Mr. L. van Sloten[1]

Veranderende rollen en contracten onder de AVG

Bb 2020/53

Met de Algemene Verordening Gegevensbescherming (AVG) zijn wijzigingen aangebracht in de definities van de verschillende rollen binnen het gegevensbeschermingsrecht. We spreken niet langer van 'bewerker' maar van 'verwerker'. In plaats van de 'verantwoordelijke', hebben we nu de mond vol van de 'verwerkingsverantwoordelijke'. Maar heeft de AVG behalve tekstuele wijzigingen ook geleid tot wezenlijke veranderingen voor de rollen van partijen (en daaruit voortvloeiende verplichtingen)? En wat betekent dit voor de contracten die partijen moeten aangaan? In dit artikel worden de meest belangrijke veranderingen en ontwikkelingen besproken voor de rollen en contracten onder de AVG, met bijzondere aandacht voor de figuur van de 'gemeenschappelijke verwerkingsverantwoordelijkheid'.

1. De verwerkingsverantwoordelijke en de verwerker

De AVG legt veruit de meeste verplichtingen ter bescherming van persoonsgegevens op aan de 'verwerkingsverantwoordelijke': de persoon of het orgaan die of dat, alleen of met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (art. 4(7) AVG). Deze definitie komt nagenoeg overeen met de oude definitie van 'verantwoordelijke' onder artikel 1(d) van de voormalige Wet bescherming persoonsgegevens (Wbp). Een verwerkingsverantwoordelijke is (en blijft) bijvoorbeeld de werkgever die bepaalt om persoonsgegevens in te voeren in een systeem voor de salarisadministratie om vervolgens aan werknemers loon uit te keren.

De AVG legt ook bepaalde verplichtingen op aan 'verwerkers', onder de Wbp 'bewerkers' geheten: een persoon of orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Als bijvoorbeeld een administratiekantoor de salarissen uitbetaalt voor een werkgever, verwerkt dit kantoor de persoonsgegevens van werknemers ten behoeve van de werkgever en dus in de rol van 'verwerker'. Een medewerker in dienst van de werkgever die zorgt voor de uitkering van salarissen kwalificeert niet als 'verwerker'. Omdat de medewerker onder rechtstreeks gezag staat van de werkgever, valt deze verwerking onder de verantwoordelijkheid van de werkgever. Dit wordt in Nederland 'intern beheer' genoemd.

Het is van belang om te bepalen welke rol of rollen – want een combinatie is ook mogelijk – de eigen organisatie vervult ten aanzien van een verwerking van persoonsgegevens, omdat daaruit de wettelijke verplichtingen en verantwoordelijkheden voortvloeien. Door de rol te bepalen wordt ook duidelijk welke contracten of regelingen nodig zijn om aan de AVG te voldoen en de eigen rechtspositie te beschermen. Onder de AVG is een juiste vaststelling van de rollen nog belangrijker geworden omdat de verplichtingen en verantwoordelijkheden voor zowel verwerkingsverantwoordelijken als verwerkers zijn uitgebreid en bovendien toezichthouders hogere boetes kunnen opleggen.

