DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

Privacy voorbij de richtlijn

Privacy ook uw zaak Wat betekent dat voor ondernemers?

De bestaande regels rondom de bescherming van persoonsgegevens worden aangescherpt met de invoering van de Algemene Verordening Gegevensbescherming. In deze whitepaper zijn de belangrijkste gevolgen voor ondernemers samengevat.

Whitepaper RWV Advocaten
M.M. Hoving 2016 ©

RWV ADVOCATEN

VAN RICHTLIJN NAAR VERORDENING

De Wet bescherming persoonsgegevens (Wbp) is momenteel het belangrijkste in Nederland geldende wettelijke kader voor verwerking van persoonsgegevens. De Wbp is tot stand gekomen op basis van de Europese 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 ('Privacyrichtlijn'). De Privacyrichtlijn heeft geleid tot een 'lappendeken' van nationale regelingen in de EU. De Europese Commissie heeft besloten om de regels voor verwerking van persoonsgegevens door de hele EU te uniformeren, door de richtlijn te vervangen door een verordening. Bij een verordening bestaat – in tegenstelling tot een richtlijn[1] – in beginsel geen vrijheid bij de implementatie in de lidstaten. In 2016 is overeenstemming bereikt over de Algemene Verordening Gegevensbescherming[2] ('AVG').

Voor internationaal opererende ondernemingen heeft de AVG uiteraard het voordeel dat de regels straks in alle Europese lidstaten grotendeels gelijkluidend zijn. Daar staat tegenover dat de verplichtingen in de AVG behoorlijk zijn uitgebreid ten opzichte van de Privacyrichtlijn en dat de sancties zijn aangescherpt. In deze whitepaper worden de belangrijkste veranderingen op een rij gezet.

Wanneer krijgt u met de verordening te maken?
De AVG wordt op 25 mei 2018 van toepassing.

Iedere onderneming verwerkt persoonsgegevens; persoonsgegevens van klanten en werknemers. Iedere organisatie krijgt dan ook te maken met de AVG. Het is verstandig om tijdig de gevolgen van de AVG voor uw organisatie in kaart te brengen.

> *"IEDERE ONDERNEMER VERWERKT PERSOONSGEGEVENS, DUS IEDERE ONDERNEMER KRIJGT TE MAKEN MET DE AVG"*

Wat gebeurt er als de AVG niet wordt nageleefd?
De gevolgen voor het niet naleven van de AVG kunnen veel groter zijn dan nu het geval is onder de Privacyrichtlijn en de Wbp. De maximale boete bedraagt op dit moment € 4.500,-[3] ; in 2018 kan de toezichthouder op dit terrein (Autoriteit Persoonsgegevens) boetes opleggen die oplopen tot 2% van de jaaromzet en – in het geval van schending van de verplichtingen rondom het melden van datalekken – zelfs tot maximaal 10% van de jaaromzet.

Welke gegevens gelden als persoonsgegevens?
Elk gegeven dat kan worden herleid naar een levend mens, geldt als een persoonsgegeven. Er is uiteraard veel meer over te zeggen dan deze ene regel; bijvoorbeeld op

[1] Bij een richtlijn geldt de bescherming van de richtlijn als 'minimumniveau', maar mogen ook strengere regels worden gehanteerd door de lidstaten. Bij een verordening mag alleen worden afgeweken indien en voor zover de verordening dat toestaat.

[2] VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016

[3] Per 1 januari 2016 zijn de boetes onder de Wbp al verhoogd voor overtredingen die te maken hebben met de meldplicht datalekken. Daarvoor kan nu al een boete worden opgelegd van maximaal 10% van de jaaromzet.

de website van de Autoriteit Persoonsgegevens vindt u meer informatie over welke gegevens als persoonsgegevens worden aangemerkt.

Wat is zorgvuldige verwerking?
Uitgangspunt onder de AVG blijft de verplichting om persoonsgegevens zorgvuldig en in overeenstemming met de wet te verwerken[4]. De AVG schept een aantal verplichtingen bij het verwerken van persoonsgegevens die hierna op hoofdlijnen zullen worden besproken. Echter, de hiervoor beschreven norm bestaat uit twee delen en dat betekent dat zelfs als aan alle (wettelijke) eisen van de AVG wordt voldaan, het nog steeds zo kan zijn dat de verwerking als onzorgvuldig wordt beoordeeld.

De bestaande wettelijke verplichtingen onder de Wbp kunnen worden onderverdeeld in de volgende categorieën:

1. Voor iedere zogenaamde verwerking van persoonsgegevens is een rechtmatige grondslag nodig.
2. Voordat u met het verwerken van persoonsgegevens start, moet u deze in sommige gevallen melden bij de Autoriteit Persoonsgegevens of intern registreren.
3. Persoonsgegevens mogen niet voor doelen worden gebruikt die onverenigbaar zijn met het doel waarvoor ze aanvankelijk zijn verkregen (het principe van 'doelbinding').
4. Degene wiens persoonsgegevens het betreft (in de wet aangeduid als: de betrokkene) heeft het recht om te weten door wie en voor welke doeleinden zijn of haar persoonsgegevens worden verwerkt ('transparantie').
5. Naast de verplichting om de betrokkene op de hoogte te brengen, moeten ook een aantal andere rechten van de betrokkene worden geborgd.
6. U dient te zorgen voor passende technische en organisatorische maatregelen ter bescherming van de juistheid, volledigheid en integriteit van de persoonsgegevens, oftewel de kwaliteit van de verwerking;.
7. Schakelt u derden in bij de verwerking van persoonsgegevens, dan dient u maatregelen te treffen om de kwaliteit van de verwerking ook bij deze zogenaamde bewerkers te waarborgen.
8. Brengt u persoonsgegevens buiten de Europese Economische Ruimte (EU/EER), dan gelden speciale voorschriften voor deze zogenaamde 'doorgifte'.

