FACTSHEET - 2 JAAR AVG

Dataprivacy: een vakgebied in ontwikkeling

Het implementeren van dataprivacy kan voor u als organisatie een uitdaging zijn. Zo kent de Algemene verordening gegevensbescherming (AVG) veel open normen, waardoor organisaties veelal op een eigen interpretatie van de bepalingen in de AVG zijn aangewezen.

Maar het vakgebied wordt steeds volwassener. Zo stellen mensen hogere eisen aan hun privacybescherming, zijn er voor organisaties verschillende normen ontwikkeld en is er aanvullende wet- en regelgeving ingegaan. Ook is de Autoriteit Persoonsgegevens als toezichthouder steeds duidelijker wat zij van organisaties verwacht. Om goed op de toekomst voorbereid te zijn, is het voor u belangrijk om ontwikkelingen op het gebied van dataprivacy al vroeg in kaart te brengen én actie te ondernemen. In deze factsheet zetten wij de huidige ontwikkelingen binnen de dataprivacy uiteen en doen wij een voorspelling over de gevolgen voor de (nabije) toekomst.

Een hogere awareness

Alle betrokkenen wiens gegevens verwerkt worden, zoals burgers, klanten en werknemers, zijn zich steeds meer bewust van de mogelijke gevolgen van privacy-inbreuken. Zo lijkt de algemene opvatting te verschuiven van 'maar ik heb toch niets te verbergen?' naar 'wat als mijn persoonsgegevens verkeerd worden geïnterpreteerd?'. Binnen de publieke sector blijkt dit onder andere uit de initiële afwijzing van de corona-app en coronawet, waarbij burgers kenbaar maakten dat zij zich grote zorgen maken om de gevolgen voor hun persoonlijke levenssfeer. Een ander voorbeeld is de publieke reactie op de profileringspraktijken van de Belastingdienst.

De Autoriteit Persoonsgegevens constateerde dat betrokkenen **steeds vaker opkomen voor hun privacyrechten**. Uit een recent onderzoek van de toezichthouder bleek dat er een **sterke toename van privacyklachten** is. Een van deze klachten resulteerde zelfs in **een boete van € 830.000 voor het BKR**, omdat het BKR – naar het oordeel van de Autoriteit Persoonsgegevens – te hoge drempels opwierp voor betrokkenen om hun persoonsgegevens in te zien.

Ook BDO ziet in de praktijk dat veel organisaties worstelen met het waarborgen van de privacyrechten van betrokkenen. Vaak wordt geleund op een ad-hoc-aanpak, waarbij de procesrisico's binnen organisaties niet goed van tevoren zijn afgewogen. Het kan dan voorkomen dat betrokkenen hun privacyrechten niet voldoende kunnen uitoefenen. Organisaties doen er daarom goed aan om na te denken over de wijze waarop zij deze rechten beschermen, vóórdat zij dergelijke verzoeken – of klachten – ontvangen. Een oplossing is bijvoorbeeld het opstellen van gestandaardiseerde procedures voor het afhandelen van privacyverzoeken; voorkomen is immers beter dan genezen.

Massaclaims

In de private sector heeft de actievere houding van betrokkenen recentelijk geleid tot het opstarten van de

eerste class actionrechtszaak. De Consumentenbond probeert Facebook via de rechter te dwingen om gebruikers te compenseren voor vermeende privacyschendingen. Het is daarbij mogelijk voor Facebookgebruikers om zich kosteloos door de Consumentenbond te laten vertegenwoordigen. Vooralsnog is de oproep een succesvolle actie gebleken, want na één dag hadden al 100.000 individuen zich aangemeld bij de Consumentenbond. Een uitspraak van de rechter zou in deze zaak tot hoge schadevergoedingen kunnen leiden, om over imagoschade voor Facebook nog maar te zwijgen. Ook kan met deze zaak een precedent worden geschapen voor toekomstige massaclaims binnen de dataprivacy. Zo is er tevens een massaclaim ingediend tegen Oracle en Salesforce. Als organisatie dient u zich er dus van bewust te zijn dat dergelijke acties in de toekomst vaker zullen voorkomen.

