FACTSHEET - 2 JAAR AVG

De AVG en contractenrecht

De Algemene verordening gegevensbescherming (AVG) en de daarmee samenhangende contracten zijn een belangrijk onderdeel geworden van het contractenrecht en komen bij veel verschillende aspecten om de hoek kijken. In deze factsheet nemen we u mee in de wereld van contractuele verplichtingen binnen de AVG. Hierin bespreken we de verwerkersovereenkomst, zowel de aandachtspunten als veel voorkomende fouten die langskomen in de praktijk.

De verschillende rollen binnen de AVG

Teneinde de verplichtingen van de AVG goed te kunnen begrijpen is het van essentieel belang de verschillende rollen van elkaar te kunnen onderscheiden. Wanneer er een verwerking van persoonsgegevens plaatsvindt kunt u drie verschillende rollen vervullen:

- *Verwerkingsverantwoordelijke:* de partij die het doel en de middelen van de gegevensverwerking bepaalt. In de praktijk is dit de partij die zeggenschap heeft over de gegevensverwerking. Deze neemt de beslissingen omtrent welke gegevens worden verwerkt, de bewaartermijn, zeggenschap heeft over toegang tot de gegevens, informatie die wordt verstrekt aan betrokkenen of aan derden en/of partijen in landen buiten de EU.
  Voorbeeld: een bedrijf dat zijn salarisadministratie uitbesteed.
- *Verwerker:* de partij die ten behoeve van de verwerkingsverantwoordelijke en onder diens verantwoordelijkheid de persoonsgegevens verwerkt. De verwerking is voor deze partij de primaire opdracht.
  Voorbeeld: de salarisadministrateur.
- *Subverwerker:* de partij die door de verwerker wordt ingeschakeld om ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens te verwerken. Deze partij kan dus gezien worden als een 'onderaannemer'.
  Voorbeeld: het softwareprogramma waarmee de salarisadministrateur werkt, zoals Microsoft.

In de praktijk kunnen situaties voordoen waarbij deze scheidslijn niet makkelijk te trekken is. Zo kunnen er bijvoorbeeld meerdere verwerkingsverantwoordelijken, zogenaamde 'mede-verwerkingsverantwoordelijke' zijn.

De verwerkersovereenkomst

Uit de AVG vloeit de verplichting voort een verwerkersovereenkomst af te sluiten tussen de verwerkingsverantwoordelijke en de verwerker. Op deze wijze wordt de verhouding van de betrokken partijen en de bijbehorende verplichtingen schriftelijk vastgelegd. De vereisten waaraan een verwerkersovereenkomst minimaal dient te voldoen staan opgesomd in artikel 28 lid 3 AVG:

- Een verklaring dat de persoonsgegevens uitsluitend verwerkt worden op schriftelijke instructie van de verwerkingsverantwoordelijke, ook inzake doorgiften van persoonsgegevens aan een land buiten de EU;
- De waarborg dat bij de verwerking vertrouwelijkheid in acht wordt genomen;
- De garantie dat **passende technische en organisatorische maatregelen** worden getroffen;
- Het toestemmingsvereiste voor het in dienst nemen van een subverwerker en de garantie dat hen dezelfde verplichtingen worden opgelegd, met name omtrent het niveau van passende technische en organisatorische maatregelen;
- De garantie dat voor zover mogelijk bijstand wordt verleend (aan de verwerkingsverantwoordelijke) bij de uitoefening van de rechten van de betrokkenen. De verwerker kan hiervoor eventuele redelijke kosten in rekening brengen bij de verwerkingsverantwoordelijke;
- Bijstand verlenen bij een datalek, eventuele melding aan betrokkenen en Data Protection Impact Assessments (DPIA's);
- Terugbezorging of verwijdering van de persoonsgegevens na verloop van de verwerkingsdiensten (waarbij wettelijke verplichtingen in acht worden genomen);
- Terbeschikkingstelling van informatie door de verwerkingsverantwoordelijke inzake de nakoming van de neergelegde verplichtingen en audits en de verplichting voor de verwerker om de verwerkingsverantwoordelijke in kennis te stellen wanneer zij vermoedt dat een instructie een inbreuk oplevert.

Daarnaast raden we u aan een bepaling op te nemen omtrent de aansprakelijkheid, waarover meer in het volgende onderdeel 'Aandachtspunten'.

Aandachtspunten

De verwerkersovereenkomst = maatwerk!

