Ministerie van Justitie en Veiligheid

Handleiding Algemene verordening gegevensbescherming

en Uitvoeringswet Algemene verordening gegevensbescherming

Handleiding Algemene verordening gegevensbescherming

en Uitvoeringswet Algemene verordening gegevensbescherming

Auteur(s):	Bart W. Schermer, Dominique Hagenauw, Nathalie Falot
Opdrachtgever:	Ministerie van Justitie en Veiligheid
Contactpersoon:	Pauline Verhaak, p.m.verhaak@minjenv.nl

Inhoudsopgave

1 Inleiding

25 mei 2018 is de Algemene Verordening Gegevensbescherming ('Verordening' of 'AVG') rechtstreeks van toepassing in alle lidstaten van de Europese Unie. De Verordening is de opvolger van de Wet bescherming persoonsgegevens in Nederland. Het doel van de Verordening is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie ('EU').
In deze handleiding worden de belangrijkste bepalingen uit de Verordening en Nederlandse Uitvoeringswet Algemene verordening gegevensbescherming (de 'Uitvoeringswet' of 'UAVG') toegelicht. De handleiding vervangt de Handleiding Wbp.
De handleiding is samengesteld door juridisch adviesbureau Considerati onder auspiciën van het Ministerie van Justitie en Veiligheid. Een externe klankbordgroep is geraadpleegd bij de totstandkoming van de handleiding. Een overzicht van vertegenwoordigde organisaties en inhoudelijk deskundigen is opgenomen in paragraaf 10.2.

Deze handleiding is gericht op iedereen die meer wil weten over de Verordening en de Uitvoeringswet, maar is primair gericht aan 'verwerkingsverantwoordelijken', dat wil zeggen, degenen die voor een bepaald doel gegevens van personen willen gaan verwerken. Deze handleiding is in het bijzonder bedoeld voor lezers die reeds enigszins op de hoogte zijn van het gegevensbeschermingsrecht en op zoek zijn naar verdere verdieping, om zo binnen hun organisatie de maatregelen die de Verordening vereist te kunnen implementeren. Voornaamste doelgroepen zijn daarmee (beginnende) functionarissen voor gegevensbescherming, privacy officers, bedrijfsjuristen, compliance managers, risk managers en security officers.

Bij het lezen van deze handleiding is het goed om de volgende twee zaken in het achterhoofd te houden.

Allereerst het vraagstuk betreffende het toepasselijk recht (zie hoofdstuk 3). De Verordening heeft rechtstreekse werking binnen de gehele Europese Unie en harmoniseert daarmee de regels voor de bescherming van persoonsgegevens. Maar, op specifieke punten biedt de Verordening lidstaten de ruimte om nadere invulling te geven aan de bepalingen. Deze invulling geschiedt via zogenaamde uitvoeringswetten. Deze handleiding is geschreven vanuit het perspectief van de Nederlandse Uitvoeringswet. Houd er rekening mee dat afhankelijk van uw specifieke situatie niet de Nederlandse, maar een andere uitvoeringswet op uw gegevensverwerkingen van toepassing kan zijn. De inhoud daarvan kan afwijken van hetgeen in deze handleiding is beschreven.

Ten tweede het vraagstuk over de interpretatie van de Verordening. De Verordening is een omvangrijk stuk wetgeving met slechts een beperkte schriftelijke toelichting. Op veel punten is het daarom (nog) onduidelijk wat de precieze invulling is die gegeven moet worden aan begrippen en bepalingen. Omdat de Verordening een Europese wet is waarvan de verdere invulling aan de toezichthouder(s) en de Europese rechter is, wordt in deze handleiding slechts zeer beperkt vooruitgelopen op de interpretatie van nu nog onduidelijke begrippen. Daar waar er in het bijzonder onduidelijkheid is over de invulling en interpretatie van begrippen wordt dit expliciet vermeld.

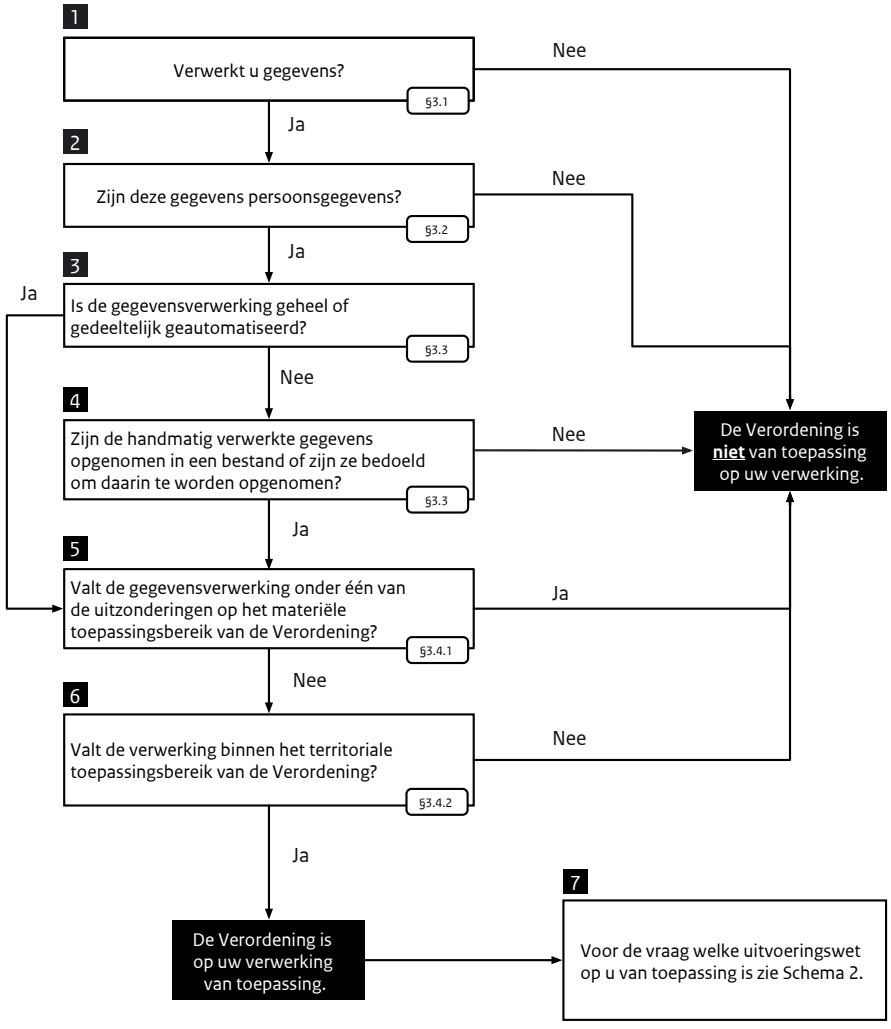
In de handleiding wordt waar nuttig verwezen naar de Uitvoeringswet Algemene verordening gegevensbescherming. Daarbij wordt opgemerkt dat het wetsvoorstel nog in de fase van de parlementaire behandeling is en kan wijzigen. In een volgende versie van de handleiding zal meer uitgebreid aandacht aan de Uitvoeringswet worden geschonken.

De elektronische versie van deze handleiding wordt in het licht van het bovenstaande periodiek herzien om de laatste ontwikkelingen op het gebied van de toepassing en de uitleg van de Verordening mee te nemen. U kunt de laatste versie van deze handleiding vinden op: *www.rijksoverheid.nl/avg*

Den Haag, 8 januari 2018
Ministerie van Justitie en Veiligheid

Stroomdiagrammen en checklists

Schema 1: Is de Verordening op u van toepassing?

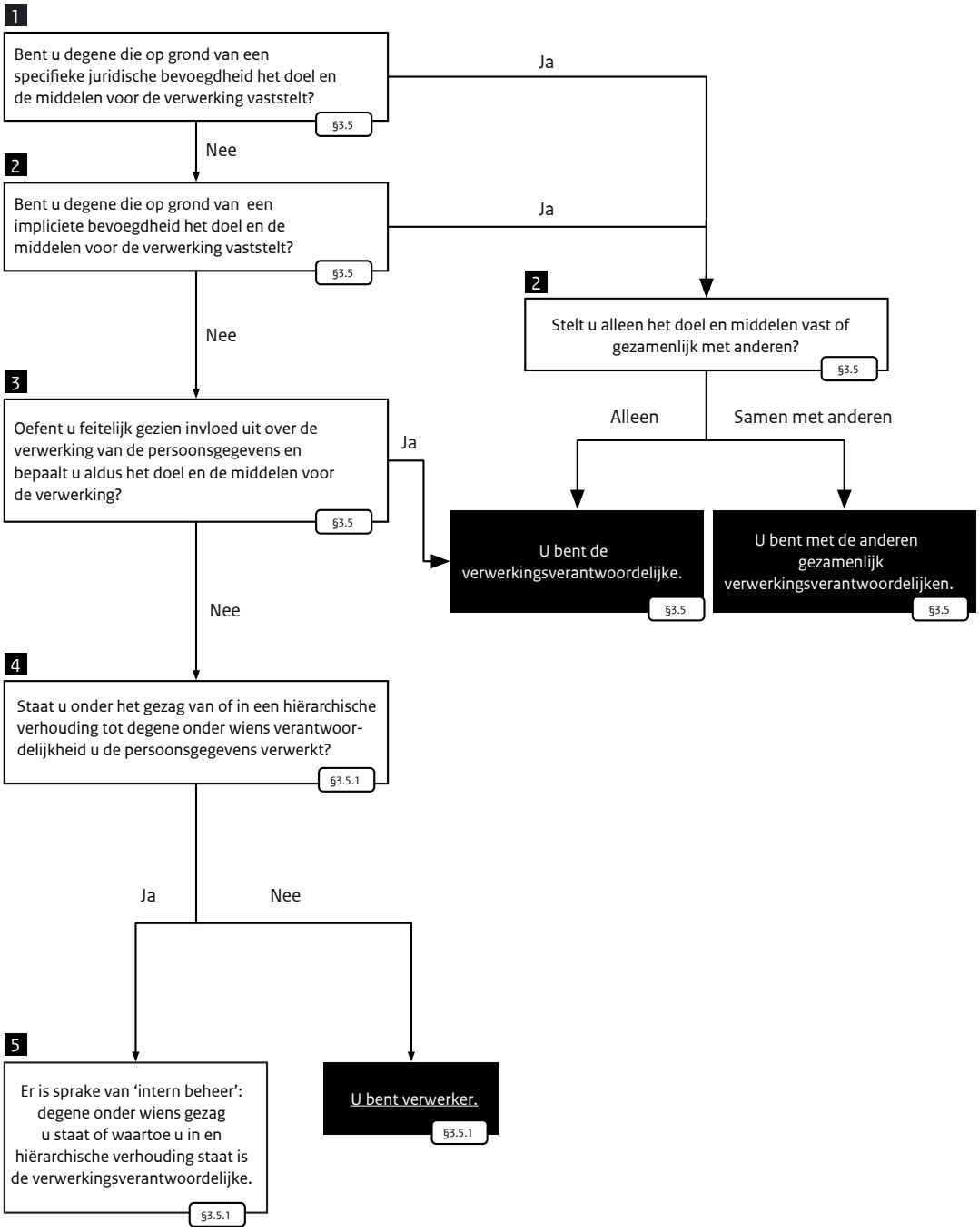


Schema 2: Welke uitvoeringswet is op u van toepassing?

