

# De Algemene Verordening Gegevensbescherming in gewonemensentaal

*Een eenvoudige uitleg over de nieuwe  
gegevensbeschermingsregels voor organisaties,  
functionarissen, studenten en andere  
geïnteresseerden*

*Herziene editie*

*Bart van der Sloot*

Amsterdam University Press

Omslagbeeld: Defense Advanced Research Projects Agency (DARPA)

Kaarten pagina 20: Bert Heesen Producties

Ontwerp omslag: Gijs Mathijs Ontwerpers

Ontwerp binnenwerk: Crius Group, Hulshout

ISBN 978 94 6372 863 8

E-ISBN 978 90 4855 208 5

NUR 740

© B. van der Sloot / Amsterdam University Press B.V., Amsterdam 2019

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j<sup>o</sup> het Besluit van 20 juni 1974, Stb. 351, zoals gewijzigd bij het Besluit van 23 augustus 1985, Stb. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 3051, 2130 KB Hoofddorp). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

# Inhoudsopgave

Belangrijkste begrippen	9
Inleiding	11
1. De Algemene Verordening Gegevensbescherming	13
1.1 Wat is de Algemene Verordening Gegevensbescherming?	13
1.2 Wanneer is de Algemene Verordening Gegevensbescherming voor mij van belang?	14
1.3 Het wie, wat, waar en waarom van de AVG	17
1.4 Waarom is het belangrijk om de Verordening te respecteren?	25
1.5 Tien misverstanden over de AVG	29
1.6 Conclusie	42
2. Wanneer is de Algemene Verordening Gegevensbescherming van toepassing?	43
2.1 Als er <i>persoonsgegevens</i>	44
2.2 Worden <i>verwerkt</i>	48
2.3 Door of in opdracht van een <i>verantwoordelijke</i>	48
2.4 <i>Het EU-recht is van toepassing</i>	55
2.5 En er is <i>geen uitzondering</i> van toepassing	58
2.6 Conclusie	62
3. Wat zijn de uitgangspunten?	65
3.1 Noodzakelijkheid, proportionaliteit en subsidiariteit	66
3.2 De Fair Information Principles	71
3.3 Legitieme verwerking van persoonsgegevens	78
3.4 Legitieme verwerking van bijzondere persoonsgegevens	86
3.5 Legitieme doorvoer van persoonsgegevens aan partijen in landen buiten de EU	94
3.6 Conclusie	102

4. Wat zijn de plichten van een verantwoordelijke?	105
4.1 Documentatieplicht	106
4.2 Intern beleid	109
4.3 Technische inbedding gegevensbeschermingsregels	110
4.4 Transparantie	111
4.5 Informatie aan het datasubject	113
4.6 Data Protection Impact Assessment	115
4.7 Data Protection Officer	120
4.8 Organisatorische veiligheidsmaatregelen	124
4.9 Technische veiligheidsmaatregelen	125
4.10 Meldplicht datalek	127
4.11 Conclusie	129
5. Wat zijn de rechten van de datasubjecten?	135
5.1 Informatie over de gegevensverwerking	138
5.2 Inzage in gegevens	139
5.3 Kopie van gegevens	139
5.4 Meenemen van gegevens	140
5.5 Rectificeren en aanvullen van gegevens	143
5.6 Het recht op vergetelheid	145
5.7 Het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming	149
5.8 Het recht van bezwaar	151
5.9 Het recht op beperking	155
5.10 Het klachtrecht	158
5.11 Conclusie	158
6. Aan welke regels moet een verantwoordelijke nog meer voldoen?	165
6.1 Zelfreguleringsmechanismen	166
6.2 De regels van de Autoriteit Persoonsgegevens, het Comité en de Commissie	170
6.3 De Uitvoeringswet	176
6.4 Sectorale regulering	187

6.5	Rechterlijke uitspraken	190
6.6	Sancties	191
6.7	Aansprakelijkheid	193
6.8	Conclusie	195
7.	Overzicht onderwerpen en artikelen	197