Van compliance naar assurance?

In de factsheet **'De AVG en informatiebeveiliging'** hebben wij het al uitgebreid gehad over ISO 27701, waarvoor organisaties zich kunnen laten certificeren. Met het behalen van dit certificaat toont een organisatie aan dat op een privacyvriendelijke manier wordt omgegaan met persoonsgegevens. In de factsheet concludeerden wij dat de markt steeds meer zekerheid zal verlangen over de privacywaarborgen van onder andere leveranciers – een ontwikkeling die eerder ook al binnen de informatiebeveiliging plaatsvond. Certificaten waarmee organisaties '*AVG-compliance*' kunnen aantonen zijn er momenteel helaas (nog) niet. De Europese wetgever heeft voor de ontwikkeling van dergelijke certificaten wel een opening gecreëerd in de AVG, namelijk in de artikelen 40 t/m 43. Hierin staat beschreven dat door de Europese en nationale toezichthouders en certificeringsorganen 'AVG-certificaten' kunnen worden ontwikkeld. Recentelijk heeft de Autoriteit Persoonsgegevens hieromtrent haar samenwerking met de Nederlandse Raad voor Accreditatie **aangekondigd**. Op de website van de Autoriteit Persoonsgegevens is ook te lezen dat er wordt gewerkt aan certificatieschema's voor de **AVG-certificaten**. Het hebben van zo'n certificaat kan een organisatie een concurrentievoordeel opleveren en betrokkenen zekerheid geven over de bescherming van hun privacy. Ook is het aannemelijk dat een organisatie met een AVG-certificaat eerder uit het vizier van de toezichthouder blijft.

Actievere houding van de Autoriteit Persoonsgegevens

Zoals reeds vermeld in de factsheet '**De AVG en toezicht door de Autoriteit Persoonsgegevens**' heeft de Autoriteit Persoonsgegevens tot nu toe geen streng boeteregime gehanteerd. Hoewel er enkele boetes zijn uitgedeeld valt de hoogte van die boetes in vergelijking met andere Europese toezichthouders relatief gezien mee. Het is evident dat de eerste twee jaar na de toepassing van de AVG de focus van de Autoriteit Persoonsgegevens in algemene zin lag op het bieden van voorlichting en advies aan organisaties. Zo worden onderwerpen als *Data Protection Impact Assessments*, het **aanstellen van een Functionaris voor de Gegevensbescherming** en **meldplicht datalekken** toegelicht door middel van uitgebreide informatie en checklists op de website van de Autoriteit Persoonsgegevens.

