De bewerkersovereenkomst onder de AVG

Een redelijke verdeling van risico's

Tineke van de Bunt & Anke Strijbos[1]

Dit artikel neemt de overeenkomst tussen de bewerker en de verantwoordelijke met betrekking tot de verwerking van persoonsgegevens door de bewerker, de bewerkersovereenkomst, onder de loep. Doel is om te beoordelen of er aanleiding bestaat om de standaarden die nu vaak gebruikt worden te herzien in verband met de inwerkingtreding van de AVG. In kaart wordt gebracht welke verplichtingen er gaan gelden voor de bewerker, en welke aansprakelijkheidsrisico's voor de bewerker enerzijds en de verantwoordelijke anderzijds. Aan de hand daarvan worden enkele manieren besproken waarop de aansprakelijkheid tussen bewerker en verantwoordelijke contractueel geregeld kan worden, met name door vrijwaringen en aansprakelijkheidsbeperkingen. Ook worden enkele suggesties gedaan om tot een uitgebalanceerde afspraak te komen tussen bewerker en verantwoordelijke.

Inleiding

Op 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van toepassing.[2] Naast de verandering in de benaming (van bewerker naar verwerker en van verantwoordelijke naar verwerkingsverantwoordelijke)[3] brengt de AVG ook veel veranderingen mee in de juridische relatie tussen bewerker en verantwoordelijke. Waar de bewerker onder de Privacyrichtlijn,[4] geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp), eigenlijk alleen maar verplicht was om de gegevens niet verder of anders te gebruiken dan conform de instructies van de verantwoordelijke, en om daarbij beveiligingsvoorschriften in acht te nemen (die in een overeenkomst moeten worden vastgelegd), geldt een belangrijk deel van de materiële verplichtingen in de AVG nu net zozeer voor de bewerker als voor de verantwoordelijke. Door de zeer hoge boetes die onder de AVG opgelegd kunnen worden aan zowel de bewerker als de verantwoordelijke wordt het bovendien van groot belang voor partijen om hun verantwoordelijkheden en aansprakelijkheden over en weer goed vast te leggen. Dat betekent dat het tijd is om de overeenkomst tussen de bewerker en de verantwoordelijke met betrekking tot de verwerking van persoonsgegevens door de bewerker, de bewerkersovereenkomst,[5] eens goed onder de loep te nemen om te beoordelen of er aanleiding bestaat om de standaarden die nu vaak gebruikt worden te herzien.

In dit artikel brengen wij in kaart welke verplichtingen er op grond van de AVG gaan gelden voor de bewerker, en welke aansprakelijkheidsrisico's er gelden voor de

Auteurs

1. Mr. C.A.M. van de Bunt is advocaat bij Vondst te Amsterdam, mr. A. Strijbos is advocaat bij Brinkhof te Amsterdam.

Noten

2. Verordening 2016/679/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

3. Wij gebruiken in dit artikel steeds de benamingen bewerker en verantwoordelijke, omdat dit naar nu geldend recht de juiste benamingen zijn.

4. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PB* L 281 van 23/11/1995, p. 0031-0050.

5. Het begrip bewerkersovereenkomst komt niet uit de Privacyrichtlijn of de Wbp, maar is een veel gebruikte aanduiding van de overeenkomst die de verantwoordelijke op grond van de Privacyrichtlijn en Wbp met de bewerker moet sluiten voor de uitvoering van verwerkingen door de bewerker. Strikt genomen zou de bewerkersovereenkomst na inwerkingtreding van de AVG een verwerkersovereenkomst moeten gaan heten, maar ook in de AVG komt de term verwerkersovereenkomst niet voor. Omwille van de leesbaarheid hebben we ervoor gekozen om in dit artikel nog de term bewerkersovereenkomst te blijven gebruiken.

bewerker enerzijds en de verantwoordelijke anderzijds, zowel als gevolg van handhaving van toezichthouders als van civiele claims van betrokkenen.[6] Aan de hand daarvan zullen wij enkele manieren bespreken waarop de aansprakelijkheid tussen bewerker en verantwoordelijke contractueel geregeld kan worden, met name door vrijwaringen en aansprakelijkheidsbeperkingen. In dit kader doen wij ook enkele suggesties om tot een uitgebalanceerde afspraak te komen tussen bewerker en verantwoordelijke.