Maar voor organisaties blijft het soms lastig om te bepalen welke rolverdeling aan de orde is. Sinds de AVG zijn dan ook wederom vragen gerezen over de interpretatie van de begrippen van verwerkingsverantwoordelijke en verwerker. Omdat de betekenis van de begrippen onder de AVG nagenoeg gelijk is gebleven, zijn eerdere interpretaties daarvan nog steeds relevant. Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker" (WP169) van de Artikel 29 Werkgroep blijft bijvoorbeeld nuttig, waarin behalve toelichting ook diverse voorbeelden zijn opgenomen. De Artikel 29 Werkgroep was het adviesorgaan ten tijde van de Wbp waarin alle EU-toezichthouders op het gebied van gegevensbescherming zitting namen en welke sinds de AVG feitelijk is opgevolgd door het Europees Comité voor gegevensbescherming of beter bekend als de European Data Protection Board (EDPB). De EDPB heeft Advies 1/2010 niet bekrachtigd – zoals zij dat wel heeft gedaan voor enkele guidelines van de Artikel 29 Werkgroep[2] – en aangekondigd nieuwe *guidelines* hierover te publiceren. Maar tot op heden is geen (concept) opinie gepubliceerd in opvolging van advies 1/2010. De European Data Protection Supervisor, welke toezicht houdt op de naleving van de gegevensbeschermingswetgeving[3] die van toepassing is op EU-instellingen, heeft eind 2019 richtsnoeren gepubliceerd die ook nuttig kunnen zijn voor niet-EU-instellingen omdat deze wetgeving gebruikmaakt van nagenoeg dezelfde definities voor 'verwerkingsverantwoordelijke' en 'verwerker'.[4] Verder heeft de Autoriteit Persoonsgegevens op haar website aanvullende Q&A's over dit onder gepubliceerd en de 'Voorbeeldlijst: verwerker of verwerkingsverantwoordelijke?'.[5] Ook biedt de Handleiding Algemene Verordening Gegevensbescherming van het Ministerie van Justitie en Veiligheid nadere toelichting.[6]

1 Leonie van Sloten is advocaat bij Brinkhof te Amsterdam.

2 Voorbeelden van guidelines die de EDPB wél heeft bekrachtigd van de Artikel 29 Werkgroep zijn de 'Guidelines on consent under Regulation 2016/679' (WP259) en 'Guidelines on transparency under Regulation 2016/679' (WP260). Een overzicht van alle 16 documenten die de EDPB heeft bekrachtigd staat weergegeven in 'Endorsement 1/2018' van 25 mei 2018.

3 Regulation (EU) 2018/1725.

4 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725', 7 November 2019.

5 Autoriteit Persoonsgegevens, 'Voorbeeldlijst: verwerker of verwerkingsverantwoordelijke?', zoals gepubliceerd op 18 september 2019. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldlijst_verwerkers_def.pdf.

6 Zie in het bijzonder paragraaf 3.5 'Ben ik verwerkingsverantwoordelijke, of ben ik verwerker?'. Raadpleegbaar via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming/Handleiding%E2%80%8B+Algemene+verordening+gegevensbescherming.pdf.

2. Gezamenlijke verwerkingsverantwoordelijkheid

Er zijn verschillende varianten van rolverdelingen tussen partijen mogelijk voor de verwerking van persoonsgegevens. Verwerkingsverantwoordelijken verstrekken persoonsgegevens niet uitsluitend aan verwerkers, maar kunnen ook persoonsgegevens aan derden verstrekken of met derden uitwisselen, welke derden deze gegevens vervolgens voor eigen doeleinden gebruiken (als derde-verantwoordelijke of *co-controller*). Daarnaast kunnen verwerkingsverantwoordelijken persoonsgegevens verstrekken aan, ontvangen of anderszins verwerken van een of meer andere verwerkingsverantwoordelijken voor (gedeeltelijk) gezamenlijke doeleinden.

Als twee of meer verwerkingsverantwoordelijken gezamenlijk doelen en middelen bepalen van de verwerking van persoonsgegevens, zijn zij gezamenlijke verwerkingsverantwoordelijken (*joint controllers*) aldus artikel 26 AVG. Gezamenlijke verantwoordelijkheid bestond al onder de Wbp (blijkens de definitie van de 'verantwoordelijke'), maar sinds de AVG is hiervoor meer aandacht gekomen.

