens, zoals bijvoorbeeld betalingsachterstanden en bijzondere persoonsgegevens, zoals gezondheidsgegevens, politieke voorkeuren en seksuele geaardheid.

Onderzoek heeft uitgewezen dat deze zogenaamde *behavioral advertising* de aanbieder slechts ongeveer 4% meer oplevert dan de meer traditionele manier van adverteren, waarbij advertenties worden getoond die passen bij datgene wat op dat moment op de website of app wordt aangeboden *(contextual advertising)*. Deze meeropbrengst zou gelijk staan aan ongeveer een schamele $ 0,00008 per advertentie.[2] De partijen die er daadwerkelijk van profiteren zijn de techgiganten achter deze technologie, zoals Google en Facebook. Dit ten koste van de privacy van de bezoeker die veelal nietsvermoedend op *'accept all cookies'* klikt. Niet voor niets is er daarom vanuit de toezichthouders en de rechtspraak steeds meer aandacht voor de manier waarop de websitebezoeker of app-gebruiker wordt geïnformeerd over het gebruik en de werking van tracking cookies en hoe om toestemming voor deze cookies wordt gevraagd.

Vereisten voor geldige toestemming

De Europese e-Privacy Richtlijn[3] is van toepassing op het gebruik van cookies en is een lex specialis ten opzichte van de Algemene Verordening Gegevensbescherming (AVG).[4] Het is de bedoeling dat deze Richtlijn op termijn wordt vervangen door de e-Privacy Verordening, maar de tekst daarvan is nog altijd niet vastgesteld. De e-Privacy Richtlijn is geïmplementeerd in onze Telecommunicatiewet (Tw).

Artikel 11.7a lid 1 Tw bepaalt dat voor het plaatsen van cookies (en soortgelijke technologieën zoals pixels, web beacons of JavaScript tags) toestemming is vereist en dat bezoekers hierover deugdelijk geïnformeerd moeten worden volgens de regels die daarvoor in de AVG zijn neergelegd. Dit betekent dat onder andere de naam van de cookies, de soorten persoonsgegevens die met de cookies worden verzameld, de categorieën ontvangers, het doel, de bewaartermijn en de naam van de partijen die de cookies plaatsen moet worden vermeld.[5]

Alleen cookies die strikt noodzakelijk zijn voor het goed functioneren van de website of app behoeven geen toestemming, alsmede cookies zonder of met slechts geringe gevolgen voor de privacy van de bezoeker, die worden gebruikt om informatie te verkrijgen over de kwaliteit of effectiviteit van

2 Zie Veronica Marotta, Vibhanshu Abhishek en Alessandro Acquisti, *Online Tracking and Publishers, Revenues: An Empirical Analysis*, 2019.

3 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2006/24/EG en Richtlijn 2009/136/EG.

4 Zie art. 95 en overweging 173 AVG.

5 Zie voor meer informatie ook www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies, onder 'Welke informatie moet ik mijn bezoekers precies geven over tracking cookies?'.

de website of app. Voor tracking cookies is dus altijd toestemming vereist.

In de loop der jaren zijn verschillende methoden bedacht om op een creatieve manier toestemming voor het gebruik van tracking cookies te verkrijgen. Zo zijn er websites die standaard het vakje voor toestemming hebben aangevinkt, die vermelden dat toestemming wordt verleend door middel van het gebruik van de website *(browse-wrap)* of die simpelweg geen toegang verlenen zolang geen toestemming wordt gegeven voor het gebruik van cookies (zogenaamde *cookiewalls)*. Ook zijn er websites met een opvallende *'accept all'* button en daarnaast een minder opvallende *'more options'* button, die het daarna pas mogelijk maakt om cookies te weigeren.

Géén vooraf aangevinkte vakjes

Het Europees Hof van Justitie heeft inmiddels in de Planet49 zaak[6] verduidelijkt dat toestemming via een ondubbelzinnige actieve handeling moet worden verleend (zoals ook volgt uit de AVG[7]) en dat vooraf aangevinkte vakjes voor het geven van toestemming daarom niet geldig zijn.

Géén cookiewalls en browse-wrap

Daarnaast hebben verschillende Europese toezichthouders (waaronder de Autoriteit Persoonsgegevens[8]) en de European Data Protection Board (EDPB) zich op het standpunt gesteld dat toestemming voor het plaatsen van cookies door gebruikmaking van browse-wrap of cookiewalls eveneens niet is toegestaan.

Browse-wrap, waarbij de gebruiker middels verder scrollen of vegen door een website of soortgelijke activiteiten 'toestemming' verleent, kan *"onder geen beding voldoen aan het vereiste van een duidelijke actieve handeling: dergelijke handelingen kunnen moeilijk te onderscheiden zijn van andere activiteiten van of interactie met een gebruiker; er kan dus niet worden vastgesteld dat ondubbelzinnig toestemming is verkregen. In een dergelijk geval is het bovendien lastig om het voor de gebruiker net zo gemakkelijk te maken zijn toestemming in te trekken als het was om deze te verlenen"* aldus de EDPB.[9]

Cookiewalls zorgen ervoor dat de inhoud van de website niet wordt getoond als de gebruiker geen toestemming verleent. Zij bieden daarmee de gebruiker volgens de EDPB geen echte keus ten aanzien van het al dan niet accepteren van cookies en voldoen daarom ook niet aan de vereisten voor geldige toestemming.[10] De Autoriteit Persoonsgegevens (AP) neemt eenzelfde standpunt in op haar website[11] en in de *'normuitleg AP over cookiewalls'*.

Toestemming weigeren niet ontmoedigen

De Franse toezichthouder, de CNIL, heeft op 31 december 2021 zowel Google als Facebook een miljoenenboete opgelegd, omdat hun cookiebanners het moeilijker maakten om cookies te weigeren dan om ze te accepteren. Volgens de CNIL wordt daarmee afbreuk gedaan aan het vereiste van een 'vrij' gegeven toestemming; vanwege deze ontmoediging zal men er immers meestal voor kiezen om toestemming te verlenen. Wat de gevolgen van deze uitspraak zullen zijn voor Nederlandse websitehouders is nog onbekend, aangezien de AP op haar website nog geen specifiek standpunt over dit onderwerp heeft ingenomen.

Complianceperikelen rondom Real Time Bidding

Boete voor IAB Europe

Onlangs heeft de Belgische Gegevensbeschermingsautoriteit (GBA) een ingrijpend boetebesluit genomen, waarin het heeft bepaald dat het *Transparency and Consent Framework* (TCF) niet voldoet aan de AVG.[12] Het TCF wordt gebruikt door meer dan 80% van alle Europese websites en apps. Het is ontwikkeld door IAB Europe (Interactive Advertising Bureau Europe) voor organisaties die deelnemen aan Real Time Bidding via het OpenRTB-protocol. Dit protocol is wereldwijd het meest gebruikte RTB-protocol, samen met het *AdBuyers* protocol van Google.

Het TCF heeft tot doel te faciliteren dat haar klanten het RTB-systeem kunnen gebruiken op een manier die voldoet aan de privacywetgeving. Het TCF werkt kort gezegd als volgt: Wanneer iemand een website of app bezoekt, verschijnt een cookiebanner of interface waarin kan worden gevraagd om toestemming voor het plaatsen van tracking cookies en soortgelijke technologieën. Deze cookiebanner is gekoppeld aan een *Consent Management Platform* (CMP), dat de gebruikersvoorkeuren registreert, zoals een gegeven of

6 HvJ EU 1 oktober 2019, C 673/17 *(Verbraucherzentrale Bundesverband/Planet49).*

7 Zie ook EDPB, *Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679*, vastgesteld op 4 mei 2020, paragraaf 7 (met verwijzing naar Art. 94 en 95 AVG).

8 De Autoriteit Consument en Markt houdt o.a. toezicht op naleving van de Telecommunicatiewet en de Autoriteit Persoonsgegevens op naleving van privacywetgeving, waaronder de AVG. Voor wat betreft naleving van cookiewetgeving, bestaat er dus een zekere overlap en kan men met beide toezichthouders te maken krijgen.

9 Zie EDPB, Richtsnoeren 05/2020, paragraaf 86.

10 Zie EDPB 'Richtsnoeren 05/2020, paragraaf 40 en 41.

11 Zie www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies, bijvoorbeeld onder 'Hoe vraag ik geldige toestemming voor tracking cookies?'.

12 Zie Beslissing GBA inzake IAB Europe: Beslissing ten gronde 21/2022 van 2 februari 2022, Dossiernummer: DOS-2019-01377.

geweigerde toestemming of bezwaar tegen een bepaalde verwerking. Het TCF vergemakkelijkt het vastleggen van deze gebruikersvoorkeuren. Ze worden gecodeerd en opgeslagen in een zogenaamde 'TC string', die vervolgens – vanwege het kleine bestandsformaat – gemakkelijk kan worden doorgegeven aan de deelnemers aan het OpenRTB-systeem. Zo weten zij waar al dan niet toestemming voor is gegeven of bezwaar tegen is gemaakt. Het CMP plaatst ook een cookie, genaamd 'euconsent-v2'. De TC-string kan in combinatie met deze cookie worden gekoppeld aan het IP-adres van de bezoeker. Het TCF is daarmee een essentiële schakel in het RTB-proces.

De GBA is van oordeel dat IAB Europe als (gezamenlijke) verwerkingsverantwoordelijke kan worden aangemerkt, omdat zij als *Managing Organisation* het TCF beheert. Zij heeft zowel een recht op toegang als een recht om alle informatie op te slaan en te verwerken die door de deelnemende organisaties wordt verstrekt.

De GBA heeft IAB Europe een boete opgelegd van € 250.000 omdat:

- IAB Europe geen rechtsgrond heeft vastgesteld voor de verwerking van de TC string en adtech-verkopers zich niet mogen baseren op een gerechtvaardigd belang. Deze grondslag werd onterecht door IAB Europe gefaciliteerd.
- de informatie die via het privacy beleid wordt verstrekt te algemeen en te vaag is, waardoor betrokkenen moeilijk controle kunnen houden over hun persoonsgegevens. Met andere woorden: "Men vraagt mensen om hun toestemming te geven, terwijl de meesten van hen niet weten dat hun profielen dagelijks talloze keren worden verkocht om hen aan gepersonaliseerde advertenties bloot te stellen", aldus Hielke Hijmans, Voorzitter van de Geschillenkamer.[13]
- het beginsel van *privacy by design and by default* onvoldoende is nageleefd en het TCF onvoldoende is beveiligd, waardoor de uitoefening van de rechten van betrokkenen niet kan worden gewaarborgd. Omdat onvoldoende controle wordt uitgeoefend op de integriteit en geldigheid van de TC strings is het bovendien mogelijk dat *"CMPs het signaal vervalsen of wijzigen om een euconsent-v2 cookie te genereren en zo een "valse toestemming" van gebruikers voor alle doeleinden en alle vendors te reproduceren"*.[14]
- IAB Europe tot slot geen verwerkingsregister heeft bijgehouden, geen Functionaris voor Gegevensbescherming heeft aangesteld en geen DPIA heeft uitgevoerd.

Naast het betalen van een boete moet IAB Europe alle persoonsgegevens wissen die via eerdere TC Strings zijn verzameld en moeten de geconstateerde inbreuken worden hersteld. IAB Europe heeft inmiddels een verplicht actieplan opgesteld en ingediend bij de GBA. Na goedkeuring moet het plan binnen 6 maanden worden uitgevoerd. IAB Europe is overigens in beroep gegaan tegen de beslissing van de GBA.[15]

Vanwege de grensoverschrijdende verwerkingen in deze zaak is het 'één-loket' of *'one-stop-shop'* mechanisme toegepast. De beslissing van de GBA als leidende toezichthouder is daarbij goedgekeurd door een groot aantal overige betrokken autoriteiten, waaronder de AP. Op de website van de AP is inmiddels vermeld dat het gebruik van TCF in de huidige vorm is verboden en dat de AP de bevindingen van de GBA ten aanzien van het actieplan en het verdere verbetertraject nauwlettend zal volgen.

Gebruik Google Analytics mogelijk niet langer toegestaan

Het gebruik van Google Analytics, een andere belangrijke schakel in het RTB-proces, is eveneens omstreden. Op 22 april 2022 heeft de AP in haar online *'Handleiding privacyvriendelijk instellen van Google Analytics'* een waarschuwing opgenomen dat Google Analytics mogelijk binnenkort niet meer is toegestaan. Google Analytics cookies worden niet alleen voor puur statistische doeleinden gebruikt, maar ook – en vooral – voor marketingdoeleinden. Dit gebeurt in ieder geval wanneer in combinatie met deze cookies ook advertenties worden getoond via Google DoubleClick, AdWords en/of AdSense.[16]

De waarschuwing van de AP is het gevolg van een tweetal eigen onderzoeken en die van andere Europese toezichthouders. Zo heeft de Oostenrijkse toezichthouder, de DSB, op 22 december 2021[17] een openbaar handhavingsbesluit genomen. Hierin is geoordeeld dat het gebruik van Google Analytics in strijd is met de Schrems II-uitspraak van het Europees Hof van Justitie.[18] Persoonsgegevens worden immers gedeeld met Google in de VS, waar geen adequaatheidsbesluit voor geldt. Naast het afsluiten van de verplichte *'standard contractual clauses'* voor gegevensoverdracht, worden onvoldoende aanvullende maatregelen getroffen tegen de mogelijkheid dat de Amerikaanse autoriteiten toegang zouden

13 Zie website GBA: www.gegevensbeschermingsautoriteit.be/burger/iab-europe-wordt-verantwoordelijk-gehouden-voor-een-mechanisme-dat-in-strijd-is-met-de-avg.

14 Zie paragraaf 485 uitspraak GBA.

15 Zie ook www.iabeurope.eu/all-news/iab-europe-appeals-belgian-data-protection-authority-ruling met eveneens een link naar een FAQ met het standpunt van IAB Europe ten aanzien van de beslissing van de GBA.

16 Zie ook de website van de AP onder 'Hoe kan ik bij Google Analytics de privacy van mijn websitebezoekers beschermen?' (www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies).

17 Besluit van de Oostenrijkse Datenschutzbehörde van 22 december 2021 (Bescheid D155.027 GA) (www.dsb.gv.at/download-links/bekanntmachungen.html).

18 HvJ EU, 16 juli 2020, C-311/18 *(Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems).*

Gebruikt de website van mijn organisatie tracking cookies?
Als je wilt weten welke impact de geschetste ontwikkelingen hebben op jouw organisatie, is het noodzakelijk om allereerst een goed beeld te hebben van de cookies die op de website worden geplaatst. Dit biedt meteen ook een goede gelegenheid voor het monitoren van de cookie policy en de cookie banner.

Achterhalen welke cookies een website gebruikt:

1. Wis de zoekgeschiedenis, waarbij ook alle cookies van het apparaat worden verwijderd.
2. Bezoek de website.
3. Klik op de rechtermuisknop, en vervolgens onderaan op *'Inspecteer element'* of *'Inspect'*.
4. Selecteer in de bovenste balk van het menu dat verschijnt *'Opslag'* of *'Application'*, waar de gebruikte cookies onder *'Storage'* zijn terug te vinden.
5. De gebruikte cookies verschijnen, inclusief de duur en het domein van waaruit ze zijn geplaatst. Dit kan de eigen website zijn *('first-party cookies')*, maar ook een andere website *('third-party cookies')*. Third-party cookies zijn meestal tracking cookies, die worden gebruikt voor marketingdoeleinden. Door de naam in te voeren van de betreffende cookie, kan via internet veelal de werking ervan worden achterhaald.

Alternatieve methode voor Google Chrome: Bezoek de website. Klik met de rechtermuisknop op het slotje in de adresbalk en vervolgens op *'Cookies'*.

Tip: Het is raadzaam om deze test op een aantal verschillende apparaten en via verschillende browsers uit te voeren, omdat de browserinstellingen van invloed kunnen zijn op de cookies die verschijnen. Mocht je organisatie ook apps gebruiken, vraag dan intern of via de app-ontwikkelaar meer informatie op over het gebruik van cookies en soortgelijke technologieën, aangezien deze methode alleen werkt voor websites.

kunnen krijgen tot deze gegevens. Uit de beslissing van de DSB blijkt bovendien dat Google – zelfs wanneer gebruik wordt gemaakt van de geanonimiseerde variant – veelal alsnog via andere gegevens de identiteit van de websitebezoeker kan achterhalen en dus ook in dat geval persoonsgegevens in de VS verwerkt.[19] Ook de Franse toezichthouder, de CNIL, heeft inmiddels om dezelfde redenen een aantal websitehouders bevolen het gebruik van Google Analytics te beëindigen.

Of de AP ook een handhavingsbesluit zal nemen naar aanleiding van haar eigen onderzoeken is nog niet duidelijk. Wel is op 25 maart 2022 bekend geworden dat de EU en de VS een principeakkoord hebben bereikt over een nieuw framework voor trans-Atlantische datatransfers ter vervanging van het ongeldig verklaarde Privacy Shield. Dit zou op termijn een oplossing kunnen bieden, maar momenteel staat het gebruik van Google Analytics dus nog op losse schroeven.