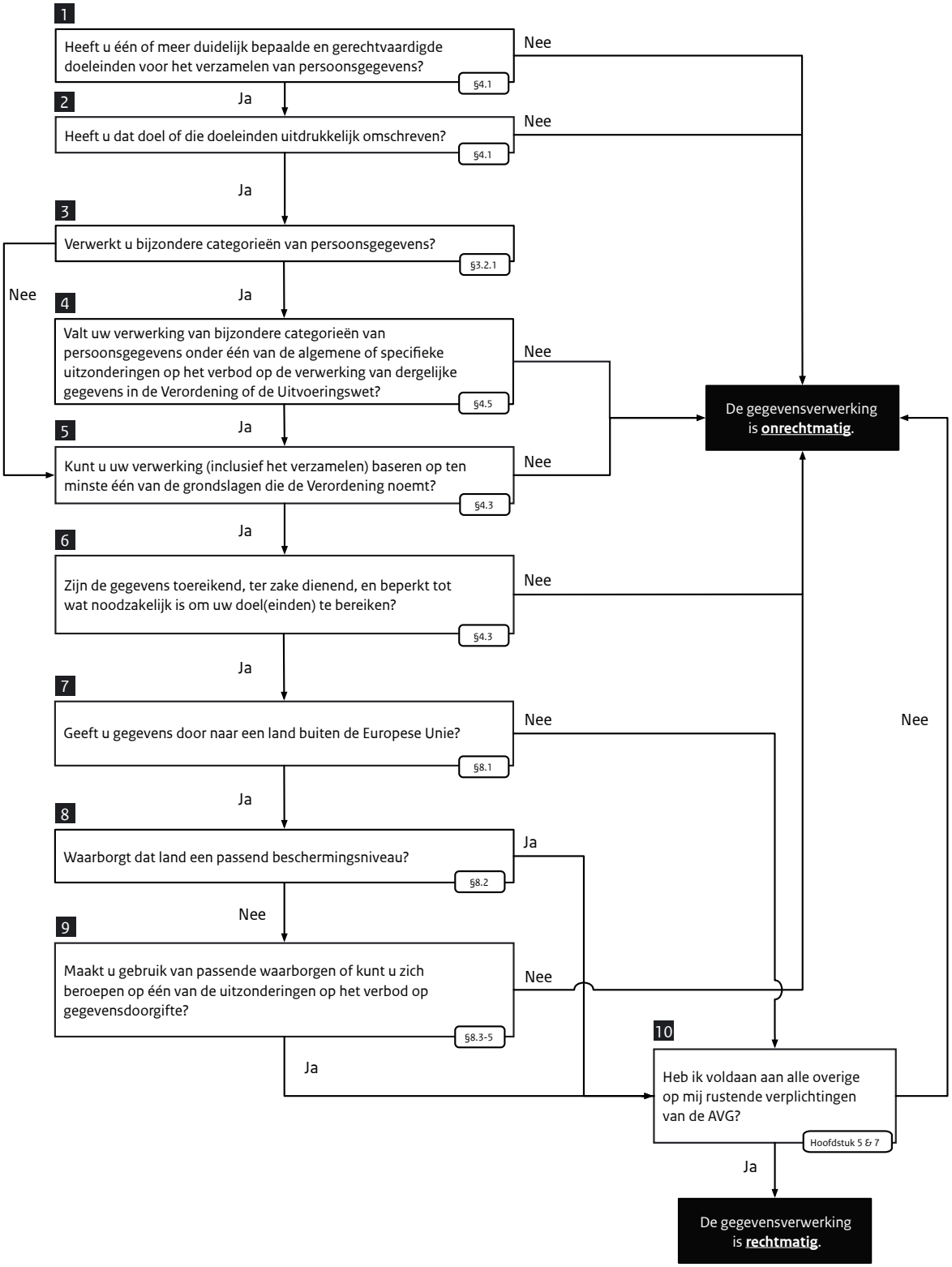
Het onderstaande schema laat voor veelvoorkomende situaties zien welke uitvoeringswetgeving van toepassing is (de Nederlandse Uitvoeringswet Algemene verordening gegevensbescherming of de uitvoeringswetgeving van een andere lidstaat). Houd er bij het gebruik van dit schema rekening mee dat het niet uitputtend is en dat voor de keuze van het toepasselijke recht ook de keuzes in de uitvoeringswetgeving van de andere lidstaten van belang zijn.

Vestigingsplaats verwerker/verwerkings-verantwoordelijke	Woonplaats betrokkene of plaats gedragingen van betrokkene	Toepasselijk recht zoals volgend uit de Verordening en de Uitvoeringswet
Buiten de Europese Unie	Buiten Nederland, buiten de Europese Unie	Verordening niet van toepassing
Buiten de Europese Unie	Buiten Nederland, binnen een andere lidstaat dan Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere lidstaat van toepassing
Buiten de Europese Unie	Binnen Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing
Binnen de Europese Unie, in een andere lidstaat dan Nederland	Binnen de Europese Unie, in deze andere lidstaat dan Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere nationale lidstaat waar de verwerkingsverantwoordelijke /verwerker is gevestigd, is van toepassing
Binnen de Europese Unie, in een andere lidstaat dan Nederland	Binnen Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere nationale lidstaat van toepassing
Binnen de Europese Unie, in een andere lidstaat dan Nederland	Buiten de Europese Unie	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere nationale lidstaat van toepassing
Binnen Nederland	Binnen Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing
Binnen Nederland	In een andere lidstaat dan Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing
Binnen Nederland	Buiten de Europese Unie	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing

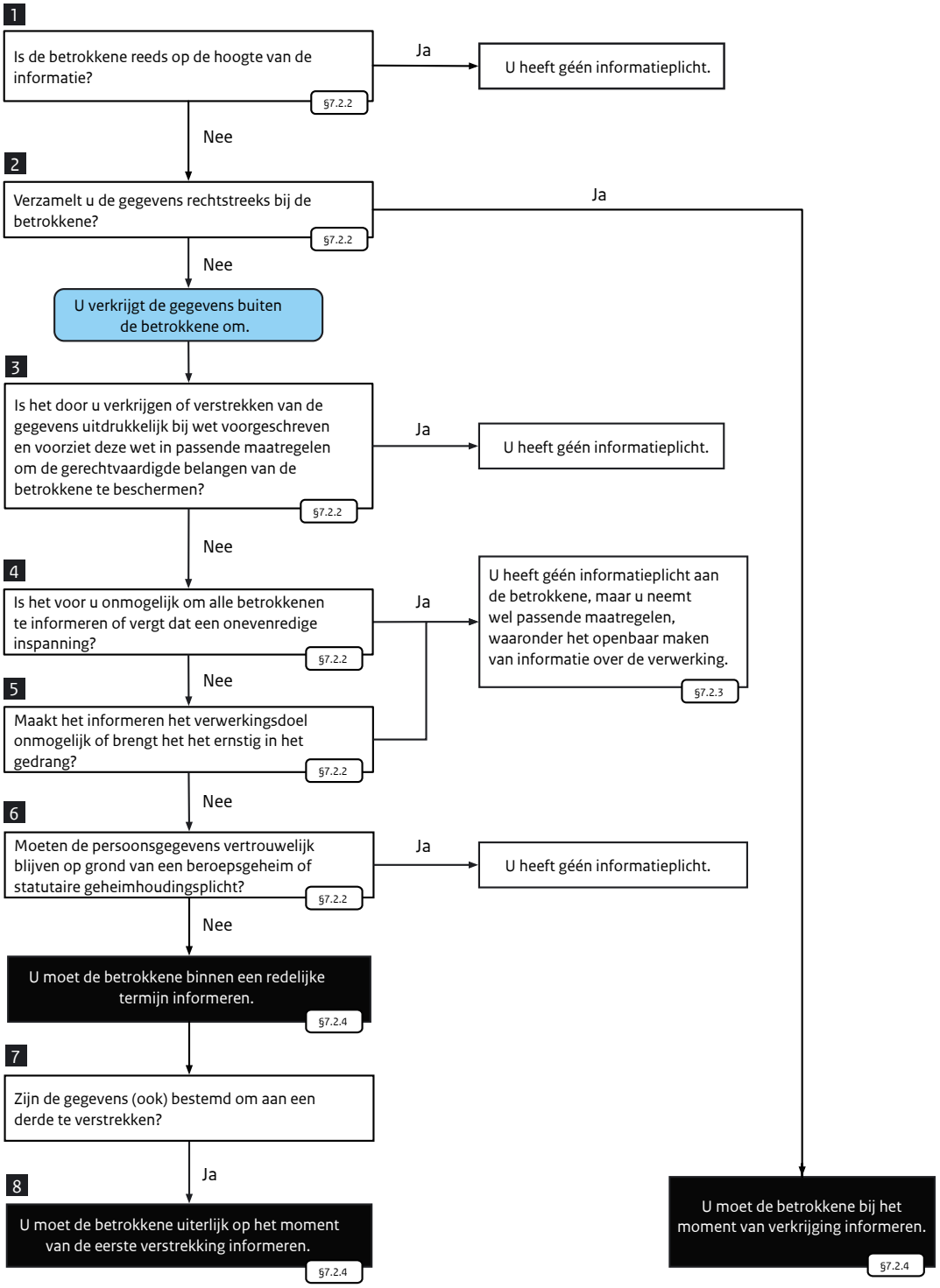
Schema 3: Bent u een verwerkingsverantwoordelijke of verwerker?



Schema 4: Is uw gegevensverwerking rechtmatig?



Schema 5: Wanneer moet u de betrokkene informeren over een verwerking van persoonsgegevens?



ZIE § 7.2.3: WELKE INFORMATIE MOET U VERSTREKKEN?

Checklist 1: Wat zijn de plichten van de verwerkingsverantwoordelijke?

Op grond van de Verordening moet elke verwerking van persoonsgegevens voldoen aan de volgende beginselen:

- de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn ("rechtmatigheid, behoorlijkheid en transparantie");
- de verwerking moet gebonden zijn aan specifieke verzameldoelen ("doelbinding");
- de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is ("minimale gegevensverwerking");
- de gegevens moeten juist zijn ("juistheid");
- de gegevens mogen niet langer worden bewaard dan nodig ("opslagbeperking");
- gegevens moeten goed beveiligd zijn en vertrouwelijk blijven ("integriteit en vertrouwelijkheid").

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en moet ook kunnen aantonen dat een verwerking van persoonsgegevens aan deze beginselen voldoet (de verantwoordingsplicht). Concreet dient de verwerkingsverantwoordelijke hiertoe:

- een register van verwerkingsactiviteiten bij te houden (de registerplicht);
- onder bepaalde omstandigheden een functionaris voor gegevensbescherming aan te stellen;
- voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling uit te voeren;
- de Autoriteit Persoonsgegevens onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit te raadplegen (voorafgaande raadpleging);
- bij het inrichten van verwerkingen rekening te houden met het principe van privacy door ontwerp en standaardinstellingen (*privacy by design & default*);
- passende beveiligingsmaatregelen te treffen met het oog op de bescherming van persoonsgegevens;
- in het geval van een datalek melding te doen bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden ook bij de betrokkenen;
- afspraken te maken met verwerkers.
- medewerking te verlenen aan de Autoriteit Persoonsgegevens.