De AVG heeft een veel groter territoriaal toepassingsgebied dan de Privacyrichtlijn en de Wbp hadden

Het is daarbij goed om te signaleren dat de AVG een veel groter territoriaal toepassingsgebied heeft dan de Privacyrichtlijn en de Wbp hadden. De AVG is namelijk ook van toepassing op bewerkers en verantwoordelijken die niet in de EU gevestigd zijn, bijvoorbeeld als zij goederen of diensten aanbieden aan betrokkenen in de EU of hun gedrag monitoren, ongeacht of zij hiervoor middelen zoals datacenters of verkoopkantoren in de EU gebruiken (artikel 3 lid 2 AVG). Bedrijven uit onder meer Amerika en Azië die goederen of diensten aanbieden in de EU zullen dus in de meeste gevallen met de AVG te maken krijgen. Mede hierdoor staat de AVG ook buiten de EU op de agenda, wat het voor Europese bedrijven vaak gemakkelijker maakt om hun buiten de EU gevestigde contractspartijen te bewegen tot het sluiten van een bewerkersovereenkomst.

De verplichtingen van de bewerker onder de Wbp en AVG

De Wbp bevat veel verplichtingen voor de verantwoordelijke, maar slechts twee expliciete verplichtingen voor de bewerker. Op grond van artikel 12 Wbp mogen bewerkers alleen handelen in opdracht van de verantwoordelijke en zijn zij gebonden aan geheimhouding. Daarnaast schrijft de Wbp in zijn algemeenheid voor dat er een bewerkersovereenkomst moet gelden tussen de bewerker en de verantwoordelijke (artikel 14 lid 2 Wbp). Daarin kan tenminste een gezamenlijke verplichting van verantwoordelijke en bewerker worden gelezen om zo'n overeenkomst aan te gaan. Bij het ontbreken van die overeenkomst loopt de bewerker bovendien het risico om zelf als verantwoordelijke te worden aangemerkt omdat er dan geen duidelijke instructies gelden, met alle wettelijke verplichtingen die dat meebrengt.

> NB. Ook als de bewerker gedurende de relatie met de verantwoordelijke bepaalde verantwoordelijkheden met betrekking tot de persoonsgegevens naar zich toetrekt of opgelegd krijgt, kan de bewerker 'van kleur verschieten' en voor deze verwerkingen een verantwoordelijke worden. Voor die verwerkingen geldt de bewerkersovereenkomst dan niet en dient de bewerker zelf te voldoen aan de kernverplichtingen van de verantwoordelijke, zoals het informeren van de betrokkenen en het hebben van een deugdelijke grondslag voor de gegevensverwerking.

Onder de AVG blijven voor de bewerker grofweg dezelfde verplichtingen gelden die op grond van de Wbp al golden (artikel 28, 29 en 32 AVG), maar deze worden aangevuld met een arsenaal aan nieuwe verplichtingen.

Veel van de nieuwe verplichtingen voor de bewerker komen wellicht bekend voor. Het zijn namelijk verplichtingen die op dit moment in de praktijk al in bewerkersovereenkomsten plegen te worden opgenomen.[7] Het gaat dan bijvoorbeeld om de verplichtingen voor bewerkers om medewerking te verlenen aan de verantwoordelijke in geval van een verzoek van een betrokkene (artikel 28 lid 3 sub e AVG), om aan de verantwoordelijke alle informatie ter beschikking te stellen en alle medewerking te verlenen die nodig is om hun nakoming van de AVG aan te tonen, waaronder het meewerken aan audits (artikel 28 lid 3 sub h AVG), en om geen sub-bewerkers in te schakelen zonder toestemming van de verantwoordelijke (artikel 28 lid 2 en 4 AVG).

Andere AVG-verplichtingen voor de bewerker zijn echt nieuw, zoals de verplichting voor bewerkers om een vertegenwoordiger aan te wijzen als zij geen vestiging hebben in de EU (artikel 27 AVG) en om in bepaalde gevallen een functionaris voor de gegevensbescherming aan te stellen (artikel 37 AVG).

De verschillende actoren met betrekking tot persoonsgegevens

De Wet bescherming persoonsgegevens onderscheidt drie relevante actoren: de betrokkene, de verantwoordelijke en de bewerker.

De betrokkene is de natuurlijke persoon waar de persoonsgegevens betrekking op hebben. Persoonsgegevens gáán over de betrokkene.

De verantwoordelijke en de bewerker zijn natuurlijke personen, rechtspersonen of bestuursorganen die persoonsgegevens gebruiken. De verantwoordelijke is degene die het doel en de middelen van dat gebruik bepaalt. Hij gebruikt de gegevens in beginsel voor zichzelf. De bewerker is degene die de gegevens gebruikt ten behoeve van de verantwoordelijke. Hij handelt steeds in opdracht van de verantwoordelijke.
Ter illustratie: als een webshop een hosting provider opdracht geeft om zijn klantgegevens op te slaan, zal de webshop voor dit gebruik van deze persoonsgegevens worden aangemerkt als verantwoordelijke, en de hosting provider als bewerker.

Onder de AVG wordt de verantwoordelijke aangeduid als verwerkingsverantwoordelijke, en de bewerker als verwerker.