# Belangrijkste begrippen

- Het *datasubject*, in het Nederlands ook wel ‘de betrokkene’ genoemd, is de persoon over wie gegevens worden verwerkt. In de zin: ‘Erik heeft blauwe ogen en een rode stropdas aan’, is Erik het *datasubject*.
- De *verantwoordelijke* voor de gegevensverwerking verwerkt deze gegevens. Hij bepaalt het doel van die verwerking, en hoe de gegevens worden verzameld, opgeslagen en gebruikt. Een pizzeria die de naam en postcode van klanten opslaat, is bijvoorbeeld een *verantwoordelijke*.
- De *verantwoordelijke* kan hierbij worden geholpen door een *verwerker*, die gegevens in opdracht van de *verantwoordelijke* verwerkt. Dit is bijvoorbeeld een bedrijf dat door de pizzeria wordt ingehuurd om gegevens op te slaan of te analyseren.
- Als een *verantwoordelijke* of *verwerker* gegevens verwerkt over burgers in de Europese Unie (EU), maar zelf niet is gevestigd in de EU, dan moet hij een *vertegenwoordiger* aanstellen. Deze persoon is het aanspreekpunt voor die organisatie binnen de EU, bijvoorbeeld als het *datasubject* een klacht wil indienen of als de handhavende overheidsinstantie onderzoek wil verrichten.
- Binnen veel data-verwerkende organisaties moet een *Data Protection Officer*, ofwel een *functionaris voor de gegevensbescherming*, worden aangesteld. Deze persoon is ervoor verantwoordelijk dat binnen een organisatie de regels over het gegevensbeschermingsrecht worden nageleefd, en is het primaire aanspreekpunt voor vragen over de Algemene Verordening Gegevensbescherming, zowel binnen de organisatie als naar buiten toe, bijvoorbeeld in het geval het *datasubject* een klacht wil indienen of als de handhavende overheidsinstantie onderzoek wil doen.
- Elk land heeft een *toezichthoudende autoriteit*. In Nederland is dat de Autoriteit Persoonsgegevens, voorheen het College bescherming persoonsgegevens.

- Deze landelijke toezichhouders waren voorheen verenigd in de zogenoemde *Artikel 29 Werkgroep* (ingesteld door artikel 29 van de Richtlijn bescherming persoonsgegevens). De adviezen van deze werkgroep waren niet-juridisch bindend, maar wel zeer invloedrijk.
- Deze werkgroep wordt in de Verordening vervangen door de *European Data Protection Board*, ofwel het *Europees Comité voor Gegevensbescherming*. Deze organisatie krijgt een sterkere positie en meer bevoegdheden dan de voormalige Artikel 29 Werkgroep.
- De *European Data Protection Supervisor* is een adviesorgaan gelijk aan de Artikel 29 Werkgroep, maar dan voor de gegevensverwerking door de Europese Unie zelf. In dat geval is niet de Algemene Verordening Gegevensbescherming van toepassing, maar een aparte Verordening. Ook de adviezen van de European Data Protection Supervisor zijn vrij invloedrijk.
- De *Unie* is een afkorting voor de Europese Unie.
- De *Commissie* is een afkorting voor de Europese Commissie, zeg maar de ‘regering’ van de Europese Unie.
- Een *lidstaat* is een land dat is aangesloten bij de Europese Unie, bijvoorbeeld Nederland, Duitsland en Italië.
- Het *Europees Hof van Justitie* is de hoogste rechter van de Europese Unie en gaat over de interpretatie van het Handvest van de grondrechten, de Algemene Verordening Gegevensbescherming en andere documenten van de Europese Unie.
- Het *Europees Hof voor de Rechten van de Mens* (EHRM) is de hoogste rechter van de Raad van Europa en gaat over de interpretatie van het Europees Verdrag voor de Rechten van de Mens (EVRM). Bij de Raad van Europa zijn vrijwel alle Europese landen aangesloten, bij de Europese Unie slechts 28 landen.



# Inleiding

*De Algemene Verordening Gegevensbescherming in gewonementaal* is vooral geschreven voor bedrijven en organisaties die willen weten aan welke regels zij zich sinds mei 2018 moeten houden, voor functionarissen voor de gegevensbescherming die een gids door het gegevensbeschermingslandschap zoeken, en voor studenten die naast het juridisch jargon in simpele taal willen weten wat de regels precies behelzen en wat de achtergrond daarvan is.

Er bestaan al de nodige boeken over de Algemene Verordening Gegevensbescherming (AVG) die per artikel juridisch commentaar geven en relevante rechtszaken bespreken. Dit boek doet dat niet. In dit boek wordt in begrijpelijk en niet-juridisch jargon uitgelegd wat de regels in de praktijk betekenen, worden schema's gegeven en de achtergrond van de regels uitgelegd, zodat duidelijk wordt *waarom* de regels er zijn.