Tenslotte dient de verwerkingsverantwoordelijke de rechten van de betrokkenen te respecteren en in te vullen (zie Checklist 3 en Hoofdstuk 7).

Checklist 2: Wat zijn de plichten van de verwerker?

De belangrijkste plichten op grond van de Verordening voor de verwerker zijn:

- de verwerker mag alleen handelen in opdracht van de verwerkingsverantwoordelijke;
- de verwerker wordt verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die hij verwerkt in opdracht van de verwerkingsverantwoordelijke (registerplicht);
- de verwerker moet passende technische en organisatorische beveiligingsmaatregelen nemen die een passend beschermingsniveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen;
- de verwerker mag geen sub-verwerkers inschakelen zonder toestemming van de verwerkingsverantwoordelijke;
- de verwerker moet de verwerkingsverantwoordelijke onverwijld op de hoogte stellen van een datalek;
- de verwerker is verplicht medewerking te verlenen bij een verzoek van de toezichthouder (Autoriteit Persoonsgegevens) in het kader van de uitoefening van diens taken;
- de verwerker dient in bepaalde gevallen een functionaris voor gegevensbescherming aan te stellen.

Checklist 3: Welke informatie moet u verstrekken aan de betrokkene?

U verzamelt de gegevens bij de betrokkene zelf
Wanneer u de gegevens bij de betrokkene zelf verzamelt, dan moet u tenminste de volgende informatie verstrekken bij de verkrijging:

- uw identiteit en uw contactgegevens, of de contactgegevens van uw vertegenwoordiger;
- indien u een functionaris voor de gegevensbescherming hebt aangesteld, de contactgegevens van deze functionaris;
- de doelen waarvoor u persoonsgegevens verwerkt;
- de grondslag waarop u de verwerking baseert;
- wanneer u de verwerking baseert op de grondslag 'gerechtvaardigd belang': wat uw gerechtvaardigd belang is;
- de eventuele ontvangers of categorieën ontvangers van de gegevens;
- in geval van verstrekking aan derde landen:
  - of er een adequaatheidsbesluit van de Commissie bestaat,
  - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd;
- de bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan;
- de rechten van de betrokkene (beschreven in hoofdstuk 7);
- in het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken;
- dat de betrokkene het recht heeft een klacht in te dienen over uw verwerking bij de Autoriteit Persoonsgegevens;
- of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die gegevens voor de betrokkene;
- in geval van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene.

Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen. U moet zelf bepalen welke aanvullende informatie naast deze verplichte elementen het eventueel zou betreffen.

Als u de persoonsgegevens voor andere doelen verder gaat verwerken, moet u de betrokkene opnieuw informeren over dat nieuwe doel en opnieuw alle hierboven genoemde informatie verstrekken, behalve voor zover de betrokkene al van die informatie op de hoogte is.

U verkrijgt de gegevens buiten de betrokkene om
Wanneer u gegevens verzamelt buiten de betrokkene om, dan moet u in beginsel dezelfde informatie verstrekken als wanneer u de gegevens van de betrokkene zelf heeft gekregen. Het enige dat u moet toevoegen is de bron waaruit de persoonsgegevens zijn verkregen. Als de bron van de informatie niet kan worden vastgesteld dient u algemene informatie over de herkomst te verstrekken.

Checklist 4: Eisen aan de verwerkersovereenkomst

In een verwerkersovereenkomst dienen tenminste de volgende zaken te worden vermeld:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Verder dient in de verwerkersovereenkomst te worden bepaald dat de verwerker:

- de persoonsgegevens alleen verwerkt onder de schriftelijke instructies van de verwerkingsverantwoordelijke, onder andere voor wat betreft de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht);
- waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- minimaal hetzelfde niveau van beveiliging van de persoonsgegevens hanteert als de verwerkingsverantwoordelijke;
- de verwerkingsverantwoordelijke alle mogelijke ondersteuning biedt bij het nakomen van diens verplichtingen met het oog op de beantwoording van verzoeken rondom de rechten van betrokkenen;
- de verwerkingsverantwoordelijke bijstaat bij het nakomen van diens verplichtingen op het gebied van de beveiliging van persoonsgegevens en de meldplicht datalekken;
- na beëindiging van de overeenkomst de in opdracht van de verwerkingsverantwoordelijke verwerkte persoonsgegevens wist of teruggeeft, en bestaande kopieën verwijdert;
- de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de Verordening rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- afspraken met betrekking tot sub-verwerkers maakt.

2 De Algemene verordening gegevensbescherming

De bescherming van persoonsgegevens is een grondrecht dat in het Handvest van de grondrechten van de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is vastgelegd. De Algemene verordening gegevensbescherming ('Verordening' of 'AVG'), is een Europese wet die de bescherming van dit grondrecht regelt.

De Verordening is vanaf 25 mei 2018 rechtstreeks toepasselijk in de hele Europese Unie en vervangt de Nederlandse Wet bescherming persoonsgegevens. De Nederlandse Wet bescherming persoonsgegevens was gebaseerd op de voorloper van de Verordening, de Europese Richtlijn gegevensbescherming (95/46/EG).

2.1 Eén gegevensbeschermingswet voor de hele Europese Unie

Een verordening is een Europese wet die rechtstreekse werking heeft in de hele Europese Unie. Dit in tegenstelling tot een richtlijn, die eerst naar nationaal recht moet worden omgezet. Er is dus geen Nederlandse implementatie van de Verordening, slechts een Nederlandse taalversie. De Verordening is dan ook gelijk voor alle lidstaten van de Europese Unie.

De Verordening heeft als wetgevend instrument voorrang op ons nationale recht. Dit betekent dat er op nationaal niveau geen wet- en regelgeving mag zijn die in strijd is met de bepalingen uit de Verordening en dat de rechten en plichten uit de Verordening rechtstreeks gelden voor personen en organisaties in Nederland. Het grote verschil ten opzichte van het systeem van de Richtlijn gegevensbescherming is dat er nu één gegevensbeschermingswet is voor de hele Europese Unie in plaats van allerlei nationale wetten die weliswaar gebaseerd zijn op dezelfde richtlijn, maar toch overal net weer anders zijn.

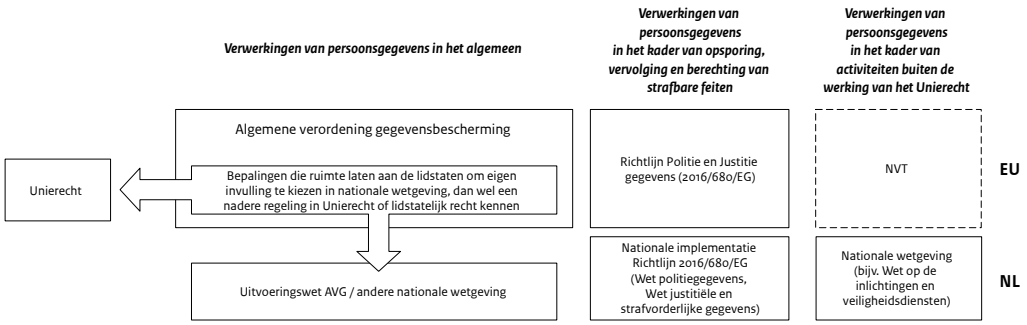
Hoewel het doel van de Verordening een geharmoniseerd gegevensbeschermingsrecht is, biedt de Verordening de lidstaten toch op een heel aantal punten ruimte om specifieke bepalingen op te nemen of uitzonderingen te maken. Het gaat dan bijvoorbeeld om de regels omtrent de verwerking van bijzondere categorieën van persoonsgegevens en de invulling van de rechten van de betrokkenen. In Nederland zijn deze specifieke bepalingen vastgelegd in de *Uitvoeringswet Algemene verordening gegevensbescherming* (de 'Uitvoeringswet' of 'UAVG') en ook in sectorale wetten die bepalingen bevatten over de verwerking van persoonsgegevens op het terrein dat zij bestrijken.

Daarnaast wordt op een aantal punten in de Verordening verwezen naar Unierecht en lidstatelijk recht voor nadere regeling. Zo eist de Verordening bijvoorbeeld dat de rechtsgronden voor het verwerken van persoonsgegevens in het kader van een wettelijke plicht of publieke taak bij Unierecht of lidstatelijk recht zijn vastgelegd (zie hoofdstuk 4). Dit betekent dat daar waar de Nederlandse overheid een taak heeft en daarbij persoonsgegevens verwerkt, dit vastgelegd moet zijn in een wet. In Nederland moet u dan bijvoorbeeld denken aan wetgeving op het gebied van belastingen, onderwijs, sociale zekerheid en volksgezondheid.

Het systeem van een Europese verordening met nadere regelingen op Unie- of lidstaatniveau betekent in de praktijk dat u in veel gevallen meerdere wetten moet raadplegen. Wanneer u wilt weten wat uw rechten en plichten zijn met betrekking tot de verwerking van persoonsgegevens, moet u eerst in de Verordening kijken. Wanneer de Verordening verwijst naar Unierecht of lidstatelijk recht (voor nadere regeling, of voor mogelijkheden om af te wijken van de 'standaardregel'), dan moet u de Uitvoeringswet en/of de specifieke (sectorale) wettelijke regeling(en) erbij pakken waar de Verordening op doelt.

Hoewel u in de meeste gevallen onder de Verordening valt wanneer u persoonsgegevens verwerkt, kent de Verordening wel enkele uitzonderingen. Zo is er bijvoorbeeld een uitzondering voor verwerkingen voor puur huishoudelijke doeleinden. Daarnaast is op bepaalde activiteiten niet de Verordening, maar een andere wet van toepassing. Het verwerken van persoonsgegevens door de politie bij het opsporen van strafbare feiten is bijvoorbeeld uitgezonderd van de Verordening. Hierop is de Wet politiegegevens van toepassing. Op dergelijke uitzonderingen op het 'materiële toepassingsbereik' van de Verordening wordt nader ingegaan in hoofdstuk 4.

Het bovenstaande levert al met al een redelijk complex samenspel van wetten en regels op. Schematisch kunnen we het systeem van gegevensbeschermingsrecht op hoofdlijnen als volgt weergeven:



2.2 Wat regelt de Verordening?

De Verordening regelt de rechtmatige en zorgvuldige omgang met persoonsgegevens binnen de Europese Unie. De Verordening bestaat uit 99 artikelen en 173 overwegingen bij deze artikelen. De artikelen geven de rechten en plichten weer, de overwegingen geven nadere duiding en uitleg over de artikelen. De Verordening heeft de volgende opbouw:

Hoofdstuk 1: Algemene bepalingen (art. 1-4)
Dit hoofdstuk stelt de algemene doelen en het toepassingsbereik (waar en wanneer is de Verordening van toepassing) vast en geeft de in de Verordening gebruikte definities.