Voor elk van deze categorieën zullen de belangrijkste wijzigingen, die de AVG brengt, worden toegelicht.

Hoe kunt u zorgen voor zorgvuldige verwerking?
Door eerst de huidige stand van zaken binnen uw organisatie op voornoemde punten in kaart te brengen, kunt u een start maken met een zorgvuldige verwerking van persoonsgegevens. Daarvoor heeft RWV Advocaten een scan ontwikkeld, waarbij eerst globaal de uitgangspositie organisatiebreed in kaart wordt gebracht. Aan de hand van de uitkomsten van deze scan wordt bepaald waar de organisatie staat en kan een - op uw organisatie en de specifieke situatie afgestemd - plan van aanpak worden opgesteld.

[4] Artikel 6 Wbp.

RECHTMATIGE GRONDSLAG

WAT

Artikel 8 Wbp bevat een limitatieve opsomming van de gronden die een verwerking van persoonsgegevens kunnen rechtvaardigen. Voor iedere verwerkingshandeling is een van de volgende gronden vereist:

a) De betrokkene heeft daarvoor zijn ondubbelzinnige toestemming verleend.
b) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene.
c) De verwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is.
d) De verwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene.
e) De verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt.
f) De verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming niet prevaleren.

Voor de zogenaamde 'bijzondere persoonsgegevens'[5] gelden (nog) striktere grondslagen voor verwerking: dit is in beginsel verboden, tenzij aan een van de wettelijk vastgelegde uitzonderingen wordt voldaan.

Het artikel gaat echter nog verder: het behelst ook dat bij elke verwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Volgens het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden verwerkelijkt.

Dit betekent dat ook wanneer er een wettelijke grondslag voor een bepaalde verwerkingshandeling van persoonsgegevens is aan te wijzen, de verantwoordelijke moet afwegen of deze te verantwoorden is vanuit het oogpunt van proportionaliteit en subsidiariteit.

In de AVG is de lijst met verwerkingsgronden op hoofdlijnen ongewijzigd; op detailniveau zijn er er wel wijzigingen. Bijvoorbeeld ten aanzien van de vereisten voor verwerking op basis van toestemming van de betrokkene. Deze – in de praktijk veel gebruikte – grondslag wordt aangescherpt; impliciete toestemming – ook al is deze ondubbelzinnig – is straks volgens de letterlijke bewoordingen niet langer mogelijk. De AVG vereist namelijk een verklaring of een duidelijke actieve handeling. In de AVG is een apart artikel opgenomen waarin wordt bepaald aan welke voorwaarden een geldige toestemming moet voldoen (artikel 7 AVG). Daarin wordt benadrukt dat het verzoek om toestemming in begrijpelijke en gemakkelijk toegankelijk vorm en in duidelijke en eenvoudige taal moet zijn

[5] Opgenomen in artikel 16 Wbp. Dit zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

opgesteld. Ook bepaalt dit artikel bijvoorbeeld dat bij de beoordeling of toestemming vrijelijk is gegeven, ten sterkste rekening moet worden gehouden met de vraag of de persoonsgegevens die in het kader van toestemming moeten worden verstrekt ook noodzakelijk zijn voor het uitvoeren van de overeenkomst.

Gegeven deze ontwikkelingen, zal het onder de AVG voor veel organisaties van toenemend belang zijn om af te wegen welke verwerkingen nog kunnen worden gegrond op toestemming van de betrokkene. In veel gevallen is het eenvoudiger om verwerkingen die nu nog op toestemming worden gebaseerd, te baseren op de gerechtvaardigde belangen van de organisatie.

WANNEER

De grondslag voor een gerechtvaardigde verwerking van persoonsgegevens dient aanwezig te zijn voordat met de betreffende verwerking wordt gestart. Dat betekent - bijvoorbeeld - dat bij verwerking op basis van toestemming, deze toestemming niet achteraf kan worden verkregen.

HOE

Er dienen procedures te zijn om de rechtmatige verwerking te waarborgen. Deze procedures dienen bekend te zijn, te worden nageleefd, periodiek te worden gecontroleerd en het beleid en de procedures dienen op zichzelf ook periodiek te worden geëvalueerd. Hiervoor kwam al naar voor dat voor de afzonderlijke grondslagen voor verwerking van persoonsgegevens in sommige gevallen specifieke regels zijn omtrent de wijze waarop van een grondslag gebruik kan worden gemaakt. Die regels kunnen vervolgens weer variëren al naar gelang bijvoorbeeld de gebruikte techniek[6], kwetsbaarheid van de betrokkene[7] en het doeleinde van de verwerking[8].

> *"DE PROCEDURES DIENEN BEKEND TE ZIJN, TE WORDEN NAGELEEFD EN PERIODIEK TE WORDEN GECONTROLEERD"*

Naast de regels die in dit verband voortvloeien uit de AVG en de Wbp, zijn er op diverse vlakken richtlijnen van de Autoriteit Persoonsgegevens en het Europese verband van toezichthouders (de zogenaamde Working Party 29, afgekort: WP29[9]).

[6] Zo bepaalt de AVG in de zogenaamde preambule onder 32 ten aanzien van toestemming die langs elektronische weg wordt verkregen: *"Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie."*

[7] De AVG bevat specifieke eisen ten aanzien van bepaalde verwerkingshandelingen die betrekking hebben op kinderen. Zie bijvoorbeeld artikel 8 AVG ten aanzien van het gebruik door kinderen van 'diensten van de informatiemaatschappij' (online geleverde diensten zoals Facebook).