Het eerste hoofdstuk geeft een globaal beeld van wat de AVG is en wat die inhoudt. Hoofdstuk 2 geeft meer precieze uitleg over wanneer de AVG van toepassing is en wanneer niet. Hoofdstuk 3 bespreekt op welke uitgangspunten en principes de AVG is gebaseerd en hoofdstuk 4 benoemt de specifieke plichten die organisaties hebben die gegevens verwerken. Hoofdstuk 5 geeft aan welke rechten personen hebben over wie gegevens worden verwerkt en tot slot geeft hoofdstuk 6 inzicht in de wetten en regels die, naast de AVG, nog meer van belang zijn en hoe het gegevensbeschermingsrecht wordt gehandhaafd.



# 1. De Algemene Verordening Gegevensbescherming

In dit eerste hoofdstuk wordt kort besproken wat het gegevensbeschermingsrecht inhoudt, hoe de nieuwe regels eruitzien en waarom het van belang is om de regels te volgen.

## 1.1 Wat is de Algemene Verordening Gegevensbescherming?

Je hebt er waarschijnlijk al eens van gehoord: de Algemene Verordening Gegevensbescherming. Daarin staan regels over wanneer jij of de organisatie waarbinnen je werkt gegevens over personen mag verzamelen, opslaan, analyseren en gebruiken. De Verordening is op vrijwel iedereen van toepassing, of je nu een bedrijf hebt dat aan *online advertising* doet of een klantenregister bezit, of dat je een zzp'er bent, de salarisadministratie van je werknemers bijhoudt of bij een overheidsdienst werkt die registers over autobezit bijhoudt. Vrijwel altijd is een deel van de gegevens die je verwerkt een 'persoonsgegeven' en is de Verordening van toepassing.

De Verordening bevat maar liefst 88 pagina's aan gedetailleerde regels waaraan je moet voldoen als je gegevens verwerkt, met niet minder dan 99 wetsartikelen en 173 overwegingen die uitleg geven aan die artikelen. In de AVG staan regels over bewaartermijnen, onder welke voorwaarden je gegevens mag verzamelen en mag delen met organisaties in andere landen, en wanneer je extra gevoelige gegevens mag verwerken, bijvoorbeeld over iemands gezondheid of etniciteit. Ook staan er verplichtingen in over transparantie, documentatie, organisatie-inrichting en de beveiliging van gegevens. Het belangrijkste is misschien dat er sanctiemogelijkheden in de Verordening zijn opgenomen. Als je niet voldoet aan de regels uit de Verordening, dan kan per overtreding een boete worden opgelegd. Die boete kan oplopen tot 20 miljoen euro of, voor een

onderneming, tot 4 procent van de totale wereldwijde jaaromzet in het voorgaande boekjaar indien dat meer is dan die 20 miljoen. Dat zijn al enorme bedragen, maar in de Verordening staan ook nog eens andere mogelijke gevolgen beschreven, zoals aansprakelijkheid voor een overtreding of het wereldkundig maken van een overtreding, wat reputatieschade kan betekenen, of weglopende klanten.

De Verordening is al in april 2016 aangenomen door de Europese Unie (EU), maar werd pas echt van toepassing per 25 mei 2018. Dat gaf bedrijven en organisaties dus twee jaar de tijd om hun processen en beleid te herformuleren en te reorganiseren om zo te voldoen aan de nieuwe regels. De Algemene Verordening Gegevensbescherming bouwt voort op de EU Richtlijn bescherming persoonsgegevens uit 1995, die in Nederland was geïmplementeerd in de Wet bescherming persoonsgegevens. Omdat er in de Richtlijn weinig mogelijkheden waren opgenomen om boetes of sancties op te leggen, hadden veel organisaties nog niet alle regels uit die Richtlijn en de daarop gebaseerde wet geïmplementeerd. In mei 2018 moest er dus in feite een dubbelslag worden gemaakt. Niet alleen moesten de regels uit de Richtlijn helemaal worden geïmplementeerd binnen alle procesonderdelen van de organisatie; daarbij moesten ook de nieuwe bepalingen uit de Verordening worden meegenomen.

