

Privacy op de werkvloer

Mr. Melanie Hermes
Ir. Arjen van Halem

Berghauser Pont Publishing
Postbus 14580
1001 LB Amsterdam
www.berghauserpont.nl
Omslagontwerp: Rosanna Zito, Zedline.
1e druk, december 2019
ISBN: 9789492952288
NUR: 825
© 2019 Berghauser Pont Publishing



Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave 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 reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet 1912 dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan Stichting Reprorecht (Postbus 3060, 2130 KB Hoofddorp, www.reprorecht.nl). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) kan men zich wenden tot Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, Postbus 3060, 2130 KB Hoofddorp, www.cedar.nl/pro).

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg besteed is, aanvaarden de auteur(s), redacteur(en) en uitgever geen enkele aansprakelijkheid voor eventuele (druk) fouten en onvolledigheden, noch voor gevolgen hiervan.

All rights reserved. No part of this publication may be reproduced in any form, by print, photo print, microfilm or any other means, without the publishers prior written permission.

Voorwoord

Op 25 mei 2018 is de Algemene verordening gegevensverwerking (AVG) in werking getreden en deze is in plaats gekomen van de Wet bescherming persoonsgegevens. Beide zijn gebaseerd op dezelfde privacy-principes, maar in de AVG zijn enkele principes verder uitgewerkt, zoals verantwoording en transparantie, van belang voor het voeren van een goed privacybeleid. Werknemers vormen in de privacywetgeving een categorie betrokkenen die extra bescherming verdient. Zo is het in de regel niet toegestaan de verwerking van persoonsgegevens van werknemers te baseren op toestemming van de betrokkene.

Bij persoonsgegevens van werknemers wordt in eerste instantie vaak alleen gedacht aan gegevens in het HR-domein. Inmiddels zijn vrijwel alle bedrijfsprocessen gedigitaliseerd (ook in het HR-domein) en zijn veel gegevens ook persoonsgegevens die binnen de arbeidsverhouding kunnen worden gebruikt en vaak ook worden gebruikt. Het thema van dit boek is derhalve “privacy op de werkplek”.

Dit boek richt zich tot alle actoren bij “privacy op de werkplek” zoals directie, HR-management, ICT, Functionarissen Gegevensbescherming, Privacy Officers, salarisadministratie en accountant met als doel het vinden van de juiste balans bij het verwerken van persoonsgegevens van werknemers. Een belangrijke actor kan ook de ondernemingsraad zijn die niet alleen specifieke bevoegdheden heeft bij de verwerking van persoonsgegevens door de onderneming, maar vooral ook namens de werknemers kan zorgen voor een juiste balans.

Het boek geeft in de eerste hoofdstukken de kaders van de AVG – zonder veel in detail te gaan - en behandelt vervolgens per hoofdstuk de regels per categorie verwerkingen (zoals sollicitatiegegevens, gezondheidsgegevens). Naast de AVG gaat het daarbij ook om wetten en regels en vooral om jurisprudentie.

De teksten in deze bundel zijn op 1 oktober 2019 afgesloten. Aan de totstandkoming is de uiterste zorg besteed. De auteurs zijn zich ervan bewust dat dit een complex onderwerp is en staan open voor tips en suggesties. Deze kunnen gestuurd worden naar a.c.hermes@hermesadvocatuur.nl zodat ze in een volgende editie meegenomen kunnen worden.

Mr. Melanie Hermes en ir. Arjen van Halem

Inhoud

Voorwoord	V
Inleiding	XIII
Over de auteurs	XVII
Bronnen en literatuur	XIX
1 De bescherming van persoonsgegevens, een introductie	1
1.1 Privacy: meer dan gegevensverwerking	1
1.2 Bescherming van persoonsgegevens: meer dan beveiliging	3
1.3 Bescherming van persoonsgegevens: meer dan compliance en risicomanagement	5
1.4 De AVG: impuls verbetering bescherming persoonsgegevens	5
1.5 Niet alleen AVG, ook aanvullende wet- en regelgeving waar relevant	6
1.6 Juiste toepassing AVG lastig in veranderende digitale wereld	7
1.7 Kernbegrip 'persoonsgegeven'	8
1.8 Persoonsgegeven en privacy	10
1.9 Privacyrisico	13
1.10 Bijzondere gegevens	14
1.11 Het doel en de context	15
2 Persoonsgegevens van werknemers in het huidige ICT-landschap	19
2.1 Inleiding	19
2.2 Enkele veranderingen in het ICT-landschap	23
3 Onboarding: de verwerking van gegevens van de sollicitant	31
3.1 Inleiding	31
3.2 De positie van de sollicitant	31
3.3 Persoonsgegevens in de sollicitatieprocedure	32