Het sluiten van een verwerkersovereenkomst is maatwerk. In de praktijk plukken veel bedrijven modellen van het internet en gebruiken deze in hun bedrijfsvoering. Hoewel een bedrijf op deze manier wellicht in de veronderstelling is op deze wijze alles goed geregeld te hebben, is niets minder waar. Bij een kritische analyse van een dergelijk model, valt op dat het model vanuit een bepaald oogpunt (verwerkersverantwoordelijke of verwerker) is opgesteld. Met name de bepalingen omtrent aansprakelijkheid en verplichtingen kunnen daardoor in uw nadeel uitvallen. Bovendien komen de artikelen omtrent de (soort) persoonsgegevens die worden verwerkt, de doeleinden van de verwerking en de beveiligingsmaatregelen niet overeen met de daadwerkelijke bedrijfsvoering. Hoewel de verwerkersovereenkomst is onderworpen aan strikte verplichtingen zoals uiteengezet in artikel 28 AVG, blijft het contractenrecht. Maatwerk is in dezen vereist.

Aansprakelijkheid tussen partijen

Met betrekking tot de aansprakelijkheid is het belangrijk een onderscheid te maken tussen het 'externe aansprakelijkheidsregime' en het 'interne aansprakelijkheidsregime'. Het externe aansprakelijkheidsregime houdt in dat iedere derde die materiële schade heeft geleden, veroorzaakt door de verwerking van de persoonsgegevens, dit kan verhalen bij de verwerkingsverantwoordelijke. Dit staat als zodanig verankerd in artikel 82 van de AVG. Een verwerker kan in dezen slechts aansprakelijk zijn voor de schade die door de verwerking is veroorzaakt, wanneer zij niet heeft voldaan aan specifieke verplichtingen die uit de verwerkersovereenkomst voortvloeien óf in strijd handelt met de (rechtmatige) instructies van de verwerkingsverantwoordelijke. Volgens ons vallen overigens boetes van de toezichthouder niet onder dit externe aansprakelijkheidsregime.

De verdeling van de aansprakelijkheid is met betrekking tot externe aansprakelijkheid dus vastgelegd in de AVG. Dit ligt echter anders wanneer het de interne aansprakelijkheid betreft tussen partijen. Dit aansprakelijkheidsregime is vaak een heikel punt. Wanneer er reeds een hoofdovereenkomst bestaat tussen partijen, wordt de aansprakelijkheid in de praktijk vaak aan het oorspronkelijke aansprakelijkheidsregime gelinkt. Bijvoorbeeld aan de geldende algemene voorwaarden. We zien echter ook vaak dat de aansprakelijkheid een-op-een wordt doorgezet, waardoor de verwerker regelmatig het onderspit delft. Het vinden van een juiste balans is hier van essentieel belang. Dit is niet altijd even makkelijk. In bepaalde branches gelden modelovereenkomsten met een onbeperkte aansprakelijkheid voor de verwerker, bijvoorbeeld in de zorg en advocatuur. Dit leidt echter tot een schijnzekerheid. Wanneer de verwerker een grote partij betreft, zullen ze hier niet mee akkoord gaan. Wanneer de verwerker daarentegen juist een kleine partij is, is de kans groot dat deze omvalt wanneer de claim zich daadwerkelijk voordoet. Een verdeling van de aansprakelijkheid naar rato kan hier een juiste oplossing bieden.

De praktische problematiek licht zich gemakkelijk toe aan de hand van een casus. De toezichthouder geeft de verwerkersverantwoordelijke, welke meerdere verwerkers heeft ingeschakeld, een waarschuwing naar aanleiding van vier eerdere beveiligingsincidenten die hebben geleid tot een datalek. Na het inschakelen van een nieuwe verwerker, doet zich hier een datalek voor met een boete van de toezichthouder als gevolg. Het feit dat deze boete uitgedeeld wordt, is echter niet volledig te wijten aan de nieuwe verwerker. Een verdeling van de aansprakelijkheid naar rato zal hier een goede en rechtvaardige oplossing bieden.