Caroline Poerbodipoero – van Gisbergen is zowel gecertificeerd Compliance Officer als gecertificeerd Data Protection Officer. Zij heeft brede werkervaring op het gebied van privacy, compliance, ondernemingsrecht, financiële dienstverlening en faillissementsrecht. Via haar bedrijf, Fortify Legal Advice B.V., is ze werkzaam op het gebied van Privacy en Compliance. Vanwege haar jarenlange ervaring in de advocatuur is ze eveneens in te schakelen als Legal Counsel.

19 Zie onder meer onderdeel D.2. Spruchpunkt 2. a) sub c en onderdeel D.3. Spruchpunkt 2. b) sub f.

MARTIN VLIEM:

“VANUIT MICROSOFT HEBBEN WIJ DE VERANTWOORDELIJKHEID OM TE HELPEN BIJ HET BESCHERMEN VAN GEGEVENS EN HET TOEPASSEN VAN PRIVACYWAARBORGEN, MAAR OOK KLANTEN HEBBEN EEN KEUZE OVER HOE ZIJ ZAKEN INRICHTEN"

Microsoft is een Amerikaans bedrijf dat computer gerelateerde producten en diensten ontwikkelt, verspreidt en ondersteunt. Door het onlangs vervallen van het Privacy Shield in 2020 is er onzekerheid ontstaan over de werkwijze en de betrouwbaarheid van Microsoft in het kader van gegevensbescherming. Kunnen zij als Amerikaans bedrijf binnen Europa wel compliant zijn? National Security Officer van Microsoft, Martin Vliem, geeft hierbij antwoord op onze vragen:

De Microsoft-organisatie in Nederland

Het moederbedrijf van Microsoft is gevestigd in Amerika, hier worden veel van de Microsoft producten ontwikkeld. Het takenpakket van Microsoft in Nederland bestaat voornamelijk uit het begeleiden van klanten, verkoop, technische expertise, consultancy, partnermanagement en support. In het verleden was dit vaak gericht op functies van technologie zoals Windows en Office, maar nu kijken we juist meer naar de digitale transformatie: wat is de impact van technologie? En hoe kan technologie van waarde zijn in de ondersteuning van bedrijfs- en organisatieprocessen?

Privacy governance

We kijken naar verschillende toepassingsgebieden van privacy. Zo hebben we de privacy naar onze eigen medewerkers toe – hier staat een interne privacy governance organisatie voor – maar ook de privacy in onze producten en dienstverlening waarin wij een verantwoordelijkheid hebben naar onze klanten. Hierin vertegenwoordig ik vooral de kant van onze zakelijke clouddienstverlening waarbij klanten ons "instructies" geven om gegevens te verwerken, omdat ze bijvoorbeeld Teams willen gebruiken of documenten online willen opslaan. Daarbij verwachten klanten dat Microsoft zijn aandeel neemt in informatiebeveiliging, het waarborgen van privacy en dat de diensten op een compliant manier ingezet kunnen worden. Om dit allemaal voorspoedig te laten verlopen hebben we een heel team in Amerika zitten wat primair het beleid uitzet. Hierbij kijken zij naar hoe we wereldwijd om moeten gaan met de verschillende vormen van privacywetgeving, welke ontwikkelingen er zijn in de wet- en regelgeving en beleidsvorming én hoe dit ingebed dient te worden in onze producten en diensten. Daarnaast begeleidt dat team de wereldwijde toepassing van dit beleid. Ieder product van Microsoft heeft zijn eigen productie (enginering) team dat uiteindelijk verantwoordelijk is voor het inbedden van het uitgezette beleid. Op het moment dat producten de markt opgaan vinden er altijd privacy reviews plaats om te beoordelen of het beleid dat we hebben op de juiste manier wordt ingezet en of de juiste registraties zijn gemaakt. En natuurlijk worden privacy maatregelen voortdurende geëvalueerd. Dit is ons standaard privacy governance proces, maar dan wel op schaal omdat we met veel development teams te maken hebben.

Connectie met Amerika

Digitalisering is een belangrijke ontwikkeling, daar hopen we een positieve bijdrage voor onze klanten aan te kunnen leveren. Maar we zien ook dat digitalisering kan betekenen dat er vormen van doorgifte van gegevens kunnen plaatvinden buiten de Europese Unie. We verbinden ons aan en geloven in de rechten en vrijheden van mensen. Privacy is daarin een ontzettend belangrijk gegeven waarin we samen met onze klanten onze verantwoordelijkheden willen en moeten nemen. Dit doen we bijvoorbeeld door zoveel mogelijk data binnen Europa te houden en op te slaan. Maar er zijn scenario's waarbij er toch doorgiftes van gegevens kunnen bestaan waarbij wij denken dat het doorgeven van gegevens noodzakelijk en proportioneel kan zijn. Daar moeten we ook transparant over zijn.

We zijn een wereldwijde cloudprovider. Dat betekent niet dat wij alleen te maken hebben met Amerikaans recht of alleen met Europees recht. We moeten aan vele verschillende vormen van wet- en regelgeving voldoen en dat is soms best een uitdaging. Zo heb ik de afgelopen periode veel vragen van klanten gekregen naar aanleiding van het vervallen van het *Privacy Shield* in 2020 en hoe wij met de gevolgen daarvan omgaan. Maar vragen aangaande privacy zijn altijd al een belangrijk aandachtspunt geweest. Want wat betekent het nou voor klanten om met een Amerikaanse clouddienstprovider in zee te gaan? Wat betekent dat voor Nederlandse soevereiniteit

in het kader van wet- en regelgeving? En hoe zit het met de AVG? Het beantwoorden van dit soort vragen en het gesprek aangaan met klanten over Amerikaanse wetgeving is niet nieuw voor ons. Voor het wegvallen van het *Privacy Shield* hebben we natuurlijk al te maken gehad met het vervallen van *Safe Harbour*. Verder was doorgifte van persoonsgegevens buiten de EU natuurlijk ook al een thema in privacywetgeving voordat de AVG van kracht werd. Hierdoor hadden we al ervaring met dit soort zaken, wat ons heeft geholpen op het moment dat de privacy shield kwam te vervallen. Zo waren we bijvoorbeeld in staat om het bereik van de "EU standard contractual clauses (SCC's)" – één van de juridische instrumenten voor doorgifte – direct te vergroten. En hebben we inmiddels ook de nieuwste versie zoals gepubliceerd door de Europese Commissie geïmplementeerd. Het stellen van privacyvragen juichen wij ook toe, want de AVG gaat immers ook over het nemen van verantwoordelijkheid. We willen dat klanten begrijpen hoe wij omgaan met en ze helpen bij gegevensbescherming. Hier zitten altijd twee kanten aan: vanuit Microsoft hebben wij de verantwoordelijkheid om te helpen bij het beschermen van gegevens en het waarborgen van privacy, maar ook de klant heeft een keuze over hoe zij zaken inrichten. Hier moeten we altijd over in gesprek blijven, want hoe doe je dit nou het beste?

Amerikaans recht en de opsporings- en inlichtingendiensten

Klanten uit Nederland en Europa maakten zich altijd al zorgen om het zomaar vorderen van gegevens door een Amerikaanse opsporings- of inlichtingendienst. Dit is niet pas na het wegvallen van het *Privacy Shield* ontstaan. Wij begrijpen dat een opsporingsdienst gegevens zou moeten kunnen vorderen, maar zijn wel van mening dat dit proportioneel en noodzakelijk moet zijn, en dat dit niet zomaar moet mogen of kunnen. We zien wel een groot verschil tussen het opvragen van gegevens van consumenten of consumentendiensten versus zakelijke clouddienstverlening. Onze klanten zijn over het algemeen zakelijke ondernemingen of overheidsinstanties en volgens het Amerikaanse beleid wordt er dan in veel mindere mate een beroep gedaan op de cloudprovider. Opsporingsdiensten kunnen immers het verzoek neerleggen bij die organisatie, eventueel via een rechtshulpverzoek, en niet zonder meer bij Microsoft. Het aantal verzoeken – zeker extraterritoriaal (gegevens opgeslagen buiten Amerika) – dat wel direct bij ons terechtkomt is daarom minimaal, deze cijfers publiceren we ook om klanten gerust te stellen en transparant te zijn. We bekijken iedere aanvraag individueel. Door middel van versleuteling verzetten we ons tegen ongevraagde toegang en daarmee proberen we af te dwingen dat Microsoft kan bemiddelen. Op het moment dat we een vordering krijgen van gegevens, werken we nooit zomaar mee. We zetten direct een proces in werking waarbij we controleren of een vordering rechtsgeldig is. Op het moment dat de vordering rechtsgeldig, proportioneel en specifiek is zullen wij de vordering direct doorverwijzen naar de desbetreffende klant, zodat zij deze kunnen afhandelen. Wij ontlenen immers geen rechten aan de gegevens van klanten.

Op het moment dat we een vordering krijgen van gegevens, werken we nooit zomaar mee.

Mochten we om wat voor reden dan ook toch worden gedwongen om mee te werken, dan zullen we met alle mogelijkheden die we hebben proberen om het toch te kunnen melden. Op het moment dat er een mogelijk conflict is tussen Europees en Amerikaans recht, zullen we als de wet ons dat toestaat direct naar de rechter gaan – omdat wij vinden dat wij niet de keuze kunnen maken tussen de twee rechtssystemen. Dit hebben we ook contractueel laten opnemen in onze *defend your data clausules*. Dit is in lijn met de EDPB guidelines (European Data Protection Board). Mocht Microsoft ondanks de extreem kleine kans toch moeten meewerken aan een vordering, dan biedt Microsoft nog mogelijkheden om een eventueel benadeelde betrokkene financieel schadeloos te stellen. Ook dit is contractueel vastgelegd. Verder zijn we veel bezig met verschillende vormen van versleuteling en hebben wij in ons contract vastgelegd dat we nooit encryptiesleutels zullen delen. Naast dit alles focussen we ons erg op transparantie, het zoveel mogelijk opslaan en verwerken van gegevens in Europa, data-flow's inzichtelijk maken, en vooral het gesprek aangaan over de risico's van en kansen op een vordering. Deze zijn namelijk extreem klein. Microsoft heeft een aantal rechtszaken tegen de Amerikaanse overheid gewonnen, waardoor wij nu meer mogen publiceren over de frequentie van vorderingen en de verschillende categorieën waar vorderingen onder vallen.

Maar ben je nou eigenlijk niet compliant als er iets van persoonsgegevens naar Amerika gaan? Wij denken dat gegevensdoorgifte mogelijk is, mits je daar de juiste waarborgen en maatregelen tegenover zet. Dat doen wij en daarom denken wij dat onze diensten op een compliant-wijze ingezet kunnen worden Maar het blijft belangrijk dat er vanuit geo-politiek nieuwe afspraken gemaakt worden, waarmee dit goed en duidelijker wordt geregeld. We doen ons best om overheden te bewegen om hier vorderingen in te maken.

Samenwerking met Microsoft veel werk?

De thematiek leidt tot een hoge informatiebehoefte en in de praktijk is het lastig om alle klanten te woord te staan. Daarbij hebben grote organisaties met een eigen juridische en technische afdeling het een stuk eenvoudiger dan kleine organisaties die daar de mogelijkheden en financiën niet toe hebben. Wat we gelukkig wel zien is dat grote organisaties communiceren of publiceren over het traject en dat kleine organisaties daarop kunnen meeliften. Uiteindelijk heeft iedere organisatie zijn eigen verantwoordelijkheid om zaken goed door te nemen, maar het kan natuurlijk helpen als al het voorwerk al is gedaan. Vanuit Microsoft proberen we de trajecten ook te versoepelen door verschillende model templates aan te bieden die organisaties dan alleen nog maar hoeven aan te vullen met hun eigen gegevens. Feit blijft dat je uiteindelijk altijd zelf begrip moet hebben van de materie en er zelf doorheen moet lopen, en dat kan een uitdaging zijn. Stel daarom altijd de volgende belangrijke vragen als je in zee gaat met een clouddienstprovider: ben ik in control over mijn gegevens? Waar staat mijn data? Beschermt de cloudprovider de gegevens? Welke extra maatregelen zijn er genomen om mijn data te beschermen? Stel die vragen, leg dat vast en start daar.

Toezichthouders

Naast alle gesprekken met klanten voeren we ook gesprekken met toezichthouders, soms op uitnodiging en soms naar aanleiding van een onderzoek. De relaties met toezichthouders verschillen heel erg. Zo hebben we met de een alleen contact tijdens het uitvoeren van een onderzoek en hebben we met de ander regelmatig contact over de ontwikkelingen in beide vakgebieden om zo van elkaar te leren. Het delen van ontwikkelingen vinden wij erg belangrijk. Een goed begrip van clouddiensten, de operatie daarvan en de continue ontwikkelingen kan complex zijn. Voor mij is het ook al een hele uitdaging om bij te blijven. Daarom denk ik dat wij en toezichthouders beiden hulp nodig hebben. De technische industrie moet niet de functie van wet- en regelgeving overnemen, maar we moeten wel informeren over de uitwerking, mogelijkheden en kanttekeningen ervan. Wij kunnen leren van toezichthouders wat de beperkingen zijn en hoe het juridisch systeem in elkaar zit. Andersom kunnen wij meer duiding geven aan en inzicht geven over de mogelijkheden en onmogelijkheden van technologie. Door het gesprek met elkaar aan te gaan hebben we al grote stappen gezet. Zo hebben we naar aanleiding van de Windows10-casus en het gesprek met de Autoriteit Persoonsgegevens (AP) de technologie aangepast, waardoor er nu meer privacy maatregelen in Windows 10 zitten evenals een viewer waarmee iedereen kan zien welke gegevens worden gedeeld met Microsoft. Dit is een continu leerproces en daar geloven wij ook in. Onze producten en diensten zijn compliant in te zetten, maar tegelijkertijd weten we ook dat er nieuwe interpretaties zullen volgen en er nieuwe ontwikkelingen zullen zijn waardoor we nieuwe aanpassingen zullen moeten doen. Elkaar blijven voeden met informatie en van elkaar leren is dan ook ontzettend belangrijk. Dit geldt niet alleen voor ons en toezichthouders, maar ook voor organisaties. Zoek elkaar op. Leer van elkaar. Verbind en ga samen het gesprek aan met ons. Maak gebruik van alle concrete handvatten die wij bieden: assessments, whitepapers, publicaties. En neem ook altijd je eigen verantwoordelijkheid – daar gaat de AVG immers ook over.

Misvattingen Microsoft

Er bestaat nog wel eens een misvatting over de zakelijke clouddienstverlening die ik graag de wereld uit zou willen helpen: het idee dat Microsoft met het bieden van zakelijke clouddiensten gebaat is bij de inhoud van data van klanten en deze data bijvoorbeeld wil doorverkopen, of er advertentie-inkomsten mee genereren. Dit is absoluut niet het geval en dit past ook niet bij het model van een zakelijke clouddienstverlening. Klanten in hun rol als opdrachtgever (verwerkingsverantwoordelijke) betalen ons (als opdrachtnemer) voor het bieden van de functionaliteiten (het opslaan van documenten, database functionaliteiten, e-mail functionaliteiten, het gebruik van Teams etc.) en blijven in controle over hun gegevens. Gegevens van klanten worden gebruikt voor het bieden van die dienstverlening en het borgen van kwaliteit, beveiliging en performance, niet voor adverteren, profileren of marktonderzoek voor Microsofts belang.

Martin Vliem werkt als National Security Officer voor Microsoft. In die rol vertegenwoordigt hij Microsoft Nederland in relatie tot diverse publieke en private organisaties rond de thema's privacy, security en compliance. Belangrijke aandachtsgebieden betreffen de normering en wetgeving rondom gegevensbescherming en het ondersteunen van due-diligence trajecten bij de adoptie van cloud computing in gereguleerde sectoren (overheid, zorg, financiële sector). Martin heeft eerder gewerkt als managing consultant voor Capgemini en is zijn carrière begonnen als universitair docent, na afronding van zijn studie wijsbegeerte van wetenschap, technologie en samenleving aan de Universiteit Twente.

DE DIVERSE UITDAGINGEN VAN DATA-ETHIEK

Koen Versmissen

Volgens Klaus Schwab van het World Economic Forum (WEF) zitten we midden in een vierde industriële revolutie. Daarin is een centrale rol weggelegd voor kunstmatige intelligentie (AI) en robots. Die versmelten met allerlei andere disruptieve technieken tot een geheel nieuwe samenleving. Een ideaalbeeld voor sommigen, dat bij anderen juist dystopische gedachten oproept. Hoe dan ook: zelfs wanneer we het WEF niet helemaal vertrouwen – dat schijnt tegenwoordig sowieso in de mode te zijn – moge duidelijk zijn dat de sterke opkomst van datagedreven algoritmen zoals analytics, business intelligence, machine learning en AI, ingrijpende maatschappelijke veranderingen met zich meebrengt. En dat roept vragen op over hoe we daar op een verantwoorde manier mee kunnen omgaan.

Kijk bijvoorbeeld naar het regeerakkoord van afgelopen december: algoritmen gaan wettelijk gecontroleerd worden op transparantie, discriminatie en willekeur; er komt een algoritmetoezichthouder om dat in de gaten te houden; mensen krijgen regie over hun eigen data; er komen regels voor data-ethiek in de publieke sector; en in Europees verband gaat paal en perk gesteld worden aan de datamacht van grote tech- en platformbedrijven.[1]

Bedrijven en overheden zullen, voor zover ze dat nog niet zijn, flink aan de bak moeten op het gebied van data-ethiek. Maar wat is data-ethiek precies, en hoe pas je het in de praktijk toe? En wat is de verhouding met compliance? Dat zijn een paar van de vragen die ik in deze bijdrage probeer te beantwoorden.