3.4	Verwerkingsgrondslag	33
3.5	Informatieverschaffing aan de sollicitant	35
3.6	Screening van de sollicitant	38
3.6.1	Inleiding	38
3.6.2	Wettelijke voorwaarden voor screening	39
3.6.3	Screening via een oud-werkgever	41
3.6.4	Strafrechtelijke screening	42
3.6.5	Screening via sociale media	46
3.7	Informatie tijdens het gesprek	47
3.7.1	Inleiding	47
3.7.2	Controleren identiteit sollicitant	48
3.7.3	Aantekeningen	48
3.7.4	Te stellen vragen	49
3.8	De aanstellingskeuring	50
3.8.1	Inleiding	50
3.8.2	Wanneer gerechtvaardigd?	51
3.8.3	Uit te wisselen gegevens	53
3.8.4	Resultaten van het onderzoek	53
3.8.5	De rol van de ondernemingsraad	54
3.9	Bewaartermijnen	54
3.9.1	Opnemen in portefeuille	54
3.9.2	Maximale reguliere bewaartermijn	56
3.9.3	Privacyrechten	56
4	Het personeelsdossier	59
4.1	Inleiding	59
4.2	De opbouw van het personeelsdossier	59
4.2.1	Inleiding	59
4.2.2	Grondslag en doelbinding	60
4.2.3	Actualiteit, juistheid en noodzakelijkheid van gegevens	62
4.2.4	Rechtmatigheid, behoorlijkheid en transparantie	67
4.2.5	Doelmatigheid	67
4.2.6	Passende beveiliging	68
4.2.7	Privacyrechten	68
4.2.8	Bewaartermijn	69

4.3	Toegang tot het personeelsdossier	71
4.3.1	Need to know-beginsel	71
4.4	Doorgifte van informatie uit het personeelsdossier	73
5	De verwerking van gegevens bij arbeidsongeschiktheid	75
5.1	Inleiding	75
5.2	Verwerkingsverbod	75
5.2.1	Inleiding	75
5.2.2	Passende waarborgen	76
5.2.3	Anonimiseren	78
5.3	De sollicitatiefase	78
5.3.1	Inleiding	78
5.3.2	De aanstellingskeuring	79
5.3.3	Het doelgroepregister	81
5.3.4	De ziekmelding	83
5.3.4.1	Te stellen vragen	83
5.3.5	Begeleiding en re-integratie van de zieke werknemer	89
5.3.5.1	Inleiding	89
5.3.5.2	De verschillende betrokken organisaties en hun rol	90
5.3.5.3	Re-integreren	96
5.3.6	Verzuimsystemen	97
5.3.7	Bewaartermijnen	99
6	Monitoring van de werknemer	103
6.1	Inleiding	103
6.2	Cameratoezicht	103
6.2.1	Inleiding	103
6.2.2	Beperkte omvang en tijdsduur	105
6.2.3	Onjuist gebruik van cameratoezicht	106
6.2.4	Bewaartermijnen	107
6.3	Toegangscontrole versus de registratie van aanwezigheid	108
6.3.1	Inleiding	108
6.3.2	Uitzonderingsgronden	108
6.3.3	Doelbinding	109
6.4	Toezicht telefoongebruik en -gesprekken	110