[8] De AVG geeft bijvoorbeeld specifieke regels voor (direct) marketingactiviteiten (artikel 21 AVG) en het verwerken van persoonsgegevens voor zogenaamde 'geautomatiseerde individuele besluitvorming' / profilering (artikel 22 AVG).

[9] Zie voor een lijst met alle richtlijnen van WP29

MELDING / REGISTRATIE

WAT

Onder de huidige wetgeving, dient iedere geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens door de verantwoordelijke te worden gemeld aan de Autoriteit Persoonsgegevens op grond van artikel 27 Wbp[10], tenzij de betreffende verwerking is vrijgesteld op grond van het Vrijstellingsbesluit Wbp.

Deze algemene meldplicht maakt geen onderdeel uit van de AVG. Daarvoor in de plaats komt de verplichting om voor risicovolle verwerkingen van persoonsgegevens een 'Privacy Impact Analyse' ('PIA') uit te voeren en daarbij – in sommige gevallen - de Autoriteit Persoonsgegevens te raadplegen[11].

Tot de inwerkingtreding van de AVG op 25 mei 2018 blijft de meldingsplicht bestaan. Tot dat moment zullen (nieuwe) verwerkingen moeten worden gemeld.

Artikel 27 lid 3 Wbp bepaalt dat de melding dient plaats te vinden bij de Autoriteit Persoonsgegevens of bij een interne functionaris voor de gegevensbescherming ('FG'). In beide gevallen zijn de meldingen openbaar, maar in het geval van melding aan de FG behoeven deze niet – zoals bij de Autoriteit Persoonsgegevens – in een internetregister te worden geplaatst. Een dergelijke functionaris voor de gegevensbescherming wordt onder de AVG overigens verplicht voor sommige organisaties[12].

Naast de verplichting om bij risicovolle verwerkingen een PIA uit te voeren, schept de AVG een verplichting om intern een register bij te houden van alle verwerkingsactiviteiten.

Vrijgesteld van deze verplichting worden organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is of gevoelige persoonsgegevens bevat. Al naar gelang de wijze waarop het tweede vereiste (incidentele verwerking) wordt uitgelegd, zullen de meeste organisaties – ook als zij minder dan 250 werknemers in dienst hebben – naar mijn mening een register moeten gaan bijhouden.

Dit register moet voor elke verwerkingsactiviteit in ieder geval de volgende informatie bevatten:

1. de naam en contactgegevens van de (mede)verantwoordelijke(n) van deze verwerkingen (en de contactpersonen, zoals een eventuele functionaris voor de gegevensbescherming);
2. de doeleinden van de verwerkingen;

[10] Hetgeen overigens niet betekent dat elke verwerkingshandeling afzonderlijk dient te worden gemeld; verwerkingshandelingen mogen gezamenlijk worden gemeld voor zover deze als een 'geheel van verwerkingen' in de zin van artikel 1, onderdeel b AVG kunnen worden beschouwd.

[11] Artikel 35 en 36 AVG. Er worden in artikel 35 lid 2 AVG drie situaties genoemd waarin de PIA verplicht is, namelijk kort samengevat: (a) bij verwerkingen waarbij geautomatiseerde individuele besluitvorming plaatsvindt die de betrokkene 'wezenlijk kan treffen', (b) bij grootschalige verwerking van gevoelige persoonsgegevens en (c) bij stelselmatige en grootschalige monitoring van openbare ruimten. Het betreft hier echter uitsluitend voorbeelden. Veiligheidshalve zal bij verwerking van grotere hoeveelheden persoonsgegevens een PIA uitgevoerd moeten worden. Dit ook teneinde invulling te geven aan de (nieuwe) verplichtingen van artikel 25 AVG ('privacy by design' en 'privacy by default'); zie daarvoor verder onder de paragraaf 'kwaliteit'.

[12] De meeste overheidsorganen en –instanties, organisaties die regelmatig en stelselmatig gebruik maken van observatie (bijvoorbeeld middels cameratoezicht) en organisaties die grootschalig gevoelige persoonsgegevens verwerken (artikel 37 lid 1 AVG).

3. de categorieën betrokkenen, bijvoorbeeld: hebben de persoonsgegevens betrekking op werknemers, oud-werknemers, leerlingen, klanten etc.;
4. de categorieën persoonsgegevens, bijvoorbeeld NAW-gegevens, financiële gegevens, BSN etc.;
5. eventuele derden ontvangers van de persoonsgegevens en doorgifte naar derde landen;
6. de bewaartermijnen die worden aangehouden voor de persoonsgegevens;
7. een omschrijving van de technische en organisatorische veiligheidsmaatregelen die door de organisatie genomen zijn.

Een specifieke meldingsplicht die per 1 januari 2016 in de Wbp is geïntroduceerd betreft de meldplicht bij datalekken[13].

"MELDING DIENT PLAATS TE VINDEN ALVORENS MET DE VERWERKING WORDT AANGEVANGEN"

Deze meldplicht is ook opgenomen in de AVG[14]. De meldplicht heeft al veel aandacht gekregen en de verschillen tussen de bestaande regeling en de AVG lijken minimaal; op de meldplicht datalekken wordt dan ook in deze whitepaper niet verder ingegaan.

WANNEER

Volgens artikel 27 lid 1 Wbp dient melding plaats te vinden 'alvorens met de verwerking wordt aangevangen'. Op het moment dat een organisatie verplicht is om een register van verwerkingsactiviteiten bij te houden en eventueel ook een functionaris voor de gegevensbescherming aan te stellen, geldt dat deze verplichtingen uiterlijk op 25 mei 2018 ingevuld dienen te zijn.