Data-ethiek

We kennen natuurlijk allemaal de Algemene Verordening Gegevensbescherming (AVG). Je zou je kunnen afvragen of we daar eigenlijk niet genoeg aan hebben als het gaat om data-ethiek. Die bevat immers toch al allerlei regels over hoe je met persoonsgegevens moet omgaan? Is er dan wel meer nodig?

Het simpele antwoord is dat algoritmen die géén persoonsgegevens verwerken – en waar de AVG dus niet over gaat – ook tot ethische vragen kunnen leiden. Denk bijvoorbeeld aan de keuzes die een zelfrijdend voertuig voortdurend neemt, en die grote gevolgen kunnen hebben als er dingen fout gaan. Maar oké, veel datagedreven algoritmen maken natuurlijk wél intensief gebruik van persoonsgegevens. In theorie biedt de AVG tal van handvatten voor het stellen van de juiste ethische vragen daarover: noodzaak, proportionaliteit, subsidiariteit, belangenafwegingen, het staat er allemaal. Alleen: in de compliancepraktijk worden deze begrippen nog te vaak gezien als hoepeltjes waar je doorheen moet springen, in plaats van dat ze – zoals bedoeld – leiden tot het stellen van wezenlijke vragen over de gegevensverwerking en het zoeken naar goede antwoorden op die vragen. Daar komt bij dat die wezenlijke

1 Op 23 april kopte de NOS: 'Akkoord over strengere EU-regels voor internetbedrijven als Google en Meta' (www.nos.nl/artikel/2426164-akkoord-over-strengere-eu-regels-voor-internetbedrijven-als-google-en-meta).

vragen bij datagedreven algoritmen voor een deel van een andere aard zijn dan bij meer doorsnee verwerking van persoonsgegevens. De gemiddelde privacy officer zou er zomaar eens niet verdacht op kunnen zijn, of de gemiddelde proceseigenaar beschikt niet over de kennis, vaardigheden en tools om er een goed antwoord op te kunnen geven.

Er is dus meer nodig. En er is ook meer. Veel meer. De afgelopen, pak 'm beet, zes, zeven jaar heeft een enorme hoeveelheid frameworks en richtlijnen voor de goede omgang met datagedreven algoritmen en AI het licht gezien. Denk bijvoorbeeld aan de Ethische richtsnoeren voor betrouwbare kunstmatige intelligentie van de EU High Level Expert Group[2], de Richtlijnen voor het gebruik van algoritmen door overheden[3] en het Ethisch kader voor datagedreven besluitvorming van het Verbond van Verzekeraars[4]. Inmiddels bestaan er zelfs diverse overzichten van wat er allemaal aan frameworks 'op de markt is'.[5] Als je door de bomen het bos niet meer ziet, dan ben je zeker niet de enige. Gelukkig zijn de overeenkomsten tussen al die verschillende frameworks in de praktijk een stuk groter dan de verschillen. Wie er een aantal naast elkaar legt, kom eigenlijk telkens zo'n beetje dezelfde principes tegen, zoals transparantie, uitlegbaarheid, voorkomen van vooringenomenheid *(bias),* accountability, beveiliging, auditeerbaarheid, menselijke tussenkomst en monitoring van de effecten.

Is het dan een kwestie van een framework uitkiezen dat bij je organisatie past?[6] Helaas, zo simpel is het natuurlijk ook niet. En wel om verschillende redenen. Ik noem er hier drie, waar ik in het vervolg nader op inga. Allereerst moeten we ons niet blindstaren op big data: ook andere gegevensverwerking roept netelige data-ethische vragen op. Ten tweede, ik merkte het hierboven al op, is ethiek beoefenen echt iets anders dan in control raken en blijven op een verzameling beheersmaatregelen. En ten slotte is altijd nog de vraag hoe je op een effectieve manier met zoiets nieuws als data-ethiek aan de slag gaat in je organisatie.

Vier soorten data-ethische uitdagingen

Voor een onderzoek naar hoe uitvoeringsorganisaties bij de overheid omgaan met data-ethische vraagstukken, hebben wij die vraagstukken geïnventariseerd. Dit was de aanleiding om vier soorten gegevensverwerkende overheden te onderscheiden, die elk tegen hun eigen typen data-ethische vragen aanlopen. Veel hiervan geldt evenzeer voor het bedrijfsleven.

Een democratische rechtsstaat kan niet zonder bureaucratie, en bureaucratie op haar beurt kan niet zonder structurele gegevensverwerking. Met andere woorden: een democratische overheid is een *dataOverheid*. Gebruikt zij informatiesystemen voor het verwerken van die data, dan spreken we van de *eOverheid*. Ligt de nadruk niet op individuele toepassingen, maar op de verwevenheid en onderlinge afhankelijkheid van gegevensverwerkingen van diverse instanties, dan kunnen we in navolging van de WRR[7] spreken over een *iOverheid*. Wordt ten slotte de stap gezet van deterministische algoritmen die werken met records van (relatief) bescheiden omvang, naar statistische algoritmen die op big data worden losgelaten, dan hebben we te maken met de *aiOverheid*.

Ik gaf hiervoor al een lijstje van typische ethische thema's van de aiOverheid. Maar we moeten oppassen dat we niet denken dat we er daarmee zijn! Springen we even helemaal terug naar de dataOverheid, dan zien we daar al de nodige ethische dilemma's. Niet allemaal datagerelateerd, overigens, maar wel van belang voor hoe je met data omgaat. Hoe vul je waarden concreet in en weeg je ze tegen elkaar af? Iemand die niet doet wat je van hem verwacht: wil die niet, of kan die niet? En wat als de wet de menselijke maat in de weg staat? Meer datagerelateerde vragen zijn hoe je omgaat met mensen die niet in het systeem passen, en met 'administratieve uitsluiting': bureaucratische processen die toegang waar mensen wel recht op hebben in de praktijk moeilijk of onmogelijk maken.

Kijken we vervolgens naar de eOverheid, dan gaan we van 'niet in het systeem passen' naar 'niet in het informatiesysteem passen', en dat heeft vaak nog vervelendere gevolgen.
En automatisering betekent ook minder mogelijkheden voor maatwerk. Bedenk ook dat niet iedereen even digivaardig is, en dat mensen sowieso maar een beperkt 'doenvermogen' hebben. Hoe ga je daar goed mee om?

---

2 Zie www.op.europa.eu/nl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1.

3 Zie www.rijksoverheid.nl/documenten/richtlijnen/2021/09/24/richtlijnen-voor-het-toepassen-van-algoritmen-door-overheden-en-publieksvoorlichting-over-data-analyses.

4 Zie www.verzekeraars.nl/branche/zelfreguleringsoverzicht-digiwijzer/ethisch-kader-datatoepassingen.

5 Zie www.dataethiek.info/zoeken-onderwerp/frameworks.

6 C.q. het framework hanteren dat in je sector verplicht is, iets dat steeds vaker aan de orde zal zijn.

7 Wetenschappelijke Raad voor het Regeringsbeleid. Rapport iOverheid. Zie www.wrr.nl/publicaties/rapporten/2011/03/15/ioverheid.

De vernetwerkte iOverheid levert voor wie er problemen mee ondervindt vooral kafkaëske toestanden op. Zelfs als er niets fout gaat, is het allemaal moeilijk te overzien en te volgen. Gebeurt er iets onverwachts, kom er dan maar eens achter wat er precies aan de hand is, en of je actie moet ondernemen. Er kunnen ook zaken wijzigen zonder dat je daarover geïnformeerd wordt, en mede daarom kan het zo goed als onmogelijk blijken om te achterhalen waar een fout zit. Correctie en herstel zijn vaak moeilijk of zelfs onmogelijk: het systeem wordt eerder geloofd dan jijzelf, en het terugdraaien van een onterecht (want op onjuiste gegevens gebaseerd) besluit stuit op allerlei juridische complicaties. En lukt het wel om zaken opgelost te krijgen: hoe weet je dan wanneer je klaar bent? Vergeten we ten slotte ook niet het *chilling effect* van dit alles: mensen gaan zich gemakkelijk terughoudender gedragen, 'geen gekke dingen doen'.

Ook iOverheidsinstanties zelf hebben vaak geen overzicht, en het is in veel gevallen onduidelijk wie er verantwoordelijk is voor de juistheid van gegevens. En over die juistheid gesproken: door gegevensdeling komen gegevens in een andere context terecht, waar er zomaar een onjuiste betekenis aan kan worden toegekend. Een laatste dilemma is de vraag: wel of niet delen? Want gegevens delen kan op onder meer privacybezwaren stuiten, maar kan mensen vaak ook enorm helpen.

Ter afsluiting van deze paragraaf herhaal ik nog maar eens: het ging hierboven specifiek over de overheid, maar veel van deze zaken zijn in de context van het bedrijfsleven net zo relevant.

Ethiek

De termen 'ethisch' en 'ethiek' zijn hierboven al verschillende keren gevallen. Maar wat bedoelen we daar eigenlijk mee? En wat heb je er precies aan? Kunnen we de genoemde problemen en uitdagingen niet met onze standaard beheers- en compliance-aanpakken tackelen? Ik denk het niet. Als je het mij vraagt is ethiek steeds meer onontbeerlijk voor organisaties die over een lange termijn succesvol willen zijn en blijven. Het kan je in ieder geval veel brengen.

Ethiek biedt houvast bij het beantwoorden van vragen die dieper gaan dan de vraag wat er wettelijk gezien mag. Bij wet- en regelgeving is het streven om eenduidige regels vast te stellen, die consequent worden toegepast. Dat zorgt ervoor, zo is het idee, dat onze rechten als burgers in een maatschappij worden gewaarborgd. Helaas is de praktijk vaak weerbarstiger. Vaak zijn situaties zo complex en genuanceerd dat het niet

Ethiek biedt houvast bij het beantwoorden van vragen die dieper gaan dan de vraag wat er wettelijk gezien mag.

meteen duidelijk is wat het juiste is om te doen. Omdat de wet daar geen uitsluitsel over geeft, of omdat de wet soms niet overeenkomt met wat ons in een specifieke situatie voorkomt als het juiste om te doen (daar heb je 'm weer: de menselijke maat). Bij de kafkaëske toestanden van de iOverheid die ik signaleerde speelt nog iets anders. We zijn het vaak voor een groot deel met elkaar eens dat sommige zaken niet werken zoals ze zouden moeten, ook als we naar onze eigen organisatie kijken. Maar door de onderlinge afhankelijkheden voelen we ons niet in staat om daar effectief verandering in te brengen. Wat je dan vaak ziet is dat de handen vertwijfeld in de lucht worden gegooid, of dat de kop in het zand gaat. Maar we zijn het aan mensen en aan de maatschappij verplicht om het niet daarbij te laten. In al deze situaties kan ethiek ons helpen om een goed perspectief op de problematiek te krijgen.

Om de kansen van digitale ontwikkelingen te kunnen blijven benutten, moeten er beslissingen worden genomen die impact hebben op mensen en hun waarden. Daarbij gaat het niet zozeer om de vraag of je een bepaalde technologie al dan niet inzet, maar om de vraag hoe je deze technologie op een verantwoorde manier implementeert in een bepaalde context, zodanig dat deze bijdraagt aan wat men een waardevol leven acht.

En dat is uiteindelijk waar ethiek over gaat: de vraag stellen hoe we met elkaar de samenleving willen inrichten. Vaak roept dat vragen op over de betekenis van fundamentele concepten, zoals rechtvaardigheid, autonomie, vrijheid en verantwoordelijkheid. In hoeverre is een arts verantwoordelijk voor schade die hij of zij berokkent aan een patiënt als gevolg van het over-

nemen van een verkeerde diagnose van een medisch algoritme? Betekent respect voor autonomie dat je mensen maximale controle moet geven over de inrichting van hun leven, zoals regie over hun eigen persoonsgegevens, of juist dat je ze bepaalde beslissingen uit handen neemt? Heeft het gebruik van surveillancecamera's impact op de vrijheid van mensen?

Ethiek biedt een oriëntatiekader en maakt conceptuele onderscheidingen om houvast te bieden bij morele dilemma's, juist daar waar je in de wet- en regelgeving geen antwoord kunt vinden. Dat wil niet zeggen dat er absolute antwoorden in de ethiek bestaan. Eerder het tegendeel. Maar ze maakt het wel gemakkelijker om met elkaar het gesprek aan te gaan over wat wenselijk is. Ethiek laat de nuance toe die nodig is om rekening te kunnen houden met verschillen tussen mensen, culturen en situaties. In een snel veranderende maatschappij, betekent dit dat je nooit klaar bent met ethiek bedrijven.

Bij het verkennen van een ethisch dilemma kunnen verschillende argumenten naar voren komen. Een intuïtief aansprekend argument is dat die keuze het beste is die tot de best mogelijke resultaten leidt. Toch is dit maar een van de criteria waarop je een ethisch dilemma kunt beoordelen. Om de verschillende soorten criteria te kunnen onderscheiden en hun sterktes en zwakheden te kunnen blootleggen, worden vaak de drie grootste ethische stromingen geraadpleegd: consequentialisme, deontologie en deugdethiek.

Het *consequentialisme* stemt overeen met het zojuist genoemde argument. Het legt de nadruk op de gevolgen van een keuze of handeling. De juiste keuze is dan de keuze die de best mogelijke resultaten oplevert, in termen van bijvoorbeeld geluk, winst of efficiëntie, onafhankelijk van bedoelingen of principes.

De *deontologie* legt juist de nadruk op fundamentele principes en morele plichten die we hebben. In sommige situaties wordt het van belang geacht om te voldoen aan een bepaald principe, ook als dat minder goede resultaten oplevert. Zo werken sommige systemen efficiënter wanneer hun algoritmen mensen mogen onderscheiden op basis van etnische achtergrond. Als samenleving hebben we echter besloten tot het non-discriminatiebeginsel. Dat mag niet zomaar geschonden mag worden, ook niet als dat meer winst of efficiëntie oplevert.

De *deugdethiek*, ten slotte, kijkt niet zozeer naar de keuze op zich, maar naar de manier waarop de samenleving er als geheel uit dient te zien, en heeft aandacht voor de vraag wat voor interacties en houdingen tussen mensen we wenselijk vinden. Deze manier van denken stelt ons in staat om nieuwe technologische toepassingen in een breder kader te zien. Het is dan niet de vraag of de technologie al dan niet toegepast mag worden, maar eerder hoe de technologie op zo een manier kan worden geïmplementeerd dat deze bijdraagt aan wat als waardevol wordt gezien.

Ethiek is dus zeker niet objectief, maar evenmin is het volledig subjectief. Het biedt een kader voor het gesprek dat we moeten voeren om met elkaar tot overeenstemming te komen. De drie stromingen maken inzichtelijk welke argumenten er naar voren te brengen zijn in een ethisch debat. Ze verwoorden elk een kern van onze morele intuïtie. Ook al staan ze vaak met elkaar op gespannen voet, toch maken ze een vruchtbaar gesprek gemakkelijker, omdat ze een helder kader bieden waarbinnen discussies over ethische zaken gevoerd kunnen worden. Ethiek helpt ons bij het komen tot een gefundeerd oordeel en is een middel voor het verbeteren en het waarborgen van het morele karakter van een gesprek over strijdige of onduidelijke morele kwesties. Op die manier biedt het ons een kompas dat helpt om onze koers te kiezen en vast te houden in een snel veranderende, onzekere, complexe en ambigue wereld.

Ethiek in actie

Ethiek kent dus een andere insteek dan wet- en regelgeving en compliance – al zie je gelukkig wel dat ze voorzichtig naar elkaar toe aan het groeien zijn. Je zou wet- en regelgeving kunnen zien als "gestolde ethiek", maar het moge inmiddels duidelijk zijn dat gestolde ethiek geen ethiek is. Ethiek gaat over dialoog, over het gesprek voeren met elkaar, over lastige vragen stellen en accepteren dat er niet altijd duidelijke antwoorden zijn. Niet zelden zijn we na een ethisch gesprek, zoals Earl C. Kelley het zo mooi formuleerde, 'as confused as ever, but on a higher level and about more important things'. Nog anders gezegd: ethiek moet schuren.

Hoe voer je dan zo'n ethische dialoog? Daarvoor komen er gelukkig steeds meer hulpmiddelen in omloop.[8] Ik bespreek er kort drie die zich specifiek richten op de ethiek van digitalisering: de aanpak begeleidingsethiek, de ethische data assistent, en het moreel beraad.