Omdat veel materiële bepalingen van de AVG gelden voor zowel de bewerker als de verantwoordelijke, wordt het voor de bewerker moeilijker om zich nog langer te verschuilen achter (de instructies van) de verantwoordelijke. De bewerker is zelfs verplicht om het de verantwoordelijke te melden als hij van mening is dat een instructie van de verantwoordelijke in strijd is met de AVG (artikel 28 lid 3 sub h AVG).

Risico op boetes en aansprakelijkheid onder de Wbp en AVG

De hierboven omschreven toename van verplichtingen en verantwoordelijkheden voor bewerkers heeft gevolgen voor de positie van zowel de bewerker als de verantwoordelijke. Daarnaast wordt de positie van beide partijen beïnvloed door het risico op hogere boetes onder de AVG, en door het daarin opgenomen aansprakelijkheidsregime.

Positie bewerker

De aansprakelijkheidspositie van bewerkers is nu geregeld in artikel 49 Wbp. Kort gezegd kan de bewerker aansprakelijk worden gesteld voor schade of nadeel als gevolg van niet-nakoming van zijn verplichtingen onder de Wbp, voor zover deze schade of dit nadeel ontstaat door zijn werkzaamheden. De bewerker heeft wel de mogelijkheid om aan de aansprakelijkheid te ontkomen, namelijk als hij kan bewijzen dat de schade of het nadeel niet aan hem kan worden toegerekend.[8]

Daarnaast loopt de bewerker een risico op bestuursdwang, dwangsommen en bestuurlijke boetes opgelegd door de Autoriteit Persoonsgegevens (AP) bij overtreding van de kernverplichtingen van de bewerker (artikel 65 en 66 lid 2 jo. 12 Wbp). De bestuurlijke boete kan oplopen tot€ 820 000,[9] of, voor rechtspersonen, ten hoogste 10% van de jaaromzet van de bewerker in het boekjaar voorafgaande aan het besluit waarbij de bestuurlijke boete wordt opgelegd.[10]

Overigens geldt dat in het geval bewerkers buiten de instructies van de verantwoordelijke handelen, zij zelf als verantwoordelijke zullen kwalificeren. Bewerkers lopen in dat geval dus een aanvullend risico op bestuursdwang, dwangsommen en bestuurlijke boetes als zij de handelingen niet conform alle voor de verantwoordelijke geldende verplichtingen uit de Wbp uitvoeren.

De opzet van de aansprakelijkheidsregeling in de AVG is gelijk aan die van de Wbp (artikel 82 lid 2 en 3 AVG). De reikwijdte van deze aansprakelijkheidsbepaling is echter veel groter, nu de AVG (veel) meer verplichtingen aan de bewerker oplegt. Wat betreft de bestuurlijke handhaving geldt dat de maximale boete onder de AVG veel hoger wordt. Op grond van artikel 83 AVG kan de boete oplopen tot € 20 000 000 of, voor rechtspersonen, 4% van de totale wereldwijde omzet van het concern waartoe de rechtspersoon behoorde in het voorgaande boekjaar.

© Luciano Lozano / Alamy

Positie verantwoordelijke

In verband met de verdeling van risico's tussen de bewerker en de verantwoordelijke is uiteraard ook het risico van de verantwoordelijke op bestuursrechtelijke handhaving en civiele aansprakelijkheid relevant.

De aansprakelijkheidspositie van de verantwoordelijke is nu ook geregeld in artikel 49 Wbp. De verantwoorde-

6. In dit artikel zullen wij niet ingaan op de situatie waarbij meerdere verantwoordelijken en/of verwerkers betrokken zijn bij een verwerking en de gevolgen daarvan op de onderlinge verdeling van aansprakelijkheid.

7. Dit zal in Nederland mede zijn ingegeven door de CBP Richtsnoeren beveiliging van persoonsgegevens, februari 2013, par. 4.2, waarin de toezichthouder de uitgangspunten schetst die zij gebruikt om te beoordelen of een bewerkersovereenkomst voldoet aan de Wbp. De richtsnoeren zijn beschikbaar via: www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.

8. Betoogd kan worden dat de aansprakelijkheid van bewerkers onder de Wbp verder gaat dan de verplichtingen die expliciet aan hem zijn opgelegd in art. 12 en 14 Wbp. Volgens de memorie van toelichting bij de Wbp moet art. 49 lid 3 Wbp zo worden uitgelegd dat bewerkers zelfstandig aansprakelijk zijn voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegeven die zijn neergelegd in hoofdstuk 1 en 2 van de Wbp (de algemene bepalingen en de beginselen betreffende de rechtmatigheid van de gegevensverwerking). Als de bewerker zijn werkzaamheden uitvoert conform de instructies van de verantwoordelijke, zou dit volgens de memorie van toelichting onvoldoende zijn om elk risico op aansprakelijk weg te nemen (*Kamerstukken II* 1997/98, 25892, 3, p. 62).
In de praktijk richt de AP haar handhaving met name op verantwoordelijken.