Hoofdstuk 2: Beginselen (art. 5-11)
Dit hoofdstuk beschrijft de beginselen waar de verwerking van persoonsgegevens aan moet voldoen, somt de rechtvaardigingsgronden voor het verwerken van persoonsgegevens op en geeft de voorwaarden waaraan toestemming voor het verwerken van persoonsgegevens moet voldoen.

Hoofdstuk 3: Rechten van de betrokkenen (art. 12-23)
Dit hoofdstuk beschrijft de rechten van de betrokkene (recht op informatie, toegang, rectificatie, verwijdering, overdraagbaarheid, bezwaar en beperking) en de mogelijke uitzonderingen en beperkingen daarop. Ook wordt de betrokkenen in dit hoofdstuk het recht geboden om niet te worden onderworpen aan geautomatiseerde besluitvorming en profilering.

Hoofdstuk 4: Verwerkingsverantwoordelijke en verwerker (art. 24-43)
Dit hoofdstuk stelt de eisen waaraan een behoorlijke verwerking van persoonsgegevens moet voldoen. Het gaat om zaken als het aanstellen van een functionaris voor gegevensbescherming, het verplicht registreren van alle verwerkingen en het beveiligen van persoonsgegevens. Ook wordt in dit hoofdstuk de verhouding tussen de verwerkingsverantwoordelijke en de verwerker geregeld. Ten slotte wordt aandacht besteed aan certificering en het gebruik van gedragscodes.

Hoofdstuk 5: Doorgiften van persoonsgegevens aan derde landen of internationale organisaties (art. 44-50)
Dit hoofdstuk stelt de voorwaarden waaronder het is toegestaan om gegevens buiten de Europese Unie te brengen.

Hoofdstuk 6: Onafhankelijke toezichthoudende autoriteiten (art. 51-59)
Dit hoofdstuk beschrijft de rol van de toezichthouder(s) op de Verordening en hun taken en bevoegdheden. In Nederland is de toezichthouder de Autoriteit Persoonsgegevens ('AP'). De rol en positie van de Autoriteit Persoonsgegevens is uitgewerkt in de Uitvoeringswet.

Hoofdstuk 7: Samenwerking en coherentie (art. 60-76)
Omdat de Verordening geldt in heel Europa, moet het toezicht op de Verordening ook geharmoniseerd zijn. Dit hoofdstuk beschrijft de samenwerking tussen de nationale toezichthouders en de manier waarop in Europees verband toezichthouders tot uniforme toepassing van de Verordening moeten komen.

Hoofdstuk 8: Beroep, aansprakelijkheid en sancties (art. 77-84)
Dit hoofdstuk beschrijft de mogelijkheden van betrokkenen om hun recht te halen. Daarnaast beschrijft dit hoofdstuk de sancties (zoals administratieve boetes) die de nationale toezichthouders kunnen opleggen.

Hoofdstuk 9: Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking (art. 85-91)
Een aantal verwerkingen van persoonsgegevens wordt vanwege hun bijzondere aard geregeld in dit hoofdstuk. Het gaat dan bijvoorbeeld om het gebruik van gegevens voor wetenschappelijk onderzoek, het gebruik van nationale identificatienummers en de verhouding tussen het gebruik van persoonsgegevens en de vrijheid van meningsuiting.

Hoofdstuk 10 en 11: Gedelegeerde handelingen, uitvoeringshandelingen en slotbepalingen (art. 92-99)
Deze hoofdstukken bevatten organisatorische en wetstechnische bepalingen zoals de regels voor bevoegdheidsdelegatie en de inwerkingtreding van de Verordening. Deze hoofdstukken blijven gezien hun aard buiten beschouwing in deze handleiding.

2.3 Wat regelt de Uitvoeringswet?

De Uitvoeringswet moet in samenhang met de Verordening worden gelezen. Daar waar de Verordening ruimte laat voor nationale regelingen of soms opdraagt tot het treffen van een regeling, komt de Uitvoeringswet in beeld. De belangrijkste gebieden waar de Uitvoeringswet een rol speelt zijn:
1. het toepassingsbereik van de Verordening;
2. de rol, positie en bevoegdheden van de nationale toezichthouder (de AP);
3. regelingen rondom het gebruik van bijzondere categorieën van persoonsgegevens;
4. regelingen omtrent (de uitzonderingen) op de rechten van de betrokkenen; en
5. regelingen voor specifieke verwerkingssituaties (zoals in relatie tot de vrijheid van meningsuiting)

Hierbij is er door de wetgever gekozen om daar waar ruimte is op grond van de Verordening het bestaande regime van de Wet bescherming persoonsgegevens te handhaven.

2.4 Welke beginselen vormen het uitgangspunt bij de bescherming van persoonsgegevens?

De Verordening gaat uit van beginselen waar elke verwerking van persoonsgegevens aan moet voldoen. Het artikel waarin deze beginselen worden genoemd (artikel 5) vormt dan ook het 'normatieve hart' van de Verordening. De algemene beginselen worden nader geconcretiseerd in de diverse bepalingen uit de Verordening, zo is bijvoorbeeld het recht van betrokkene op informatie (zie hoofdstuk 7) een uitwerking van het transparantiebeginsel.

Elke verwerking van persoonsgegevens moet in lijn zijn met de volgende beginselen:

a) De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn ("rechtmatigheid, behoorlijkheid en transparantie")
Uitgangspunt is dat persoonsgegevens alleen mogen worden verwerkt voor gerechtvaardigde doeleinden. Dit betekent dat de verwerking noodzakelijk moet zijn met het oog op het bereiken van specifiek in de Verordening genoemde doelen, dan wel dat er toestemming is verkregen van degene wiens gegevens worden verwerkt (zie hoofdstuk 4). Wanneer het gerechtvaardigd is om persoonsgegevens te verwerken, dan moet de verwerking ervan vervolgens netjes en verantwoord gebeuren. Ten slotte moet duidelijk zijn voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt. Persoonsgegevens verwerken zonder dat ook maar iemand daarvan weet is niet toegestaan.

b) De verwerking moet gebonden zijn aan specifieke verzameldoelen ("doelbinding")
Persoonsgegevens mogen alleen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer de gegevens later voor een ander doel worden gebruikt, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel.

c) De gegevens moeten toereikend, ter zake dienend en beperkt tot het noodzakelijke zijn ("minimale gegevensverwerking")
Wanneer persoonsgegevens worden verwerkt dan moeten zij voor het doel toereikend en ter zake dienend zijn. Verder mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel. Met andere woorden, er mogen gelet op het doel, niet te veel, maar ook niet te weinig gegevens worden verwerkt voor het doel. Wanneer u namelijk te weinig gegevens verwerkt, dan kan er ten onrechte een onvolledig beeld ontstaan van de betrokkene.

d) De gegevens moeten juist zijn ("juistheid")
De verwerkingsverantwoordelijke (zie hoofdstuk 3 en Schema 3) moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd.

e) De gegevens mogen niet langer worden bewaard dan nodig ("opslagbeperking")
Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Wanneer de gegevens niet langer noodzakelijk zijn, dan moeten zij worden vernietigd of gewist.

f) De gegevens moeten goed beveiligd zijn en vertrouwelijk blijven ("integriteit en vertrouwelijkheid")
Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Voor al de bovenstaande beginselen geldt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving en kan aantonen dat de gegevensverwerking in lijn is met de beginselen (de verantwoordingsplicht).[1]

Lees meer:

Artikel 2 AVG | Overwegingen 14 - 21 (materieel toepassingsbereik)
Artikel 5 AVG | Overweging 39 (beginselen inzake de verwerking van persoonsgegevens)
Uitvoeringswet Algemene verordening gegevensbescherming

[1] Wanneer in deze handleiding wordt gesproken over het 'naleven van de eisen uit de Verordening' dan wordt daar ook de naleving van de Uitvoeringswet Algemene verordening gegevensbescherming (en eventuele andere uitvoeringswetten) onder begrepen.

3 Is de Verordening op mijn gegevensverwerkingen van toepassing?

Wanneer u gegevens verwerkt, dan kan de Verordening op u van toepassing zijn. De Verordening is van toepassing wanneer er sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Daarnaast is de Verordening van toepassing op de handmatige verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Om de vraag te kunnen beantwoorden of de Verordening op u van toepassing is, moet u daarom allereerst het volgende vaststellen (zie Schema 1):

1. *Verwerk ik gegevens?*
2. *Zijn deze gegevens persoonsgegevens?*
3. *Verwerk ik deze gegevens geheel of gedeeltelijk geautomatiseerd, of zijn ze opgenomen in een bestand, dan wel bestemd om opgenomen te worden in een bestand?*

Wanneer u deze drie vragen met 'ja' heeft beantwoord moet u de volgende vraag beantwoorden:

4. *Valt mijn verwerking binnen het toepassingsbereik van de Verordening?*

Als u deze vraag positief beantwoordt, dan is de Verordening op uw verwerking van toepassing. U moet dan alleen nog vaststellen wat uw juridische hoedanigheid is onder de Verordening, omdat deze bepaalt welke regels op u van toepassing zijn. Hiertoe stelt u zichzelf de volgende vraag:

5. *Ben ik de verwerkingsverantwoordelijke, of ben ik een verwerker?*

De **verwerkingsverantwoordelijke** is degene die 'doel en middelen' bepaalt voor de verwerking. Met andere woorden, de verwerkingsverantwoordelijke bepaalt hoe en waarom er persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke is de (rechts)persoon die letterlijk de verantwoordelijkheid heeft voor het naleven van de Verordening. De **verwerker** handelt in opdracht van de verwerkingsverantwoordelijke bij het verwerken van persoonsgegevens, zonder onder diens rechtstreeks gezag te staan. Op de verwerker rust de plicht om de instructies van de verwerkingsverantwoordelijke op te volgen. Daarnaast zijn er enkele bepalingen uit de Verordening ook direct van toepassing op de verwerker. Voor een verdere uitleg zie paragraaf 3.5.

Hieronder wordt dieper ingegaan op de vragen die u helpen te bepalen of de Verordening op u van toepassing is.

3.1 Verwerk ik gegevens?

Allereerst moet u vaststellen of de handelingen die u verricht met de gegevens 'verwerkingen' zijn.

Een verwerking is volgens de Verordening elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens. Veel voorkomende bewerkingen zijn:
- verzamelen;
- vastleggen;
- opslaan;
- wijzigen;
- opvragen;
- raadplegen;
- gebruiken;
- verstrekken;
- wissen en vernietigen.

In de praktijk komt het er dus op neer dat een verwerkingshandeling al snel een verwerking van persoonsgegevens in de zin van de Verordening is.

3.2 Verwerk ik persoonsgegevens?

De Verordening is niet van toepassing op de verwerking van alle soorten gegevens, maar alleen op de verwerking van *persoonsgegevens*.

Persoonsgegevens zijn alle gegevens die:
1) betrekking hebben op;
2) een geïdentificeerde, of;
3) identificeerbare;
4) natuurlijke persoon.

De natuurlijke persoon op wie de gegevens betrekking hebben wordt de **betrokkene** genoemd.

