

# Inhoudsopgave

Voorwoord	II
Begrippen en afkortingen	13
1 Inleiding	17
1.1 Persoonsgegevens en betrokkene	19
1.2 Verwerken	21
2 Heeft u te maken met de AVG?	25
2.1 Waar worden de gegevens verwerkt?	25
2.2 Hoe worden de gegevens verwerkt?	26
2.3 Rollen	26
2.4 Rolverdeling	28
2.4.1 <i>Kerntaken</i>	29
2.4.2 <i>Dienstverlening</i>	30
2.4.3 <i>Meerdere betrokken partijen</i>	31
2.5 Tips & Tricks	33
2.6 Wat verandert er?	34
3 Privacymanagement	37
3.1 Accountability	37
3.2 Privacymanagement	38
3.3 De functionaris voor gegevensbescherming (FG)	40
3.3.1 <i>Taken</i>	41
3.3.2 <i>Rol en positie</i>	41
3.4 Het verwerkingsregister	43
3.5 Privacy Impact Assessments	44
3.5.1 <i>Wanneer verplicht?</i>	44
3.5.2 <i>Onderdelen</i>	45
3.5.3 <i>Voorafgaande raadpleging</i>	46
3.6 Privacy by design	46
3.7 Informatiebeveiliging	48

INHOUDSOPGAVE

3.8	De meldplicht datalekken	49
3.8.1	<i>Wat is een datalek?</i>	49
3.8.2	<i>Registratieplicht</i>	50
3.8.3	<i>Meldplicht</i>	50
3.9	Privacymanagement voor verwerkers	52
3.10	Tips & Tricks	53
3.11	Wat verandert er?	53
4	Het gegevensverwerkende proces	55
4.1	Rechtmatige en behoorlijke verwerking	55
4.1.1	<i>Rechtmatig</i>	55
4.1.2	<i>Behoorlijk</i>	56
4.2	Doelbinding	56
4.3	Minimale gegevensverwerking	58
4.4	Juistheid	59
4.5	Grondslagen	59
4.5.1	<i>Overeenkomst</i>	60
4.5.2	<i>Wettelijke verplichting</i>	60
4.5.3	<i>Levensbelang</i>	61
4.5.4	<i>Overheidstaak</i>	61
4.5.5	<i>Belangenafweging</i>	62
4.5.6	<i>Toestemming</i>	63
4.5.7	<i>Welke grondslag?</i>	64
4.6	Bijzondere gegevens	65
4.7	Strafrechtelijke gegevens	67
4.8	Profilering	68
4.9	Tips & Tricks	69
4.10	Wat verandert er?	69
5	De betrokkene	71
5.1	Informeren van de betrokkene	71
5.2	Inzage	72
5.3	Verbetering	73
5.4	Verwijdering	73
5.5	Overdraagbaarheid	74
5.6	Bezwaar	75
5.7	Algemene regels	76
5.8	Rechtsmiddelen	78
5.9	Tips & Tricks	79
5.10	Wat verandert er?	79

6	Doorgiften naar buiten de EU	83
6.1	Adequaatheidsbesluit	83
6.2	Binding corporate rules	84
6.3	Andere instrumenten	85
6.4	Generieke uitzonderingen	85
6.5	Tips & Tricks	86
6.6	Wat verandert er?	86
7	De Autoriteit Persoonsgegevens	89
7.1	Taken	89
7.2	Bevoegdheden	90
7.3	Corrigerende maatregelen	90
7.4	Boetes	90
7.5	Internationale samenwerking	92
7.6	Tips & Tricks	92
7.7	Wat verandert er?	93
8	In ontwikkeling	95
8.1	Nederlandse wetgeving	95
8.1.1	<i>Algemene regels</i>	95
8.1.2	<i>Sectorspecifieke regels</i>	98
8.2	Gedragcodes en certificering	99
9	In de praktijk – Grip op de AVG	101
9.1	Fase 1: Uitdenken	101
9.1.1	<i>Organisatie-DPIA</i>	101
9.1.2	<i>Kapstokbeleid</i>	103
9.2	Fase 2: Implementeren	105
9.2.1	<i>Plannen</i>	105
9.2.2	<i>Doen</i>	106
9.3	Fase 3: Beheren	108
9.3.1	<i>Incidentgebaseerd</i>	109
9.3.2	<i>Cyclisch</i>	109
9.3.3	<i>Periodiek</i>	110
9.4	Documentatie	110
9.5	Voor verwerkers	111
	Nawoord	113
	Trefwoordenregister	115
	Over de auteurs	119