## **1.2 Wanneer is de Algemene Verordening Gegevensbescherming voor mij van belang?**

Zoals gezegd is de Algemene Verordening Gegevensbescherming van toepassing op vrijwel alle processen waarin data een rol spelen. Het belang van de Verordening is dus groot. Voorbeelden van situaties waarin de AVG van toepassing is op een organisatie zijn:

1. Je bent net met een vriend een pizzeria gestart en houdt in een klantenbestand de naam, het adres en de bestelling van klanten bij. Dan verwerk je persoonsgegevens over je klanten en is de Algemene Verordening Gegevensbescherming op je bedrijf van toepassing. Zowel iemands naam, iemands adres als iemands bestellingen zijn namelijk persoonsgegevens.

2. Je runt een bedrijf en hebt werknemers in dienst. Dan verwerk je persoonsgegevens van je werknemers, namelijk in verband met hun salaris, hun ziektemeldingen, verlof, bankgegevens, naam, woonplaats en adres. Al deze data zijn aan te merken als persoonsgegevens. Een aantal daarvan, zoals gegevens over ziektemeldingen, worden zelfs gezien als 'bijzondere persoonsgegevens', waar extra juridische waarborgen voor gelden. Als je de financiële administratie outsourcet naar bijvoorbeeld een accountskantoor, dan is de Algemene Verordening Gegevensbescherming nog steeds op je van toepassing; sterker nog, jij bent ervoor verantwoordelijk dat ook het accountskantoor zich houdt aan de AVG.
3. Je hebt een lokale politieke partij opgericht en treedt op als voorzitter van de vereniging. Zodra je vereniging leden krijgt, is de Verordening op je van toepassing. Sterker nog, voor politieke partijen gelden er extra strenge regels, omdat iemands politieke voorkeur soms erg gevoelig kan liggen.
4. Je bent de eigenaar van een chocolaterie en introduceert een klantenkaart waarmee vaste klanten korting kunnen krijgen op producten en jij persoonlijke advertenties kunt aanbieden op basis van hun klantprofiel. Ook dan is de Algemene Verordening Gegevensbescherming van toepassing; er staan speciale regels in de Verordening die beschrijven wanneer en onder welke voorwaarden je klanten mag profileren.
5. Je bent als huisarts onderdeel van een maatschap. Dan verwerk je medische gegevens over je patiënten. Dat mag natuurlijk voor zover dat nodig is voor de zorg voor de patiënt, maar de Verordening stelt wel dat het hier om zeer gevoelige persoonsgegevens gaat. Daarom moeten er extra maatregelen en waarborgen worden getroffen, bijvoorbeeld door voor een extra goede beveiliging van het patiëntendossier te zorgen.
6. Je hebt een website en gebruikt cookies om te weten welke berichten mensen aanklikken, hoe lang ze op bepaalde sites blijven. Op basis daarvan wil je persoonlijke advertenties aanbieden. Ook dan is de AVG van toepassing; sterker nog, je zult waarschijnlijk een knop op je website moeten maken,

zodat bezoekers direct zien dat je persoonlijke gegevens over hen verzamelt en die gebruikt om advertenties aan te bieden, maar dat ze zich met die knop daar direct voor kunnen afmelden.

7. Je runt een privéarchief over de geschiedenis van Roermond en hebt daartoe een aantal archieven en documenten opgekocht van privé-instellingen, bedrijven en particulieren. Ook daarin staat waarschijnlijk informatie over personen. Zelfs als je hun namen zwart maakt, dan nog is het vaak mogelijk om door indirecte gegevens over iemand te achterhalen wie het is. De zin: 'De persoon die van 1979-1984 directeur was van de plaatselijke VVV', is ook een persoonsgegeven. Ook op deze indirecte persoonsgegevens is de AVG van toepassing.
8. Je hebt een meubelzaak en in het computersysteem staan de namen en contactpersonen voor leveranciers en afnemers. Er staat bijvoorbeeld dat je vorig jaar al vijf keer een lading beukenhout hebt afgenomen van mevrouw De Wit, eigenaar van De Wit & Co BV, en dat meneer De Bruijn vorige week een tafel van € 14.995,- heeft gekocht. Ook dan is de Algemene Verordening Gegevensbescherming van toepassing op het register – zelfs de naam van een bedrijf, zoals De Wit & Co BV, kan een persoonsgegeven zijn.
9. Je beheert een stichting die op basis van een erfenis kleinschalige kunstprojecten steunt. Bij het toekennen van beurzen aan kunstenaars registreer je hun naam, rekeningnummer, adres en overige relevante informatie. Ook op dit bestand en de bijbehorende documentatie is de Algemene Verordening Gegevensbescherming van toepassing.
10. Je runt een website met daarop een discussieforum en maakt daarbij gebruik van software, en van een website-host en Cloud provider die in de Verenigde Staten van Amerika zijn gevestigd. Ook dan is de Algemene Verordening Gegevensbescherming van toepassing. Sterker nog, het is maar zeer de vraag of je gebruik mag maken van de diensten van deze Amerikaanse bedrijven, zeker nu de gegevens gedeeltelijk in de Verenigde Staten worden opgeslagen.