Ad 1) Gegevens die betrekking hebben op
Wil er sprake zijn van persoonsgegevens dan moeten de gegevens allereerst betrekking hebben op een persoon. Met andere woorden: de gegevens moeten over de persoon gaan, ze moeten iets over die persoon zeggen. Wanneer de gegevens niét iets zeggen over een concreet persoon, dan zijn het geen persoonsgegevens. De prijs van een auto in een catalogus van een autodealer is bijvoorbeeld géén persoonsgegeven, want dit gegeven heeft geen betrekking op een persoon. Wanneer echter de dealer in zijn orderverwerkingssysteem vastlegt dat 'Jan Jansen' de betreffende auto heeft gekocht voor een bepaalde prijs, dan is er wel sprake van persoonsgegevens omdat de gegevens over de auto dan betrekking hebben op Jan Jansen.

Ad 2) Geïdentificeerde
Gegevens hebben alleen betrekking op een natuurlijke persoon wanneer deze *geïdentificeerd* is of *identificeerbaar* is. Een persoon is *geïdentificeerd* wanneer deze uniek van alle andere personen binnen een groep te onderscheiden is. Een persoon is *identificeerbaar* wanneer deze nog niet geïdentificeerd is, maar dit zonder onevenredige inspanning wel mogelijk is.

Om de identiteit van een persoon vast te stellen wordt doorgaans gebruik gemaakt van gegevens die een unieke, persoonlijke relatie tot die persoon hebben, zogenaamde 'identificatoren'. Bij identificatoren kan allereerst worden gedacht aan gegevens zoals een naam, adres en geboortedatum. Deze gegevens zijn in combinatie met elkaar dusdanig uniek voor een bepaalde persoon, dat een persoon op basis ervan met

zekerheid of grote waarschijnlijkheid geïdentificeerd kan worden. Deze gegevens worden in het maatschappelijk verkeer normaliter ook gebruikt om personen van elkaar te onderscheiden. We spreken daarom van direct identificerende gegevens.

Personen kunnen ook geïdentificeerd worden op basis van andere, minder directe identificatoren. Denk hierbij aan uiterlijke kenmerken (lengte, postuur en haarkleur), sociale en economische kenmerken (beroep, inkomen of opleiding) en online identificatoren zoals IP-adressen. Hoewel deze gegevens op zichzelf ons meestal nog niet in staat stellen om een persoon te identificeren, kunnen zij door hun onderlinge samenhang of door koppeling aan andere gegevens alsnog leiden tot identificatie. We spreken daarom van *indirect identificerende* gegevens.

Of iets een persoonsgegeven is voor u, is dus afhankelijk van de vraag of het gegeven of de gegevens die u verwerkt u in staat stellen om iemand direct of indirect te identificeren (uniek te onderscheiden binnen een groep). Wanneer de persoon nog niet geïdentificeerd is (wat doorgaans het geval is als u geen direct identificerende gegevens verwerkt) moet u bepalen of de persoon niet alsnog identificeerbaar is.

Ad 3) identificeerbaar
Een persoon is identificeerbaar indien zijn identiteit nog niet is vastgesteld, maar dit redelijkerwijs, zonder onevenredige inspanning, wel kan gebeuren. Dit gebeurt meestal op de volgende wijze:
- gegevens worden gekoppeld aan direct identificerende gegevens; of
- gegevens zijn door hun onderlinge combinatie dusdanig uniek dat ze maar op één persoon betrekking kunnen hebben.

De eerste mogelijkheid is het koppelen van indirect identificerende gegevens aan direct identificerende gegevens. Wanneer bijvoorbeeld een telefoonnummer (indirect identificerend) via een telefoonboek gekoppeld kan worden aan een naam (direct identificerend), dan is het telefoonnummer een persoonsgegeven. Bij de beoordeling of gegevens gekoppeld kunnen worden gaat het niet alleen om de gegevens die de verwerkingsverantwoordelijke in zijn bezit heeft. Ook gegevens die bijvoorbeeld via internet openbaar toegankelijk zijn kunnen worden meegewogen in de beslissing of iemand identificeerbaar is.

De tweede mogelijkheid is dat door een combinatie van gegevens een dusdanig uniek beeld ontstaat dat de gegevens maar op één persoon betrekking kunnen hebben. Een voorbeeld van een dergelijke spontane identificatie is: ‘een 39-jarige mannelijke jurist woonachtig aan de Oxfordlaan te Leiden’. Het is zeer onwaarschijnlijk dat deze combinatie op meer dan één geïdentificeerde persoon betrekking heeft.

Bij de beoordeling of er sprake is van identificeerbaarheid moeten de mogelijkheden van de verwerkingsverantwoordelijke (of een derde) om de identificatie tot stand te brengen worden meegewogen. Het gaat dus niet om de hypothetische mogelijkheid dat gegevens gekoppeld of gecombineerd kunnen worden, maar om de vraag of de verwerkingsverantwoordelijke dit zonder onevenredige inspanning kan. Hierbij speelt ook de hoedanigheid van de verwerkingsverantwoordelijke een belangrijke rol. Niet iedere verwerkingsverantwoordelijke beschikt namelijk over dezelfde middelen, technologieën en mogelijkheden om een persoon te identificeren. Het kan dus zijn dat een gegeven voor de ene verwerkingsverantwoordelijke wel een persoonsgegeven is, maar voor de andere verwerkingsverantwoordelijke niet.

Ad 4) natuurlijke persoon
De Verordening is alleen van toepassing op de verwerking van gegevens over natuurlijke personen. Gegevens over organisaties (ondernemingen en dergelijke) zijn géén persoonsgegevens, omdat zij geen betrekking hebben op een natuurlijke persoon. Dit is slechts anders wanneer de organisatie vereenzelvigd kan worden met een natuurlijke persoon. Zo zegt de omzet van een eenmanszaak iets over het inkomen van de eigenaar van de eenmanszaak. Wanneer u gegevens verwerkt van personen binnen een organisatie (bijvoorbeeld medewerkers), dan is er ook sprake van de verwerking van persoonsgegevens.

De Verordening is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn. Wanneer de gegevens van een overledene iets zeggen over een andere persoon (meer specifiek de nabestaanden) dan kunnen het wel persoonsgegevens zijn, maar dan betreffen ze niet de overledene, maar de andere, levende persoon.

Nota bene
Of een gegeven (voor u) een persoonsgegeven is hangt dus af van diverse factoren. Wanneer u twijfelt of iets een persoonsgegeven is, dan is het verstandig om het gegeven zekerheidshalve toch als zodanig te behandelen. U loopt dan niet het risico dat wanneer het uiteindelijk toch om een persoonsgegeven blijkt te gaan, u niet de noodzakelijke maatregelen heeft getroffen om de Verordening na te leven.

3.2.1 Bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

De Verordening maakt een onderscheid tussen 'gewone' persoonsgegevens en bijzondere categorieën van persoonsgegevens. Bijzondere categorieën van persoonsgegevens zijn gegevens die gezien hun aard extra gevoelig zijn. Het gaat specifiek om: gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

De verwerking van deze bijzondere categorieën persoonsgegevens is verboden, tenzij er een specifieke uitzondering van toepassing is, of de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking (zie paragraaf 4.5).

Naast de bijzondere categorieën van persoonsgegevens zijn ook persoonsgegevens van strafrechtelijke aard dusdanig gevoelig dat daar een speciale regeling voor is. De verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag, is alleen toegestaan als dat gebeurt onder toezicht van de overheid, of als het specifiek bij wet is geregeld. Alleen de overheid mag een omvattende registratie van strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen bijhouden. Onder omstandigheden mogen ook andere (private) partijen persoonsgegevens van strafrechtelijke aard verwerken, bijvoorbeeld met het oog op het bijhouden van een zwarte lijst. Het bijhouden van dergelijke lijsten is wel aan strenge regels onderworpen (waaronder een vergunningsplicht).

3.2.2 Gevoelige gegevens

Bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard vormen categorieën persoonsgegevens waarvan in de Verordening is vastgesteld dat zij gezien hun gevoeligheid een speciale regeling behoeven. Maar ook gegevens die niet 'bijzonder' in de zin van de Verordening zijn kunnen aldus de Autoriteit Persoonsgegevens gevoelig zijn. Denk hierbij bijvoorbeeld aan financiële data of locatiegegevens. De maatregelen die u moet nemen om persoonsgegevens te beschermen zijn mede afhankelijk van de gevoeligheid van de gegevens en het risico dat zij kunnen vormen voor de betrokkene bij verkeerd gebruik of misbruik.

3.2.3 Nationaal identificatienummer

Een nationaal identificatienummer is een bij wet vastgesteld uniek nummer. In Nederland is het bekendste nationale identificatienummer het burgerservicenummer (BSN). Deze nummers mogen alleen worden gebruikt voor in de wet voorgeschreven doelen. Voor andere dan in de wet voor deze nummers genoemde doelen is het verwerken ervan niét toegestaan. Voorbeelden van wetten waarin het gebruik van het BSN is geregeld zijn de Wet algemene bepalingen burgerservicenummer, de Wet gebruik burgerservicenummer in de zorg en de Wet persoonsgebonden nummers in het onderwijs.

3.2.4 Pseudonimisering en anonimisering

Persoonsgegevens kunnen gepseudonimiseerd en geanonimiseerd worden. In het eerste geval is er nog steeds sprake van persoonsgegevens, in het tweede geval niet.

Pseudonimisering

Het doel van pseudonimiseren is het verhullen van iemands identiteit voor derden. Bij pseudonimisering worden identificerende gegevens gescheiden van niet-identificerende gegevens en vervangen door kunstmatige identificatoren. Een voorbeeld van een pseudonimisering is het vervangen van de NAW-gegevens van een patiënt in een onderzoeksdatabase door een uniek patiëntnummer. De medische gegevens worden dan gekoppeld aan het patiëntnummer in plaats van aan de NAW-gegevens. Hierdoor is voor buitenstaanders niet zichtbaar wie de persoon is waar de medische gegevens aan toebehoren. Alleen degene die de koppeling kan maken tussen de NAW-gegevens van patiënt en het unieke nummer (bijvoorbeeld de arts) is in staat om de medische gegevens te koppelen aan de geïdentificeerde patiënt.

Gepseudonimiseerde gegevens moeten niet worden verward met anonieme gegevens. Omdat er een koppeling tot stand kan worden gebracht tussen de gepseudonimiseerde gegevens en identificerende gegevens zijn gepseudonimiseerde gegevens onverkort persoonsgegevens. De Verordening is dan ook volledig van toepassing op gepseudonimiseerde gegevens. Wel geeft de Verordening aan dat pseudonimisering een goede maatregel is om persoonsgegevens te beschermen en te beveiligen. Bij het nemen van passende technische en organisatorische maatregelen ter bescherming van persoonsgegevens moet daarom ook pseudonimisering van gegevens overwogen worden.

Anonieme gegevens

De Verordening is niet van toepassing op anonieme gegevens, immers deze gegevens zijn niet terug te voeren op een geïdentificeerde of identificeerbare natuurlijke persoon. Wanneer u persoonsgegevens verwerkt en deze gegevens anonimiseert, dan is de Verordening niet langer van toepassing. Houd er wel rekening mee dat de gegevens daadwerkelijk anoniem zijn en er geen mogelijkheden zijn tot identificatie door bijvoorbeeld herleiding, koppeling of deductie. Daarnaast is het anonimiseren van persoonsgegevens zelf wél een verwerkingshandeling.