HOE

De reeds bestaande meldingsplicht wordt hier niet verder toegelicht, aangezien deze reeds langere tijd bestaat en binnen afzienbare termijn zal verdwijnen.

De AVG geeft een aantal globale voorschriften voor het uitvoeren van een PIA (en de daar eventueel mee gepaard gaande consultatie van de toezichthouder) en het opzetten en gebruik van het register (bijvoorbeeld dat het register schriftelijk of in elektronische vorm wordt bijgehouden[15]). Er bestaat daarbinnen vrijheid om deze verplichtingen in te vullen.

Er dienen procedures te zijn om de tijdige registratie en uitvoering van een PIA te waarborgen, deze procedures dienen bekend te zijn, te worden nageleefd, periodiek te worden gecontroleerd en het beleid en de procedures dienen op zichzelf ook periodiek te worden geëvalueerd.

[13] Artikel 34 a Wbp.

[14] Artikelen 32-34 AVG.

[15] Artikel 30 lid 3 AVG.

TRANSPARANTIE

WAT

De verantwoordelijke moet actief en ongevraagd de betrokkene van de gegevensverwerking op de hoogte stellen. Dit wordt ook wel aangeduid als het 'transparantiebeginsel'.

Dit transparantiebeginsel is vastgelegd en nader uitgewerkt in artikel 33 en artikel 34 Wbp. Daarin is vastgelegd dat de verantwoordelijke de betrokkene zijn identiteit meedeelt en de doeleinden van de verwerking. In aanvulling daarop wordt die informatie verstrekt die 'nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen'.

De verplichting is niet in alle gevallen gegeven. De wet kent een beperkt aantal uitzonderingen:

a) Als de betrokkene al weet dat zijn persoonsgegevens door de betreffende verantwoordelijke worden verwerkt (artikel 33 lid 1 Wbp).
b) Op het moment dat de verantwoordelijke de persoonsgegevens niet rechtstreeks van de betrokkene verkrijgt, maar via een derde, kan het verschaffen van informatie aan de betrokkene achterwege blijven als verschaffing onmogelijk blijkt of een onevenredige inspanning kost, dan wel als de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven.
c) In een aantal bij wet geregelde gevallen die met name voor verwerking van persoonsgegevens door overheidsinstellingen van belang zijn (als omschreven in artikel 43 en 44 Wbp).

In de AVG wordt de te verstrekken informatie verder uitgebreid en geconcretiseerd. Onder de verplicht te verschaffen informatie staat nu ook:

1. een beschrijving van de grondslag en een beschrijving van de gerechtvaardigde belangen als de verwerking daarop is gebaseerd (zie hiervoor onder 'rechtmatige grondslag')[16];
2. de periode dat de persoonsgegevens worden bewaard[17] en
3. informatie over de rechten van betrokkene (zoals het recht op inzage, rectificatie, etc.)[18].

WANNEER

Voor gegevens die rechtstreeks van de betrokkene worden verkregen geldt dat de informatie voorafgaand aan de verkrijging moet worden verstrekt. De AVG bepaalt dat informatie verschaft moet worden bij (en niet, zoals thans in de Wbp is bepaald, voorafgaand aan) de verkrijging van de persoonsgegevens[19]. Praktisch gezien betekent dit echter dat het voorafgaand aan de verkrijging wordt verstrekt.

Voor gegevens die van derden worden verkregen, geldt dat deze moeten worden verstrekt:

a) op het moment van vastlegging van de betreffende gegevens; of
b) wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van

[16] Artikel 13 lid 1 sub c en d AVG.

[17] Artikel 13 lid 2 sub a AVG.

[18] Artikel 13 lid 2 sub b tot en met f AVG.

[19] Artikel 13 lid 1 AVG.

de eerste verstrekking (wanneer de informatie werd verkregen om aan derden te worden verstrekt).

HOE

Er dienen procedures te zijn om de informatieverschaffing te waarborgen. Deze procedures dienen bekend te zijn, te worden nageleefd, periodiek te worden gecontroleerd en het beleid en de procedures dienen op zichzelf ook periodiek te worden geëvalueerd.

Hoewel in de wet zelf geen regels zijn vastgelegd omtrent de wijze waarop de informatie dient te worden verstrekt, bevat de toelichting op de wet hiervoor wel voorschriften. Ook in de AVG wordt hierover het nodige opgemerkt. Zowel algemene regels voor de informatieverstrekking[20], alsook meer specifieke regels voor de informatieverstrekking over – bijvoorbeeld – profilering.[21]

"IN HET KADER VAN (DIRECT) MARKETING ZAL DE KLANT IN ALLE GEVALLEN VOORAFGAAND AAN DE VERWERKING OP ZIJN RECHTEN MOETEN WORDEN GEWEZEN"

In het kader van (direct) marketing, zal de klant in alle gevallen voorafgaand aan de verwerking op zijn recht dienen te worden gewezen om verdere verwerking te stoppen. Indien de verwerking is gebaseerd op toestemming volgt dat uit artikel 7 lid 3 van de AVG:

> *"De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan."*

Indien de verwerking is gebaseerd op het rechtmatige belang van de verantwoordelijke, vloeit dit voort uit artikel 21 lid 2 van de AVG:

> *"Wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt, heeft de betrokkene te allen tijde het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing, met inbegrip van profilering die betrekking heeft op direct marketing."*

En lid 4:

> *"Het in de leden 1 en 2 bedoelde recht wordt uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene gebracht en duidelijk en gescheiden van enige andere informatie weergegeven."*

[20] Zie bijvoorbeeld preambule AVG sub 58 en 63: *"Overeenkomstig het transparantiebeginsel moet informatie die bestemd is voor het publiek of voor de betrokkene beknopt, eenvoudig toegankelijk en begrijpelijk zijn en moet duidelijke en eenvoudige taal en, in voorkomend geval, aanvullend visualisatie worden gebruikt.."* En sub 63: zie volgende noot.