Voor vrijwel alle organisaties is het dus van belang om kennis te nemen van de Algemene Verordening Gegevensbescherming en ook als privépersoon verwerk je op dagelijkse basis persoonsgegevens. Dit boek biedt een eenvoudige introductie in de vrij uitvoerige regels. Als je gelijk aan de slag wilt met het implementeren van de Verordening, ga dan direct naar hoofdstuk 3 en 4. Daarin staan de kernprincipes en concrete verplichtingen uit de Algemene Verordening Gegevensbescherming, waaraan je sinds mei 2018 moet voldoen.

Als je niet bij een organisatie werkt maar gewoon geïnteresseerd bent in wat de AVG inhoudt, is dit boek ook interessant. Worden je persoonsgegevens verwerkt door een organisatie, dan kun je in dit boek lezen waaraan zij zich moeten houden en welke rechten je hebt als zij dat niet doen. Ben je vooral geïnteresseerd in je eigen rechten, ga dan direct naar hoofdstuk 5.

### **1.3 Het wie, wat, waar en waarom van de AVG**

Het is belangrijk om te begrijpen wat de achtergrond is van de Algemene Verordening Gegevensbescherming. Daarom hieronder kort het wie, wat, waar en waarom van de Verordening.

#### **1.3.1 Wie?**

In Europa bestaat een best complex web aan organen en instituties, waarbij met name het verschil tussen de Europese Unie en de Raad van Europa van belang is.

De AVG is afgekondigd door de Europese Unie. Daarom is het belangrijk om te weten welke landen tot de Europese Unie behoren en waarmee de Europese Unie zich bezighoudt. Ten eerste is dit van belang om te weten op wie de Algemene Verordening Gegevensbescherming betrekking heeft. Ten tweede is het van belang omdat de Verordening bepaalt dat binnen de Europese Unie persoonsgegevens wel mogen worden doorgegeven, bijvoorbeeld van Nederland naar Duitsland, maar dat gegevens vanuit de EU

naar een land daarbuiten alleen mogen worden doorgevoerd als dat andere land of de specifieke organisatie waaraan de gegevens worden doorgegeven dezelfde soort standaarden voor het gegevensbeschermingsrecht hanteert als binnen de Europese Unie.

De Europese Unie heeft het Handvest voor de Grondrechten uit 2000, de Algemene Verordening Gegevensbescherming en andere wetten op bijvoorbeeld het gebied van het telecommunicatierecht aangenomen. Het Europees Hof van Justitie (HvJ) is het gerechtshof van de Europese Unie, die uitspraken doet over het Handvest, de Verordening en de andere documenten van de Europese Unie.

De Raad van Europa heeft al in 1950 het Europees Verdrag voor de Rechten van de Mens (EVRM) aangenomen. Dit Verdrag wordt gecontroleerd door het Europees Hof van de Rechten van de Mens (EHRM). Dit gerechtshof van de Raad van Europa doet uitspraken over de interpretatie van het EVRM.

Aanvankelijk was de taakverdeling tussen de Raad van Europa en de Europese Unie helder: de Raad van Europa ging over de mensenrechten en de EU over economische aangelegenheden—het is immers de voortzetting van de Europese Gemeenschap voor Kolen en Staal. Langzamerhand is de Europese Unie zich echter ook gaan toeleggen op het gebied van mensenrechten en is de bescherming van Europese grondrechten door de Raad en de Unie steeds meer naar elkaar gegroeid. Wel heeft de EU van oudsher weinig zeggenschap over de nationale veiligheid; daar gaan de lidstaten in principe zelf over.

De Algemene Verordening Gegevensbescherming is dus van de Europese Unie en moet worden gerespecteerd door alle landen die zijn aangesloten bij de EU.