## Voorwoord

Voor organisaties neemt het belang van gegevens in een snel tempo toe. In mijn rol als Digicommissaris heb ik vooral te maken met de digitale overheid. Een digitale overheid is in al haar aspecten van functioneren afhankelijk van gegevens of data. Het woord “digitaal” is bijna overbodig. Alle processen, producten en diensten zijn afhankelijk van gegevens en gegevensuitwisseling. Daarbij gaat het steeds meer om gegevens die betrekking hebben op personen. Immers, de omgeving wenst steeds meer dienstverlening op maat, betere handhaving en fraudebestrijding. Ook verwacht de omgeving dat de overheid zich niet voor de gek laat houden en dat gegevens zoveel mogelijk maar eenmaal hoeven te worden aangeleverd.

Dit alles vraagt om kaders met betrekking tot wet- en regelgeving die de privacy en veiligheid van onze inwoners waarborgen. Nationaal hadden we daarvoor de WBP ontwikkeld, maar het is goed dat er volgend jaar een Algemene Verordening Gegevensbescherming (AVG) in werking treedt die op Europees niveau onze gemeenschappelijke normen op het gebied van privacy en gegevensbescherming borgt. Zeker in een tijd dat deze normen internationaal bepaald niet vanzelfsprekend zijn. De AVG vormt ook een belangrijk element in relatie tot de generieke digitale infrastructuur (GDI) die ik samen met betrokken overheden in onze overheidsbrede sturing regisseer. Alle elementen van die GDI hebben raakvlakken met deze regelgeving, of het nu eID, DigiD, berichtenbox of basisregistraties betreft, om een paar onderdelen te noemen. De impact van de AVG op deze voorzieningen is groot, er is nog veel werk te doen om te zorgen dat we in alle opzichten aan het gestelde kader voldoen. Overheidsbrede aspecten van de AVG zullen ook in de governance van de GDI aan de orde komen.

## VOORWOORD

Het is goed dat publicaties als deze verschijnen die overheidsorganisaties zowel als bedrijven een handvat bieden hoe dit aan te pakken, en helpen er in de praktijk grip op te krijgen. Ik wens iedereen die daarmee aan de slag gaat veel wijsheid en succes toe bij het implementeren van de AVG.

Bas Eenhoorn

Digicommissaris  
Nationaal Commissaris Digitale Overheid

## I Inleiding

Dit boek gaat over de Algemene Verordening Gegevensbescherming (AVG).<sup>1</sup> Dit is de laatste in een inmiddels lange rij van privacywetten. De eerste daarvan ontstonden zo'n vijftig jaar geleden, als reactie op het feit dat steeds meer grote bedrijven en overheidsinstanties gebruik gingen maken van mainframe computers. Daarop konden zij voor het eerst grote hoeveelheden gegevens over personen opslaan en met destijds ongekende snelheid en nauwkeurigheid verwerken. Het publiek zag de mogelijkheden die deze ontwikkeling bood, maar maakte zich ook zorgen over de "onzichtbaarheid" van zulke gegevensverwerking en de mogelijke nadelige gevolgen ervan. Dit leidde ertoe dat eind jaren zestig in de VS de *Fair Information Processing Principles* werden opgesteld. Deze vonden vervolgens hun weg in Amerikaanse en later ook in Europese privacywetgeving. Waarbij we de term "privacy", zoals we dat in de rest van dit boek ook zullen doen, gebruiken terwijl we eigenlijk de bescherming van persoonsgegevens bedoelen. Maar dat is zo'n mond vol ... Het zijn echter wel twee van elkaar te onderscheiden rechten. Het Handvest van de EU benoemt het recht op bescherming van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens beide als fundamentele rechten van Europese burgers. Hierin is Europa uniek. Elders in de wereld wordt privacy niet of beperkt als grondrecht gezien, en het recht op bescherming van persoonsgegevens al helemaal niet.