Subverwerkers

Zoals reeds benoemd onder de kop 'De verwerkersovereenkomst' dient er in de verwerkersovereenkomst ook een bepaling opgenomen te worden omtrent het inschakelen van subverwerkers, met name in de verhouding verwerker-subverwerker. De AVG bepaalt dat een subverwerker niet ingeschakeld mag worden zonder de toestemming van de verwerkingsverantwoordelijke. Er wordt echter ruimte gelaten voor partijen om te bepalen of er voor ieder specifiek geval toestemming vereist is of dat algemene toestemming voldoet. Indien u in de rol van verwerker verkeert, is het belangrijk voorafgaand aan het sluiten van de verwerkersovereenkomst eventueel huidig gebruik van subver-

werkers aan te kaarten. Op deze wijze kunt u de toestemming voor de huidige subverwerkers reeds afhechten. In een eerder verschenen **factsheet** is het thema beveiliging al aan de orde gekomen. De AVG vereist dezelfde mate van beveiliging (inhoudende technische en organisatorische beveiligingsmaatregelen) voor de subverwerker als voor de verwerker. Deze verplichtingen dienen dus een-op-een doorgezet te worden. In de praktijk blijkt dit een heikel punt, met name wanneer er gebruik wordt gemaakt van grote partijen zoals Microsoft. Daarin behoort een onderhandeling omtrent de te treffen beveiligingsmaatregelen over het algemeen niet tot de opties. Wij adviseren derhalve dat u tijdens de onderhandelingen met de verwerkingsverantwoordelijke schriftelijk vastlegt dat de verwerkingsverantwoordelijke akkoord gaat met de voorwaarden van de subverwerker. Niet alleen de grootte van de subverwerker kan een belemmering vormen, ook de locatie van de subverwerker is van belang.

Doorgifte persoonsgegevens binnen en buiten de EU

De toepasselijkheid van de AVG is vrij extensief. Binnen de EU geldt hetzelfde beschermingsniveau[1]. In de praktijk zien we vaak verwarring omtrent de toepasselijkheid van de AVG ontstaan op het moment dat een verwerker of subverwerker zich buiten Europa bevindt begint de verwarring omtrent de toepasselijkheid van de AVG. Een treffend voorbeeld hiervan was de beruchte en veelgebruikte 'verouderingsapp' FaceApp. De politie gaf destijds een waarschuwing af door te zeggen dat de AVG niet van toepassing zou zijn, gezien het een Russische app was. Een klassieke fout, waarbij de politie wellicht eerst een privacy-expert had moeten raadplegen. De AVG is van toepassing voor organisaties (en personen) die in de EU gevestigd zijn en persoonsgegevens verwerken. Het is daarbij irrelevant of het persoonsgegevens van EU-burgers of niet-EU-burgers betreft. Daarnaast geldt de AVG óók voor organisaties (en personen) die niet in de EU gevestigd zijn, maar wel gegevens verwerken van burgers in de EU. Dit laatste was de situatie bij FaceApp. Het is hierbij overigens irrelevant of er voor de goederen of diensten aan de betrokkene wordt betaald. De reikwijdte van de AVG is vrij extensief, waardoor het van essentieel belang is om de AVG goed te begrijpen en na te leven.

Mocht u bijvoorbeeld gebruikmaken van een verwerker of subverwerker in Canada, dan is de AVG nog steeds van toepassing omdat deze persoonsgegevens van EU-burgers verwerkt. Voor bepaalde derde landen geldt er een zogenaamde 'adequaatheidsbeslissing', een verklaring van de Europese Commissie dat de nationale wetgeving een passend beschermingsniveau biedt. Bij deze landen hoeven geen aanvullende waarborgen getroffen te worden. In de Verenigde Staten geldt bijvoorbeeld het EU-VS Privacy Shield. Dit is een voorbeeld van een adequaatheidsbeslissing met als beperking dat deze alleen geldt voor ontvangende bedrijven die zich hebben gecertificeerd en aan deze principes voldoen. Het EU-VS Privacy Shield staat echter momenteel onder druk. Het is nog onduidelijk hoe dit er in de toekomst uit zal gaan zien.

Wilt u weten voor welke landen een adequaatheidsbesluit geldt? Raadpleeg de website van de Europese Commissie . Wanneer er geen adequaatheidsbesluit bestaat voor het land waarin uw verwerker of subverwerker zich bevindt, zijn naast de verwerkersovereenkomst wel aanvullende waarborgen vereist, zoals een modelcontractbepaling ('Standard Contractual Clauses') opgesteld door de Europese Commissie of bindende bedrijfsvoorschriften (BCR). De Standard Contractual Clauses bieden slechts een oplossing in twee verhoudingen: verwerkingsverantwoordelijke – verwerker en verkeringsverantwoordelijke – verwerkingsverantwoordelijke. De verhouding tussen verwerker en subverwerker is hier nog niet geborgd. Een mogelijke oplossing in een dergelijk geval zou kunnen zijn dat de verwerkingsverantwoordelijke een machtiging verleend aan de verwerker om een Standard Contractual Clause af te sluiten met de subverwerker. Momenteel is er een zaak gaande omtrent de vraag of Standard Contractual Clauses wel voldoende waarborgen bieden om de rechten en vrijheden van betrokkenen te beschermen. Op 16 juli 2020 wordt hier een uitspraak over gedaan door het Europees Hof van Justitie.