6.4.1	Inleiding	110
6.4.2	Dure telefoongesprekken	111
6.4.3	Opnemen van (telefoon)gesprekken	112
6.4.4	Privégesprekken	114
6.5	E-mail en internet	115
6.5.1	Inleiding	115
6.5.2	Incidentele controle	116
6.6	Trackingsystemen	118
6.6.1	Inleiding	118
6.6.2	De black box	120
6.6.3	Informatievoorziening werknemer	120
6.7	Controleren van gebruik verdovende middelen	121
6.7.1	Inleiding	121
6.7.2	Grondslag	121
6.7.3	Voorschriften	122
6.7.4	Testen op gebruik verdovende middelen	123
7	Controle van het gedrag van de werknemer	129
7.1	Inleiding	129
7.2	Gebruik van informatiesystemen door de werknemer	129
7.2.1	Inleiding	129
7.2.2	Need-to-know-principe	129
7.2.3	Ontslag na misbruik informatiesysteem	131
7.3	Gebruik van eigen apparaten	133
7.4	Thuiswerken	135
7.4.1	Inleiding	135
7.4.2	Controle van de werkplek	135
7.4.3	Privacywaarborgen	137
7.5	Sociale media	139
7.5.1	Inleiding	139
7.5.2	Socialemedia-code	139
7.5.3	Sociale media en ontslag	143
8	Offboarding: vertrek van een medewerker	145
8.1	Inleiding	145

8.2	In te leveren zaken	145
8.2.1	Inlogcodes, toegangspassen en andere identificatiemiddelen	145
8.3	Opschonen personeelsdossier	146
8.3.1	Inleiding	146
8.3.2	Opschoning door de werknemer	147
8.3.3	Bewaartermijnen	148
8.4	Sociale media	149
8.4.1	Inleiding	149
8.4.2	Concurrentie- en relatiebeding	149
8.5	Overdracht van het personeelsdossier	150
8.6	Referenties	151
8.7	Privégedragingen en ontslag	152
8.7.1	Inleiding	152
8.7.2	Basis voor het ontslag	153
8.7.3	Gedragsregels	154
8.7.4	Veelvoorkomende voorbeelden	155
9	Hoofdpijnen beleid 'privacy op de werkplek'	157
9.1	Inleiding	157
9.2	Managementrollen	158
9.3	Gegevensbeschermingseffectbeoordeling (DPIA)	159
9.4	Ondernemingsraad	161
9.5	Functionaris voor de gegevensbescherming	163
9.6	Register	165
9.7	Transparantie	166
9.8	HR	167

Inleiding

Wie met personeel werkt, heeft te maken met strenge eisen. Niet alleen vanuit het arbeidsrecht of vanuit fiscale wetgeving, maar meer nog (en ook meer dan ooit) vanuit privacywetgeving. Werkgevers beschikken immers over behoorlijk wat persoonlijke informatie. Dat begint al met de kopie van het legitimatiebewijs waarover de werkgever dient te beschikken, maar het geldt ook voor informatie over arbeidsongeschiktheid en waar nodig ook het strafrechtelijk verleden, bijvoorbeeld in functies waarvoor een Verklaring Omtrent het Gedrag (VOG) vereist is. Weet u bijvoorbeeld hoe in uw organisatie medische informatie wordt bewaard? En weet u ook hoe uw casemanager dit aanpakt? Wie vervolgens door middel van camerabeelden de werkplek wenst te beveiligen komt voor nieuwe vraagstukken te staan, om nog maar te zwijgen van de werkgever die zijn bedrijfswagens wenst te tracken.

Daar komt nog bij dat de werkgever niet alleen voorzichtig dient om te gaan met de persoonsgegevens van zijn personeel, maar ook dat hij maatregelen moet treffen om zijn personeel veilig met de persoonsgegevens van klanten, leveranciers en overige betrokkenen om te laten springen. Het eenmalig uitrollen van enkele AVG-documenten en -procedures is daarbij onvoldoende. Een bedrijf, en daarmee de bedrijfsprocessen zullen voortdurend evolueren, en daarbij moet men ook de privacybeschermende maatregelen doorlopend evalueren. Dit zien we ook bijvoorbeeld in de financiële sector; integriteitsregels gelden als een groot goed, maar wie niet regelmatig op dit vlak zijn personeel traint, krijgt het deksel op de neus wanneer vanwege integriteitskwesaties sanctionerende maatregelen zijn getroffen en de werknemer dit aan de rechter voorlegt.