Een hoofddoel van de AVG is de bescherming van persoonsgegevens. Maar de AVG heeft *nóg* een hoofddoel, en dat is het mogelijk maken van het vrije verkeer van persoonsgegevens binnen de EU. Het idee is dat gegevens binnen de hele EU vrijelijk kunnen stromen doordat de AVG daar overal een gelijk niveau van bescherming garandeert. Een gevolg van deze twee hoofddoelen is dat de bescherming van persoonsgegevens voortdurend een afweging vraagt tussen de belangen van de personen over wie persoonsgegevens verwerkt worden en de belangen van degenen die die gegevens verwerken. Dat privacy en gegevensbescherming grondrechten zijn, doet daar niet aan af. Grondrechten kunnen ingeperkt worden als dat noodzakelijk is in een democratische samenleving, en in het bijzonder als er anders een zwaarwegender inbreuk zou ontstaan op andere grondrechten van burgers, zoals de vrijheid van meningsuiting en van informatie, de vrijheid van ondernemerschap, en het recht op een eerlijk proces.

<sup>1</sup> In het Engels bekend als de GDPR (General Data Protection Regulation).

In al deze zaken is de AVG niet nieuw, al bevat zij in vergelijking met haar voorganger, Richtlijn 95/46/EU, wel een aantal wijzigingen. De meeste daarvan zijn uitbreidingen of aanscherpingen van wat er eerder was. Er zijn als het gaat om regels voor de gegevensverwerking zelf maar een paar echt nieuwe zaken, met name het recht op dataportabiliteit en het recht om vergeten te worden.

In een ander opzicht is de AVG echter wel geheel nieuw, en laat zij een frisse wind waaien op privacygebied. Het gaat dan niet om de regels voor de gegevensverwerking zelf, maar om alles wat een gegevensverwerkende organisatie moet doen om ervoor te zorgen dat zij het naleven van die regels structureel waarborgt, en daarover ook rekenschap kan afleggen. Dat goed inregelen gaat van vrijwel alle gegevensverwerkende organisaties ten minste een grote inspanning vergen, en vaak zelfs een cultuuromslag. Met (bij het verschijnen van dit boekje) nog ruim een jaar te gaan is het al bijna een onmogelijke opgave om dat allemaal klaar te hebben op het moment dat op 25 mei 2018 de AVG in werking treedt. De kans is gelukkig niet zo heel groot dat de toezichthouder, de Autoriteit Persoonsgegevens (AP), direct na die datum enorme boetes gaat uitdelen. Zolang u ten minste kunt aantonen dat u er wel al een tijd serieus mee bezig bent en duidelijke stappen in de goede richting gezet heeft. In hoofdstuk 3 leggen we u precies uit wat de AVG van u verlangt, en in hoofdstuk 9 leggen we u een concrete aanpak voor om daarmee aan de slag te gaan.

In de overige hoofdstukken nemen we u mee door de wondere wereld van de AVG. Daarbij hebben we als lezer de “geïnteresseerde leek” in gedachten, die binnen zijn organisatie aan de slag wil of moet met privacy, maar er nog niet of nauwelijks mee bekend is. Als u alleen in huiselijk of privéverband gegevens verwerkt, dan kunt u dit boekje met een gerust hart neerleggen: de AVG geldt niet voor u.

#### **Huiselijk of privéverband**

De volgende criteria kunnen helpen om te bepalen of er sprake is van verwerking in huiselijk of privéverband, in het bijzonder in een internetcontext. Hoe meer vragen u met “ja” beantwoordt, hoe kleiner de kans dat dat zo is.

- Worden de gegevens verspreid naar een onbepaald aantal personen, in plaats van naar een beperkte gemeenschap van vrienden, familieleden of bekenden?
- Betreft het gegevens over personen die geen huiselijke of privérelatie hebben met degene die ze verwerkt?
- Suggesteren de schaal en de frequentie van de verwerking dat het gaat om een vakmatige of voltijdse activiteit?
- Zijn er aanwijzingen dat een aantal individuen handelt op gezamenlijke en georganiseerde wijze?
- Is er mogelijk negatieve impact op personen, waaronder inbreuk op hun privacy?

We veronderstellen geen bekendheid met de huidige Wet bescherming persoonsgegevens. Omdat we vooral ook een beknopt, pragmatisch en hanteerbaar boekje wilden maken, hebben we bewust een groot aantal details en juridische finesses weggelaten. Wilt u in een bepaald geval het naadje van de kous weten, dan ontkomt u er dus niet aan om de AVG zelf erop na te slaan.<sup>2</sup>

Voordat we de inhoud van de AVG induiken, behandelen we hieronder eerst nog drie fundamentele begrippen die het hele boek en de hele AVG door terugkomen: persoonsgegevens, betrokkene en verwerken.