Hoewel een verwerker of subverwerker in een derde land aan de AVG gebonden kan zijn doordat het persoonsgegevens van EU-burgers verwerkt, zijn de verwerkersovereenkomsten in sommige gevallen dus wel aan een aantal extra vereisten verbonden.

Brexit

Momenteel geldt er met betrekking tot de brexit nog een overgangsperiode tot 31 december 2020. Na afloop van deze overgangsperiode, ligt als oplossing een adequaatheidsbesluit het meest voor de hand bij het uittreden van de EU. Mocht dit er niet komen, dan gelden dezelfde maatregelen als voor derde landen en zal er een gedragscode, bindende bedrijfsvoorschriften of een modelcontractbepaling vereist zijn. In het geval van reeds lopende verwerkersovereenkomsten zou een addendum opgesteld moeten worden met de aanvullende vereisten. Voor welke oplossing gekozen gaat worden is nu nog onduidelijk, dit zal de tijd moeten uitwijzen.

Blijf kritisch op uw rol!

Het klinkt misschien raar, maar wanneer u te maken heeft met de verwerking van persoonsgegevens is het heel belangrijk om kritisch te blijven op uw eigen rol. Het kan namelijk zijn dat u bij bepaalde activiteiten van kleur verschiet en in plaats van verwerker, al dan niet onbewust de rol van verwerkersverantwoordelijke op u neemt en andersom. Het belangrijkste is om u te blijven afvragen wie het doel en de middelen van de verwerking bepaalt. Deze rollen kunnen door elkaar lopen. Blijf dus kritisch omtrent uw eigen aandeel in de verwerking van persoonsgegevens. Uw rol bepalen is niet altijd even gemakkelijk. Uiteraard helpen wij u graag bij het analyseren van uw rol.

1 Hieronder rekenen we ook de landen van de EER (Noorwegen, Liechtenstein en IJsland), aangezien zij een gelijkwaardig niveau van bescherming van persoonsgegevens waarborgen.

Veel gemaakte fouten

In de praktijk blijkt het voor de ondernemer lang niet altijd even makkelijk om de AVG contractuele verplichtingen op de juiste wijze toe te passen. We attenderen u dan ook graag op de meest gemaakte fouten:

- In de praktijk blijkt dat partijen vaak hun eigen rol als verwerker of verwerkersverantwoordelijke verkeerd kwalificeren. Hierdoor worden verwerkersovereenkomsten niet altijd goed gesloten;
- Partijen denken een verwerkersovereenkomst te kunnen vastleggen in algemene voorwaarden. Een separate verwerkersovereenkomst is echter vereist;
- Bedrijven plukken een model verwerkersovereenkomst van het internet en veranderen slechts de namen. Hierdoor komt de praktijk niet overeen met wat er in de verwerkersovereenkomst staat vermeld omtrent o.a. de (soort) persoonsgegevens, doeleinden en de genomen beveiligingsmaatregelen. Nogmaals: een verwerkersovereenkomst is maatwerk! Het is belangrijk deze kritisch door te nemen.

Wat kan BDO voor u betekenen?

Vanuit de AVG volgt de verplichting om een verwerkersovereenkomst af te sluiten. Hier worden strikte eisen aan gesteld. De privacyexperts van BDO hebben ruime ervaring met het opstellen en beoordelen van verwerkersovereenkomsten, zowel vanuit het perspectief van de verwerkersverantwoordelijke als (sub)verwerker. Voorbeelden van werkzaamheden die we voor u kunnen uitvoeren zijn:

- het opstellen van verwerkersovereenkomsten;
- het beoordelen van verwerkersovereenkomsten en eventuele risico's hiervan in kaart brengen;
- het adviseren omtrent privacygerelateerde vraagstukken.

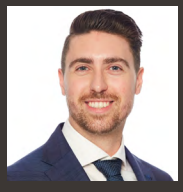
Tot slot

Deze factsheet is onderdeel van de serie '2 jaar AVG' van BDO Advisory. In de volgende editie wordt ingegaan op de AVG en het toezicht van de Autoriteit Persoonsgegevens.

Meer informatie?

Wilt u meer informatie over dit onderwerp? Neem dan contact op met:

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



Stefan Zrnic
Jurist Tech & Privacy Law
T 06 - 51 29 22 20
E stefan.zrnic@bdo.nl

06/2020 – AD2040