In dit boek wordt beoogd om die middelen aan te reiken die nodig zijn om de privacy op de werkvloer te borgen. Dit boek is daarmee een handig hulpmiddel voor eenieder die te maken heeft met de verwerking van persoonsgegevens van werknemers. Wij menen dat het boek in ieder geval relevant zal zijn voor de afdelingen HR en ICT, de ondernemingsraad, het

management en de directie, maar ook bijvoorbeeld voor de salarisadministrateur, het administratiekantoor en de accountant.

Voor een uitgebreide, algemene artikelsgewijze behandeling van de AVG verwijzen wij u naar andere bronnen. In dit boek bespreken wij vooral de onderdelen die van belang zijn voor het thema 'privacy op de werkplek'. Het vormt dan ook nadrukkelijk geen algemene inleiding op de AVG, maar zoekt de diepte op binnen dit thema.

De kern van dit boek bestaat uit een zestal thematische hoofdstukken waarin, gebaseerd op wet- en regelgeving en jurisprudentie, de spelregels uiteengezet worden voor de verschillende categorieën persoonsgegevens van werknemers:

- Hoofdstuk 3: gegevens in verband met sollicitaties ('onboarding')
- Hoofdstuk 4: gegevens in het personeelsdossier
- Hoofdstuk 5: gegevens in verband met arbeidsongeschiktheid
- Hoofdstuk 6: gegevens in het kader van de controle van het gedrag van werknemers
- Hoofdstuk 7: gegevens in het kader van monitoring van werknemers (zoals cameratoezicht)
- Hoofdstuk 8: werknemersgegevens in verband met de beëindiging van het dienstverband ('offboarding')

Deze hoofdstukken hebben het karakter van een naslagwerk. Hierbij beseffen wij dat niet alle onderwerpen (uitvoerig) behandeld worden. Een voorbeeld is de wettelijk of contractueel verplichte doorgifte van persoonsgegevens aan Belastingdienst, UWV, pensioenfondsen et cetera. Dit is een verplichte doorgifte, zodat hierover in het kader van dit boek niet veel bijzonderheden te delen zijn. Ook het brede scala aan applicaties in HR-omgeving voor competentie-management, leren, beoordeling & feedback, surveys wordt in deze uitgave niet meegenomen, omdat het te ver voert om al deze applicaties te bespreken. Hiervoor gelden uiteraard dezelfde algemene wettelijke bepalingen als voor de verwerkingen die wél worden besproken.

In hoofdstuk 1 worden de belangrijkste begrippen van informationele privacy en de wettelijke basis besproken. Kernboodschap is dat bescherming meer inhoudt dan slechts de in te regelen informatiebeveiliging, al is dat wel een randvoorwaarde voor een goede implementatie van de AVG. Informatiebeveiliging wordt hier en daar aangestipt (bijvoorbeeld waar het gaat om specifieke eisen bij bijzondere gegevens), maar niet uitvoerig besproken.

Hoofdstuk 2 schetst vanuit het veranderende ICT-landschap dat de scope van persoonsgegevens tegenwoordig veel ruimer is dan het traditionele HR-domein. Applicaties en netwerksystemen leggen op grote schaal direct of indirect persoonsgegevens vast die ook voor allerlei nevendoeleinden kunnen worden gebruikt. In hoofdstuk 6 (over gedrag) en 7 (over monitoring) wordt dit verder uitgewerkt.

Ten slotte wordt in hoofdstuk 9 verkend op welke wijze bij de invoering van nieuwe applicaties de samenwerking tussen de actoren in een organisatie gestalte krijgt.

De ondernemingsraad kan hierin een belangrijke rol spelen. De AVG noemt de ondernemingsraad weliswaar niet, maar de Wet op de ondernemingsraden geeft de ondernemingsraad wel een duidelijke rol via het instemmingsrecht bij de verwerking van persoonsgegevens (artikel 27.1.k) en zelfs bij het invoeren van de technische mogelijkheid tot het verwerken van gegevens over prestatie, aanwezigheid en gedrag (artikel 27.1.l). Zoals dat hoofdstuk ook besluit: alleen bij een goede samenwerking en dialoog komt de juiste balans tot stand tussen het gerechtvaardigd belang van de werkgever en het privacybelang van de werknemer.

Om de functie van naslagwerk te ondersteunen is er een uitgebreid trefwoordenregister opgenomen. Ten slotte is er een bijlage gemaakt met een aantal nuttige bronnen voor aanvullende informatie.