Reden hiervoor is in de eerste plaats dat de AVG een specifieke verplichting in het leven heeft geroepen voor gezamenlijk verwerkingsverantwoordelijken in artikel 26 AVG: zij zijn verplicht om op transparante wijze hun respectievelijke verantwoordelijkheden om te voldoen aan de AVG vast te stellen in een "onderlinge regeling", vooral wat betreft de uitoefening van de rechten van betrokkene, waar ook informatieverstrekking over de gegevensverwerking onder valt. Uit deze onderlinge regeling moet blijken welke rol ieder van de gezamenlijk verwerkingsverantwoordelijken vervult en wat ieders verhouding is met de betrokkene. De afspraken die de gezamenlijke verwerkingsverantwoordelijken maken over de uitoefening van de rechten van betrokkenen belet de betrokkene overigens niet om zijn/haar privacy-rechten uit te oefenen jegens ieder van de verwerkingsverantwoordelijken. Verder moet "de wezenlijke inhoud" van de regeling aan de betrokkenen beschikbaar worden gesteld. Deze kan bijvoorbeeld worden opgenomen in een privacyverklaring. Een onderlinge regeling hoeft overigens niet te worden bepaald indien de verantwoordelijkheden al volledig zijn vastgesteld in toepasselijk EU-recht of het recht van een EU-land.

In de tweede plaats is er meer aandacht voor gezamenlijke verwerkingsverantwoordelijkheid door drie recente uitspraken van het Hof van Justitie van de Europese Unie (*Wirtsschaftsakademie*[7], *Jehovan todistajat*[8] en *Fashion ID*[9]). Uit deze uitspraken blijkt dat partijen die persoonsgegevens delen in het kader van een zekere samenwerking en met een zeker belang bij de verwerking (onverwacht) kunnen kwalificeren als 'gezamenlijke verwerkingsverantwoordelijken', ook als een van de verwerkingsverantwoordelijken veel minder invloed kan uitoefenen op de gegevensverwerking dan de andere.[10] In *Wirtsschaftsakademie* bepaalde het Hof - onder de voormalige EU Privacyrichtlijn - dat een beheerder van een fanpagina op Facebook gezamenlijk verantwoordelijk is met Facebook voor de verwerking van persoonsgegevens. Daarbij gaf het Hof te kennen dat voor de kwalificatie van verwerkingsverantwoordelijke het niet noodzakelijk is dat deze toegang heeft tot de persoonsgegevens. In *Jehovan todistajat* bepaalde het Hof dat de geloofsgemeenschap gezamenlijk verwerkingsverantwoordelijke is voor aantekeningen die leden maken en bewaren na huisbezoeken voor het verkondigen van het geloof. Tot deze conclusie kwam het Hof ondanks dat de gemeenschap zelf geen toegang had tot de aantekeningen of geen instructies daartoe had gegeven. Vervolgens oordeelde het Hof in *Fashion ID* – ditmaal onder de voormalige EU Privacyrichtlijn maar met oog voor de AVG – dat de beheerder van een website die een Facebook plug-in invoegt waardoor de browser van websitebezoekers persoonsgegevens van bezoekers doorzendt naar Facebook, gezamenlijk met Facebook verwerkingsverantwoordelijke is. Volgens het Hof was de verantwoordelijkheid van de beheerder wel beperkt tot de verwerking waarvan de beheerder daadwerkelijk doel en middelen vaststelt, dus enkel het verzamelen en doorzenden van de persoonsgegevens.

Toezichthouders kunnen bovendien bij vaststelling van 'gezamenlijke verantwoordelijkheid' aan meerdere (rechts) personen een boete opleggen wegens schending van de AVG. De Autoriteit Persoonsgegevens (AP) heeft dit al gedaan in het boetebesluit aan Uber. De AP stelde vast dat Uber BV en Uber Technologies, Inc. gezamenlijke verwerkingsverantwoordelijken waren voor het niet-tijdig melden van een datalek en ieder hoofdelijk aansprakelijk voor de boete van € 600.000.[11] Hoewel in de bewerkersovereenkomst de zeggenschap was neergelegd bij Uber BV, constateerde de AP dat beide rechtspersonen feitelijke invloed hadden op de verwerking gelet op o.a. de gezamenlijke vaststelling van het doel van de gegevensverwerking, vaststelling van het informatiebeveiligingsbeleid, beslissingen over opslag van de gegevens en de ontwikkeling en het aanbieden van de Uber-app alsmede het uitvoeren van updates.