9. Besluit van 10 november 2015 tot wijziging van de bedragen van de categorieën, bedoeld in art. 23 lid 4 van het Wetboek van Strafrecht (*Stb.* 2015, 420).

10. Zie voor de concrete invulling voor het AP de Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015, zoals laatstelijk gewijzigd op 6 juli 2016, met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016).

lijke kan aansprakelijk worden gesteld voor schade of nadeel als gevolg van niet-nakoming van zijn verplichtingen onder de Wbp, tenzij hij bewijst dat de schade hem niet kan worden toegerekend. Daarnaast loopt de verantwoordelijke een risico op bestuursdwang, dwangsommen en bestuurlijke boetes opgelegd door de AP en strafrechtelijke sancties bij overtreding van zijn verplichtingen op grond van de Wbp (artikel 65, 66 en 75 Wbp).

De aansprakelijkheidspositie van de verantwoordelijke blijft onder de AVG gelijk (artikel 82 lid 2 en 3 AVG). Wat betreft de bestuurlijke handhaving geldt voor de verantwoordelijke, net als voor de bewerker, dat de bestuurlijke boete die de AP kan opleggen substantieel zal toenemen.

Verdeling van risico's in bewerkersovereenkomsten

Status quo

De Wbp en de AVG verbieden verantwoordelijken en bewerkers in beginsel niet om onderling afspraken te maken over de verdeling van aansprakelijkheids- en boeterisico's.[11] Er heerst echter nog verwarring over de vraag of artikel 82 lid 5 AVG de vrijheid van partijen tot het maken van onderlinge afspraken over het daar specifiek geregelde geval beoogt te beperken.[12] Onderlinge afspraken tussen bewerkers en verantwoordelijken hebben in ieder geval geen externe werking. Betrokkenen of toezichthouders hoeven zich daar dus niets van aan te trekken.

Tot voor kort was het in de praktijk gebruikelijk dat verantwoordelijken en bewerkers onbeperkte aansprakelijkheid accepteerden voor schade als gevolg van schending van de contractuele afspraken over de verwerking van persoonsgegevens. Partijen maakten ook regelmatig gebruik van een vrijwaring, waarbij de bewerker de verantwoordelijke vrijwaarde voor alle vorderingen, schade, kosten en boetes als gevolg van de verwerking van persoonsgegevens door de bewerker.

Sinds de invoering van de boetebevoegdheid van de AP per 1 januari 2016 is deze praktijk onder druk komen te staan. We verwachten dat deze praktijk onder de AVG verder onder druk zal komen te staan, vanwege het grotere risico op overtredingen door de bewerker en de verdere verhoging van de maximale boetes onder de AVG. Bovendien zullen er meer gevallen zijn waarin zowel de verantwoordelijke als de bewerker beboet kunnen worden.

Denk bijvoorbeeld aan het geval dat er een datalek heeft plaatsgevonden als gevolg van onvoldoende beveiliging van persoonsgegevens door de bewerker. De AP zou dan in sommige gevallen aan zowel de verantwoordelijke als de bewerker een boete kunnen opleggen. Een onbeperkte aansprakelijkheid en/of een vrijwaring namens de bewerker zou er dan toe kunnen leiden dat de bewerker niet alleen zijn eigen boete moet betalen, maar ook de boete van de verantwoordelijke. Dit kan voor de bewerker wrang uitpakken, omdat de maximale boete onder de AVG geen vast bedrag is, maar een bedrag dat gerelateerd is aan de wereldwijde jaaromzet van het concern van de verantwoordelijke. Stel, de bewerker in kwestie is een start-up die een HR-oplossing in de cloud aanbiedt en de verantwoordelijke is een grote multinational die deze HR-oplossing afneemt. De (maximale) boete van de verantwoordelijke wordt in dat geval gerelateerd aan de (hoge) internationale jaaromzet van de multinational, en kan enorm hoog uitpakken. De start-up die als gevolg van de contractuele afspraken opdraait voor deze boete van zijn opdrachtgever zal een dergelijke hoge boete niet kunnen dragen, zeker niet