8 Zie www.dataethiek.info/zoeken-onderwerp/tools.

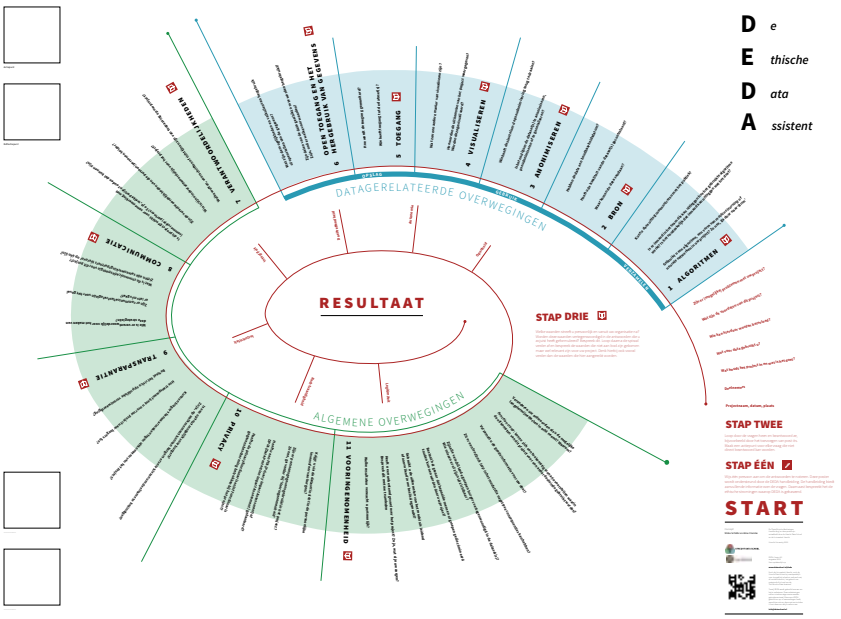
Figuur 1: Aanpak begeleidingsethiek

Aanpak begeleidingsethiek

De aanpak Begeleidingsethiek[9] is ontwikkeld door ECP, in samenwerking met hoogleraar ethiek Peter-Paul Verbeek. De aanpak ziet ethiek niet als beoordelaar, maar als ethische begeleider van de introductie van technologie in de samenleving. Na het beschrijven van de feiten volgt een dialoog over de betrokken actoren, de effecten van de voorgenomen inzet van de technologie, en de waarden die daarbij in het geding zijn. Dit leidt tot concrete handelingsopties op de gebieden technologie, omgeving en gebruik.

Ethische Data Assisten

De Ethische Data Assistent[11] is ontworpen door de Utrecht Data School, en erg populair in overheidskringen. Kern van de methode is een grote poster die teams kunnen gebruiken om op een gestructureerde wijze in gesprek te gaan over de verschillende ethische kwesties die kunnen ontstaan in de verschillende fasen van een dataproject. De thema's zijn: algoritmen, bron, anonimiseren, visualiseren, toegang, open toegang en het hergebruik van gegevens, verantwoordelijkheden, communicatie, transparantie, privacy en voor-ingenomenheid.



Figuur 2: De Ethische Data Assistent[10]

9 Zie www.ecp.nl/project/aanpak-begeleidingsethiek.

10 *Bekijk de volledige afbeelding op www.dataschool.nl/wp-content/uploads/sites/272/2019/10/DEDA_3_0.pdf.*

11 Zie www.dataschool.nl/deda.

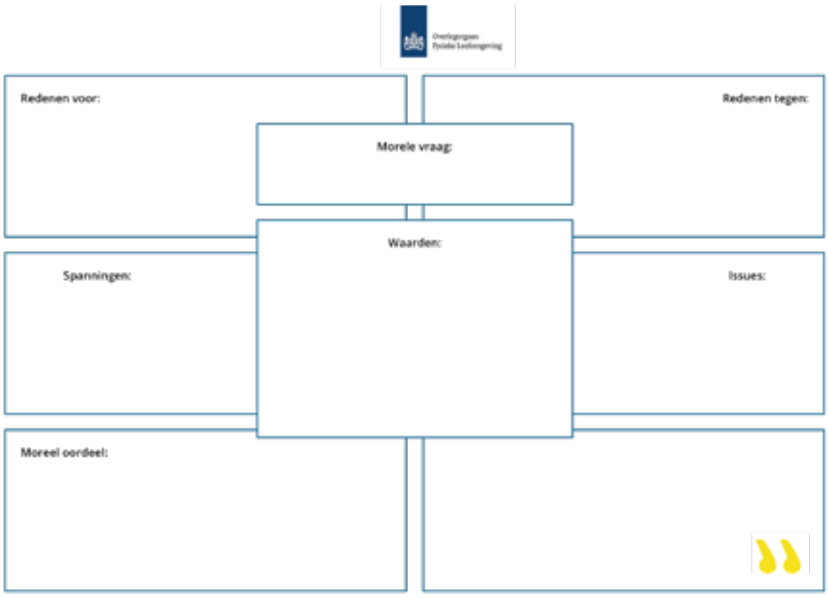
Moreel beraad

Het Moreel Beraad[12], tot slot, is een aanpak voor ethische dialoog die is ontwikkeld door het Overlegorgaan voor de Fysieke Leefomgeving. Deze bestaat uit een stappenplan gecentreerd om een canvas dat een morele vraag centraal stelt, de redenen voor en tegen in kaart helpt brengen, evenals de spanningen, waarden en issues, om tot slot te komen tot een moreel oordeel.

Ethiek in de organisatie

Ter afsluiting wil ik kort wat zeggen over de ethiek in de organisatie. Want als je overtuigd bent dat ethiek je meerwaarde kan bieden, hoe geef je daar dan in de praktijk handen en voeten aan? De VNG heeft hierover onlangs een mooie handreiking voor gemeenten gepubliceerd.[13] Bij het CIP (Centrum voor Informatiebeveiliging en Privacy) vind je verschillende podcasts en opnamen van webinars die op deze vraag ingaan.[14] Hier wil ik vooral nog even kort stilstaan bij de aanpak die Charles Radclyffe en Richard Nodell propageren in hun artikel 'Ethical by design'.[15] Zij bespreken verschillende mogelijke aanpakken van ethiekmanagement, en vullen dat aan met een volwassenheidsmodel. Daarin onderscheiden ze zeven aspecten waaraan je de volwassenheid van een organisatie op data-ethiekgebied kunt herkennen: diversiteit, integratie in ontwerpprocessen, de 'sophistication' van de ethische dialoog, het intern aanmoedigen van het aankaarten van ethische kwesties, training en bewustwording, het betrekken van belanghebbenden en het bieden van daadwerkelijke transparantie. Ze geven voor elk aspect ook een voorbeeld hoe dat concreet ingevuld kan zijn op een bepaald niveau van volwassenheid. Dat biedt mooie aanknopingspunten om stap voor stap data-ethiek in de organisatie te laten landen.

Koen Versmissen is eigenaar van Goedzo data-ethiek, initiatiefnemer van www.dataethiek.info. Hij heeft ruim twintig jaar ervaring op privacygebied, onder andere bij de Autoriteit Persoonsgegevens en als consultant en trainer. De laatste jaren gaat zijn interesse vooral uit naar data-ethiek: hoe gaan we goed om met datagedreven algoritmes? En vooral: hoe voeren we op een goede manier het gesprek over de dilemma's die we op dat gebied tegenkomen?



Figuur 3: Moreel Beraad

12 Zie www.overlegorgaanfysiekeleefomgeving.nl/publicaties/1962327.aspx.

13 Zie www.vng.nl/publicaties/handreiking-digitale-ethiek.

14 Zie www.cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/ethiek-awareness-en-meer.

15 Zie www.osf.io/gj2kf.

ALS JE HET NIET EENVOUDIG KUNT UITLEGGEN, SNAP JE HET ZELF NIET

DE AVG EN HET MOETEN UITLEGGEN VAN ONDERLIGGENDE LOGICA BIJ AUTOMATISCHE BESLUITVORMING

Hans Kooij

In Europa wordt druk onderhandeld over de Artificial Intelligence (AI) Act.[1] Diverse Nederlandse en Europese toezichthouders zoals De Autoriteit Financiële Markten (AFM), De Nederlandsche Bank (DNB) en de Autoriteit Persoonsgegevens hebben zich reeds uitgelaten over de inzet van kunstmatige intelligentie in opinie papers of in speerpunten voor hun toezicht de afgelopen en komende jaren. Binnen ondernemingen wordt AI en daarmee automatische besluitvorming in toenemende mate onderdeel van de bedrijfsvoering. Dat brengt kansen en risico's met zich mee. In dit artikel behandelt Hans Kooij, Compliance Expert bij Achmea, de reikwijdte van de AVG-verplichting om onderliggende logica uit te leggen van volledig geautomatiseerde besluitvorming als dat grote impact kan hebben op iemand.

Het verbod op volledig geautomatiseerde besluitvorming met grote impact op een betrokkene

In artikel 22 van de Algemene verordening gegevensbescherming (AVG) is het recht opgenomen om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (waaronder profilering) gebaseerd besluit waaraan rechtsgevolgen zijn verbonden of die de betrokkene anderszins in aanmerkelijke mate treft.

In hetzelfde artikel worden ook de uitzonderingen benoemd wanneer de betrokkene dit recht niet heeft. De uitzonderingen zijn kort gezegd:

a. Noodzakelijk voor aangaan of uitvoering van een overeenkomst met de betrokkene;
b. Toegestaan bij wet;
c. Uitdrukkelijke toestemming.[2]

Artikel 22 AVG is geformuleerd als een recht voor de betrokkene. Net als een beroep op het recht op inzage kan gesteld worden dat de betrokkene dit recht actief moet inroepen. De verwerkingsverantwoordelijke moet vervolgens binnen een maand laten weten wat er met dat verzoek wordt gedaan.[3] De Europese toezichthouders interpreteren artikel 22 evenwel als een verbod.[4] Ook de Nederlandse regering gaat daarvan uit.[5] Uiteindelijk zal rechtspraak hier duidelijkheid over moeten geven. Gezien de grote belangen voor de praktijk zijn procedures te verwachten als Europese privacytoezichthouders hierop gaan handhaven. Ook omdat zij suggereren dat het niet enkel

1 Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence, COM/2021/206 final.

2 Deze uitzonderingen van artikel 22 lid 2 corresponderen met artikel 6 lid 1 sub b en c en artikel 9 lid 2 sub a AVG.

3 In artikel 12 lid 3 AVG wordt immers verwezen naar artikel 22 AVG en uit de formulering hiervan blijkt niet dat het (enkel) gaat om de extra waarborgen die de verwerkingsverantwoordelijke conform artikel 22 lid 3 AVG moet treffen.

4 GROEP GEGEVENSBESCHERMING ARTIKEL 29, 17/NL, WP251rev.01, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, Vastgesteld op 3 oktober 2017 Zoals laatstelijk gewijzigd en vastgesteld op 6 februari 2018, hoofdstuk IV.

5 Memorie van toelichting Uitvoeringswet Algemene verordening gegevensbescherming, pag. 38.

gaat om de gevolgen van een besluit om te bepalen of iemand zwaar wordt getroffen, maar ook de verwerking zelf al iemand zwaar kan treffen. Een verregaande manier van profileren qua omvang en diepgang zou dan iemand zwaar treffen als een automatisch besluit daarop wordt gebaseerd ook al heeft dat besluit op zichzelf geen grote gevolgen (een voorbeeld van *behavioural advertising* wordt benoemd).[6] Een dergelijke verwerking zou dan enkel op grond van een van eerder in dit artikel genoemde uitzonderingen van artikel 22 AVG zijn toegestaan en niet op grond van bijvoorbeeld het gerechtvaardigd belang dat een onderneming heeft bij het uitvoeren van marketing.[7] Het interpreteren van artikel 22 AVG als verbod heeft ook invloed op de informatieplicht richting betrokkene(n).[8] In dit artikel wordt gezien de gezaghebbende mening van de toezichthouders (zogenoemde *soft law*) en de interpretatie van de Nederlandse wetgever evenwel verder uitgegaan van een 'verbod tenzij'.

Om het verbod opzij te kunnen zetten zal een onderneming de verwerking zo moeten inrichten dat een van de uitzonderingen van toepassing is. De AVG stelt dan een aantal aanvullende eisen. Het recht op menselijke tussenkomst moet worden geborgd en daarnaast moet de betrokkene zijn standpunt kenbaar kunnen maken en heeft hij het recht het besluit aan te vechten.[9] Om dat te kunnen doen moet de betrokkene snappen dat er een automatische beslissing over hem wordt genomen die grote impact kan hebben.

Informeren over onderliggende logica, belang en verwachten gevolgen

Wil de betrokkene zinvol zijn rechten kunnen uitoefenen, dan moet hij ervan op de hoogte zijn dat automatische besluitvorming plaatsvindt en kunnen snappen op basis van welke logica het besluit is genomen. De AVG kent daarom een specifieke invulling van het transparantiebeginsel. Als een onderneming gebruik maakt van geautomatiseerde besluitvorming in de zin van artikel 22 AVG dan moet in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal informatie worden gegeven over de onderliggende logica, alsmede het belang en de verwachte gevolgen voor de betrokkene.[10] Op welk moment moet een verwerkingsverantwoordelijke onderneming dit doen en hoever strekt deze verplichting?

6 17/NL, WP251rev.01, hoofdstuk IV, B.

7 Conform artikel 6 lid 1 sub f AVG.

8 Bijvoorbeeld ten aanzien van de wijze van het formuleren van toestemming. Toestemming conform art. 6 lid 1 sub a AVG is dan niet mogelijk, het moet uitdrukkelijke toestemming zijn conform artikel 9 lid 2 sub a AVG.

9 Artikel 22 lid 3 AVG.

10 Artikel 12 lid 1 AVG jo. artikel 13 lid 2 sub f en 14 lid sub g AVG.

Het tijdstip van informeren en daarmee de (relevante) informatie die gegeven kan worden

De AVG stelt regels over het tijdig op de hoogte stellen van de betrokkene. Artikel 13 AVG gaat ervan uit dat de betrokkene voorafgaand aan een verwerking en uiterlijk 'bij de verkrijging van de persoonsgegevens' geïnformeerd wordt. In artikel 14 AVG wordt die verplichting herhaald, maar het tijdstip van informeren ligt hier – omdat gegevens niet rechtstreeks van de betrokkene worden verkregen – binnen een redelijke termijn, maar uiterlijk binnen één maand, na de verkrijging ervan. Als persoonsgegevens evenwel voor een ander doel zijn verzameld maar daarna verder worden verwerkt, dan moet vóór die verdere verwerking informatie over dat andere doel en alle relevante aanvullende informatie gegeven worden. Bij automatische besluitvorming in de zin van artikel 22 AVG zal de betrokkene dus vrijwel altijd vooraf geïnformeerd moeten worden.

Dit onderscheid tussen vooraf of achteraf moeten informeren is belangrijk voor de praktijk. De inhoud van de informatie die gegeven kan worden, verschilt dan namelijk wezenlijk. Vooraf kan enkel algemene logica over het toegepaste model verstrekt worden. Zoals de categorieën persoonsgegevens die worden meegenomen bij de geautomatiseerde besluitvorming en de belangrijkste drivers van het betreffende model waarmee het automatische besluit wordt genomen.

Als na een genomen besluit de betrokkene geïnformeerd moet worden over de in zijn geval exact toepaste onderliggende logica, zou dat veel verder gaan. Hoewel het, afhankelijk van het besluit, klantvriendelijk kan zijn om een dergelijke uitleg te geven, is een dergelijke verplichting niet ondubbelzinnig opgenomen in de AVG. In de overwegingen bij de AVG is wel opgenomen "(…) het recht op menselijke tussenkomst, om zijn standpunt kenbaar te maken, om uitleg over de na een dergelijke beoordeling genomen besluit te krijgen (…)" hetgeen lijkt te zien op uitleg over de beslissing die na menselijke tussenkomst wordt genomen.[11] Ik lees daarin geen plicht om uitleg te geven over de onderliggende toegepaste logica in het individuele geval.[12]

> Uiteindelijk is een goed begrip van de betrokkene over wat er met zijn gegevens gebeurt en hoe ze verwerkt worden het belangrijkst.

Kan een betrokkene dan niet achteraf via het recht op inzage alsnog informatie krijgen over de in zijn geval toegepaste onderliggende logica? Het recht van inzage heeft het bij automatische besluitvorming ook over nuttige informatie over de onderliggende logica en de verwachte gevolgen.[13] 'Verwachte gevolgen' veronderstelt dat deze nog niet zijn ingetreden. De Rechtspraak in Nederland geeft een soortgelijk beeld. De Rechtbank Amsterdam overweegt dat bij automatische besluitvorming in de zin van artikel 22 AVG de belangrijkste beoordelingscriteria aan de betrokkene moeten worden gegeven zodat hij kan begrijpen op grond van welke criteria het besluit is genomen en daarmee in staat wordt gesteld de juistheid en rechtmatigheid van de gegevensverwerking te controleren.[14]

Daarbij mag, na een evenwichtige belangenafweging, ook rekening worden gehouden met de rechten of vrijheden van anderen zoals het zakengeheim of de intellectuele eigendom en met name aan het auteursrecht dat de software beschermt.[15] Een geruststelling voor bedrijven die bang zijn voor hun intellectuele eigendom, bedrijfsgeheimen of voor *gaming the system* waarbij betrokkenen met kennis van de geautomatiseerde besluitvorming het besluit proberen te beïnvloeden in hun voordeel.

---

11 Overweging 71 AVG.

12 Het Europees parlement heeft in de onderhandelingen een veprlichting voorgesteld, in lijn met overweging 71, maar die is uiteindelijk niet letterlijk in artikel 22 overgenomen. Zie European Parliament Committee on Civil Liberties, Justice and Home Affairs, *Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) - A7-0402/2013* (European Parliament 2013) A7–0402/2013, Amendment 115 lid 5. www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN.

13 Artikel 15 lid 1 sub h AVG.

14 R.o. 4.41, www.uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019.

15 Overweging 63 AVG.

Informeren over de onderliggende logica bij automatische besluitvorming in de zin van artikel 22 AVG richting de betrokkene betreft mijn inziens de belangrijkste drivers van een model.