### **1.3.2 Waar?**

Het continent Europa kent officieel zo'n 50 landen en daarvan zijn er maar liefst 47 aangesloten bij de Raad van Europa. Alleen landen als Wit-Rusland en Vaticaanstad zijn geen lid. Dat betekent dat veruit de meeste Europese landen gebonden zijn aan het



Europees Verdrag voor de Rechten van de Mens. De Europese Unie heeft veel minder lidstaten, namelijk 28 en op termijn 27, vanwege de Brexit. Er zijn dus officieel maar 28 landen direct gebonden aan de Algemene Verordening Gegevensbescherming.

Toch zal de Verordening om twee redenen een groter effect hebben: Ten eerste omdat de Verordening stelt dat persoonsgegevens alleen mogen worden doorgevoerd naar landen buiten de Europese Unie als ze een 'adequaat beschermingsniveau' hebben. Omdat veel bedrijven buiten de Europese Unie gegevens hebben over EU-burgers zullen andere landen of de organisaties die daar zijn gevestigd zich moeten houden aan de regels van de EU, of anders de gegevens over de EU-burgers moeten verwijderen.

Ten tweede omdat een aantal landen zich heeft gecommitteerd aan een deel van de regels van de Europese Unie via de Europese Vrijhandelszone, namelijk IJsland, Noorwegen en Liechtenstein. Zij moeten zich ook aan de AVG houden. Ook Zwitserland is lid van de Vrijhandelszone, maar dat land heeft ervoor gekozen om de AVG niet direct van toepassing te laten zijn op zijn grondgebied, maar de regels over te nemen in een nationale wet. Daarnaast is er een aantal landen dat graag lid wil worden van de Europese Unie, en die zijn dus in het algemeen geneigd om de regels van de EU te volgen. Dat zijn Albanië, Montenegro, Servië, Macedonië, Bosnië en Herzegovina, Kosovo en, voorlopig althans nog, Turkije.

Het belangrijkste is om de 28 landen van de Europese Unie te onthouden. Dat zijn: België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Koninkrijk der Nederlanden, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Verenigd Koninkrijk en Zweden.

### 1.3.3 Wat?

De nieuwe regels over het gegevensbeschermingsrecht staan in een Verordening: de Algemene Verordening Gegevensbescherming. De oude regels stonden in een Richtlijn: de Richtlijn bescherming persoonsgegevens. Dat is EU-jargon en er is een



De landen binnen de EU



De landen binnen de Raad van Europa

groot verschil tussen een Richtlijn en een Verordening. Het belangrijkste om te onthouden is dat omdat er nu een Verordening is, je vanaf mei 2018 primair moet kijken naar de regels in de Verordening en pas in tweede instantie naar de Nederlandse wetgeving. Pas als er in de Algemene Verordening Gegevensbescherming staat dat landen, zoals Nederland, op een bepaald punt zelf hun eigen interpretatie van de regels kunnen geven, heeft het zin om naar de Nederlandse wettelijke bepalingen uit de zogenoemde Uitvoeringswet te kijken (zie paragraaf 6.3). Dat is maar op een klein aantal punten het geval.

Het verschil tussen een Richtlijn en een Verordening is vrij technisch:

- Een Richtlijn is een document dat is aangenomen door de EU, maar dat landen vervolgens in nationale wetten moeten overnemen (dat wordt ‘implementatie’ genoemd). De Richtlijn bescherming persoonsgegevens moest dus in Nederland worden geïmplementeerd en dat is gebeurd in de Wet bescherming persoonsgegevens. Ook andere landen van de EU, zoals Duitsland, België en Frankrijk, hadden soortgelijke nationale wetten waarin ze de regels uit de Richtlijn implementeerden. Er is bij een Richtlijn wat speelruimte voor landen om hun eigen interpretatie van de regels te geven en de regels op hun eigen manier vast te leggen in nationale wetgeving. Dit leidt er dus toe dat elk land een iets andere nationale wet heeft, en er verschil is tussen het gegevensbeschermingsrecht in bijvoorbeeld Duitsland en Nederland.
- Een Verordening heeft in tegenstelling tot een Richtlijn ‘direct effect’. Dat betekent dat burgers zich direct op de Verordening kunnen beroepen, en dus hebben organisaties die persoonsgegevens verwerken de Verordening als zodanig te respecteren. Waar er concrete regels, plichten en rechten in de Algemene Verordening Gegevensbescherming staan, hoeven deze regels niet op nationaal niveau in wetten te worden neergelegd (zoals bij een Richtlijn het geval is). De regels worden dus op EU-niveau afgekondigd, waardoor dezelfde regels gelden voor alle landen. Dit wordt in juridisch jargon ook wel harmonisering genoemd.