Verplichtingen voor bewerkers op basis van de AVG

- Bewerkers die geen vestiging hebben in de EU moeten een vertegenwoordiger aanwijzen (artikel 27 AVG).
- Bewerkers moeten de verwerkingsverantwoordelijke onmiddellijk in kennis stellen indien naar hun mening een instructie in strijd is met de wet (artikel 28 lid 3 sub a AVG)
- Bewerkers zijn verplicht medewerking te verlenen aan de verantwoordelijke in geval van een verzoek van een betrokkene (artikel 28 lid 3 sub e AVG)
- Bewerkers moeten de verantwoordelijke ondersteunen bij het eventueel uitvoeren van een voorafgaande raadpleging van de toezichthouder of een gegevensbeschermingseffectenbeoordeling (artikel 28 lid 3 sub f AVG)
- Bewerkers dienen de persoonsgegevens na de voltooiing van de verwerking ten behoeve van de verantwoordelijke terug te geven of te wissen (artikel 28 lid 3 sub g AVG)
- Bewerkers dienen de verantwoordelijke alle informatie ter beschikking te stellen en alle medewerking te verlenen die nodig is om hun nakoming van de AVG aan te tonen, waaronder het meewerken aan audits (artikel 28 lid 3 sub h AVG)
- Bewerkers mogen geen sub-bewerkers inschakelen zonder toestemming van de verantwoordelijke. Als er sub-bewerkers worden ingeschakeld, blijft de eerste bewerker verantwoordelijk voor het nakomen van zijn verplichtingen jegens de verantwoordelijke (artikel 28 lid 2 en 4 AVG)
- Bewerkers zijn verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die zij verwerken in opdracht van de verantwoordelijke (artikel 30 lid 2 AVG)
- Bewerkers zijn verplicht medewerking te verlenen aan een verzoek van de toezichthouder (artikel 31 AVG)
- Zodra bewerkers kennis hebben gekregen van een datalek, dienen zij de verantwoordelijke zonder onredelijke vertraging op de hoogte te stellen van het datalek (artikel 33 lid 2 AVG)
- Bewerkers dienen in bepaalde gevallen zelf een functionaris voor de gegevensbescherming aan te stellen (artikel 37 AVG).
- Bewerkers mogen persoonsgegevens alleen buiten de EER doorgeven als dat in overeenstemming is met de strenge bepalingen daarover in de AVG (artikel 44 AVG).

Om te voorkomen dat deze super cap een wassen neus is, is het van belang om daarnaast duidelijk op te nemen voor welke schadesoorten aansprakelijkheid al dan niet wordt uitgesloten

naast zijn eigen (maximale) boete. De overeengekomen onbeperkte aansprakelijkheid en/of een vrijwaring kan er op die manier voor zorgen dat de start-up omvalt. Deze uitkomst is onwenselijk voor beide partijen. Voor de opdrachtgever heeft dit immers grote gevolgen voor de continuïteit van de dienstverlening.

> NB. In dit voorbeeld wordt de boete veroorzaakt door een schending van een verplichting door de bewerker, die niet door de verantwoordelijke is veroorzaakt. Het is echter ook denkbaar dat een boete of schade wordt veroorzaakt door 1. een schending door de verantwoordelijke, die niet door de bewerker wordt veroorzaakt, 2. een schending door de bewerker, die het gevolg is van de instructies van de verantwoordelijke, of 3. een schending die in meer of mindere mate te wijten is aan beide partijen. In die gevallen speelt een vergelijkbare problematiek en ook voor die gevallen dient de bewerkersovereenkomst een heldere verdeling van aansprakelijkheid te bevatten. De mogelijkheden die wij hierna bespreken zijn ook bruikbaar voor de hier genoemde gevallen.

In de volgende paragraaf zullen wij een aantal mogelijkheden schetsen voor een gebalanceerde(re) verdeling van risico's tussen verantwoordelijken en bewerkers in de bewerkersovereenkomst. Deze mogelijkheden kunnen verwerkt worden in de bewerkersovereenkomst zelf en/of de (hoofd)overeenkomst tussen de opdrachtgever en de leverancier voor de levering of ontwikkeling van diensten of producten, waarvan de bewerkersovereenkomst doorgaans onderdeel zal uitmaken. Daarbij is van belang dat beide overeenkomsten goed op elkaar worden afgestemd, om te voorkomen dat de standaardregelingen in de hoofdovereenkomst over aansprakelijkheid en overmacht afbreuk doen aan eventuele specifieke regelingen die partijen in de bewerkersovereenkomst hebben afgesproken.

Mogelijkheden voor een redelijke risicoverdeling

Beperking van aansprakelijkheid

Zoals uit het hierboven genoemde voorbeeld blijkt, kan de inwerkingtreding van de AVG er voor zorgen dat een onbeperkte aansprakelijkheid en/of vrijwaring onwenselijke gevolgen heeft, met name als de omvang van bewerker en verantwoordelijke substantieel verschilt. Een mogelijkheid om de risico's in een dergelijk geval redelijker te verdelen, zou kunnen zijn dat er voor schending van wettelijke en contractuele regels in de context van bescherming van persoonsgegevens wordt afgesproken dat er een aparte, hogere aansprakelijkheidslimiet geldt naast of in aanvulling op een standaard aansprakelijkheidslimiet die partijen zijn overeengekomen. De hoogte van een dergelijke 'super cap' kan worden gerelateerd aan de volgende factoren:

- de omzet van de aansprakelijke partij;
- de hoogte van een eventuele boete die aan de aansprakelijke of de gelaedeerde partij wordt opgelegd; en/of
- de contractwaarde.