[21] Preambule AVG sub 63: *"Elke betrokkene dient dan ook het recht te hebben, te weten en te worden meegedeeld voor welke doeleinden de persoonsgegevens worden verwerkt, indien mogelijk hoe lang zij worden bewaard, wie de persoonsgegevens ontvangt, welke logica er ten grondslag ligt aan een eventuele automatische verwerking van de persoonsgegevens en, ten minste wanneer de verwerking op profilering is gebaseerd, wat de gevolgen van een dergelijke verwerking zijn."*

DOELBINDING

WAT

De verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, is alleen toegestaan als de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld. Dit principe bij de verwerking van persoonsgegevens wordt aangeduid met de term 'doelbinding'.

Het doelbindingsvereiste bestaat uit twee onderdelen:
1. de verplichting om de doeleinden nauwkeurig te omschrijven; en
2. om de verzamelde persoonsgegevens niet verder te verwerken voor doeleinden die daarmee niet verenigbaar zijn.

In de AVG blijft het doelbindingsvereiste bestaan[22]. Aanvankelijk werd voorgesteld om verdere verwerking toe te staan voor doeleinden die onverenigbaar zijn met de aanvankelijke doeleinden, mits er wettelijke grondslag voor verdere verwerking aanwezig is. In de AVG is deze algemene uitzondering niet opgenomen. Wel is bepaald dat verdere verwerking voor doeleinden die onverenigbaar zijn met de aanvankelijk aangewezen doeleinden mogelijk is met toestemming van de betrokkene[23].

Verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt in de AVG niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd[24].

Naast deze uitzonderingen en enkele bijzondere situaties[25], zal de verantwoordelijke dan ook moeten toetsen of de verdere verwerking verenigbaar is met het doel waarvoor de gegevens zijn verzameld. In de AVG worden een aantal gezichtspunten genoemd die bij een dergelijke toets in ieder geval in aanmerking dienen te worden genomen:

- ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
- de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt;
- de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
- het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

[22] Artikel 5 lid 1 sub b AVG.

[23] In de considerans sub 50 van de AVG staat: *"Wanneer de betrokkene zijn toestemming heeft gegeven… …, moet de verwerkingsverantwoordelijke de mogelijkheid hebben de persoonsgegevens verder te verwerken, ongeacht of dat verenigbaar is met de doeleinden."* Zie ook artikel 6 lid 4 AVG.

[24] Waarbij dan wel een aantal voorwaarden moeten worden vervuld, zoals omschreven in artikel 89 AVG. Deze bepaling – en dan met name de 'statistische doeleinden' – biedt ruimte voor commerciële doeleinden, maar de voorwaarden (zie ook WP29 Opinie 203) zijn strikt.

[25] Lidstaten krijgen beperkte bevoegdheid om wettelijke uitzonderingen te creëren op het vereiste van doelbinding.

WANNEER

De doeleinden voor de verwerking van persoonsgegevens dienen te worden bepaald voorafgaand aan de verzameling van persoonsgegevens[26]. Beoordeling van de verenigbaarheid van verdere verwerking dient (eveneens) plaats te vinden voordat met verdere verwerking wordt aangevangen.

HOE

Er dienen procedures te zijn om de doelbinding van de gegevensverwerking te waarborgen. Deze procedures dienen bekend te zijn, te worden nageleefd, periodiek te worden gecontroleerd en het beleid en de procedures dienen op zichzelf ook periodiek te worden geëvalueerd.

"ER DIENEN PROCEDURES TE ZIJN OM DE DOELBINDING VAN DE GEGEVENSBEWERKING TE WAARBORGEN"

Hiervoor is reeds gewezen op de (niet limitatieve) lijst van gezichtspunten die in de beoordeling dienen te worden meegenomen. In Opinie 203 van WP29 is uitvoerig beschreven op welke wijze de hiervoor geschetste toetsen dienen plaats te vinden.

[26] Zie artikel 5 lid 1 sub b AVG en Opinie 203 van WP29 p. 15.

RECHTEN BETROKKENEN

WAT

Naast het hiervoor reeds behandelde recht op informatie op grond van het 'transparantiebeginsel', creëert de Wbp een aantal andere rechten voor een betrokkene. Deze rechten zijn in de AVG gehandhaafd en verder uitgebreid. De belangrijkste reeds in de Wbp vastgelegde rechten voor een betrokkene zijn:

- het recht om op verzoek inzage te krijgen in de op hem betrekking hebbende persoonsgegevens[27];
- het recht op rectificatie[28], meer in het bijzonder: het recht om persoonsgegevens te laten verbeteren, aan te vullen, te verwijderen, of af te schermen als deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt[29];
- het recht om zich tegen verdere verwerking te verzetten als deze is gebaseerd op het 'algemeen belang', een 'gerechtvaardigd belang van de verantwoordelijke'[30], of als daarbij sprake is van direct marketing[31].