## 1.1 Persoonsgegevens en betrokkene

De AVG definieert persoonsgegevens als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). Daarmee is de term *betrokkene* gedefinieerd: dat is degene over of van wie persoonsgegevens worden verwerkt. Maar hoe breed moet de term “alle informatie over” uitgelegd worden, en wanneer is een persoon precies geïdentificeerd of identificeerbaar?

### Identificeerbaar

Dat laatste werkt de AVG verder uit: als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Vooral van belang in deze definitie is dat er al snel sprake is van identificeerbaarheid. Bijvoorbeeld in het geval van pseudonimiseren. Daarbij worden direct identificeerbare gegevens losgeknipt van de overige gegevens en vervangen door een pseudoniem dat slechts onder bepaalde voorwaarden (of soms zelfs helemaal niet) toegankelijk is. Hoewel degene die met de pseudoniemen werkt zelf niet in staat is om de identiteit te achterhalen, zou hij dat met hulp van degene die de pseudoniemen beheert wel kunnen. Zodra er sprake is van een redelijke verwachting dat zoiets zou kunnen gebeuren is er sprake van identificeerbaarheid. Maar zelfs als het niet zou lukken om de identiteit (in de zin van bijvoorbeeld naam en adres) te achterhalen, dan nog kan iemand als identificeerbaar worden beschouwd. Wanneer een persoon bijvoorbeeld op een bepaalde manier behandeld wordt op basis van gedragsgegevens die gekoppeld zijn aan zijn gebruikersnaam voor een bepaalde dienst dan geldt hij als identificeerbaar,

<sup>2</sup> Zie [www.gripopdeAVG.nl](http://www.gripopdeAVG.nl), en Jan Berkvens en Cathérine Jakimowicz, *Tekstuitgave Privacyverordening*, Boomjuridisch 2016.



zelfs als degene die de dienst verleent geen flauw idee heeft bij welke persoon die gebruikersnaam hoort.

#### **Identificeerbaar**

De Artikel 29 Werkgroep is een werkgroep van de privacytoezichthouders van de EU-lidstaten. Zij heeft onder meer een groot aantal adviezen gepubliceerd over de interpretatie van onderdelen van de privacywetgeving. Voor een groot deel behouden die adviezen onder de AVG hun relevantie.

“Advies 4/2007 over het begrip persoonsgegevens” gaat uitgebreid in op de vraag wanneer er sprake is van persoonsgegevens. Verreweg de meeste aandacht gaat daarbij uit naar de begrippen “geïdentificeerd” en “identificeerbaar”, onder andere aan de hand van de voorbeelden hieronder.

##### *röntgenfoto*

Een röntgenfoto van een vrouw werd gepubliceerd in een wetenschappelijk tijdschrift met vermelding van haar zeer ongewone voornaam. Door de combinatie van de voornaam van de vrouw en het feit dat haar familieleden en kennissen wisten dat zij aan een bepaalde ziekte leed, was zij voor hen identificeerbaar. De röntgenfoto moet in dit geval daarom als persoonsgegevens worden beschouwd.

##### *publicatie van videobewakingsbeelden*

Een winkelier installeert in zijn zaak een systeem voor camerabewaking. Hij hangt in de zaak foto's op van winkeldieven die met het bewakingssysteem zijn opgenomen. Na een waarschuwing van de politie maakt hij het gezicht van de dieven onherkenbaar. Maar ook dan bestaat nog steeds de mogelijkheid dat de personen op de foto's worden herkend door vrienden, familie of burens aan hun haardracht, lichaamsfiguur of kleding. Er is dus sprake van persoonsgegevens.

##### *farmaceutische onderzoeksgegevens*

Ziekenhuizen en artsen sturen uit patiëntendossiers afkomstige gegevens door aan een bedrijf met het oog op medisch onderzoek. De namen van de patiënten worden niet vermeld, maar alleen willekeurig toegekende volgnummers. De namen van de patiënten zijn uitsluitend bekend bij de betrokken artsen, die door het medisch beroepsgeheim zijn gebonden. De gegevens bevatten geen aanvullende informatie die door middel van combinatie identificatie van de patiënten mogelijk maakt. Bovendien zijn alle andere juridische, technische of organisatorische maatregelen genomen om te voorkomen dat de betrokkenen geïdentificeerd of identificeerbaar worden. In deze omstandigheden kan geoordeeld worden dat er bij de gegevensverwerking door het farmaceutisch bedrijf geen redelijkerwijs in te zetten middelen zijn waarmee de betrokkenen kunnen worden geïdentificeerd. Er is dan geen sprake van persoonsgegevens.