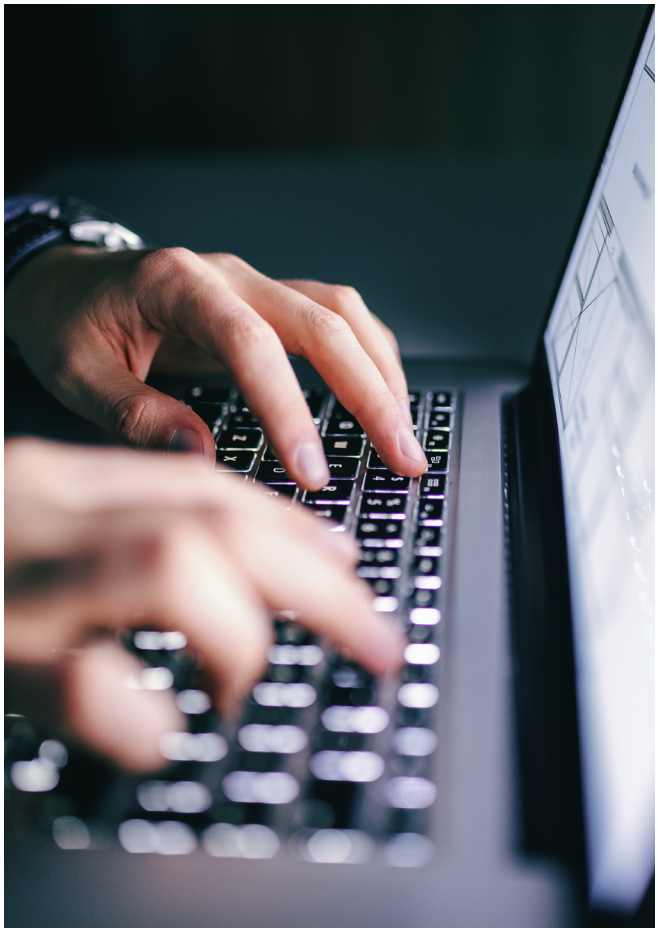
Deze focus van de Autoriteit Persoonsgegevens gaat echter veranderen. In het beleidsdocument 'Focus AP 2020-2023 dataprotectie in een digitale samenleving' is te lezen dat de Autoriteit Persoonsgegevens zich in de periode 2020-2023 meer zal gaan richten op de focusgebieden 'datahandel', 'digitale overheid' en 'artificial intelligence & algoritmes'. Concreet betekent dit dat met name de doorverkoop van data en behavioral advertising goed in de gaten gehouden zal worden. Daarnaast zal toezicht gehouden worden op de verantwoordelijkheid van de overheid met betrekking tot het verantwoord omgaan met (vaak gevoelige en bijzondere) persoonsgegevens van burgers, waarbij de aandacht gaat naar databeveiliging, smart cities en samenwerkingsverbanden tussen organisaties. Bewustwording van de risico's die inherent zijn aan de huidige technologische ontwikkelingen is met name op het gebied van artificial intelligence en algoritmes van belang.

Bovendien geeft de Autoriteit Persoonsgegevens aan de komende jaren in toenemende mate te gaan handhaven. Op welke wijze de Autoriteit Persoonsgegevens dit gaat bewerkstelligen is nog onduidelijk, omdat zij naar eigen zeggen momenteel met een capaciteitsprobleem kampt. Uit **extern onderzoek** blijkt dat zowel de bezetting als het budget meer dan dubbel zo groot zou moeten worden. Daarentegen heeft de Nederlandse overheid aangekondigd het budget voor de komende jaren te verlagen. Voor de jaren 2021 tot en met 2025 is een budget van ongeveer € 18,5 miljoen uitgetrokken, terwijl het budget voor 2020 € 19,3 miljoen bedraagt. Aangezien het een voorlopige begroting betreft blijft de **Autoriteit Persoonsgegevens – zo geeft zij op haar website aan – hoopvol** voor extra budget.

Toch blijkt het oordeel van de Autoriteit Persoonsgegevens niet altijd zaligmakend. Zo bleek onlangs dat in de zaak Voetbal TV de autoriteit onterecht een boete van € 575.000 uitdeelde, omdat zij van mening was dat een commercieel belang niet onder de grondslag 'gerechtvaardigd belang' geschaard kon worden. De rechter nuanceerde dit echter en oordeelde dat de vaststelling dat eiseres geen gerechtvaardigd belang had niet voldoende zorgvuldig was genomen. Bovendien stelde de rechter dat niet alleen juridische, maar ook feitelijke, economische en ideële belangen als gerechtvaardigd belang kunnen kwalificeren. Daarnaast volgt dat belangen niet van tevoren uitgesloten mogen worden. Iets wat de Autoriteit Persoonsgegevens wél deed met zijn zienswijze omtrent het gerechtvaardigd belang (en nog steeds doet met betrekking tot de grondslag toestemming in de relatie werkgever – werknemer). Hopelijk brengt een vergroting van de capaciteit tevens met zich mee dat dergelijke verkeerde interpretaties van de AVG, met grote gevolgen, niet meer voor zullen komen.