Daarnaast kent de AVG de volgende 'nieuwe' rechten voor een betrokkene:

- het 'recht om vergeten te worden', oftewel om de verantwoordelijke te verplichten om alle op hem betrekking hebbende persoonsgegevens te wissen als (verdere) verwerking inbreuk maakt op de wet[32];
- het recht om verdere verwerking tijdelijk te schorsen in een aantal omstandigheden[33];
- het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft;
- het recht op gegevensoverdracht als de verwerking is gebaseerd op toestemming van de betrokkene.[34]

Onder het regime van de AVG dient de verantwoordelijke de betrokkene ook op deze rechten te

[27] Dit gaat dus om een verzoek van de betrokkene en niet om de informatie die de verantwoordelijke uit eigener beweging dient te verstrekken op grond van hetgeen is opgemerkt onder het 'transparantiebeginsel'. Artikel 35 Wbp en artikel 15 AVG.

[28] Artikel 36 Wpb en artikel 16 AVG.

[29] Er rust ook een verplichting op de verantwoordelijke om dergelijke wijzigingen door te geven aan derden aan wie hij de persoonsgegevens eerder heeft verstrekt (artikel 38 Wbp en artikel 19 AVG).

[30] Oftewel de grondslagen onder artikel 8 sub e en f Wbp. Zie artikel 40 Wbp en artikel 21 AVG.

[31] Artikel 41 Wbp en artikel 21 lid 3 AVG.

[32] Het recht bestaat bijvoorbeeld wanneer het bewaren van de persoonsgegevens niet langer nodig is voor het doel waarvoor deze zijn verstrekt of wanneer de toestemming waarop verwerking berust wordt ingetrokken. Zie bijv. preambule AVG sub 65 en de uitspraak van het Hof van Justitie van de EU Case C-131/12 (Google / Gonzales).

[33] Artikel 18 AVG.

[34] Dit betreft een nieuw recht dat is gecreëerd in de AVG (artikel 20 AVG) en dient om 'dataportabiliteit' te bevorderen en 'lock in' te voorkomen.

wijzen, wanneer hij persoonsgegevens rechtstreeks van de betrokkene verkrijgt[35]. Voor sommige rechten dient dit zelfs op een zeer expliciete wijze te geschieden: bijvoorbeeld ten aanzien van het recht van verzet bepaalt de AVG in artikel 21 lid 4 dat dit recht uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene wordt gebracht en duidelijk en gescheiden van enige andere informatie weergegeven.

WANNEER

"DE WBP EN DE AVG BEVATTEN VOORSCHRIFTEN VOOR DE MANIER WAAROP IN SOMMIGE GEVALLEN MOET WORDEN GEREAGEERD"

De betrokkene kan deze rechten uitoefenen op ieder gewenst moment. De Wbp en de AVG bevatten termijn waarbinnen de verantwoordelijke de rechten dient op te volgen:

- het recht om op verzoek inzage te krijgen: 4 weken na ontvangst verzoek[36];
- het recht op rectificatie: 4 weken na ontvangst verzoek[37];
- het 'recht om vergeten te worden': 'zonder onredelijke vertraging'[38];
- het recht om verdere verwerking tijdelijk te schorsen: geen beslistermijn opgenomen;
- het recht op bezwaar/verzet: 4 weken na ontvangst verzoek[39];
- het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft: geen termijn opgenomen;
- het recht op gegevensoverdracht: geen termijn opgenomen.

HOE

Er dienen procedures te zijn om de rechten van betrokkenen te waarborgen. Deze procedures dienen bekend te zijn, te worden nageleefd, periodiek te worden gecontroleerd en het beleid en de procedures dienen op zichzelf ook periodiek te worden geëvalueerd.

De Wbp en de AVG bevatten ook voorschriften voor de manier waarop in sommige gevallen dient te worden gereageerd (via welke media, met welke informatie, etc.).

[35] Artikel 13 lid 2 AVG.

[36] Artikel 35 lid 1 Wbp (geen termijn in de AVG).

[37] Artikel 36 lid 2 Wbp (artikel 16 AVG stelt: onverwijld).

[38] Artikel 17 lid 1 AVG.

[39] Artikel 40 lid 3 Wbp: er moet binnen vier weken worden beslist en vervolgens – indien gehonoreerd – terstond worden gestaakt. Artikel 41 bevat een verzetrecht voor werving voor charitatieve doelen en die bevat ook een termijn van 4 weken die, merkwaardig genoeg, kan worden verlengd. De AVG bevat, nog merkwaardiger, geen termijn voor dit recht.

KWALITEIT

WAT

Op de verantwoordelijke rust de verplichting om toe te zien op de kwaliteit van de verwerking van persoonsgegevens[40]. Onder het begrip 'kwaliteit' kunnen vier eisen uit artikel 5 lid 1 van de AVG worden geschaard. Naast de hiervoor reeds behandelde vereisten van een wettelijke grondslag en doelbinding, moeten persoonsgegevens:

1. toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking');
2. juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ('juistheid');
3. worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ('opslagbeperking')[41];
4. door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan is gewaarborgd, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

Deze eisen lopen overigens over in en vallen deels samen met de eisen van proportionaliteit en subsidiariteit die hiervoor reeds aan de orde zijn geweest.