**Alle informatie over**

Als de AVG zegt dat persoonsgegevens alle informatie over een persoon zijn, bedoelt ze dan ook echt *alle* informatie? Het antwoord is: jazekeer! Je kunt het zo gek niet bedenken, als informatie op wat voor manier dan ook iets zegt over of gekoppeld is aan een identificeerbare persoon, dan zijn het persoonsgegevens. De vorm doet niet ter zake. Het kan gaan om digitale gegevens of gegevens op papier. Ook foto's en video-opnamen van personen zijn persoonsgegevens. Zelfs weefselmateriaal waaruit DNA-gegevens kunnen worden afgeleid merkt de AVG aan als persoonsgegevens.

Veel mensen denken in eerste instantie aan direct identificerende gegevens zoals naam en adres. Maar het begrip persoonsgegeven is dus veel en veel breder. Een aantal voorbeelden:

- naam, adres, geboortedatum, titulatuur, geslacht;
- e-mailadres, telefoonnummer, zakelijk adres, huisadres, locatie;
- werkgever, functie, leidinggevende, personeelsnummer;
- loopbaan, opleidingen, competenties;
- medische dossiers;
- antwoorden, klachten, meningen, publicaties;
- inhoud van e-mails, surfgedrag;
- overtredingen, veroordelingen;
- loginnamen, wachtwoorden;
- identificatienummers;
- IP-adressen, tracking cookies, RFID-nummers, MAC-adressen.

En zo zouden we nog wel een tijdje kunnen doorgaan.

Gegevens over overleden personen worden niet beschouwd als persoonsgegevens. Wel kunnen ze soms ook iets zeggen over nog levende personen, en in dat geval zijn het weer wel persoonsgegevens over hen.

Ook gegevens over bedrijven zijn soms persoonsgegevens, namelijk als het gaat over een eenmanszaak, vennootschap onder firma, commanditaire vennootschap of maatschap. In veel gevallen zult u niet bekend zijn met de precieze rechtsvorm van bedrijven waarmee u van doen heeft, en dan zult u gegevens over die bedrijven daarom ook als persoonsgegevens moeten beschouwen.

**1.2 Verwerken**

De AVG definieert niet het begrip verwerken, wel het begrip *verwerking*. Dat is "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geauto-

matiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens”. Hier geldt eigenlijk hetzelfde als voor het begrip persoonsgegevens: er is al heel snel sprake van. Het begrip verwerken dekt de hele levenscyclus van informatie, en alles wat u doet of zou kunnen doen met persoonsgegevens valt eronder. Tekenend is in dat opzicht het woordje “zoals” dat aan de forse opsomming hierboven voorafgaat.

Een samenhangend geheel aan bewerkingen van persoonsgegevens vormt dus een verwerking. Maar ook alle afzonderlijke delen. Voor elk van die onderdelen gelden de regels van de AVG. Wanneer bijvoorbeeld partij A gegevens opvraagt bij betrokkenen om ze gepseudonimiseerd door te geven aan partij B, dan zijn het opvragen door A, het opslaan door A, het pseudonimiseren door A, het verstrekken door A, het ontvangen door B, het opslaan door B en het gebruik door B allemaal verwerkingen van persoonsgegevens, die elk moeten voldoen aan de regels van de AVG.





rolverdeling

## 2 Heeft u te maken met de AVG?

De kans is groot dat u, als lezer van dit boek, binnenkort aan de slag gaat met de AVG. In dit hoofdstuk leest u of dat voor uw organisatie noodzakelijk is en zo ja: welke onderdelen van de wet voor u gelden. Daarvoor is van belang waar de gegevensverwerking plaatsvindt, op welke manier de gegevens worden verwerkt, en welke rol u daarbij heeft.

### 2.1 Waar worden de gegevens verwerkt?

De AVG is weliswaar een verordening van de EU, maar haar tentakels reiken verder dan de lidstaten. Zij is namelijk ook van toepassing op organisaties die niet in de EU gevestigd zijn, maar die wel gegevens verwerken gericht op personen in de EU.