Privacy op wereldniveau

Het privacyvraagstuk speelt niet alleen in Nederland, maar houdt ons wereldwijd bezig. Zo is op 16 juli jl. het 'Privacy Shield', welke een betrouwbaar gegevensbeschermingsniveau moest waarborgen voor dataverkeer tussen Europa en de Verenigde Staten, door het Europees Hof van Justitie ongeldig



verklaard in de uitspraak Schrems II. Een uitspraak met immens grote gevolgen voor zowel de publieke als de private sector omdat een 'Privacy Shield' niet meer gebruikt mag worden als grondslag voor de overdracht van persoonsgegevens uit de Europese Economische Ruimte naar de Verenigde Staten. In de Schrems II-uitspraak is geen overgangsperiode opgenomen, waardoor van het één op het andere moment een bestaande uitwisseling van data naar een derde land als de Verenigde Staten niet meer voldoet aan de AVG. Naast het ongeldig verklaren van het 'Privacy Shield' wordt er in de uitspraak door het Europese Hof van Justitie tevens een kritische noot geplaatst bij het gebruik van Standard Contractual Clauses ('SCC') waardoor het de vraag is of het gebruik van modelcontractbepalingen voldoende is om aan de AVG te voldoen. Daags na de uitspraak werd door de European Data Protection Board (EDPB) getracht door middel van **frequently asked questions** het een en ander toe te lichten. Desondanks zaten ondernemers met de handen in het haar door het ontbreken van praktische 'guidance'. Inmiddels zijn op 11 november jl. door de EDPB **aanbevelingen** over de doorgifte van persoonsgegevens na Schrems II gepubliceerd. De aanbevelingen vormen een '**roadmap**' van zes stappen welke bedrijven kunnen volgen. Deze aanbevelingen staan open voor publieke consultatie.

De Autoriteit Persoonsgegevens geeft aan dat de huidige SCC nog wel een geldige grondslag kunnen bieden voor doorgifte naar derde landen onder de strikte voorwaarde dat een bedrijf voldoende aanvullende maatregelen neemt om de veiligheid van de doorgifte te waarborgen.

Praktische tip: Sluit aanvullende bepalingen op de SCC, waarbij u het risico verlegt!

- Importeur verklaart dat er geen nationale wetgeving is die rechten en plichten uit hoofde van de verwerkersovereenkomst, SCC en/of AVG in de weg staat.
- Sluit een informatieplicht af omtrent wezenlijke wijzigingen in documentatie van (sub)verwerker.

Ook de Europese Commissie heeft een **nieuw concept model verwerkersovereenkomst** gepubliceerd. Deze staat tot 10 december dit jaar open voor consultatie. In de praktijk wordt er veel onderhandeld over verwerkersovereenkomsten, waardoor een dergelijk model een goed startpunt zou kunnen zijn voor de onderhandelingen. Opvallend is dat van de artikelen in dit model niet afgeweken kan worden, maar slechts aanvullende afspraken kunnen worden gemaakt (zolang deze uiteraard niet afwijken van de andere afspraken). Daarnaast valt op dat in dit model een separate bijlage dient te worden toegevoegd waarin extra (beveiligings)maatregelen worden getroffen in het geval dat er bijzondere persoonsgegevens worden verwerkt.

Het is afwachten tot zowel de 'roadmap' en de modelcontractbepalingen in definitieve vorm worden gepubliceerd. Tot die tijd kan BDO helpen met het opstellen en reviewen van uw verwerkersovereenkomst.

De e-privacyverordening; een hoofdpijndossier voor de EU?