Onderliggende logica in gemakkelijk toegankelijke vorm en duidelijke en eenvoudige taal

Aan de manier waarop de betrokkene vooraf moet worden meegenomen in de belangrijkste onderliggende logica van de automatische besluitvorming stelt de AVG een aantal eisen. De informatie moet worden gegeven in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal.[16] Een extensieve uitleg van beslisbomen voldoet typisch niet aan deze voorwaarden. Inzichten uit de gedragswetenschappen tonen aan dat mensen beperkt rationeel handelen en niet alle informatie die zij krijgen gebruiken in hun besluitvorming.[17] Meer uitleg en meer informatie betekent niet dat betrokkenen de geautomatiseerde besluitvorming beter zullen bevatten.[18]

Wat kan helpen is visualisatie. Zoals het weergeven van zogenaamde 'maatmannen' waarbij de kenmerken van die maatmannen verschillen en daarmee de uitkomsten van de automatische besluitvorming. Bij interactieve visualisatie kan een betrokkene zelf variabelen veranderen en de potentiële gevolgen op de besluitvorming inzichtelijk krijgen. Bijvoorbeeld door bij een autoverzekering die gebaseerd is op het rijgedrag de gemiddelde of snelle rijder i.c.m. de regio te visualiseren om het effect op de premie van de autoverzekering weer te geven. Ook het meenemen van de beoogde doelgroep is hierin belangrijk. Vraag de doelgroep om zijn of haar mening en toets of deze de automatische besluitvorming snapt dan wel hoe hierover het beste uitleg gegeven kan worden.[19]

Uiteindelijk is een goed begrip van de betrokkene over wat er met zijn gegevens gebeurt en hoe die verwerkt worden het belangrijkst. Alleen dan kan de betrokkene ook effectief ingrijpen en bij de verwerkingsverantwoordelijke aangeven dat bepaalde conclusies in zijn geval niet kloppen of persoonsgegevens onjuist zijn.

16 Artikel 12 AVG.

17 Kahneman, D. (2003), *Maps of bounded rationality: Psychology for behavioral economics*, American Economic Review, 93, 1449–1475.

18 Dietram A Scheufele, *Messages and Heuristics: How audiences form attitudes about emerging technologies*, in Engaging Science: thoughts, deeds, analysis and action, gepubliceerd op 22 juni 2009.

19 In lijn met art. 35 lid 9 AVG.

Een beperkte(re) externe uitleg neemt niet weg dat intern de beheersing op orde moet zijn

Binnen een onderneming moet (het gebruik van) een algoritme waarop de automatische besluitvorming berust verantwoord en, waar nodig, getoetst kunnen worden. De kerngedachte achter artikel 22 AVG is namelijk dat iemand niet de negatieve kenmerken van een bepaalde groep krijgt tegengeworpen terwijl hij of zij deze kenmerken helemaal niet hoeft te hebben.[20] In de toelichting bij de Wet bescherming persoonsgegevens werd voorheen de 'menselijke waardigheid' benoemd.[21] Een onderneming die automatische besluitvorming toepast die iemand zwaar treft doet dus verstandig aan een beheerste en integere bedrijfsvoering. Daarbij horen passende wiskundige en statistische procedures en een proces van interne *checks and balances*, om verantwoord de automatische besluitvorming toe te passen en verantwoording af te kunnen leggen.[22] Niet in de laatste plaats moet een onderneming de eigen automatische besluitvorming kunnen doorgronden om daarover een zinvolle uitleg aan betrokkenen te kunnen geven. Om die reden tot slot een citaat dat wordt toegeschreven aan Albert Einstein en een herhaling van de titel van dit artikel: **"Als je het niet eenvoudig kunt uitleggen, snap je het zelf niet."**

Hans Kooij is Compliance Expert bij het Competence Center van Achmea Compliance. Naast Privacy houdt hij zich bezig met PARP, Uitbesteding en Data Ethics. Hans studeerde Management, Economie en Rechten aan het Windesheim te Zwolle en Rechten in Groningen.

20 Memorie van toelichting Uitvoeringswet Algemene verordening gegevensbescherming, pag. 38.

21 Memorie van toelichting 25 892 Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) bij artikel 42 van voorheen de Wet bescherming persoonsgegevens.

22 Conform artikel 5 lid 2 AVG moet de verwerkingsverantwoordelijke kunnen aantonen aan de principes van artikel 5 lid 1 AVG te voldoen. De passende wiskundige en statistische procedures worden benoemd in overweging 71 AVG. De privacytoezichthouder van België heeft hiervoor bijvoorbeeld diverse tips gegeven. Commissie voor de bescherming van de persoonlijke levenssfeer, *Big Data Rapport AH-2016-0154*, www.privacycommission.be/publications/big-data-rapport.pdf.

ALLEEN EEN ÉCHTE DPIA TELT
BASISBEGINSELEN, PRAKTIJKTIPS EN BELANG VAN EEN DPIA

Francis Joung en Sander van de Molen

In dit artikel beschrijven we een aantal belangrijke elementen uit de theorie en het juridisch kader over DPIA's. Ook geven we een aantal tips over hoe een DPIA in de praktijk uit te voeren. Daarvoor putten we uit het door ons geschreven Handboek DPIA's[1] en uit de cursussen die we al enige tijd hierover geven. Verder lichten we toe waarom DPIA's steeds belangrijker worden.

THEORIE: Wat is een DPIA?

Een data protection impact assessment (DPIA)[2] is een instrument om privacyrisico's van een gegevensverwerking in kaart te brengen, zodat een organisatie passende maatregelen kan nemen om de risico's te verkleinen.

Waarom zijn DPIA's belangrijk?

DPIA's zijn belangrijk voor een organisatie:

a. Om het benodigde inzicht in verwerkingen te verkrijgen. Om de privacybelangen van betrokkenen[3] (b.v. haar klanten, cliënten, patiënten, burgers, leerlingen, medewerkers etc.) te kunnen beschermen, moet zij inzicht[4] hebben in de (privacy)risico's van haar dataverwerkende processen.
b. Om aan te kunnen tonen dat voor privacyrisico's in processen passende beheersmaatregelen zijn genomen.
c. Omdat deze op grond van de AVG verplicht zijn bij processen met hoge privacyrisico's voor betrokkenen.

Wie is verantwoordelijk voor de uitvoering?

Een veel voorkomende misvatting is dat de FG verantwoordelijk is voor het uitvoeren van een DPIA. Dat is niet het geval. Het uitvoeren van een DPIA is de verantwoordelijkheid van de verwerkingsverantwoordelijke (artikel 35, lid 2 AVG). De DPIA kan door iemand anders worden uitgevoerd, maar de verwerkingsverantwoordelijke blijft daarvoor eindverantwoordelijk.

Op welk tijdstip moeten ze worden uitgevoerd?

Art. 35 lid 1 AVG is duidelijk: 'vóór de verwerking'.[5] Dit is ook in lijn met de door de AVG voorgeschreven aanpak van *Privacy by Design* en *Privacy by Default*.[6] Het idee van toch maar alvast starten met een verwerking en daarna een DPIA uitvoeren gaat in tegen de AVG en maakt een organisatie kwetsbaar voor acties vanuit de Autoriteit Persoonsgegevens (AP) en claims van betrokkenen. Een organisatie is namelijk verplicht bij hoog risico privacy verwerkingen voor de start van de verwerking de risico's voor betrokkenen voldoende te mitigeren met beheersmaatregelen.

Een andere breed levende misvatting is dat bij pilots en bij experimenten waarbij wel persoonsgegevens worden verwerkt geen DPIA's nodig zijn, omdat je dan nog niet in productie bent. Dat is onjuist, want zodra er sprake is van verwerking van (echte) persoonsgegevens met een hoog risico is een DPIA verplicht.

---

1 Francis Joung en Sander van de Molen, *Handboek DPIA's*, Berghauser Pont, 2020. Zie: www.privacyteam.nl/dpia/bestellen/handboek-dpia-s.

2 Zie ook de richtsnoeren van de WP29 WP 248 van 4 april 2017 (en laatstelijk gewijzigd en vastgesteld op 4 oktober 2017), pagina 4: 'Een gegevensbeschermingseffectbeoordeling is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken'.

3 Maar ook om haar eigen organisatiebelangen te waarborgen (denk aan reputatieschade, aantasting van haar relaties met partners door privacy-inbreuken).

4 Dit inzicht krijg je alleen door een inventarisatie en risicoanalyse van die processen.

5 Zie ook de overwegingen 90 en 93 van de AVG.

6 De beginselen van gegevensbescherming van privacy door ontwerp en door standaardinstellingen (zie artikel 25 en overweging 78 van de AVG).

Wanneer is een DPIA verplicht?

Een DPIA is verplicht bij nieuwe of te wijzigen verwerkingen die een hoog risico inhouden voor de betrokkenen. Dit bepaal je door een verwerking achtereenvolgens te toetsen aan:

1. De tekst van artikel 35 lid 3 AVG.[7]
2. De lijst van de AP van soorten verwerkingen waarvoor een DPIA verplicht is.[8]
3. De negen criteria van de WP29[9] in de WP 29 Richtlijnen voor DPIA's.[10]
4. Indien slechts één van de criteria uit stap 3 aan de orde is moet je zelfstandig beoordelen of er toch dusdanige risico's zijn dat een DPIA nodig is.[11]

Wanneer een verwerking voldoet aan een van deze vier punten is een DPIA verplicht.

Alleen een échte DPIA telt!

Let overigens goed op. Alleen een goed en compleet uitgevoerde DPIA is een échte DPIA. Indien een organisatie geen DPIA uitvoert of deze niet compleet en juist is uitgevoerd, dan loopt de organisatie een risico op een (standaard) boete van € 310.000.[12] Nog belangrijker dan het risico van de boete is natuurlijk dat een organisatie zonder deugdelijk uitgevoerde DPIA geen zicht heeft op de privacyrisico's en benodigde beheersmaatregelen voor die verwerking, hetgeen tot grote privacyrisico's voor betrokkenen kan leiden.

Zonder een deugdelijk uitgevoerde DPIA heeft een organisatie, bij een hoogrisicoverwerking, geen zicht op de privacy-risico's en benodigde beheersmaatregelen voor de verwerking van persoonsgegevens.

---

7 Dat geeft aan dat een DPIA verplicht is bij:
- een systematische en uitgebreide beoordeling van persoonlijke aspecten gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die gevolgen hebben voor mensen;
- een grootschalige verwerking van bijzondere of strafrechtelijke gegevens;
- stelselmatige en grootschalige monitoring van een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

8 Op grond van artikel 35 lid 4 AVG heeft de AP een lijst opgesteld van soorten verwerkingen waarvoor een DPIA verplicht is. Zie: www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf. Het gaat hier meestal om grootschalige en/of stelselmatige verwerkingen.

9 Artikel 29 Werkgroep. Deze werkgroep bestaat uit de privacy toezichthouders van de EU-landen (waaronder de AP). Zij hebben een groot aantal richtlijnen en aanbevelingen gepubliceerd om een uniforme interpretatie en toepassing van de privacywetgeving (Richtlijn 95/46/EG, de voorganger van de AVG) te bevorderen. Zij is met de komst van de EDPB opgeheven.

10 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, die zijn vastgesteld door WP29 en geaccordeerd door EDPB. Bij twee hits op deze criteria is een DPIA verplicht.

11 Dit is aangegeven in WP 29 Richtlijnen voor DPIA's p. 13.

12 Zie hiervoor de boetebeleidsregels van de Autoriteit Persoonsgegevens: www.autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties.

PRAKTIJK: Stappen om rekening mee te houden bij het uitvoeren van een DPIA

Op basis van onze ervaring met DPIA's zijn wij van mening dat de volgende stappen nodig zijn voor een succesvolle uitvoering van een DPIA.

Stap 1: Opdracht van de directie/management

Het verkrijgen van draagvlak bij de directie/het management is een belangrijke randvoorwaarde. Zij stellen de benodigde middelen (budget en mankracht) ter beschikking. Ook zullen zij aan de organisatie duidelijk moeten maken dat meewerken aan de DPIA belangrijk is en prioriteit heeft. Zonder deze opdracht is het praktisch zeer lastig een DPIA uit te voeren, omdat medewerkers de noodzaak er niet van inzien en daardoor zelfs mogelijk niet willen meewerken.

Stap 2: Maak een plan van aanpak

Na het verkrijgen van de opdracht werk je in een plan van aanpak de volgende elementen verder uit:

- Een beschrijving van de (nieuwe of te wijzigen) verwerking
- De te doorlopen stappen bij de uitvoering
- De benodigde disciplines/soorten medewerkers
- De activiteiten die zij gaan uitvoeren
- Een inschatting van de te reserveren tijd voor die medewerkers
- Een tijdplanning
- Het benodigde budget

Stap 3: De scope van de DPIA

Maak concreet welk deel van het verwerkingsproces onder de loep wordt genomen. Bijvoorbeeld: Vanaf welke bronsystemen zijn welke databases, hardware en servers in scope, tot en met welke output naar welke processen, systemen, zowel intern of extern.

Een duidelijke scope is essentieel om een DPIA effectief te kunnen uitvoeren. Een onduidelijke scope kan leiden tot veel misverstanden en extra werk.

Stap 4: De stappen bij de uitvoering van de DPIA

Het is belangrijk om een DPIA volgens een vaste structuur uit te voeren en daarbij alle benodigde stappen te doorlopen. Een goed DPIA-model[13] mét toelichting helpt daarbij. Alleen zo voer je een juiste en volledige DPIA uit.

Bij de uitvoering maak je de volgende stappen:

- Een analyse van het juridisch kader, inclusief sectorspecifieke regels
- Het zo nodig op basis van eisen uit het juridisch kader aanvullen van de vragenlijst van het DPIA-model
- Het zoveel mogelijk vooraf invullen van de vragen van het DPIA-model
- Het houden van een workshop met stakeholders/kenners proces
- De analyse van antwoorden en documentatie
- Het verder invullen van het DPIA-model en het opstellen van een concept DPIA-rapport
- De review van het concept rapport
- Vragen van advies van de FG
- Maken van het definitieve DPIA-rapport

Stap 5: De benodigde disciplines

Breng in beeld welke disciplines en medewerkers daadwerkelijk de benodigde inhoudelijke (detail) kennis van het te onderzoeken proces hebben. Bij een nieuw op te zetten proces betreft dit medewerkers en managers die duidelijk voor ogen hebben hoe dat nieuwe proces eruit zou moeten gaan zien (doel, benodigde persoonsgegevens, applicaties, afdelingen etc.). Bij een bestaand proces gaat het om medewerkers die exact weten welke soorten data en persoonsgegevens, op welke wijze, met welke programmatuur/software, draaiend op welke hardware, waar, voor welk doel, door welke afdelingen worden verwerkt. Denk hierbij ook aan procesarchitecten, business consultants, security specialisten, ICT'ers, (product)juristen en compliance officers.

Stap 6: Betrekken en inzetten medewerkers bij de uitvoering

Het is belangrijk om medewerkers vooraf goed te informeren over hun rol in de DPIA en wat er van hen gevraagd wordt. Betrek medewerkers bijvoorbeeld bij de DPIA door een workshop te organiseren. Denk eraan om voorafgaand aan een DPIA workshop de deelnemers goed te informeren over bijvoorbeeld de informatiebeveiliging of om ze alvast samen met een inhoudsdeskundige al zoveel mogelijk te laten invullen van een deel van het DPIA-model, zoals bijvoorbeeld het eerste onderdeel van een DPIA, de beschrijving van de gegevensverwerking.[14]

Stap 7: Tijdplanning

Werk uit wie, wanneer, welke acties gaat uitvoeren en wie, wanneer, welk product oplevert, bijvoorbeeld welke vragen de DPIA uitwerkt. Deze planning dient uiteraard tijdig met alle betrokkenen te worden gedeeld, zodat zij weten wat er wanneer van hen wordt verwacht.

13 Het Handboek DPIA's bevat een aantal praktische modellen met een uitgebreide toelichting, zodat je niets mist.

14 Dan kan daarop worden voortgeborduurd in de workshop en kun je met de deelnemers in de workshop werkafspraken maken over wie welk deel van de DPIA verder gaat uitwerken.

Stap 8: Benodigd budget
Maak een concrete begroting, zodat helder is voor het management welke kosten voor de DPIA moeten worden gemaakt (specificeer zowel de interne als externe kosten).

Stap 9: Wie voert het uit?
Om te voorkomen dat belangrijke privacyrisico's worden gemist dienen DPIA's in onze visie, zeker bij complexere processen met mogelijk hogere risico's, te worden begeleid door een privacy specialist of een team met voldoende specialistische (DPIA) kennis en ervaring. Deze specialist(en) moet(en) beschikken over:

- diepgaande kennis van de AVG en de overige op het te onderzoeken proces toepasselijke privacyregels;
- diepgaande kennis van organisatie en processen (waarom zo ingericht/doen we dingen zo);
- ervaring met privacymanagement-inrichtingseisen;
- communicatief sterk zowel naar business/medewerkers als naar management;
- ervaring in multidisciplinair werken;
- ervaring met het uitvoeren van DPIA's.