Partijen kunnen de bovengenoemde factoren ook combineren. Denkbaar is bijvoorbeeld dat de super cap wordt bepaald op het hoogste bedrag van de volgende bedragen: 1. drie keer de totale vergoeding die verschuldigd is in een bepaald contractjaar en 2. de omzet van de aansprakelijke partij in een bepaald contractjaar. Ook is denkbaar dat een aparte super cap wordt opgenomen voor boetes, die wordt bepaald op het bedrag van de maximale boete die aan de aansprakelijke partij kan worden opgelegd.

Om te voorkomen dat deze super cap een wassen neus is, is het van belang om daarnaast duidelijk op te nemen voor welke schadesoorten aansprakelijkheid al dan niet wordt uitgesloten. Denk bijvoorbeeld aan reputatieschade als gevolg van negatieve publiciteit bij een onderzoek of boete van een toezichthouder. Deze schade kan in sommige gevallen nog hoger uitpakken dan de boete of dwangsom die de toezichthouder oplegt, maar wordt in overeenkomsten doorgaans uitgesloten als 'indirecte of gevolgschade'.

Denk, als verantwoordelijke, ook aan schade als gevolg van verlies of corruptie van data. Deze schadesoort wordt door bewerkers steeds vaker aangemerkt als vorm van indirecte schade. Ook zien wij in de praktijk een enkele keer dat bewerkers verlies of corruptie van data opnemen als voorbeeld van een overmachtssituatie. Hoewel het niet helemaal duidelijk is wat onder verlies of corruptie van data moet worden verstaan, bestaat het risico dat dergelijke bepalingen zo worden uitgelegd dat deze feitelijk neerkomen op een inperking van de aansprakelijkheid van de bewerker voor aansprakelijkheid in verband met de verwerking van persoonsgegevens. Dit zou bijvoorbeeld

11. De contractsvrijheid van partijen wordt wel beperkt in het geval dat een van de partijen gevestigd is in een land buiten de EER en partijen de doorgifte van persoonsgegevens buiten de EER willen legitimeren door gebruikmaking van de EU Model Clauses. De EU Model Clauses bevatten namelijk een standaard aansprakelijkheidsbepaling en een optionele vrijwaringsbepaling. Partijen kunnen hier wel van afwijken, maar dit wordt over het algemeen als onwenselijk beschouwd. Partijen dienen bij het aanpassen van de EU Model Clauses namelijk alsnog een vergunning voor de doorgifte te verkrijgen.

12. Art. 82 lid 5 AVG zou zo kunnen worden geïnterpreteerd dat het de mogelijkheid voor verantwoordelijken en bewerkers beperkt om onderling hun aansprakelijkheid specifiek voor schade van derden als gevolg van hun respectievelijke schending van de AVG geheel uit te sluiten.

het geval kunnen zijn in de situatie dat een medewerker van de bewerker een USB-stick of laptop met persoonsgegevens van de verantwoordelijke in de trein vergeet, waardoor data verloren gaan. Een dergelijk datalek kan leiden tot boetes of claims van derden.

Als gevolg van de hiervoor beschreven contractuele exoneraties kan een schending van de bewerker, die niet door de verantwoordelijke is veroorzaakt, alsnog voor risico van de verantwoordelijke komen. Als verantwoordelijke verdient het daarom de voorkeur om reputatieschade of schade als gevolg van verlies of corruptie van data niet klakkeloos op te nemen als voorbeelden van indirecte

Veel grote bewerkers, zoals bijvoorbeeld Google Apps en Amazon Web Services, zullen standaardvoorwaarden hebben waarover door kleine en middelgrote verantwoordelijken niet of nauwelijks te onderhandelen valt

schade (of als overmachtssituatie). Andersom is het uiteraard raadzaam dat ook de bewerker kritisch kijkt naar de uitgesloten schadesoorten.

Indien de beperking van aansprakelijkheid wordt gerelateerd aan de omzet van de aansprakelijke partij, zou dat in sommige gevallen kunnen betekenen dat een 'grote' opdrachtgever niet alle schade kan verhalen die deze opdrachtgever lijdt als gevolg van een fout van zijn 'kleine' leverancier. Om die situatie te voorkomen zou een dergelijke opdrachtgever er verstandig aan kunnen doen om zijn kleine leverancier contractueel te verplichten om zich deugdelijk te verzekeren voor risico's als gevolg van een schending van relevante privacywetgeving, en de cap te relateren aan het hoogste van de volgende twee bedragen: het bedrag dat de verzekeraar aan de leverancier uitkeert en het bedrag op basis van de super cap. Er zijn diverse verzekeraars die dergelijke verzekeringen tegen bijvoorbeeld datalekken en boetes van toezichthouders aanbieden. Deze contractuele verplichting biedt ook uitkomst wanneer een 'kleine' bewerker een groot aantal opdrachtgevers heeft en dus bij een incident dat alle opdrachtgevers treft een veelheid van claims kan verwachten. Ook in dit geval is de kans dat de bewerker alle schade kan dragen klein en kan een adequate verzekering voorkomen dat de bewerker ten onder gaat.