De huidige regels voor telecombedrijven zijn neergelegd in de e-privacyrichtlijn uit 2002. Met de huidige digitale ontwikkelingen sluit deze richtlijn niet meer aan op de huidige situatie en zal deze vervangen worden door de e-privacyverordening. De e-privacyverordening ziet op de regulering van elektronische communicatiediensten, welke hoofdzakelijk bestaan uit het overbrengen van signalen. Ook persoonlijke communicatiediensten vallen hieronder, zoals bijvoorbeeld WhatsApp, Skype, etc. Door middel van de e-privacyverordening wordt beoogd de gegevensbescherming omtrent elektronische communicatie te waarborgen, een betere aansluiting te vinden op de AVG en de regelgeving te harmoniseren. In de verordening wordt met name de regelgeving omtrent direct marketing, het plaatsen van cookies en het gebruik van metadata die op het internet verkregen worden gereguleerd. In de praktijk zal dit betekenen dat we steeds meer richting een opt-in systeem gaan, waarbij een actieve toestemming van de gebruiker is vereist.

De European Data Protection Board (EDPB) benadrukt dat 'de e-privacyverordening niet gezien mag worden als een obstakel voor de ontwikkeling van nieuwe technologieën en diensten, maar integendeel nodig is om marktdeelnemers gelijke concurrentievoorwaarden en juridische zekerheid te bieden'.

Ondanks opgelopen vertraging door de COVID-19-pandemie, is recent een nieuw voorstel voor de tekst voor de e-privacyverordening gepubliceerd. Deze tekst is op 11 november 2020

besproken door de Europese Raad. Het doel is om eind 2020 een akkoord over de definitieve tekst van de e-privacyverordening te bereiken. Als er overeenstemming wordt bereikt, zal de verordening rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, waaronder Nederland.

Om op de hoogte te blijven van de laatste ontwikkelingen met bijbehorende consequenties voor de elektronische communicatiediensten, is het voor organisaties van groot belang om de ontwikkelingen rondom de e-privacyverordening goed in de gaten te houden.

Europa koploper in privacywetgeving

Met name in Europa speelt privacy een steeds prominentere rol binnen onze samenleving. De awareness onder burgers in Europa groeit – mede door de komst van de AVG – enorm. Europa wordt gezien als de koploper met betrekking tot de privacywetgeving en de bewustwording hieromtrent. We verwachten dat dit voorlopig zo zal blijven. Privacy zou daarom op termijn dan ook een unique selling point van Europa kunnen vormen, waardoor Europa voor organisaties als veilige haven voor onlineprivacy kan dienen. Ook andere delen van de wereld lijken langzaam in beweging te komen. Dit is bijvoorbeeld te zien aan de invoering van de California Consumer Privacy Act (CCPA) op 1 januari jl. Hoewel het doel van de CCPA vergelijkbaar is met de AVG, is deze Californische wet nog niet gelijkwaardig aan het beschermingsniveau van de AVG. Het belangrijkste verschil is dat in Californië uit wordt gegaan van een opt-out systeem in tegenstelling tot het Europese opt-in systeem. Europa blijft dus voorlopig nog even koploper wat betreft dataprivacy.

Conclusie

Dataprivacy blijft een vakgebied dat wereldwijd continu in ontwikkeling is. In de toekomst verwachten we dat dataprivacy een steeds prominentere rol gaat innemen binnen organisaties nu de awareness omtrent privacyrechten in de samenleving steeds groter wordt. In de praktijk zijn er – mede door de Schrems II-uitspraak – echter nog wel wat struikelblokken te overwinnen. Zo hopen we dat Europa daadkrachtiger zal optreden en een actievere rol op zich zal nemen in het kader van het aandragen van pragmatische oplossingen voor organisaties.

Tot slot

Dit artikel vormt het laatste onderdeel van de serie '2 jaar AVG' van BDO Advisory.

Meer informatie?

Heeft u in de tussentijd vragen over dit artikel of wenst u ondersteuning op het gebied van dataprivacy binnen uw onderneming, neem dan gerust contact met ons op.

Tessa Janssen
Jurist Tech & Privacy Law
T 030 - 284 98 06
E tessa.janssen@bdo.nl

Ruben Tienhooven
Adviseur Cybersecurity/Privacy
T 06 - 23 21 48 71
E ruben.tienhooven@bdo.nl

12/2020 - AD2070