3. Gevolgen van de rollen voor contractering

Als persoonsgegevens door een verwerker worden verwerkt, moeten er bindende afspraken worden gemaakt – doorgaans in de vorm van een verwerkingsovereenkomst – tussen de verwerkingsverantwoordelijke en de verwerker. Daarin wordt afgesproken dat de verwerker uitsluitend persoonsgegevens mag verwerken op instructie van de

7 Arrest van het Hof van Justitie van de EU (Grote kamer) van 5 juni 2018 in de zaak C-210/16 (ECLI:EU:C:2018:388).

8 Arrest van het Hof van Justitie van de EU (Grote kamer) van 10 juli 2018 in de zaak C-25/17 (ECLI:EU:C:2018:551).

9 Arrest van het Hof van Justitie van de EU (Tweede kamer) van 29 juli 2019 in de zaak C-40/17 (ECLI:EU:C:2019:629).

10 Zie verder ook de opmerking van de EDPS in haar Guidelines met verwijzing naar Fashion ID: "*a general level of complementarity and unity of purpose could already trigger a situation of joint controllership, if the purposes and (essential elements of the) means of the processing operations are jointly determined*" (EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725', pagina 23).

11 Autoriteit Persoonsgegevens, Boetebesluit Uber. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_uber.pdf.

verwerkingsverantwoordelijke. In artikel 28 lid 3 AVG staat opgesomd welke andere afspraken partijen ten minste verplicht zijn te maken over o.a. vertrouwelijkheid, technische en organisatorische maatregelen en het melden van datalekken, teruggave of verwijdering van persoonsgegevens en audits. De AVG omvat meer vereisten dan de Wbp dat deed. Het kan wenselijk zijn om aanvullende afspraken te maken, bijvoorbeeld omtrent medewerking aan *data protection impact assessments* (DPIA's), de uitoefening van rechten van betrokkenen of aansprakelijkheid. Op de verwerker rust de wettelijke verplichting om geen andere (sub)verwerker in dienst te nemen zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke (artikel 28 lid 2 AVG). Deze toestemming kan indien nodig ook in de verwerkersovereenkomst worden geregeld. Als een verwerker een (sub)verwerker inschakelt, is bovendien een sub-verwerkingsovereenkomst verplicht (art. 28 lid 4 AVG).

Als persoonsgegevens door gezamenlijk verantwoordelijken worden verwerkt is tussen hen geen verwerkingsovereenkomst nodig of gewenst, maar is enkel een "onderlinge regeling" vereist. Indien sprake is van veel partijen, kan dit enige administratieve verlichting bieden. Hoewel geen formele vereisten gelden, is het wel aan te raden om de onderlinge regeling op schrift te stellen. Afhankelijk van de complexiteit van de samenwerking, kan deze onderlinge regeling in een overeenkomst of in een bepaling worden gevat. Belangrijk is om hierin aan te geven waar specifiek de gezamenlijke verantwoordelijkheid op ziet. Verder kunnen aanvullende afspraken worden gemaakt bijvoorbeeld over wat te doen bij datalekken, uitvoering van DPIA's, inschakelen van verwerkers, schadeclaims van betrokkenen of handhaving door toezichthouders. Partijen zullen niet altijd happig zijn om gezamenlijke verantwoordelijkheid aan te nemen omdat zij vrezen dat zij (in eerste instantie) ook aansprakelijk kunnen worden gehouden voor boetes en schade bij een eventuele schending van de AVG door hun partners. Gelet op *Fashion ID* brengt gezamenlijke verantwoordelijkheid echter niet gelijkwaardige verantwoordelijkheid met zich mee.

Voor zover uw organisatie persoonsgegevens verwerkt in samenwerking met derde partijen, kan het verstandig zijn om een herbeoordeling te maken of uw organisatie tezamen met deze partijen kan worden beschouwd als 'gezamenlijk verwerkingsverantwoordelijken'. Als daarvan sprake is, moeten partijen alsnog zorgen voor een onderlinge regeling, eventueel eerder tussen hen overeengekomen verwerkingsovereenkomsten beëindigen en relevante AVG-documentatie updaten (zoals de privacyverklaring, de procedure voor de uitoefening van de rechten van betrokkenen, etc.).