Lees meer:

Artikel 4 AVG | Overwegingen 26-29, 34, 35, 38, 91 (definities)
Artikel 9 AVG | Overwegingen 51-56 (bijzondere categorieën van persoonsgegevens)
Artikel 10 AVG | (Persoonsgegevens van strafrechtelijke aard)
Artikel 87 AVG | (Nationaal identificatienummer)
Artikelen 22-30 UAVG | (Bijzondere categorieën van persoonsgegevens)
Artikelen 31-33 UAVG | (Persoonsgegevens van strafrechtelijke aard)
Artikel 46 UAVG | (Verwerking nationaal identificatienummer)

Groep Gegevensbescherming Artikel 29, *Advies 4/2007 over het begrip persoonsgegeven*.
Goedgekeurd op 20 juni 2007, 01248/07/NL WP136

Groep Gegevensbescherming Artikel 29, *Advies 5/2014 over anonimiseringstechnieken*.
Goedgekeurd op 10 april 2014, 0829/14/NL WP 216

Website Autoriteit Persoonsgegevens: Onderwerp zwarte lijst (*www.autoriteitpersoonsgegevens.nl*)

3.3 Is er sprake van de geheel of gedeeltelijk geautomatiseerde verwerking of opname in een bestand?

De Verordening is alleen van toepassing wanneer er sprake is van:
- een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens; of
- wanneer persoonsgegevens opgenomen zijn in een bestand of daartoe bestemd zijn.

Bij geautomatiseerde verwerking moet u denken aan alle in paragraaf 3.1 genoemde bewerkingen die worden uitgevoerd met behulp van computers, smartphones, tablets, servers, databases et cetera. Met andere woorden, er is al snel sprake van een geheel of gedeeltelijk geautomatiseerde verwerking.

Er is ook sprake van de verwerking van persoonsgegevens wanneer deze in een bestand worden opgenomen of bestemd zijn om daarin opgenomen te worden. Een bestand onder de Verordening is een gestructureerde verzameling persoonsgegevens die via een bepaalde logica toegankelijk is. Denk hierbij bijvoorbeeld aan een archiefkast of een geordende verzameling naamkaartjes. Wat losse papieren op een bureau met daarin de namen van personen vormen geen bestand.

Puur mondelinge overdracht van gegevens is ook geen verwerking van persoonsgegevens. Echter, in de meeste gevallen worden de uitkomsten van dergelijke gesprekken vastgelegd, waardoor er vaak alsnog een verwerking van persoonsgegevens plaatsvindt. Een hulpverlener bijvoorbeeld die met een collega mondeling de situatie van een cliënt bespreekt verwerkt geen persoonsgegevens, maar als de diagnose of het plan van aanpak vervolgens wordt vastgelegd in een cliëntsysteem, dan is dat wel een verwerking van persoonsgegevens.

3.4 Valt mijn verwerking binnen het toepassingsbereik van de Verordening?

Wanneer u persoonsgegevens verwerkt is de kans zeer groot dat uw verwerking onder het toepassingsbereik van de Verordening valt. Maar er zijn uitzonderingen. Om te bepalen of uw verwerking onder de Verordening valt, moet u vaststellen of uw verwerking valt binnen het materiële én territoriale toepassingsbereik van de Verordening. Het materiële toepassingsbereik betreft de vraag *waarop* de Verordening van toepassing is. Het territoriale toepassingsbereik betreft de vraag *waar* de Verordening van toepassing is (binnen het grondgebied van de Europese Unie en in bepaalde situaties daarbuiten).

3.4.1 Is de Verordening op alle verwerkingen van persoonsgegevens van toepassing?

Zoals hierboven is beschreven is de Verordening van toepassing op de verwerking van persoonsgegevens. Maar de Verordening is niét op alle verwerkingen van toepassing. De volgende verwerkingen zijn uitgesloten van de Verordening:

- *Verwerkingen in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen*
  Deze uitzondering heeft betrekking op het beleid van de lidstaten op het gebied van de nationale veiligheid. In Nederland wordt de verwerking van persoonsgegevens in het kader van de nationale veiligheid bijvoorbeeld geregeld in de Wet op de inlichtingen- en veiligheidsdiensten.

- *Verwerkingen door lidstaten in het kader van het gemeenschappelijk buitenlands- en veiligheidsbeleid*
  Het gemeenschappelijk buitenlands- en veiligheidsbeleid wordt door de lidstaten binnen de Europese Raad en de Raad van ministers (de 'Raad') vastgesteld. Wanneer er in het kader van dit beleid persoonsgegevens worden verwerkt, is de Verordening daarop niet van toepassing. In plaats daarvan worden regels ter bescherming van de persoonlijke levenssfeer vastgesteld door de Raad.

- *Verwerkingen door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit*
  De Verordening is niet van toepassing op verwerkingen in het kader van zuiver persoonlijke of huishoudelijke activiteiten. Er is sprake van zuiver persoonlijke of huishoudelijke activiteiten wanneer u persoonsgegevens alleen voor uw privédoelen gebruikt en dit gebruik niet samenhangt met zakelijke activiteiten.

  Voorbeelden van persoonlijke of huishoudelijke doelen zijn het bijhouden van persoonlijke adresbestanden, het mailen met vrienden en familie en het gebruik maken van sociale netwerken zolang dat geen enkel verband houdt met zakelijke activiteiten. De Verordening geldt wél voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor persoonlijke of huishoudelijke activiteiten. Met andere woorden, wanneer u Facebook of Twitter voor persoonlijke doeleinden gebruikt, dan is de Verordening niet op u van toepassing, maar wel op Facebook en Twitter.

- *Verwerkingen door politie en justitie in het kader van de opsporing en vervolging van strafbare feiten*
  De Verordening is niet van toepassing op verwerkingen door politie en justitie voor zover het gaat over de opsporing en vervolging van strafbare feiten. Op deze activiteiten is de Europese richtlijn gegevensbescherming, opsporing en vervolging van toepassing (richtlijn 2016/680/EG). In Nederland wordt deze Richtlijn geïmplementeerd in de Wet politiegegevens en de Wet Justitiële en strafvorderlijke gegevens.

Het bovenstaande betekent uiteraard niet dat wanneer u onder de hierboven genoemde uitzonderingen valt u met de persoonsgegevens kunt doen wat u wilt. Doorgaans is een andere, meer specifieke gegevensbeschermingswet van toepassing.

3.4.2 Waar is de Verordening van toepassing?

De Verordening geldt niet voor de hele wereld. Grofweg beperkt het territoriale bereik van de Verordening zich tot de volgende situaties:

- Organisaties (en personen) die in de Europese Unie gevestigd zijn en persoonsgegevens verwerken;
- Organisaties (en personen) die niét in de Europese Unie gevestigd zijn, maar wel gegevens verwerken van burgers in de EU.

In de praktijk betekent dit, dat wanneer u persoonsgegevens verwerkt in de Europse Unie of over personen in de Europese Unie, de Verordening op u van toepassing is. U kunt dit doen via een organisatie in de Europese Unie, maar ook via een organisatie buiten de EU.

Organisaties (en personen) die in de EU gevestigd zijn en persoonsgegevens verwerken
De Verordening is van toepassing op de verwerking van persoonsgegevens in het kader van een vestiging van de verwerkingsverantwoordelijke, of de verwerker, in de Europese Unie, ongeacht of de verwerking zelf in de EU plaatsvindt. Het gaat dan om de situatie waarin één of meer vestigingen van de verwerkingsverantwoordelijke of verwerker in de Europese Unie een bepaalde (economische) activiteit uitvoert, waarbij persoonsgegevens worden verwerkt. De rechtsvorm van de vestiging(en) is hierbij niet relevant, ook dochter- of bijkantoren zijn vestigingen in de zin van de Verordening. Het begrip vestiging veronderstelt wel dat er een fysieke vestiging is waar reële activiteiten worden verricht.

Als u als verwerkingsverantwoordelijke of verwerker niet in Nederland maar in een andere lidstaat van de EU bent gevestigd, zal de Verordening dus onverkort op u van toepassing zijn.

Houd er ook rekening mee dat het niet uitmaakt of u gegevens van Europese burgers verwerkt, van niet EU-burgers die zich op het grondgebied van de Europese Unie bevinden, of zelfs van niet Europeanen buiten de EU. Het criterium is dat u in de Europese Unie gevestigd bent. Wanneer u bijvoorbeeld in de Europese Unie gevestigd bent en enkel gegevens van Japanners of Amerikanen verwerkt, dan moeten die ook worden beschermd volgens de regels van de Verordening.

Organisaties (en personen) die niét in de EU gevestigd zijn, maar wel gegevens verwerken van burgers in de EU.
Om ervoor te zorgen dat betrokkenen die zich in de EU bevinden de bescherming krijgen die de Verordening biedt, ook als de verwerkingsverantwoordelijke of verwerker niet in de EU is gevestigd, is de Verordening van toepassing op de verwerking van hun persoonsgegevens door deze organisaties als ze verband houdt met:

- het aanbieden van goederen en diensten aan deze betrokkenen in de EU, ongeacht of een betaling is vereist;
- het monitoren van hun gedrag, voor zover dit gedrag in de EU plaatsvindt.

Om te bepalen of goederen of diensten worden aangeboden aan betrokkenen in de Europese Unie, moet worden nagegaan of de verwerkingsverantwoordelijke of verwerker klaarblijkelijk voornemens is geweest dit te doen. De toegankelijkheid van een website in de EU, de taal waarin gecommuniceerd wordt met de betrokkene, hanteren van de euro als valuta in transacties en het vermelden van klanten in de EU zijn bijvoorbeeld indicatoren dat goederen of diensten worden aangeboden aan betrokkenen in de Europese Unie.

Om te bepalen of een verwerkingsverantwoordelijke of verwerker gedrag monitort of controleert van betrokkenen dient te worden vastgesteld of natuurlijke personen bijvoorbeeld op het internet worden gevolgd, onder meer voor het opstellen van profielen.

Ten slotte is de Verordening van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de EU is gevestigd, maar wel op een plaats waar krachtens het internationaal publiekrecht het recht van de lidstaat van toepassing is. Denk hierbij aan ambassades en consulaten.

Uitvoeringswet
Lidstaten, waaronder Nederland, hebben op een aantal terreinen bevoegdheden gekregen om nationale wetgeving aan te nemen ter specificatie van de algemene regels. Denk dan aan bijvoorbeeld specifieke uitzonderingen voor wetenschappelijk onderzoek of vereisten in het kader van de arbeidsrelatie. Door gebruik te maken van deze ruimte kunnen op een aantal terreinen verschillen ontstaan tussen lidstaten. In zulke gevallen is het belangrijk te weten welk recht op uw verwerking van toepassing is.

De Nederlandse Uitvoeringswet is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van de verwerkingsverantwoordelijke of verwerker in Nederland. Daarnaast is de Uitvoeringswet van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in Nederland bevinden door een verwerkingsverantwoordelijke of verwerker die niet in de EU is gevestigd, als de verwerking verband houdt met:

- het aanbieden van goederen en diensten aan deze betrokkenen in Nederland, ongeacht of een betaling is vereist;
- het monitoren van hun gedrag, voor zover dit gedrag in Nederland plaatsvindt.