Vrijwaring

Om tot een gebalanceerde verdeling van risico's te komen, zouden verantwoordelijken en bewerkers allereerst – in afwijking van de voorheen gangbare praktijk – een wederkerige vrijwaring in hun overeenkomst kunnen opnemen. Een vrijwaring door de verantwoordelijke ondervangt bijvoorbeeld het risico op schade en boetes dat veroorzaakt wordt door een schending door de bewerker van de AVG als gevolg van de instructies van de verantwoordelijke. Vanuit het perspectief van de verantwoordelijke geldt daarbij als aandachtspunt dat deze vrijwaring niet te ruim wordt geformuleerd. Voorkomen moet worden dat de bewerker als gevolg van deze vrijwaring alle aansprakelijkheid ontloopt in een situatie waarin de bewerker zelf ook debet is aan de schade of boete. Met andere woorden: de vrijwaring moet niet zo ruim zijn geformuleerd dat de gevrijwaarde partij geen prikkel meer heeft om aan zijn verplichtingen te voldoen.

De suggestie die wij eerder bespraken met betrekking tot de super cap is vervolgens ook toepasbaar op de vrijwaringen over en weer. Een beroep op een vrijwaring kwalificeert als een nakomingsvordering en niet als vordering tot schadevergoeding, maar toch is het in de praktijk gebruikelijk om de aansprakelijkheidsbeperking(en)- en uitsluitingen ook van toepassing te verklaren op vrijwaringen.

Om tot een gebalanceerde verdeling van risico's te komen zouden partijen voorts kunnen bepalen dat de vrijwaring niet geldt als de gevrijwaarde partij zich op de vrijwaring beroept voor zover dat te wijten is aan zijn eigen schending van de overeenkomst of wet. Deze mogelijkheid komt er op neer dat partijen de eigen schuld regeling uit het BW van overeenkomstige toepassing verklaren op de vrijwaring, en is met name relevant vanuit het perspectief van de bewerker. Een bewerker zou hier een beroep op kunnen doen, in het geval dat bijvoorbeeld een boete rechtstreeks voortvloeit uit verwerkingen die aan hem zijn opgedragen door de verantwoordelijke, en die hij ook conform de schriftelijke instructies van de verantwoordelijke heeft uitgevoerd. Als er in een dergelijk geval bijvoorbeeld zowel aan de verantwoordelijke als aan de bewerker een boete wordt opgelegd, kan de uitkomst dat de bewerker geheel voor dit risico dient op te draaien onredelijk zijn. Deze mogelijkheid biedt ook uitkomst in situaties waarbij beide partijen steken hebben laten vallen, bijvoorbeeld de bewerker die een datalek veroorzaakt door tekortschietende beveiliging, maar dat wel tijdig bij de verantwoordelijke meldt, die vervolgens nalaat het op zijn beurt tijdig bij de toezichthouder te melden. Ook in zo'n situatie kan het onredelijk zijn om de bewerker geheel voor de boete van de verantwoordelijke te laten opdraaien, als deze boete door de toezichthouder is opgelegd wegens schending van de meldplicht.

Verder kunnen partijen voorwaarden opnemen waaraan moet worden voldaan voordat een beroep gedaan kan worden op de vrijwaring, zoals gebruikelijk is bij vrijwaringen in de context van inbreuken op de intellectuele eigendomsrechten. De vrijwarende partij zou bijvoorbeeld kunnen eisen dat de vordering van een betrokkene of een onderzoek of bindende aanwijzing van de toezichthouder onmiddellijk gemeld wordt, dat de afhandeling van de vordering, het onderzoek of de bindende aanwijzing door of in overleg met de vrijwarende partij wordt afgehandeld en dat geen erkenningen of andere uitlatingen worden gedaan met betrekking tot de relevante verwerkingsactiviteiten zonder de voorafgaande schriftelijke toestemming van vrijwarende partij.