Denkbaar is bijvoorbeeld dat een privacy coördinator van een klein ziekenhuis die voor de eerste keer een DPIA moet uitvoeren steun zoekt bij ervaren collega's van een groter ziekenhuis in de regio. In bepaalde sectoren steunen netwerken van privacy specialisten/FG's elkaar met kennis en voorbeelden. Het is aan te bevelen dat de meer met DPIA's ervaren privacy-specialisten hun minder ervaren collega's ondersteunen door hen tips te geven over hoe deze goed uit te voeren en geanoniseerde voorbeelden te delen van goed uitgevoerde DPIA's.

Een andere optie is om hiervoor een externe DPIA-specialist in te schakelen die twee of drie DPIA's uitvoert in nauwe samenwerking met de interne medewerkers (bijvoorbeeld privacy coördinatoren) die beoogd zijn om zich als DPIA-specialist van de organisatie te gaan ontwikkelen, zodat zij hierna hierna zelfstandig DPIA's kunnen gaan uitvoeren.

Bij complexe DPIA's is het aan te bevelen om een projectleider aan te stellen.

BELANG: Waarom worden DPIA's steeds belangrijker?

Er is sinds de invoering van de AVG, alweer vier jaar geleden, onder het grote publiek een groeiende belangstelling voor en bewustzijn over privacy en de risico's en rechten die daaruit voortvloeien. Mensen moeten erop kunnen vertrouwen dat hun persoonsgegevens met respect worden behandeld. Als organisaties dit niet (aantoonbaar) doen, dan verliezen ze het vertrouwen van het publiek.

We maken mee dat betrokkenen zelf om DPIA's over bepaalde verwerkingen vragen aan organisaties, denk van een burger aan een gemeente. De Autoriteit Persoonsgegevens is sinds een jaar ook veel actiever gaan handhaven en vraagt bij onderzoeken die zij uitvoert (denk aan het onderzoek over Smart-cities[15]) ook steeds vaker DPIA's op bij organisaties om hun compliance te kunnen beoordelen. Kortom, het is belangrijk om als organisaties ook je DPIA's op orde te hebben. We hopen je met ons artikel een aantal handvatten te geven.

Mr. J.F.A. (Francis) Joung CIPP/E is van huis uit jurist en was van 2002 tot 2016 werkzaam in verschillende rollen als privacy specialist in de financiële sector, onder meer als bedrijfsjurist, functionaris gegevensbescherming, compliance officer en privacy officer. Hij adviseert privacy consultant cliënten in diverse branches, om hun organisatie en processen privacy compliant te maken, maar ook praktisch en werkbaar te houden. Van de (risico-)analyse, het opstellen van beleid en procedures tot en met de implementatie daarvan.

Mr. A.C.M. (Sander) van de Molen CIPP/E is jurist en privacy professional, en mede-eigenaar van PrivacyPeople en Privacy-Team. Hij heeft veel ervaring op het gebied van compliance en privacy. Hij is voor verschillende partijen werkzaam als FG, voert audits en nulmetingen uit en ondersteunt klanten met DPIA's. Eén van zijn specialiteiten is het aantoonbaar maken van naleving van wet- en regelgeving, onder andere d.m.v. EasyPrivacy®, software om privacy als proces te borgen en de naleving te monitoren en aantoonbaar te maken.

▶ *Francis Joung en Sander van de Molen*
Handboek DPIA's
ISBN 9789492952424

15 www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoeksrapport_smart_cities_def.pdf

PETER VAN DEN BOSCH:

"TOEZICHTHOUDER MOET DIALOOG AANGAAN"

In 2020 kreeg Bureau Krediet Registratie (BKR) een boete opgelegd door de Autoriteit Persoonsgegevens (AP). Aanleiding was een onderzoek naar de werkwijze bij inzage van persoonsgegevens. Eenmaal per jaar hadden mensen recht op een gratis overzicht van hun kredietregistratie. Voor extra inzages vroeg BKR eerst een kleine bijdrage. Dat zou in strijd zijn met de AVG. Hoe heeft BKR deze sanctie ervaren? Welke lessen zijn er geleerd? Bestuursvoorzitter Peter van den Bosch blikt terug.

'Sinds 2009 ben ik bestuursvoorzitter van BKR. Daarvoor heb ik altijd bestuurlijke functies bij banken gehad. Ik ben ooit begonnen als managementtrainee. In die periode moest ik ook hypotheekadvisering doen. Veel mensen kochten in die tijd een woning die nog gebouwd moest worden. Daardoor hadden ze vaak twee hypotheken. Eind jaren zeventig brak de crisis uit. De korte rente ging naar twaalf procent, de inflatie sloeg toe en de woningmarkt zakte finaal in. Niemand kon die dubbele lasten nog betalen. Ik was alleen maar mensen aan het helpen met problemen als gevolg van kredietverstrekking.

Die ervaring heeft m'n verdere loopbaan bepaald. Ik heb altijd gevonden dat kredietverstrekking belangrijk is, omdat het economische ontwikkeling mogelijke maakt. Maar er zit ook een keerzijde aan. Mensen kunnen erdoor in de problemen komen.

BKR is een onafhankelijke stichting zonder winstoogmerk. Op ons hoofdkantoor in Tiel werken 130 mensen. We willen zoveel mogelijk Nederlanders met een gezond financieel huishouden en zo weinig mogelijk mensen met problematische schulden. We doen dat door kredietverstrekkers informatie te geven over het verleden van consumenten. Dat gebeurt tijdens het proces van kredietverstrekking.

Iedere kredietverstrekker is wettelijk verplicht om bij ons informatie aan te leveren over verstrekte kredieten en achterstanden. Daarnaast moet hij ook gegevens bij BKR opvragen op het moment dat een consument een krediet aanvraagt. De bank beslist uiteindelijk of eventuele problemen dusdanig zijn opgelost dat er weer nieuw krediet verstrekt kan worden.

Daarnaast doen we aan vroegsignalering. Dat is een essentiële, maatschappelijke rol. Energiebedrijven, ziektekostenverzekeraars en woningcorporaties geven ons signalen als er achterstanden zijn. Die geven wij dan weer door aan gemeenten. Zij kunnen dan contact met mensen leggen. Gemeenten zijn dat verplicht in het kader van de Wet Gemeentelijke Schuldhulpverlening (WGS).

BKR is ook marktleider in identiteitsverificatie. Als je bij een bank of notaris komt, moet je je legitimeren. Vervolgens wordt je identiteit gecheckt via BKR. Hiervoor hebben we connecties met de KLPD (vreemdelingendocumenten), de RDW (rijbewijzen) en de RvIG (paspoorten). Verder beheren we de fraude-registers van de banken.

Veranderingen door de AVG

BKR is altijd voorloper geweest op het gebied van privacy. We hebben een database met gevoelige, financiële informatie van zo'n twaalf miljoen mensen. Dat vraagt om de hoogste standaarden. Als een van de weinige organisaties in Nederland hebben we lang een privacy certificering gehad. We voldeden aan de oude normering. Toen de AVG in 2018 z'n intrede deed, is deze komen te vervallen.

Zodra het nieuwe normenkader definitief is, zullen we weer opgaan voor certificering. In de praktijk houden we ons uiteraard volledig aan de normen die nu worden gehanteerd.

BKR is nauw betrokken geweest bij de totstandkoming van de AVG. Zowel in Nederland als in Europees verband. We voelden allemaal wel dat er iets moest veranderen. Als financiële info bij datahandelaren terechtkomt en wordt doorverkocht, dan gebeuren er onwenselijke dingen. Er was geen zicht op, er waren geen restricties.

Veel mensen weten niet dat Europese wetgeving, door de wijze waarop deze tot stand komt, één groot compromis is. Daar waar de conceptwet misschien iets te streng was, gingen de scherpe kantjes eraf. Regels werden principes. Dat geeft meer ruimte voor interpretatie, maar zorgt ook voor meer onduidelijkheid.

Er zijn drie belangrijke zaken veranderd ten opzichte van vóór 2018. Bedrijven moeten een aantoonbare reden hebben waarom ze informatie verzamelen en vervolgens aangeven wat ze ermee doen. Bijvoorbeeld de afsluiting van een verzekeringsovereenkomst of de oplegging van een verkeersboete. De consument moet in beginsel toestemming geven om bepaalde info te mogen gebruiken. Dat is allemaal veel explicieter geworden. Daarnaast heeft de consument recht op inzage in de gegevens die worden gebruikt.

Omdat we er vooraf al intensief mee bezig waren, hebben zich weinig grote dilemma's voorgedaan bij implementatie van de AVG. We hebben vergelijkbare bedrijven in andere landen bezocht en uitgewisseld binnen de branchevereniging ACCIS. Er zijn privacy assessments opgesteld voor alle processen die met privacy te maken hadden, er is een functionaris gegevensbescherming aangesteld en er is advies ingewonnen bij externe juristen.

Dat is *ongoing business*. Je moet immers blijvend voldoen aan de AVG. Net als banken gebruikt BKR *privacy by design*. Zodra er iets verandert in producten of processen, wordt er opnieuw zo'n privacy assessment gedaan. Om te kijken of de zaken na de verandering nog steeds voldoen aan de privacyregels.

Als bestuursvoorzitter heb ik veel inhoudelijke kennis opgebouwd op dit gebied. Heb je dat niet, laat dan regelmatig een externe meekijken of je processen nog steeds op orde zijn. Een certificering kan hierbij helpen.

Onderzoek Autoriteit Persoonsgegevens

In 2018 startte de Autoriteit Persoonsgegevens (AP) een onderzoek bij BKR. Achteraf bleken vier klachten rond het inzagerecht de aanleiding te zijn. De teneur hiervan was dat inzage in de kredietregistratie altijd gratis zou moeten zijn, ongeacht hoe vaak iemand informatie wil opvragen.

Toen we begonnen met de implementatie van de AVG kon iemand eenmaal per jaar gratis een (papieren) kredietoverzicht krijgen. Je vulde een formulier in, deed een kopie van je paspoort erbij en binnen een week ontving je het via de post. Maar tijden veranderen. We wisten ook dat er consumenten waren die behoefte hadden aan een *fast track* en aanvullende dienstverlening. Die wilden vaker kijken hoe ze ervoor stonden, omdat ze bijvoorbeeld met een geschil zaten. Iedere dag bij wijze van spreken.

Omdat we dat als extra dienstverlening zagen, boven op de mogelijkheid voor een gratis inzage, hebben we een abonnement in het leven geroepen. Voor een kleine bijdrage van 4,95 euro per jaar konden mensen voortaan digitaal inzage krijgen. Onbeperkt. Alles voortdurend online klaarzetten was een dure methode, maar we vonden toch dat we die mogelijkheid moesten bieden. Het ging het om een kleine groep. Gingen we dat voor iedereen doen, dan zou het onbetaalbaar worden.

In de AVG stond ook dat de consument gratis inzagerecht heeft, maar niet continu. Artikel 63 geeft expliciet aan dat "drempels" geoorloofd zijn en spreekt over "redelijke tussenposen". Er moest dus een bepaalde periode tussen zitten. We hebben hierbij ook naar de Schufa gekeken, de Duitse BKR. Daar had de Privacy Autoriteit gezegd dat het redelijk is dat de consument maximaal één keer per jaar gratis inzage kan krijgen. Voor meerdere inzagen mocht een betaling worden gevraagd. Dat hebben wij overgenomen. Nog steeds is dat de huidige praktijk in Duitsland.

De AP kwam echter tot de conclusie dat ze het niet met ons eens waren. Ze vonden dat BKR onrechtmatig drempels opwierp. Inzage moest te allen tijde gratis zijn. Onbeperkt en voor alle consumenten. Daar zaten we behoorlijk mee in onze maag. Het aantal aanvragen was op dat moment 160.000 per jaar. Ons argument dat een consument gemiddeld maar eens in de 75 jaar inzage deed en we één keer per jaar redelijk vonden, vond geen gehoor.

Toch hebben we op dat moment besloten om het snel te gaan aanpassen en dan maar alles gratis aan te bieden. Dat hebben we ook aan het AP gemeld, want we wilden geen ruzie met een toezichthouder. Vervolgens hebben we een persbericht de wereld ingestuurd dat we de AP op bezoek hadden gehad, dat we heel zorgvuldig hadden getracht de wet te implementeren, dat de AP hier opmerkingen over had, dat we het hiermee oneens waren, kijk naar alle landen om ons heen, maar dat we wel de uitspraak van de AP gingen opvolgen. Door de inzage gratis aan te bieden, is het aantal inzages aanzienlijk gestegen. Inmiddels voorzien we jaarlijks in 1.600.000 verzoeken. Dat is gemiddeld eens in de 7,5 jaar.

Boete zonder waarschuwing

Tijdens het onderzoek ging de AP van alles opvragen. Ze legden niet uit waar ze mee bezig waren, we konden geen vragen stellen, ze wilden niet met ons praten. Ik heb zelfs brieven aan de voorzitter van de AP gestuurd om in gesprek te komen. Dat is categorisch geweigerd. We voelden ons totaal niet gehoord. Hun opstelling is dat je het maar met de uitspraak moet doen. Als je hen vraagt of je vooraf iets mag toetsen of het in lijn is met de wet, dan zeggen ze dat ze het daarvoor te druk hebben.

Nadat we dus alles conform de wens van de AP in 2019 hadden aangepast, kregen we als klap op de vuurpijl in 2020 een boete van 830.000 euro. BKR had drempels opgeworpen, terwijl we dat allang hadden aangepast! En dan te bedenken dat de vier

klachten van "pseudoklanten" waren. Er waren geen gedupeerden in het spel. Er waren geen gegevens weggeraakt, er was niks stiekem verkocht en iedereen die dat wilde had gewoon gratis inzage gehad.

We waren dus enorm verbaasd. We begrijpen er nog steeds niks van. Was dit nou een groot probleem in Nederland? Of wilde de AP hiermee een voorbeeld stellen? Laten zien dat ze een sterke waakhond is waarmee niet te sollen valt? Uiteraard zijn we tegen de boete in beroep gegaan. Dat loopt sinds 2020. We blijven het zeer onterecht vinden. Het is disproportioneel. Bovendien behandelde de AP ons anders dan andere bedrijven. Boetes worden vaak pas gegeven als bedrijven hun zaken niet snel genoeg aanpassen of als er gedupeerde consumenten in het spel zijn.

Ik heb nog nooit meegemaakt dat een toezichthouder geen dialoog aangaat. Dat mis ik volledig bij de AP. Waarom niet gewoon met mensen om de tafel? Dat kan een hoop rechtszaken voorkomen. Het onderzoek en de boete hebben ons het volgende geleerd. Je kunt het nog zo goed doen, je kunt denken dat je alles op orde hebt, maar het kan je toch opeens overkomen.

Met een wet die meer *principle* dan *rule based* is, weet je nooit of je het goed doet. Als de AP de principes vervolgens als regels invult, dan ben je kwetsbaar als organisatie. Geloof me, we hebben de film talloze malen teruggedraaid. Toch zouden we opnieuw dezelfde besluiten nemen.

Mijn tip is om bij iedere verandering voor goede assessments te zorgen. Twijfel je over zaken? Probeer dan vooraf in contact te komen met de toezichthouder. Lukt dat niet, raadpleeg dan goede juristen. Intern of extern.

Mocht de AP vinden dat je iets niet goed hebt gedaan, zet dan in op een dialoog voor verbetering. Ook al zeggen ze dat ze daar niet voor zijn ingericht. Partijen moeten de druk opvoeren dat ze advies en feedback nodig hebben. Het belang van privacy is groot.'

Peter W. van den Bosch MBA RB (1958) studeerde Bedrijfskunde aan de Rijksuniversiteit Groningen. Hij werkte in diverse bestuursfuncties bij onder meer Fortis Bank, Levob en Achmea, tot hij in 2009 benoemd werd tot bestuursvoorzitter van de Stichting Bureau Krediet Registratie (BKR) in Tiel.

Peter nam deel aan diverse branche-initiatieven. Zo was hij voorzitter van de Vereniging van Financieringsondernemingen (VFN), voorzitter van het Financierings Data Netwerk (FDN), bestuurslid van het Hypotheken Data Netwerk (HDN), lid van het platform Stichting Financiële Dienstverlening (StFD, voorloper van de AFM), lid van de Raad van Advies van de Nederlandse Vereniging voor Volkskrediet (NVVK) en vicepresident van de Association of Consumer Credit Information Suppliers (ACCIS) in Brussel.

Daarnaast was hij gastdocent aan de Technische Universiteit in Leiden en tevens lid van de adviesraad van Delft University Toptech Growing Adaptive. Voorts was hij vicevoorzitter van de Raad van Commissarissen bij woningcorporatie SCW in Tiel. Op dit moment vervult hij nog de volgende nevenfuncties: lid van de Raad van Toezicht bij het Nationaal Instituut voor Budgetvoorlichting (Nibud), vicevoorzitter van de Stichting Certificering voor Makelaars (SCVM) en bestuurslid bij het Tuchtcollege Makelaardij Nederland (TCMNL).

WAT WE KUNNEN LEREN VAN ANDERMANS 'FOUTEN'

Melissa Veen, Edwin van Tongerlo en Niels Arends

Met het rechtstreeks van toepassing worden van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 is de Autoriteit Persoonsgegevens (AP) aangewezen als toezichthouder op de AVG en de Uitvoeringswet AVG. Hiermee heeft zij de bevoegdheid gekregen om organisaties te sanctioneren wanneer zij de AVG overtreden. Een van de sanctiemogelijkheden die de AP hierbij heeft gekregen is het opleggen van een boete van maximaal 20 miljoen euro, of 4% van de wereldwijde jaaromzet van de organisatie.