Dit betekent dus dat wanneer de verwerkingsverantwoordelijke of verwerker is gevestigd in Nederland, de Uitvoeringswet van toepassing is. Daarnaast betekent het dat de Nederlandse Uitvoeringswet van toepassing is op de verwerking van persoonsgegevens van betrokkenen in Nederland in het kader van het aanbieden van goederen of diensten aan hen of het monitoren van hun gedrag, wanneer de verwerkingsverantwoordelijke of verwerker niet in de EU is gevestigd.

Als de verwerkingsverantwoordelijke of verwerker daarentegen wél in de EU is gevestigd, maar niet in Nederland, is in beginsel de nationale wetgeving van de lidstaat waar de organisatie in kwestie gevestigd is van toepassing. De Nederlandse Uitvoeringswet is dan dus niet van toepassing.

Op basis van het bovenstaande kunnen we de volgende schematische weergave geven van het territoriale toepassingsbereik:

Vestigingsplaats verwerker/verwerkings-verantwoordelijke	Woonplaats betrokkene of plaats gedragingen van betrokkene	Toepasselijk recht zoals volgend uit de Verordening en de Uitvoeringswet
Buiten de Europese Unie	Buiten Nederland, buiten de Europese Unie	Verordening niet van toepassing
Buiten de Europese Unie	Buiten Nederland, binnen een andere lidstaat dan Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere lidstaat van toepassing
Buiten de Europese Unie	Binnen Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing
Binnen de Europese Unie, in een andere lidstaat dan Nederland	Binnen de Europese Unie, in deze andere lidstaat dan Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere nationale lidstaat waar de verwerkingsverantwoordelijke /verwerker is gevestigd, is van toepassing
Binnen de Europese Unie, in een andere lidstaat dan Nederland	Binnen Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere nationale lidstaat van toepassing
Binnen de Europese Unie, in een andere lidstaat dan Nederland	Buiten de Europese Unie	Verordening van toepassing, nationale beperkingen en uitzonderingen van de andere nationale lidstaat van toepassing
Binnen Nederland	Binnen Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing
Binnen Nederland	In een andere lidstaat dan Nederland	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing
Binnen Nederland	Buiten de Europese Unie	Verordening van toepassing, nationale beperkingen en uitzonderingen Nederlands recht van toepassing

Houd er bij het gebruik van dit schema rekening mee dat het niet uitputtend is en dat voor de keuze van het toepasselijke recht ook de keuzes in de uitvoeringswetgeving van de andere lidstaten van belang zijn.

Als ik niet in de Europese Unie ben gevestigd, val ik dan niet onder de Verordening?
Wanneer u als verwerkingsverantwoordelijke niet gevestigd bent in een lidstaat van de Europese Unie, maar op grond van de bovenstaande regels wél onder het toepassingsbereik van de Verordening valt, dan bent u verplicht om schriftelijk een vertegenwoordiger aan te stellen. De vertegenwoordiger vertegenwoordigt u in verband met uw verplichtingen krachtens de Verordening en vormt het aanspreekpunt voor de toezichthouder.

Lees meer:

Artikel 2 AVG | Overwegingen 14-21 (materieel toepassingsbereik)
Artikel 3 AVG | Overwegingen 22-25 (territoriaal toepassingsbereik)
Artikel 27, 4 lid 17 AVG | Overweging 80 (vertegenwoordiger)
Artikel 3 UAVG | (Schakelbepaling verwerkingen buiten werkingssfeer Unierecht)
Artikel 4 UAVG | (Territoriale reikwijdte)

Groep Gegevensbescherming Artikel 29, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain*, adopted on 16 December 2015, 176/16/EN WP 179 update

Groep Gegevensbescherming Artikel 29, *Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker*. Goedgekeurd op dinsdag 13 december 2016 Laatstelijk herzien en goedgekeurd op 5 april 2017, 16/NL WP 244 rev.01

3.5 Ben ik de verwerkingsverantwoordelijke, of ben ik een verwerker?

De verplichtingen uit de Verordening zijn van toepassing op de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon (een bedrijf, een stichting, een overheidsorgaan enzovoorts) die alleen of tezamen met anderen het *doel* en de *middelen* vaststelt voor de verwerking.

Om te bepalen wie verantwoordelijk is voor een verwerking is het antwoord op de onderstaande vraag doorslaggevend:

- *Waarom vindt deze verwerking plaats en wie heeft het initiatief daartoe genomen?*

Wanneer u degene bent die bepaalt welke persoonsgegevens worden verzameld, voor welk doel dit gebeurt en de manier waarop dit plaatsvindt (met welke middelen), dan bent u de verwerkingsverantwoordelijke (zie Schema 3).

Bij het beoordelen wie de verwerkingsverantwoordelijke is kunnen we grofweg drie categorieën van situaties onderscheiden:

1) de verwerkingsverantwoordelijkheid vloeit voort uit een uitdrukkelijke juridische bevoegdheid;
2) de verwerkingsverantwoordelijkheid vloeit voort uit een impliciete bevoegdheid; en
3) de verwerkingsverantwoordelijkheid vloeit voort uit feitelijke invloed.

Ad 1) Uitdrukkelijke juridische bevoegdheid
Deze situatie doet zich voor wanneer een bepaalde bevoegdheid, taak of plicht die het verwerken van persoonsgegevens behelst expliciet is opgedragen aan de verwerkingsverantwoordelijke. Bijvoorbeeld de verwerking van persoonsgegevens door de Belastingdienst.

Ad 2) Impliciete bevoegdheid
Deze situatie doet zich voor wanneer er niet een expliciete bevoegdheid bestaat tot het verwerken van persoonsgegevens, maar op grond van de gangbare juridische regels en de maatstaven die gelden in het maatschappelijk verkeer de verwerkingsverantwoordelijkheid toekomt aan een specifieke natuurlijke of rechtspersoon. Denk hierbij bijvoorbeeld aan een werkgever die de gegevens van zijn medewerkers verwerkt of een vereniging die de gegevens van haar leden verwerkt.

Ad 3) Feitelijke invloed
In deze situatie wordt de verwerkingsverantwoordelijkheid vastgesteld op basis van de feitelijke invloed die partijen kunnen uitoefenen op de verwerking van de persoonsgegevens. Hierbij wordt allereerst gekeken naar de juridische verhoudingen tussen partijen. Contractuele bepalingen omtrent de verantwoordelijkheidsverdeling vormen een relevant aanknopingspunt voor het bepalen van de verantwoordelijkheid voor een verwerking, maar zijn niet van doorslaggevende aard. Het gaat erom wie daadwerkelijk de beslissingen neemt en feitelijk bepaalt wat er met de gegevens gebeurt.

Wanneer persoonsgegevens ten behoeve van een rechtspersoon worden verwerkt, dan wordt de rechtspersoon aangemerkt als de verwerkingsverantwoordelijke, niet de individuele werknemer die het besluit heeft genomen om persoonsgegevens te verwerken. Wanneer u bijvoorbeeld als marketing manager van een warenhuis besluit om een e-mail campagne te starten, dan bent u niet persoonlijk de verwerkingsverantwoordelijke, maar het warenhuis waarvoor u werkt (de rechtspersoon). De rechtspersoon heeft namelijk de formeel-juridische bevoegdheid tot het nemen van beslissingen.

Gezamenlijke verwerkingsverantwoordelijken
Wanneer de verantwoordelijke samen met anderen doel en middelen bepaalt, dan is er sprake van gezamenlijke verantwoordelijkheid. Dit is bijvoorbeeld het geval als een computerfabrikant en een fitnessbedrijf samen een smartwatch ontwikkelen die gezondheidsgegevens registreert en de beide partijen gezamenlijk bepalen hoe en waarom deze gezondheidsgegevens worden verwerkt.

Bij gezamenlijke verantwoordelijkheid moeten de partijen onderling duidelijke afspraken maken over wie invulling geeft aan de diverse rechten en plichten uit de Verordening. Het is met name van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen.[2] Ongeacht de afspraken tussen de gezamenlijke verwerkingsverantwoordelijken blijven zij hoofdelijk aansprakelijk voor de naleving van de Verordening.

3.5.1 Ben ik een verwerker?

Verwerkingsverantwoordelijken schakelen regelmatig personen of organisaties in die voor hen persoonsgegevens verwerken. Wanneer u *ten behoeve van een verwerkingsverantwoordelijke* persoonsgegevens verwerkt, *zonder dat u aan diens rechtstreekse gezag onderworpen bent*, dan bent u een verwerker.

U verwerkt gegevens ten behoeve van de verwerkingsverantwoordelijke
U verwerkt ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens wanneer de verwerking van persoonsgegevens uw primaire opdracht is. Met andere woorden, uw dienstverlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Wanneer de verwerking van persoonsgegevens niet uw primaire opdracht is, maar het een uitvloeisel is van een andere vorm van dienstverlening, dan bent u als dienstverlener zélf de verwerkingsverantwoordelijke voor deze verwerking. Oftewel, het enkele feit dat u een opdracht krijgt van de verwerkingsverantwoordelijke is niet voldoende om te kunnen spreken van verwerkerschap, de opdracht moet gericht zijn op het verwerken van persoonsgegevens.

Een goed voorbeeld is een administratiekantoor dat namens een bedrijf de salarisadministratie voert. De opdracht aan het administratiekantoor is het uitvoeren van de salarisadministratie, wat neerkomt op het verwerken van de persoonsgegevens van de medewerkers. In dit geval is het administratiekantoor verwerker. Een ander voorbeeld is een aanbieder van gegevensopslag in de cloud, wanneer de dienst puur ziet op het opslaan van gegevens, dan is de cloud-aanbieder een verwerker.

Een handelsinformatiebureau dat bedrijven in staat stelt om de kredietwaardigheid van consumenten te beoordelen is daarentegen meestal géén verwerker. De opdracht is immers 'beoordeel voor mij de kredietwaardigheid van deze consument'. Hoewel bij de beoordeling van de kredietwaardigheid weliswaar persoonsgegevens worden gebruikt en het handelsinformatiebureau opdrachtnemer is, bepaalt het handelsinformatiebureau zelf hoe zij de opdracht uitvoert en welke gegevens zij daar eventueel voor aanwendt (doel en middelen). Het handelsinformatiebureau is daarmee zelf verwerkingsverantwoordelijke en niet verwerker. Een ander voorbeeld is het aanbieden van online diensten. Wanneer een cloud-aanbieder bijvoorbeeld een fitness app aanbiedt aan bedrijven om medewerkers gezond en fit te houden en deze app verwerkt daartoe de gegevens van medewerkers, dan is de cloud-aanbieder verwerkingsverantwoordelijke. Een laatste voorbeeld betreft zorgaanbieders die in opdracht van een gemeente zorg leveren. Zij doen dit weliswaar in opdracht van de gemeente, maar bepalen zelf doel en middelen voor de concrete invulling van hun zorgtaken.