Waarschuwingsverplichting
In het kader van zowel een vrijwaring als een beperking van aansprakelijkheid geldt dat het nuttig kan zijn om te bepalen dat de bewerker aan de bel moet trekken als hij van mening is dat bepaalde instructies van de verantwoordelijke in strijd zijn met de AVG. Als voorwaarde voor een beroep op de vrijwaring en/of de beperking van aansprakelijkheid zou daarom opgenomen kunnen worden dat de bewerker de verantwoordelijke waarschuwt als hij denkt dat dat het geval is. Waarschuwt de bewerker niet, dan kan hij geen beroep doen op de vrijwaring of beperking van aansprakelijkheid. Hij heeft dan zelf immers ook schuld aan de overtreding. Dit instrument zal in de praktijk lastig toe te passen zijn, omdat het voor een verantwoordelijke niet of nauwelijks mogelijk is om te bewijzen dat de bewerker zich er (tijdig) van bewust was dat een instructie in strijd was met de AVG. Omdat de AVG inmiddels in artikel 28 lid 3 sub h een dergelijke waarschuwingsplicht bevat, zal de praktijk in de komende jaren wellicht nadere handvatten bieden voor de invulling van de bewijsrechtelijke aspecten van de waarschuwingsplicht.

Regelen van materiële verplichtingen
Wij realiseren ons dat er allerlei redenen zijn waarom partijen niet tot een evenwichtige verdeling van risico's kunnen of willen komen met behulp van de door ons geschetste regelingen voor aansprakelijkheid en vrijwaringen. Veel grote bewerkers, zoals bijvoorbeeld Google Apps en Amazon Web Services, zullen standaardvoorwaarden hebben waarover door kleine en middelgrote verantwoordelijken niet of nauwelijks te onderhandelen valt.

Het is daarom juist in die situaties van belang om de kans dat er een incident plaatsvindt dat tot schade leidt zoveel mogelijk te verkleinen. Dat kunnen verantwoordelijken en bewerkers doen met behulp van heldere afspraken over het gebruik van persoonsgegevens en de verdeling van verantwoordelijkheden.

Voor beide partijen is het bijvoorbeeld van belang om afspraken te maken over dataminimalisatie (en dit is ook verplicht onder de AVG). Als de verantwoordelijke minder persoonsgegevens aan de bewerker verstrekt, verkleint dit de kans dat er iets mis gaat met de gegevens. Als de bewerker minder persoonsgegevens verkrijgt of zijn toegang tot persoonsgegevens beperkt is, is zijn kans om een misstap te begaan met betrekking tot persoonsgegevens vanzelfsprekend minder groot. De operationele maatregelen die getroffen kunnen worden, zullen sterk afhangen van het type werkzaamheden dat de bewerker verricht. Als de bewerker bijvoorbeeld software ontwikkelt voor de verantwoordelijke, verdient het de voorkeur af te spreken dat de bewerker de software zal testen met fictieve testdata in plaats van met echte persoonsgegevens. Partijen zouden de kans op een datalek kunnen voorkomen door persoonsgegevens alleen versleuteld te versturen en op te slaan. Partijen zouden daarnaast zoveel mogelijk geanonimiseerde of gepseudonimiseerde gegevens kunnen gebruiken.

Om risico's verder te beperken kunnen partijen een verplichting opnemen om elkaar te informeren over de manier waarop bepaalde verplichtingen uit de Wbp of AVG vormgegeven zijn en een recht om de overeenkomst te beëindigen indien er redelijke twijfel bestaat over de compliance van de andere partij.

Conclusie
De bewerkersovereenkomst is in veel gevallen bij uitstek een standaardovereenkomst waarbij gebruik wordt gemaakt van een template waar nauwelijks aan gesleuteld of over onderhandeld wordt. Veel bedrijven zullen in de inwerkingtreding van de AVG wel een reden zien om hun template bewerkersovereenkomst onder de loep te nemen, maar daarbij zal waarschijnlijk met name aandacht zijn voor de aanvullende eisen die de AVG stelt aan de inhoud van de bewerkersovereenkomst (artikel 28 lid 3 AVG). Omdat de opzet van de wettelijke regeling over de verdeling van aansprakelijkheid tussen de bewerker en de verantwoordelijke in de AVG niet verandert, zal men de aansprakelijkheidsclausule mogelijk over het hoofd zien. Dat terwijl de risico's voor zowel bewerker als verantwoordelijke en voor zowel kleine als grote ondernemingen substantieel anders zijn geworden en nog veel verder zullen veranderen als gevolg van de inwerkingtreding van de AVG.

In dit artikel hebben wij geprobeerd om een overzicht te geven van mogelijke regelingen ten aanzien van aansprakelijkheid die in de bewerkersovereenkomst kunnen worden opgenomen om die aansprakelijkheidsrisico's op een redelijke manier te verdelen. Er zijn verschillende knoppen waaraan partijen kunnen draaien om dit te bereiken, zoals vrijwaringen over en weer, super caps, schadeposten die al dan niet voor vergoeding in aanmerking komen, de invulling van het eigen schuld leerstuk, enz. Uiteraard vraagt elk geval om een eigen analyse en wij zijn ons er bovendien van bewust dat de creatieve jurist nog legio andere mogelijkheden zal kunnen bedenken om tot een adequate regeling te komen in een specifiek geval. •