Van die bevoegdheid heeft de AP sinds 2018 verschillende malen gebruik gemaakt. Het leek ons daarom voor deze editie van De Compliance Officer goed om te analyseren of er lessen getrokken kunnen worden uit de door de AP gepubliceerde boetebesluiten. Lessen waarmee we andere organisaties kunnen behoeden voor boetes van de AP, maar waar we met name ook kunnen bijdragen aan een betere bescherming van persoonsgegevens van burgers.

Analyse

Veel van de boetes die de AP oplegt hebben betrekking op de overtreding van artikel 32, 33 en/of 34 van de AVG. Artikelen vallend onder afdeling 2, Persoonsgegevensbeveiliging. Boetes als gevolg van onvoldoende beveiliging van persoonsgegevens en het niet of niet tijdig melden van datalekken aan de AP (en eventueel de betrokkenen). Wij hebben een selectie van deze boetebesluiten geanalyseerd. Eerst leggen we de focus op overtredingen van artikel 32 AVG gemaakt door medische instellingen; vervolgens hebben we een drietal boetes geanalyseerd waarbij artikel 33 en 34 zijn overtreden.

Overtredingen van art. 32, 1e lid AVG

Binnen de medische wereld worden met name veel bijzondere persoonsgegevens (artikel 9 AVG) verwerkt. Gegevens waarvoor geldt dat zij niet mogen worden verwerkt, tenzij er sprake is van een wettelijke uitzondering. Voor alle persoonsgegevens geldt dat zij passend beveiligd (artikel 32 AVG *"(…) een op het risico afgestemd beveiligingsniveau (…)"*) dienen te worden. Dat betekent dat de beveiligingsmaatregelen moeten zijn afgestemd op de risico's die de verwerking van de gegevens voor de betrokken personen met zich meebrengen.

Voor medische gegevens geldt dat de verwerking ervan een hoog risico met zich meebrengt. En dat dus het beveiligingsniveau hierop aangepast dient te zijn. Dat juist binnen de medische wereld – aan de 'grote' stichtingen HagaZiekenhuis en het Amsterdamse ziekenhuis OLVG en een kleine, niet bij naam genoemde, orthodontiepraktijk[1] - de laatste jaren boetes zijn opgelegd vanwege een overtreding van artikel 32 AVG, wekt dan ook verbazing.

In alle drie de gevallen was sprake van een overtreding van art. 32, 1e lid van de AVG. De AP is op grond van dit artikel van mening dat organisaties, hoe bescheiden ook, degelijke, proportionele beheersmaatregelen moeten inrichten op organisatorisch en technisch niveau om eventuele datalekken te voorkomen.

1 Boetebesluit AP betref. StichtingHagaZiekenhuis (2019): www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf; Boebesluit AP betref. StichtingOLVG (2020): www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf; Boebesluit AP betref. orthodontiepraktijk (2021): www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_orthodontiepraktijk.pdf

Maar wat bedoelt de AP met 'proportionele beheersmaatregelen'? In het geval van de orthodontiepraktijk was de oplossing gemakkelijk: zorg voor een website met een versleutelde verbinding. Het niet gebruik maken van een beveiligde websiteverbinding was niet proportioneel gezien de gevoelige aard van de gegevens die via de website verzonden konden worden, de stand van de huidige techniek en de beperkte kosten die het zorgdragen voor een versleutelde verbinding met zich meebrachten. Kortom: een overtreding van artikel 32 lid 1 AVG en een boete van €12.000.

Mogelijk interessanter is het oordeel van de AP in de boetebesluiten opgelegd aan het OLVG en het HagaZiekenhuis. Kort gezegd zijn in het geval van beide ziekenhuizen fouten geconstateerd bij de verwerking van gevoelige informatie, de toegang daartoe (authenticatie) en de monitoring van de toegang tot complexe informatiesystemen (monitoring van logging).

In geval van het HagaZiekenhuis kon personeel toegang krijgen tot persoonsgegevens door 'enkel' gebruik te maken van een gebruikersnaam en wachtwoord. Volgens de AP geeft dit onvoldoende waarborg tegen het lekken van persoonsgegevens en moet de beveiliging van gevoelige gegevens gelaagd worden ingericht. Met andere woorden: gebruikers horen buiten de hantering van een gebruikersnaam en wachtwoord ook gebruik te maken van een ander identificatiemiddel (2-factor-authentication).[2]

Eenzelfde oordeel velde de AP ten aanzien van het OLVG. Ook al stonden de fysieke informatiesystemen bij het OLVG binnen een beveiligde ruimte, de AP oordeelde dat alleen een gelaagde beveiliging van de informatiesystemen *zelf* proportioneel was.[3] Zodoende werd aangeraden dat gebruikers bij de toegang tot informatiesystemen, naast het invullen van een gebruikersnaam en wachtwoord, ook gebruik behoorden te maken van een aan het systeem te koppelen *token* of identificatiepas.[4] Een gelaagdheid van beveiliging die geldt voor zowel de toegang tot informatiesystemen op de werkvloer als daarbuiten (dus ook thuis).[5]

Opvallend is dat de AP niet expliciet de tijdelijke vergemakkelijking van toegang veroordeelt. Medewerkers van het HagaZiekenhuis waren namelijk niet genoodzaakt om herhaaldelijk in te loggen op informatiesystemen, maar konden gebruik maken van een zogenoemde *grace period*, een tijdspanne van vier uur waarbinnen de systeembeveiliging geen identificatie vereiste. Het HagaZiekenhuis gaf zelf aan dat het deze grace periods zou afschaffen, maar de AP deed hier verder geen uitspraak over.

De AP sprak beide ziekenhuizen ook aan op het onverantwoordelijk lage aantal periodieke checks, controles en steekproeven op de inzage van persoonsgegevens door medewerkers. Zo vonden er geen systematische controles op *logging* plaats en werd er net zomin aandacht gegeven aan systematische en/of automatische signalering bij overschrijding van bepaalde grenswaarden door bijvoorbeeld niet (direct) bevoegde medewerkers.[6] Ook ten aanzien van logging geldt volgens de AP echter het proportionaliteitsvereiste: hoe gevoeliger de gegevens, hoe meer aandacht er moet worden besteed aan het systematisch onderzoeken en beoordelen van gegevensinzage.

> Hoe gevoeliger de gegevens, hoe meer aandacht er moet worden besteed aan het onderzoeken en beoordelen van de gegevensinzage.

2 Boetebesluit AP betref. StichtingHagaZiekenhuis (2019) 12.

3 Boebesluit AP betref. StichtingOLVG (2020) 9.

4 Idem.

5 Idem, 7.

6 Boetebesluit AP betref. StichtingHagaZiekenhuis (2019) 13 – 16; Boebesluit AP betref. StichtingOLVG (2020) 9 – 13.

Let wel: De toepassing van proportionele beveiliging van persoonsgegevens *an sich* garandeert volgens de AP echter niet dat onbevoegde inzage wordt voorkomen.[7] Het is een belangrijke maatregel die bijdraagt aan het voorkomen van onbevoegde toegang, maar organisaties moeten nog steeds zelf toezicht houden/monitoren op de naleving van beveiligings- en privacy statuten en zorgen voor actueel beveiligingsbeleid en -maatregelen die voldoen aan de op dat moment geldende toepasselijke maatstaven. Ook het extern laten toetsen/auditen van het informatiebeveiligingsbeleid ontslaat de organisatie niet van die verantwoordelijkheid.

Overtredingen van artikel 33 en 34 AVG

De artikelen 33 en 34 zien op inbreuken in verband met persoonsgegevens met een risico voor de rechten en vrijheden van natuurlijke personen, oftewel: datalekken (artikel 33 lid 1 AVG). Aan elk datalek ligt een beveiligingsincident ten grondslag. Of dat nou het gevolg is van onvoldoende beveiliging van systemen of het versturen van (gevoelige en/of bijzondere) persoonsgegevens via een onbeveiligde e-mail. Dat betekent overigens uiteraard niet dat elk beveiligingsincident ook een datalek is.

In navolging van de analyse op boetebesluiten in het kader van onvoldoende beveiliging leek het ons daarom goed om te kijken of er mogelijk ook een rode draad te vinden is in de gepubliceerde boetebesluiten die toezien op overtreding van artikel 33 en 34 van de AVG. De artikelen die zien op de (meld)verplichtingen op het moment dat er sprake is van een datalek bij een organisatie.

Wij hebben hiervoor gekeken naar de boetebesluiten inzake de PVV Overijssel voor het niet melden van een datalek en die van Booking.com en Uber vanwege het te laat melden hiervan. De korte conclusie is dat de oorzaak van de datalekken en de manier waarop door de organisaties met de meldplicht is omgegaan zo verschillend is, dat er geen rode draad uit de boetebesluiten te destilleren is.

Desondanks zijn er wel een aantal aandachtspunten te benoemen met betrekking tot de meldplicht van datalekken, wanneer er zich onverhoopt een datalek bij een organisatie voordoet.

7 Boebesluit AP betref. StichtingOLVG (2020) 16.

1. Het is van belang voor de organisatie om goed in kaart te brengen en helder te hebben wie de verwerkingsverantwoordelijke is ten aanzien van de verwerking van de persoonsgegevens. Op de verwerkingsverantwoordelijke rusten immers de (meldings)verplichtingen uit de artikelen 33 en 34 AVG. Zeker in het geval van bijvoorbeeld moeder/dochterrelaties waartussen een verwerkersovereenkomst is gesloten zal niet altijd meteen duidelijk zijn waar de verwerkingsverantwoordelijkheid ligt. In het onderhavige geval kan er mogelijk zelfs sprake zijn van gezamenlijke verantwoordelijkheid.[8]
2. Indien er sprake is van gezamenlijke verantwoordelijkheid zijn beide organisaties zelfstandig verantwoordelijk voor het doen van de melding aan de AP.[9] Uiteraard hoeft een melding maar één keer gedaan te worden, maar men kan niet naar de ander wijzen op het moment dat er überhaupt geen melding is gedaan.
3. De AVG schrijft voor dat de verwerkingsverantwoordelijke uiterlijk 72 uur nadat hij kennis heeft genomen van het datalek een melding moet doen bij de AP. Het is daarom van belang om exact te weten op welk moment deze termijn in gaat. Uit het boetebesluit van Booking.com blijkt dat de 72-uurstermijn niet per se bij het allereerste signaal ingaat. Ondanks dat het niet expliciet is vermeld, lijkt het er in dit specifieke geval op dat de AP pas bij het tweede signaal is uitgegaan van een 'structureel' karakter en dat daarna pas de termijn is gaan lopen.[10] Dit kan echter ook het gevolg zijn geweest van de specifieke omstandigheden van het geval. Het lijkt derhalve niet raadzaam om dit als uitgangspunt te nemen.
4. De reeds genoemde 72-uurstermijn zie toe op het feit dat een organisatie enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. Wanneer echter na 72 uur nog geen duidelijkheid is verkregen over de exacte omstandigheden van de inbreuk, dient men melding te doen op basis van de reeds beschikbare gegevens. Deze melding kan bij het verkrijgen van de volledige informatie namelijk altijd nog worden aangevuld of ingetrokken.[11]
5. De AP kijkt tijdens een onderzoek in navolging van een datalekmelding niet alleen naar wat de AVG voorschrijft, maar ook naar het interne beleid inzake de afhandeling van datalekken en de daarbij behorende meldprocedure.[12]
6. Indien een datalek (waarschijnlijk) een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen en dus ook gemeld dient te worden aan de betrokkene, dan dienen alle betrokkenen op *individuele basis* geïnformeerd te worden. Er kan dan bijvoorbeeld niet worden volstaan met een nieuwsbericht op de organisatiewebsite.[13]
7. De beoordeling of een datalek mogelijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dient gemaakt te worden op het moment van het datalek. Dat kort na het ontstaan van het datalek de gevolgen van het risico nog niet zijn ingetreden is geen reden om geen melding te doen bij de AP.[14]

Hebben we iets geleerd?

Op basis van de analyse van de zes genoemde boetebesluiten kan geconcludeerd worden dat er meerdere oorzaken kunnen leiden tot een overtreding van eenzelfde artikel uit de AVG. Dat brengt helaas met zich mee dat specifieke lessen leren uit de overtredingen van deze organisaties moeilijk is. Veel is, zoals gebruikelijk in het juridische, afhankelijk van de omstandigheden van het geval.

Wel kunnen we de conclusie trekken dat het ten aanzien van artikel 32 lid 1 AVG met name gaat om proportionaliteit. De genomen beheersmaatregelen moeten proportioneel zijn ten aanzien van het risico dat een verwerking met zich meebrengt voor de rechten en vrijheden van natuurlijke personen. Wat proportioneel is, is dan onder meer afhankelijk van het type organisatie, van de stand van de techniek en van de persoonsgegevens die worden verwerkt. Autorisatie tot de betreffende informatie en de logging en monitoring van de daadwerkelijke toegang tot de persoonsgegevens wordt hierbij door de AP van groot belang geacht.

Voor wat betreft het melden van datalekken is er in het geheel geen gemene deler in de omstandigheden te vinden in de geanalyseerde boetebesluiten, anders dan dat er in alle drie de gevallen sprake was van een overtreding van de meldverplichting(en). Wel volgen uit deze besluiten een aantal aandachtspunten om in acht te nemen in de situatie dat er een datalek binnen de organisatie heeft plaatsgevonden. We hopen hiermee toch wat handvatten te hebben aangereikt in de uitdagingen waar de bescherming van persoonsgegevens mee gepaard gaan.

8 Boetebesluit AP betref. Uber (2018) 12.

9 Boetebesluit AP betref. Uber (2018) 6.

10 Boetebesluit AP betref. Booking.com (2021) 12 – 13.

11 Boetebesluit AP betref. Uber (2018) 12.

12 Boetebesluit Booking.com (2021) 12 – 13.

13 Boetebesluit betref. Uber (2018) 28.

14 Boetebesluit betref. Uber (2018) 30

HOE BEN IK IN CONTROL TEN AANZIEN VAN HET PRIVACY-RISICO?

Joost Damen

Op 25 mei 2018 was het na lang wachten toch zo ver. De invoering van de Algemene Verordening Gegevensbescherming (AVG) was definitief. Waar een deel van de AVG toch echt oude wijn in nieuwe zakken was[1], werden er met de invoering van de AVG ook een aantal grote veranderingen doorgevoerd. Een van die veranderingen was de introductie van de verantwoordingsplicht (artikel 5 lid 2 AVG). Wat houdt deze verantwoordingsplicht eigenlijk in, waarom is deze ingevoerd en op welke wijze kan de organisatie hieraan invulling geven? In deze bijdrage laat ik mijn licht schijnen op deze vragen en leg ik uit hoe TKP, als verwerker voor pensioenuitvoerders, handen en voeten geeft aan de verantwoordingsplicht.

Wat is de verantwoordingsplicht en waarom is deze ingevoerd?

De verantwoordingsplicht houdt (kort gezegd) in dat de verwerkingsverantwoordelijke moet kunnen aantonen dat de beginselen van de AVG worden nageleefd. De Europese wetgever maakt in overweging 11 van de AVG duidelijk waarom de verantwoordingsplicht is opgenomen. Zij geeft aan dat een doeltreffende bescherming van persoonsgegevens onder andere een versterking vereist van de verplichtingen van degenen die persoonsgegevens verwerken. Om die reden is de verantwoordingsplicht ingesteld. Met het opnemen van de verantwoordingsplicht in de AVG heeft de wetgever de bewijslast omgekeerd. Niet de toezichthouder moet bewijzen dat er sprake is van het *niet* voldoen aan de AVG, maar de organisatie moet aantonen dat wél wordt voldaan.

Vanuit intrinsiek oogpunt zie ik de verantwoordingsplicht als een hulpmiddel voor de organisatie om in control te zijn ten aanzien van de risico's van het niet voldoen aan de AVG. Door de verantwoordingsplicht serieus te nemen kan de organisatie aantonen dat zij voldoet aan de verwachtingen van de betrokkenen waarvan de persoonsgegevens worden verwerkt en andere stakeholders. De organisatie wordt door de verantwoordingsplicht gedwongen goed na te denken over de risico's die aanwezig zijn op het gebied van gegevensbescherming en op welke wijze deze effectief kunnen worden beheerst. In mijn ogen is de beste manier om bovenstaande doelen te bewerkstelligen via een privacy management control programma waarbij aandacht is voor de plan-do-check-act-cyclus.

Het serieus nemen van de verantwoordingsplicht geeft de organisatie een competitief voordeel ten opzichte van concurrenten die hun zaken op dit gebied (mogelijk) minder goed voor elkaar hebben. Een bijkomend voordeel is dat – mocht er ondanks alle maatregelen die zijn genomen toch een schending zijn van de AVG – de organisatie kan aantonen dat zij voldoende maatregelen heeft genomen om dit risico te beheersen. Dit kan leiden tot een matiging van eventuele maatregelen van de toezichthouder.

1 De doelstellingen en beginselen van de Richtlijn 95/46/EG bleven immers overeind volgens overweging 9 van de AVG.

Hoe voldoe ik aan de verantwoordingsplicht?