Over de auteurs

Melanie Hermes is zelfstandig advocaat en is gespecialiseerd in het arbeids- en privacyrecht. Zij geeft over deze onderwerpen trainingen en heeft al vele MKB-ondernemers geholpen bij de implementatie van de AVG binnen hun bedrijf. Daarnaast is zij de functionaris voor de gegevensbescherming voor diverse bedrijven.

Arjen van Halem is zelfstandig onderzoeker en adviseur op het gebied van technologie en arbeid, meestal in opdracht van (internationale) vakorganisaties en ondernemingsraden. De laatste jaren heeft hij zich sterk beziggehouden met ‘privacy op de werkplek’ als adviseur van ondernemingsraden bij grotere ondernemingen.

Bronnen en literatuur

De Autoriteit Persoonsgegevens heeft een laagdrempelige website gelanceerd over privacy: hulpbijprivacy.nl.

Checklist CBP over screening van de werknemer: autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/cbp_screening.pdf.

AP over screening van de werknemer: autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/screening.

NVP Sollicitatiecode: nvp-hrnetwerk.nl/sollicitatiecode/.

Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, opgesteld in opdracht van het Ministerie van Justitie en Veiligheid, 8 januari 2018.

Meer informatie over de Verklaring Omtrent het Gedrag (VOG): justis.nl/producten/vog/.

Het opiniestuk van de Artikel 29-werkgroep over dataverwerking op het werk: Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work.

Meer informatie over de Risico-inventarisatie en -evaluatie is te vinden via: arboportaal.nl/onderwerpen/arbobeleid.

Meer informatie over de aanstellingskeuring: aanstellingskeuringen.nl/.

Hoe u een klacht indien bij de AP leest u terug via: autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-indienen-bij-de-ap.

De Autoriteit Persoonsgegevens heeft een webpagina over het personeelsdossier ingericht: autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/personeelsdossiers.

Hoe als werkgever of inlener om te gaan met het legitimatiebewijs leest u uitgebreid via <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/identiteitsbewijs>.

Meer informatie over anonimiseringstechnieken leest u via WP29, Advies 5/2014 over anonimiseringstechnieken, WP 216, 10 april 2014.

Het Abrona-rapport geeft meer inzicht in de gegevens die u (niet) mag vragen bij een ziekmelding: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_abrona_definitieve_bevindingen_openbare_versie.pdf.

Eveneens meer informatie over de informatie die u (niet) mag vragen bij een ziekmelding: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_de_zieke_werknemer.pdf.

Informatie over internationale verschillen in privacywet- en regelgeving:

- DLA Piper: www.dlapiperdataprotection.com/
- BakerMcKenzie: www.globaltmt.bakermckenzie.com/data-privacy-security

1 De bescherming van persoonsgegevens, een introductie

1.1 Privacy: meer dan gegevensverwerking

Het recht om met rust gelaten te worden. Met deze benadering van het ‘right to privacy’ uit 1890 begint het moderne westerse denken over privacy. Achtergrond destijds was de bescherming van bekende Amerikanen tegen de nieuwe media van toen (‘newspaperization’ met instant camera’s, krantenbedrijven, etc.).

Sindsdien heeft ‘privacy’ zich ontwikkeld tot het grondrecht ‘bescherming van de persoonlijke levenssfeer’ dat is verankerd in vele internationale verdragen en in de Nederlandse Grondwet.

Sinds 1983, toen de gehele Grondwet is gemoderniseerd, staat in artikel 10: “Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.” De persoonlijke levenssfeer omvat overigens meer dan alleen de verwerking van persoonsgegevens (waar de AVG betrekking op heeft). Ook de grondrechten huisrecht, briefgeheim en eerbiediging van de lichamelijke integriteit vallen eronder, maar ook het recht om niet te worden bespied of afgeluis-terd.