#### **De organisatie heeft een vestiging in de EU**

Elke organisatie (of persoon) die gevestigd is in de EU, Noorwegen, IJsland of Liechtenstein valt onder de AVG.<sup>1</sup> Maar ook vestigingen in de EU van organisaties die hun hoofdkantoor elders hebben staan. De vestigingen in Dublin van het Californische Facebook en Google moeten zich dus ook aan de AVG houden.<sup>2</sup> En alle verwerkingen die horen bij een organisatie of vestiging in de EU vallen onder de AVG, zelfs al vinden ze ergens anders plaats.

Het territorium van landen is trouwens groter dan u zich misschien in eerste instantie heeft gerealiseerd. Onder meer ambassades, schepen, vliegtuigen en boorplatforms vallen er onder.

<sup>1</sup> Waarom ook in Noorwegen, IJsland en Liechtenstein? Dat is omdat naast alle EU-lidstaten ook die landen lid zijn van de Europese Economische Ruimte (EER), en veel EU-verordeningen ook daar van toepassing zijn. Vanwege de onbekendheid van de EER geven we in dit boek de voorkeur aan de term "EU", maar we bedoelen dan dus telkens de hele EER.

<sup>2</sup> Wanneer er precies sprake is van een vestiging is niet altijd even helder. Volgens de juristen moet het gaan om een "plaats van bestendige economische activiteit". Daarvan blijkt nogal snel sprake te zijn. Bijvoorbeeld als je als buitenlands bedrijf ergens in de EU een "mannetje" hebt zitten die dingen voor je doet, zelfs wanneer die zich niet heeft ingeschreven in het Handelsregister.

### De verwerking is gericht op personen in de EU

Organisaties van buiten de EU vallen onder de AVG wanneer hun gegevensverwerking gericht is op personen die zich in de EU bevinden.<sup>3</sup> Concreet:

- als ze hun goederen of diensten aanbieden, al dan niet tegen betaling;
- als ze hun gedrag monitoren.

Van gedragsmonitoring is bijvoorbeeld sprake als een website *tracking cookies* plaatst bij een Europese bezoeker. Google heeft zoekwebsites met de extensies en in de taal van de meeste EU-lidstaten, en biedt daar dus diensten aan.

## 2.2 Hoe worden de gegevens verwerkt?

Vrijwel elke gegevensverwerking gebeurt tegenwoordig digitaal. Zodra er een computer, mobiele telefoon, tablet, digitale camera of ander slim apparaat in het spel is dat persoonsgegevens verwerkt, valt de verwerking onder de AVG. Het gaat er dus niet om dat alles digitaal gebeurt: ook als u deels handmatig werkt, heeft u te maken met de AVG.

Kunt u dan onder de AVG uitkomen door persoonsgegevens helemaal handmatig te verwerken? Het antwoord is in de meeste gevallen: nee. De AVG is ook van toepassing op gegevens op papier, zolang u die tenminste op een gestructureerde manier bijhoudt en er redelijk eenvoudig in kunt zoeken. Het op papier bijhouden van een relatiebestand of personeelsdossiers is daarom geen manier om onder de AVG uit te komen.

## 2.3 Rollen

Als een organisatie puur voor haar eigen doeleinden gegevens verwerkt, zonder dat er andere partijen bij betrokken zijn, dan is duidelijk dat zij er zelf verantwoordelijk voor is. De enige die erop aangesproken kan worden dat zij netjes met die gegevens omgaat, is de organisatie zelf. In de praktijk zijn er echter vaak meerdere partijen betrokken bij een gegevensverwerking. Technologische ontwikkelingen zorgen er bovendien voor dat die werkelijkheid in rap tempo complexer wordt.

Om in ingewikkelde situaties duidelijkheid aan te brengen onderscheidt de AVG twee fundamentele rollen: de *verwerkingsverantwoordelijke* en de *verwerker*.<sup>4</sup> De

<sup>3</sup> Het maakt dus niet uit of het wel of geen burgers of ingezetenen van de EU zijn, het gaat er puur om dat iemand zich in een EU-lidstaat bevindt.

<sup>4</sup> Handig om te weten: in het Engels heten deze respectievelijk de *data controller* en de *data processor*.