Nu het 'waarom' van de verantwoordingsplicht is uitgelegd, gaan we verder met het 'hoe'. In artikel 5 lid 2 AVG staat:

"De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (verantwoordingsplicht)."

Dit is verder uitgewerkt in artikel 24 lid 1 AVG:

"Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd."

Uit de eerste zinsnede van artikel 24 lid 1 komt duidelijk naar voren dat er gekozen is voor een risico gebaseerde benadering. De maatregelen die genomen moeten worden, moeten in verhouding staan tot het risico dat de verwerking met zich meebrengt. Indien er sprake is van een proces met een vrij eenvoudige verwerking en weinig of niet-gevoelige persoonsgegevens, zullen er (over het algemeen) minder beheersingsmaatregelen nodig zijn om te voldoen aan de verantwoordingsplicht dan bij een proces met complexe en/of meerdere verwerkingen met veel en/of bijzondere persoonsgegevens. Hetzelfde principe geldt voor de organisatie als geheel. Een bloemenwinkel zal gezien de aard en hoeveelheid persoonsgegevens die worden verwerkt, minder beheersingsmaatregelen nodig hebben dan een ziekenhuis.

Het voldoen aan de verantwoordingsplicht is geen afvinkoefening. Al staan in de AVG wel een aantal verplichte maatregelen die genomen moeten worden om aan te tonen dat de organisatie aan de verantwoordingsplicht heeft voldaan. De verplichte maatregelen zijn het opstellen en bijhouden van een verwerkingsregister en een datalekkenregister, het uitvoeren van Data Privacy Impact Assessments (DPIA) bij verwerkingen met een (waarschijnlijk) hoog risico en, wanneer hierover onduidelijkheid bestaat, het vastleggen van de onderbouwing waarom het aanstellen van een functionaris gegevensbescherming (FG) niet verplicht is.

Naast deze verplichte maatregelen is het over het algemeen nodig om aanvullende maatregelen te nemen waarmee aangetoond kan worden dat wordt voldaan aan de verantwoordingsplicht. Denk hierbij aan het aansluiten bij een gedragscode of het behalen van certificeringen, het opstellen (en monitoren van naleving) van beleidstukken op het gebied van privacy en informatiebeveiliging, het sluiten van verwerkersovereenkomsten met verwerkers (of vastleggen waarom er geen sprake is van een verwerker) en transparantie over de verwerking van persoonsgegevens in bijvoorbeeld het jaarverslag.[2] Deze maatregelen zijn naar mijn mening het minimum waaraan moet worden voldaan. Het invoeren van een privacy management control programma waarbij aandacht is voor de plan-do-check-act cyclus is de beste manier om te borgen dat continue evaluatie en actualisatie van de beheersingsmaatregelen, zoals vereist wordt in de laatste zinsnede van artikel 24 lid 1 AVG, plaatsvindt en er geen sprake is van het eenmalig afwerken van een vinkenlijst.

Hoe gaat TKP om met de verantwoordelijkheidsplicht?

In artikel 28 AVG staat dat een verwerkingsverantwoordelijke uitsluitend een verwerker mag aanstellen als die verwerker afdoende garanties geeft met betrekking tot het toepassen van passende technische en organisatorische maatregelen zodat de verwerking aan de vereisten van de AVG voldoet. De oplettende lezer ziet dezelfde bewoording terug uit artikel 24 lid 1 AVG. Ook de verwerker moet kunnen aantonen dat zij voldoet aan de vereisten vanuit de AVG (en de verwerkersovereenkomst).

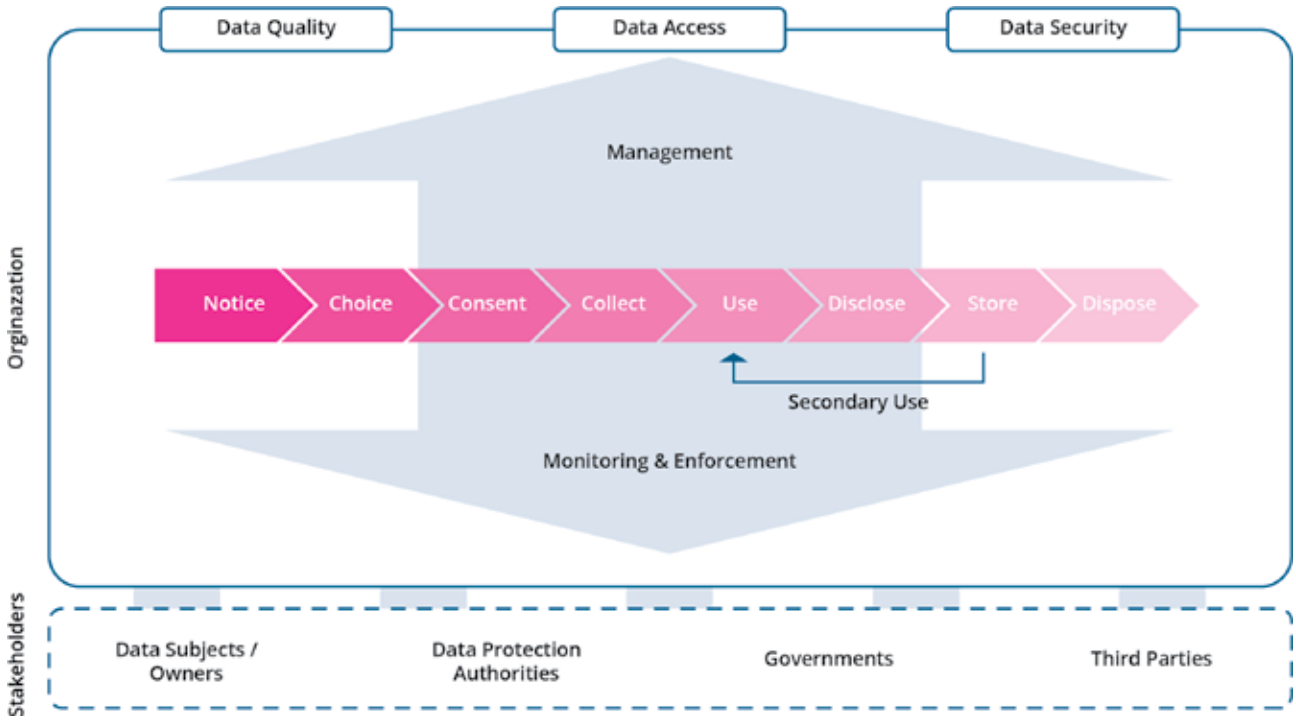
TKP voert voor meerdere pensioenuitvoerders de (gehele) pensioenadministratie uit, waaronder het doen van pensioenuitkeringen en premieoplegging aan werkgevers. Dat betekent dat TKP namens de pensioenuitvoerders veel persoonsgegevens verwerkt van onder andere deelnemers en werkgevers.[3] TKP is daarom al in 2017 gaan nadenken over de vraag hoe te voldoen aan de verantwoordingsplicht. Destijds en ook bij de invoering van de AVG waren er nog geen gedragscodes of certificeringen beschikbaar waarbij aangesloten kon worden. Na het bestuderen van verschillende frameworks is besloten dat het Privacy Control Framework (PCF) van Norea[4], de Nederlandse beroepsorganisatie van gekwalificeerde IT-auditors, het beste aansloot bij de wensen van TKP, omdat het gebaseerd is op een informatielevenscyclusmodel en gebruikt kan worden om geaudit te worden.

---

2 Zie www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht.

3 Indien sprake is van een eenmanszaak, v.o.f., C.V. of maatschap.

4 www.norea.nl



Figuur 1: Informatielevenscyclus zoals weergegeven in het Privacy Control Framework

Het voert te ver om in dit artikel de gehele informatielevenscyclus uitgebreid te behandelen. Maar kort gezegd is in het PCF voor elke fase van de informatielevenscyclus bepaald welke onderwerpen van toepassingen zijn en zijn hiervoor beheersingsdoelstellingen en beheermaatregelen opgenomen. Een belangrijk onderdeel van het PCF is de evaluatie van die maatregelen. In totaal zijn in het PCF 32 privacy onderwerpen opgenomen met 95 beheersingsmaatregelen. In het PCF geeft Norea zelf aan dat "Met de implementatie en uitvoering van de maatregelen [van het PCF] kan met een redelijke mate van zekerheid geborgd worden dat de beheersingsdoelstelling waartoe die maatregelen behoren wordt behaald."[5]

Het PCF kan daarom door entiteiten worden gebruikt om vast te stellen of de maatregelen ten aanzien van privacybescherming adequaat zijn, of om te bepalen in hoeverre de huidige maatregelen dienen te worden aangepast om te voldoen aan (wijzigingen in) wetgevingskaders (zoals de AVG).

Daarbij moet overigens wel de kanttekening worden gemaakt (zoals Norea zelf ook doet) dat omdat de AVG veelomvattend is niet alle details zijn uitgewerkt en een nadere invulling van sommige normen nodig is. In de praktijk merken wij dat deze uitwerking naar voren komt bij het invullen door de organisatie van de betreffende norm. Een voorbeeld van de beheersingsdoelstelling en bijbehorende beheersingsmaatregelen in de fase Inzage en kwaliteit van de gegevens in het PCF staat op de pagina hiernaast.

Voor TKP heeft het gebruik van het PCF tot doel om aan de eigen organisatie inzichtelijk te maken welke maatregelen zijn getroffen om de bescherming van persoonsgegevens te borgen. Daarnaast is het doel om aantoonbaar te maken richting de eigen organisatie én haar klanten dat TKP de risico's omtrent het niet voldoen aan de AVG voldoende beheerst. Periodiek toetst het Privacy Office van TKP door het integraal invullen van het PCF of aan de gestelde privacyregels in het privacy normenkader is voldaan. Dit noemt TKP het uitvoeren van het Privacy Control Program (PCP). Eventuele bevindingen worden vastgelegd, gerapporteerd aan het management en gemonitord zodat adequate opvolging geborgd wordt conform de plan-do-check-act-cyclus. Ieder jaar laat TKP de uitvoering van het PCP

5 Norea Handreiking Privacy Control Framework, versie 2.0, augustus 2019, pagina 6.

Het serieus nemen van de verantwoordingsplicht is een must.

auditen door een (onafhankelijke) auditor. De auditrapportage hiervan wordt integraal met de pensioenuitvoerders gedeeld. Op deze manier kunnen ook de pensioenuitvoerders vaststellen in hoeverre TKP in control is ten aanzien van het privacy-risico.

Tot slot

De invoering van de verantwoordingsplicht was een van de belangrijkste wijzigingen bij de invoering van de AVG. Hiermee is uitdrukkelijk de verantwoordelijkheid voor het kunnen aantonen van het voldoen aan de AVG bij de verwerkingsverantwoordelijke neergelegd. Het voldoen aan deze verplichting vergt van de organisatie dat zij (serieus) werk maakt van privacy management. In de AVG staan een aantal verplichte maatregelen die genomen moeten worden in het kader van de verantwoordingsplicht. Het doorvoeren van aanvullende maatregelen is in mijn ogen echter nodig om hieraan te voldoen.

Het aantonen van het voldoen aan de verantwoordingsplicht kan op verschillende manieren worden vorm gegeven. TKP heeft er voor gekozen om dit aan te tonen middels het Privacy Control Framework van Norea dat jaarlijks wordt getoetst door een (onafhankelijke) auditor. Op die manier toont TKP aan de pensioenuitvoerders en de betrokkenen aan dat zij in control is ten aanzien van het risico van het niet voldoen aan de AVG. Mijn advies aan alle Compliance en Privacy officers dan wel FG's is om de eigen organisatie bewust te maken van het feit dat het serieus nemen van de verantwoordingsplicht een must is. Enerzijds vanwege het risico op niet voldoen aan de AVG, anderzijds omdat het uitvoeren van een goed doordacht privacy management control programma een concurrentievoordeel met zich mee brengt.

Joost Damen is Compliance officer bij TKP. Daarnaast is hij lid van de Commissie Governance en Compliance, voorzitter van de werkgroep Compliance en lid van de werkgroep AVG van de Pensioenfederatie. Joost studeerde Nederlands recht (specialisatie bedrijfsrecht) aan de Rijksuniversiteit Groningen en is CIPP-E. Joost heeft meer dan 15 jaar ervaring als compliance en privacy officer in de financiële sector.

Verzoek tot rectificatie (DCR)

Beheersingsdoelstellingen:
Een rectificatieverzoek van de betrokkenen wordt op de juiste wijze afgehandeld. Betrokkenen kunnen bepalen of hun persoonsgegevens correct/up-to-date zijn en zij kunnen deze corrigeren.

Fase informatielevenscyclusmanagement: **Inzage en kwaliteit van gegevens**

Beheersingsmaatregelen:

DCR01	De entiteit heeft procedures ingericht om adequaat te reageren op rectificatie-verzoeken van betrokkenen. Indien de betrokkene het recht op rectificatie uitoefent, corrigeert de entiteit de persoonsgegevens onverwijld.	VV

HET IS OORLOG
MAAR NIEMAND DIE HET ZIET

Melissa Veen

In Het is oorlog maar niemand die het ziet vertelt onderzoeksjournalist Huib Modderkolk hoe afhankelijk de wereld is geworden van technologie, welke risico's dat met zich meebrengt en hoe belangrijk cybersecurity hierin is. Hij neemt je mee in een 'onzichtbare' wereld waarin (digitale) handelingen worden verricht die, soms zelfs globaal, enorme gevolgen hebben of hebben gehad. Denk bijvoorbeeld aan de beïnvloeding van hele kiezersgroepen door de Russen bij de door Donald Trump gewonnen Amerikaanse verkiezingen eind 2016, het platleggen van de Rotterdamse haven in 2017 of het verijdelen van de ontwikkeling van schadelijke wapens door Iran middels het saboteren van onderdelen die via Schiphol worden getransporteerd. Verrassend hierbij is met name ook de grote rol die Nederland speelt in deze voor het oog niet zichtbare wereld.

Met geduld, doorzettingsvermogen en af en toe een beetje geluk weet Huib Modderkolk informatie uit bronnen te krijgen waarmee hij onder meer geheime operaties van de AIVD en MIVD uit de doeken doet, een inkijkje geeft in de informatie die Edward Snowden in 2013 geopenbaard heeft en je meeneemt in de manier waarop bijvoorbeeld China en Rusland zich hebben ontpopt tot meesters in het digitaal ontfutselen en manipuleren van informatie om dit voor eigen gewin in te zetten.

Uit het boek blijkt ook dat Nederland in de jaren '10 heel belangrijk was in de wereld van digitale spionage. Niet alleen door de informatie die door de AIVD en MIVD – qua werknemerspopulatie toch vrij kleine organisaties – werd verkregen en hoe zij daarmee een belangrijke bondgenoot werden van de machtige, groots opgezette inlichtingendiensten in Groot-Brittannië en de Verenigde Staten, maar ook door de datacenters die in ons land staan en door de specialistische kennis van het bedrijf Fox-IT waar grif gebruik van werd gemaakt als er weer ergens een vorm van spionage werd ontdekt.

Huib Modderkolk
Het is oorlog maar niemand die het ziet
ISBN 9789057599804

Bij het lezen van dit boek rolde ik van de ene verbazing in de andere. De onthullingen die de auteur doet over geheime diensten en digitalisering, over de manier waarop staten hacken inzetten als wapen om macht te verkrijgen en over ogenschijnlijk kleine incidenten die grote gevolgen hebben gehad voor honderdduizenden mensen ter wereld. Het boek geeft het enorme belang weer van informatiebeveiliging, maar geeft ondertussen ook een gevoel van moedeloosheid omdat de mate van beveiliging eigenlijk nooit goed genoeg zal zijn om kwaadwillende partijen buiten de deur te houden. Het voelt alsof digitale privacy een utopie is geworden.

Ook maak ik me zorgen. Nederland was blijkbaar een belangrijke speler in de wereld van geheime diensten en spionage. Echter, door (onder meer) (te) weinig investeringen in (de ontwikkelingen op het gebied van) databeveiliging is Nederland die positie kwijtgeraakt aan landen als Rusland en China. Landen die hier wel enorme (financiële) effort in hebben gestopt. Landen met ogenschijnlijk veel minder scrupules en minder regels ten aanzien van de bescherming van persoonsgegevens en de privacy van burgers. Heeft dit gevolgen voor Nederland en haar burgers, en, zo ja, welke?

De in het boek beschreven situaties zijn echter met name toegespitst op het verkrijgen van informatie over staten, bedrijven en groeperingen. Hierdoor lijkt de impact van deze grootschalige digitale spionage en infiltratie voor de individuele burger (doorgaans) beperkt. Dit zorgt ervoor dat mijn gevoelens van moedeloosheid en zorgen wel aanwezig zijn, maar dat die van verbazing over alles wat er plaatsvindt in een onzichtbare wereld met zichtbare gevolgen, overheerst. Een fantastisch boek om te lezen als je werkzaam bent in de wereld van informatiebeveiliging en privacy, maar ook als je gewoon eens wilt weten wat er zich in een onzichtbare wereld zo dichtbij, afspeelt!

Onthullingen over geheime diensten en digitalisering, de manier waarop staten hacken inzetten als wapen om macht te verkrijgen, en ogenschijnlijk kleine incidenten die grote gevolgen hebben gehad voor honderdduizenden mensen ter wereld.

Compliance vacature

Kom jij ons team als

senior compliance/ privacy adviseur

versterken?

Mail ons: werken@compliance-instituut.nl