Concreter brengt het voorgaande mee dat er passende - op de aard en risico's van verwerking afgestemde - technische en organisatorische beschermingsmaatregelen worden getroffen. Die verplichting bestaat ook al onder het huidige recht[42], maar onder de AVG wordt deze op een aantal vlakken verduidelijkt en aangescherpt:

a. Veel nadruk wordt gelegd op het kunnen afleggen van verantwoording omtrent de keuzes die een organisatie maakt op het gebied van de verwerking van persoonsgegevens. Organisaties moeten kunnen aantonen dat hierover is nagedacht en dat het beleid wordt gehandhaafd ('accountability')[43];
b. Het nadenken over de risico's van verwerking van persoonsgegevens, het waarborgen van voornoemde criteria daarbij en het nemen van daarop afgestemde beschermingsmaatregelen, dient niet aan het einde van (nieuwe) projecten, waarbij persoonsgegevens worden verwerkt, plaats te vinden, maar al vanaf het begin ('privacy by design')[44];
c. Het beleid dient zodanig te zijn dat producten en diensten standaard zijn ingesteld om de hoogste mate van privacy te bieden. In dat geval is privacy als

[40] Artikel 15 lid 2 Wbp.

[41] Met uitzondering van de opslag voor doeleinden omschreven in artikel 89 AVG (statistische doeleinden, etc.): die mag – mits voldaan aan de randvoorwaarden – langer duren.

[42] Artikel 13 Wbp.

[43] Artikel 5 lid 2 AVG.

[44] Preambule AVG sub 78 en 108 en artikel 25.

het ware ingebouwd in de systemen ("privacy by default")[45].

Artikel 32 lid 1 AVG schrijft in zijn algemeenheid voor dat er een beleid dient te zijn ten aanzien van de genomen technische en organisatorische maatregelen en de periodieke (her)evaluatie daarvan:

1. *"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:*
   a) *de pseudonimisering en versleuteling van persoonsgegevens;*
   b) *het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;*
   c) *het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;*
   d) *een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking."*

WANNEER

Aan de kwaliteitseisen van verwerking van persoonsgegevens moet doorlopend worden voldaan.

"AAN DE KWALITEITSEISEN VAN VERWERING VAN PERSOONSGEGEVENS MOET DOORLOPEND WORDEN VOLDAAN"

HOE

Er dienen procedures te zijn om de kwaliteit van de gegevensverwerking te waarborgen. Deze procedures dienen bekend te zijn, te worden nageleefd, periodiek te worden gecontroleerd en het beleid en de procedures dienen op zichzelf ook periodiek te worden geëvalueerd.

Voor de criteria die tezamen de kwaliteit van de verwerking van persoonsgegevens bepalen geeft de Wbp geen nadere invulling. Deze eisen hangen af van de specifieke situatie: als er grootschalig bijzondere persoonsgegevens worden verwerkt, liggen de eisen hoger dan bij kleinschalige verwerking van niet-gevoelige persoonsgegevens. Er wordt aanbevolen om 'sectorspecifieke' regels en gedragscodes op te stellen hiervoor[46]. In de AVG zijn enkel algemene voorschriften opgenomen voor de beveiliging van persoonsgegevens[47].

Voor meer algemene aspecten van verwerking van persoonsgegevens zijn door de Autoriteit Persoonsgegevens en WP29 wel richtlijnen opgesteld, zoals bijvoorbeeld ten aanzien van cameratoezicht[48], (onderdelen van) personeelsdossiers[49], beveiliging[50] en datalekken[51].

[45] Zie noot 42.

[46] Zie artikel 25 en 26 Wbp.

[47] Artikel 32-34 AVG.

[48] Zie de op 28 januari 2016 gepubliceerde beleidsregels van de Autoriteit Persoonsgegevens op dit gebied.

[49] Beleidsregels 'de zieke werknemer' d.d. 21 april 2016 van de Autoriteit Persoonsgegevens.

[50] Richtsnoeren beveiliging persoonsgegevens van de Autoriteit Persoonsgegevens uit februari 2013.

[51] Richtsnoeren meldplicht datalekken gepubliceerd door de Autoriteit Persoonsgegevens op 8 december 2015.

BEWERKERS

WAT

Onder een 'bewerker'[52] wordt verstaan: een persoon of organisatie die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen[53]. Het is vrijwel ondenkbaar in de huidige tijd dat een organisatie (als verantwoordelijke) persoonsgegevens verwerkt, zonder daarbij gebruik te maken van bewerkers. Trends als bijvoorbeeld couldcomputing, software as a service (SAAS) en het gebruik van analysetools om internetverkeer te monitoren, zorgen ervoor dat voor vrijwel iedere verwerkingsactiviteit gebruik wordt gemaakt van bewerkers, zoals softwareleveranciers, Google Analytics en cloudproviders.

De Wbp verplicht een verantwoordelijke die gebruik maakt van een bewerker om:

- zorg te dragen dat deze bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen en toe te zien op de naleving van die maatregelen[54];
- zorg te dragen dat de bewerker uitsluitend in zijn opdracht de gegevens verwerkt (en daarmee onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen)[55];
- een (schriftelijke) overeenkomst te sluiten met de bewerker waarin de afspraken ten aanzien van het voorgaande zijn vastgelegd[56].

Onder de AVG worden zowel de verplichtingen die rusten op de verantwoordelijke uitgebreid (bij het gebruikmaken van bewerkers) als ook de verplichtingen die op de bewerkers zelf rusten.

De verplichtingen die de AVG aan een bewerker oplegt zijn:

1. een bewerker moet in sommige gevallen een eigen register bijhouden van de verwerkingsactiviteiten die worden verricht[57];
2. een bewerker mag niet zonder instemming van de verantwoordelijke werkzaamheden ten behoeve van de verantwoordelijke uitbesteden aan een derde[58];
3. wanneer werkzaamheden worden uitbesteed, dient de bewerker alle op hem rustende verplichtingen (eveneens) op te leggen aan deze 'subbewerker'[59];

[52] In de Nederlandse vertaling van de AVG verwarrend genoeg aangeduid als 'verwerker'.

[53] Artikel 1 lid e Wbp.