De Grondwet laat ook zien dat het recht op bescherming van de persoonlijke levenssfeer niet absoluut is. Via wetgeving kunnen hier beperkingen aan worden gesteld. De AVG is hiervan een goed voorbeeld. De Grondwet lijkt te suggereren dat de persoonlijke levenssfeer alleen betrekking heeft op wat we ‘privé’ noemen: de woning, de brief of het eigen lichaam. De persoonlijke levenssfeer heeft echter ook betrekking op onder meer het openbare domein (denk aan het stemgeheim en het verbod op heimelijk cameratoezicht) en de arbeidsrelatie. Met het aangaan van een arbeidsrelatie houdt het recht op bescherming van de persoonlijke

levenssfeer immers niet op. En dat geldt niet alleen voor de verwerking van persoonsgegevens (het controleren van e-mails), maar ook voor lichamelijke integriteit (denk aan visitatie en drugstesten), relationele privacy (bijvoorbeeld een relatie tussen twee collega's) en ruimtelijke privacy (het controleren van lockers).

In dit boek richten we ons op de bescherming van persoonsgegevens, het domein van de AVG. Het is een hulpmiddel in de zoektocht naar een balans tussen het recht van de werkgever op het verwerken van gegevens die noodzakelijk zijn voor het functioneren van de onderneming en het recht van de werknemer op bescherming van de verwerking van persoonsgegevens. Een goede balans vinden is niet makkelijk.

Ten eerste zijn de opvattingen over de grenzen van de persoonlijke levenssfeer cultureel bepaald. Zelfs tussen de westerse landen zijn de verschillen groot. Zo liggen gegevens over inkomens in de Verenigde Staten veel minder gevoelig, maar gegevens over leeftijd juist meer. Ook tussen Europese landen zijn er verschillen. De Europese AVG brengt daarin geen verandering en biedt daar in artikel 88 voor werknemers zelfs de ruimte voor. Zo wordt in Duitsland door werkgevers de geloofsovertuiging van werknemers geregistreerd ten behoeve van de afdracht van de 'Kirchensteuer'¹. In Nederland is daar geen wettelijke grondslag voor. Ook tussen mensen zijn de verschillen groot. Kijk maar naar het gebruik van sociale media. Zo hoor je werknemers weleens zeggen: 'Mijn baas mag alles van me weten, ik heb geen geheimen.'

Ten tweede verandert wat wij gewoon vinden bijna net zo snel als de technologie. Kijk maar naar cameratoezicht. De eerste camera's leidden tot veel ongemak en discussie. Nu hangen ze overal in steden en langs snelwegen.

Wat het daarbij lastig maakt is dat wet- en regelgeving weinig concrete grenzen biedt over wat wel en niet mag. Het gaat steeds om de context.

¹ Kerkbelasting die wordt afgedragen via de werkgever.

Tegen deze achtergrond is de norm ‘redelijke verwachting van bescherming van de persoonlijke levenssfeer’ ontwikkeld. Wat een redelijke verwachting is, hangt steeds af van tijd en plaats. De AVG biedt in samenhang met vele andere wetten het kader om de juiste balans te vinden.

1.2 Bescherming van persoonsgegevens: meer dan beveiliging

De AVG, maar ook de hier aan voorafgaande Europese Richtlijn is gebaseerd op een achttal principes die door de OESO in 1980 zijn vastgesteld:

- Beperk het verzamelen van persoonsgegevens.
- Gebruik alleen de gegevens die relevant zijn voor het doel en voldoende up-to-date zijn.
- Verzamel de gegevens alleen voor een specifiek doel.
- Gebruik de gegevens niet voor een ander doel dan omschreven.
- Zorg voor voldoende beveiligingsmaatregelen.
- Geef openheid over het gebruik van persoonsgegevens.
- Het individu heeft het recht om te achterhalen of er gegevens over hem worden verzameld en het recht deze te corrigeren, aan te vullen of te laten verwijderen.
- De beheerder is verantwoordelijk voor de naleving van de beginselen.

Deze principes zijn ook het fundament van veel wetgeving buiten Europa.

De naam van de Europese Verordening, de Algemene verordening *gegevensbescherming*, kan de indruk wekken dat – net als bij de Wet *bescherming* persoonsgegevens – de kern van dataprivacy de *beveiliging* van persoonsgegevens is. En dat als die beveiliging van de gegevens op orde is (met encryptie, ISO-standaards, contracten), er aan de AVG wordt voldaan. Maar dat is niet zo. Bescherming van persoonsgegevens gaat ook over beperking van de toegang en over beperking van de verwerking