[54] Artikel 14 lid 1 Wbp.

[55] Artikel 12, 13 en 14 lid 2 Wbp.

[56] Artikel 14 lid 5 Wbp.

[57] Die gevallen lopen parallel aan de gevallen waarin de verantwoordelijke een register dient bij te houden.

[58] Zie artikel 28 lid 2 AVG.

[59] Artikel 28 lid 4 AVG.

4. de verplichting om de verantwoordelijke in kennis te stellen van instructies die een inbreuk op de AVG opleveren[60].

Onder de AVG zijn de vereisten die contractueel tussen de verantwoordelijke en de bewerker dienen te worden vastgelegd uitgebreid[61]. In de praktijk zal dit betekenen dat de meeste 'bewerkersovereenkomsten' zullen moeten worden aangepast. Dat is de voornaamste uitbreiding ten opzichte van de Wbp voor de verwerkingsverantwoordelijke.

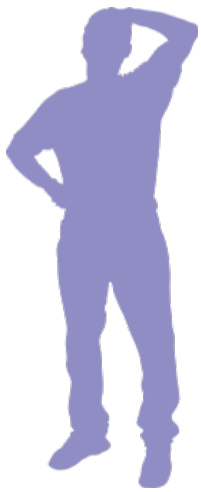
"ONDER DE AVG ZIJN DE VEREISTEN UITGEBREID DIE CONTRACTUEEL TUSSEN DE VERANTWOORDELIJKE EN DE BEWERKER DIENEN TE WORDEN VASTGELEGD"

WANNEER

Aan de verplichtingen, die de AVG aan een bewerker oplegt, dient te worden voldaan voordat een bewerker met het verwerken van persoonsgegevens start.

HOE

Voor bewerkersovereenkomsten zijn modelbepalingen opgesteld. Voor wat betreft de technische en organisatorische bepalingen die een verantwoordelijke aan een bewerker moet opleggen, zal echter specifiek naar de situatie moeten worden gekeken. Ook hier dient een schaalbare – aan de risico's van de verwerking gekoppelde – aanpak te worden gehanteerd. Het klakkeloos werken met standaardcontracten is dan ook niet aan te bevelen.



[60] Artikel 28 lid 3 laatste zin AVG.

[61] Zie de opsomming in artikel 28 lid 3 AVG.

DOORGIFTE

WAT

De Wbp en de AVG bevatten tenslotte regels voor doorgifte van persoonsgegevens.

Worden persoonsgegevens doorgegeven aan een 'derde'[62] buiten de EU[63] (een 'derde land'), dan verschillen de eisen voor dergelijke 'ontvangers' met die welke gelden voor binnen de EU gevestigde ontvangers.

Heeft de Europese Commissie een 'adequaatheidsbesluit' genomen ten aanzien van het derde land, dan is voor doorgifte geen specifieke toestemming nodig[64]. Het derde land wordt dan geacht een passend beschermingsniveau te bieden.

Als er geen adequaatheidsbesluit is genomen ten aanzien van een derde land, mag alleen doorgifte aan een daar gevestigde derde plaatsvinden indien 'passende waarborgen' zijn getroffen. Dit kan in de vorm van een verdrag[65], of – op individueel niveau – middels een modelcontract, 'Binding Corporate Rules' of ondubbelzinnige toestemming van de betrokkenen, dan wel toestemming van de Minister van Justitie[66].

WANNEER

Er dient aan aanvullende verplichtingen ten aanzien van doorgifte van persoonsgegevens te worden voldaan als deze gegevens worden doorgegeven naar een derde land.

HOE

Ook voor doorgifte van persoonsgegevens aan derde landen zijn modelcontracten opgesteld[67].

[62] Dat kan zijn een 'bewerker', maar ook een concernvennootschap of een internationale organisatie.

[63] En de EER: Liechtenstein, Noorwegen, IJsland.

[64] Artikel 45 lid 1 AVG.

[65] Bekendste verdrag in dit verband was het 'safe harbor' verdrag tussen de VS en de EU dat in 2015 van tafel is gegaan op grond van de uitspraak van het HvJEU.

[66] Artikel 77 Wbp.

[67] Hiervoor zijn momenteel drie modelcontracten van toepassing (ook wel standard contractual clauses of SCC's genoemd).

Haagweg 149 • Leiden • www.rwv.nl • 071-7502200

MR. DRS. MARTIJN HOVING

Aan RWV Advocaten verbonden sinds 1998 en werkzaam als ondernemingsrecht- en insolventierechtadvocaat. Richt zich binnen het ondernemingsrecht vooral op het opzetten van samenwerkingsverbanden tussen bedrijven en instellingen en het adviseren en procederen bij geschillen daarover. Treedt regelmatig op als curator en bewindvoerder bij insolventies en behandelt in dat kader ook kwesties over onder meer zekerheidsrecht en bestuurdersaansprakelijkheid.

Zijn bedrijfskundige achtergrond plus ervaring als ondernemer, manager, bewindvoerder en advocaat stellen Martijn in staat snel te zien waar de kansen liggen, maar ook wat de grootste risico's zijn. Het slaan van bruggen tussen die twee ziet hij als zijn grootste uitdaging als advocaat. Communicatie is daarbij essentieel: *"Ontdekken waar de werkelijke wensen en belangen liggen door te luisteren en die te vertalen naar juridische oplossingen, daar ga ik voor."*

Martijn is zeer geïnteresseerd in de veranderingen die nieuwe technologieën teweeg brengen binnen onze maatschappij. Regelmatig adviseert en publiceert hij over de juridische aspecten van nieuwe technologieën, digitalisering en 'big data'.