Als verwerker heeft u geen zeggenschap over de verwerkingen. U mag alleen handelen onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies. Op het moment dat u als verwerker zelfstandig beslissingen gaat nemen over de doelen van de verwerking en de middelen, dan wordt u zelf verantwoordelijk voor die (nieuwe) verwerkingen. Wanneer bijvoorbeeld het administratiekantoor besluit om de medewerkers die in de salarisadministratie zijn opgenomen te e-mailen om te vragen

[2] Omwille van de leesbaarheid wordt in deze handleiding primair de mannelijke vorm gehanteerd op plaatsen waar het ook om de vrouwelijke of andere vormen kan gaan.

of zij niet ook klant willen worden bij het administratiekantoor, dan bepaalt zij zelf het doel en de middelen en wordt aldus zelf verwerkingsverantwoordelijke voor deze nieuwe verwerking. Een ander voorbeeld is een cloud-aanbieder die in opdracht van een verwerkingsverantwoordelijke gegevens opslaat, maar de bij hem opgeslagen gegevens ook geautomatiseerd analyseert om zo interessante trends en inzichten te ontdekken die verkocht kunnen worden. Voor de geautomatiseerde analyse is de cloud-aanbieder zelf verwerkingsverantwoordelijke.

U bent niet aan het rechtstreeks gezag van de verwerkingsverantwoordelijke onderworpen
Er is alleen sprake van verwerkerschap als de verwerker niet aan het rechtstreeks gezag van de verwerkingsverantwoordelijke is onderworpen. Wanneer u ondergeschikt bent aan de verwerkingsverantwoordelijke of er anderszins sprake is van een hiërarchische verhouding (u bent bijvoorbeeld medewerker, gedetacheerd bij de verwerkingsverantwoordelijke of een ZZP'er die werkt onder de instructies van uw opdrachtgever), dan is er geen sprake van verwerkerschap. In Nederland wordt deze situatie aangeduid als *intern beheer*.

Op de verwerker rusten andere verplichtingen dan op de verwerkingsverantwoordelijke. Daarnaast moeten er (schriftelijke) afspraken gemaakt worden tussen de verwerkingsverantwoordelijke en de verwerker. Hierop wordt in de hoofdstukken 5 en 6 nader ingegaan.

Lees meer:

Artikel 24 AVG | Overwegingen 74-77, 83 (verantwoordelijkheid van de verwerkingsverantwoordelijke)
Artikel 26 AVG | Overweging 79 (gezamenlijke verantwoordelijkheid)
Artikel 28, 29, 4 lid 8 AVG | Overweging 81 (verwerkers)

Groep Gegevensbescherming Artikel 29, *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*

4 Is mijn gegevensverwerking legitiem?

Als u heeft vastgesteld dat de Verordening op uw verwerkingen van toepassing is, dan moet u er voor zorgen dat deze in overeenstemming met de vereisten uit de Verordening plaatsvinden. Hierbij geldt dat een verwerking van persoonsgegevens altijd aan de eisen van proportionaliteit en subsidiariteit moet voldoen (zie paragraaf 4.3). Voor verwerkingsverantwoordelijken die in het kader van een taak in het publieke belang persoonsgegevens verwerken, geldt bovendien dat u in overeenstemming met de algemene beginselen van behoorlijk bestuur moet handelen.

4.1 Voor welke doelen mag ik persoonsgegevens verzamelen?

U mag op grond van de Verordening persoonsgegevens slechts verwerken voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. U mag dus geen persoonsgegevens verwerken zonder dat hiervoor een doel is bepaald. Gegevens verzamelen omdat deze 'in de toekomst nog weleens van pas kunnen komen' is dus niet toegestaan. Wel mag u persoonsgegevens voor meerdere doelen tegelijkertijd verwerken. U moet dan uiteraard wel de verschillende doeleinden duidelijk hebben bepaald.

Daarnaast moet het doel of moeten de doeleinden uitdrukkelijk omschreven zijn. Dit betekent dat u, voordat u begint met het verzamelen of anderszins verwerken van persoonsgegevens, moet vastleggen waarvoor u deze persoonsgegevens nodig hebt.

Tenslotte moet het doel gerechtvaardigd zijn. Het is hierbij van belang om te borgen dat de verwerking kan worden gebaseerd op één van de rechtsgrondslagen als genoemd in de Verordening (zie hiervoor paragraaf 4.3).

Lees meer:
Artikel 5 AVG | Overweging 39 (beginselen inzake verwerking van persoonsgegevens)

4.2 Mag ik de gegevens ook gebruiken voor andere doelen dan waarvoor ik ze oorspronkelijk verzameld heb?

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt. U mag de persoonsgegevens dan voor dat doel of die doelen gebruiken.
Verdere verwerking wordt onder de verordening toegestaan in drie situaties:

1. Er is sprake is van een verenigbaar doel
   Persoonsgegevens mogen verder worden verwerkt voor andere doelen, als die doelen verenigbaar zijn met het oorspronkelijke verzameldoel. Om te bepalen of een nieuw doel verenigbaar is, moet worden gekeken naar een aantal elementen:
   - het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter de twee doelen bij elkaar liggen, hoe eerder de verdere verwerking van persoonsgegevens verenigbaar is met het oorspronkelijke doel.
   - de context waarin de persoonsgegevens zijn verzameld. Hierbij moet met name worden gekeken naar de relatie tussen u en de betrokkene in kwestie en de redelijke verwachtingen die de betrokkene heeft ten aanzien van het verdere gebruik van zijn persoonsgegevens door u. Verwacht de betrokkene bijvoorbeeld dat gegevens die zijn verzameld in de context van het verkopen van goederen hergebruikt worden om verzekeringspremies te berekenen?
   - de aard van de persoonsgegevens. Wanneer het bijvoorbeeld gevoelige persoonsgegevens betreft, geldt dat deze een hoger beschermingsniveau verdienen en dat deze minder snel voor andere doelen mogen worden gebruikt.

- de mogelijke gevolgen van de verdere verwerking voor betrokkenen.
- het bestaan van passende waarborgen. Als u bijvoorbeeld de persoonsgegevens heeft versleuteld of, gepseudonimiseerd zullen deze eerder voor andere doelen mogen worden gebruikt dan wanneer geen waarborgen zijn getroffen.

2. Betrokkene heeft toestemming gegeven voor de verdere verwerking (ook in het geval het doel van de verdere verwerking niet verenigbaar is met het oorspronkelijke doel).

3. Op basis van een Unierechtelijke of lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in de verordening bedoelde doelstellingen van algemeen belang (ook in het geval het doel van de verdere verwerking niet verenigbaar is met het oorspronkelijke doel). Bij wijze van voorbeeld wordt genoemd de specifieke wettelijke plicht voor verwerkingsverantwoordelijke om bepaalde gegevens aan een overheidsorgaan te verstrekken.

Als een verwerkingsverantwoordelijke gegevens verder verwerkt voor een ander doel dan waarvoor de gegevens zijn verzameld en dat doel is niet verenigbaar met het oorspronkelijke doel, dan heeft hij voor die verwerking een specifieke wettelijke grondslag nodig of toestemming van betrokkene. De verwerkingsverantwoordelijke die de gegevens ontvangt, zal voor de verwerking van de verstrekte gegevens ook zelf een zelfstandige rechtsgrondslag nodig hebben.

Het verder verwerken van persoonsgegevens ten behoeve van wetenschappelijk en historisch onderzoek, voor statistische doeleinden en voor archiveringsdoeleinden in het algemeen belang wordt in de Verordening verenigbaar geacht. Deze verwerkingen moeten dan wel zijn onderworpen aan passende technische en organisatorische waarborgen om ervoor te zorgen dat zo min mogelijk persoonsgegevens worden verwerkt, bijvoorbeeld door persoonsgegevens te pseudonimiseren. U moet er daarbij voor zorgen dat de persoonsgegevens ook alleen voor deze doelen worden verwerkt. Wanneer de persoonsgegevens ook voor andere doelen worden verwerkt, dan vallen deze verwerkingen niet onder de uitzondering en zal voor die doelen moeten worden bepaald of deze verenigbaar zijn of niet.

Lees meer:
Artikel 6(4) AVG | Overweging 50 (rechtmatigheid van de verwerking)

UAVG Memorie van Toelichting paragraaf 4.2.3.

4.3 Wanneer is mijn verwerkingsdoel gerechtvaardigd?

Elke gegevensverwerking moet gerechtvaardigd zijn. Uw verwerking is gerechtvaardigd wanneer u het doel van de verwerking kunt baseren op één van de zes rechtsgrondslagen die in de Verordening worden gegeven. Kunt u dat niet, dan is het niet toegestaan persoonsgegevens te verwerken. De lijst van rechtsgrondslagen is limitatief, u kunt dus geen andere gronden aanvoeren.

De zes grondslagen zijn niet allemaal even relevant voor alle verwerkingsverantwoordelijken. Welke rechtsgrondslag u kunt gebruiken hangt onder andere af van de vraag of u een publieke of private organisatie bent en met welk doel u de persoonsgegevens wilt verwerken.

De rechtsgrondslagen zijn niet cumulatief. Ook is er geen hiërarchische volgorde van de rechtsgrondslagen. U hoeft dus niet alle zes de grondslagen af te lopen om te bepalen welke voor uw verwerking gebruikt kan worden. Slechts één van de grondslagen hoeft van toepassing te zijn om uw verwerking te rechtvaardigen.

De zes rechtsgrondslagen zijn:

a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De grondslagen b tot en met f zijn 'noodzakelijkheidsgrondslagen': alleen wanneer de verwerkingen noodzakelijk zijn voor de in deze grondslagen genoemde doelen dan is de verwerking gerechtvaardigd. In de vraag of een verwerking noodzakelijk is ligt besloten of de verwerking van gegevens 1) proportioneel is en 2) of de verwerking voldoet aan de eis van subsidiariteit.

Allereerst moet de verwerking proportioneel zijn. Dit betreft de vraag naar effectiviteit en evenredigheid. Als u met de verwerking van de gegevens niet het gestelde doel kunt bereiken, of dat is zeer onwaarschijnlijk, dan is deze verwerking niet snel proportioneel. Het tweede element van de proportionaliteitstoets betreft de evenredigheid. Het legitieme doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt.

Subsidiariteit betreft de vraag of het genoemde doel niet op een andere, minder ingrijpende wijze (bijvoorbeeld door géén of minder persoonsgegevens te verwerken) kan worden bereikt. Wanneer u bijvoorbeeld vermoedens heeft dat één specifieke medewerker fraude pleegt, is het niet noodzakelijk om alle werknemers te controleren.

U hoeft dus niet altijd toestemming te hebben van de betrokkene om uw gegevensverwerking te legitimeren. Als u hard kunt maken dat uw verwerking van persoonsgegevens noodzakelijk is voor één van de onder b tot en met f genoemde doelen, dan hoeft u geen toestemming te krijgen. Kunt u niet hard maken dat uw verwerking van persoonsgegevens noodzakelijk is ten behoeve van één van deze doelen, dan zult u terug moeten vallen op de toestemming om de verwerking alsnog te legitimeren. Houd er hierbij wel rekening mee dat ook wanneer u toestemming als grondslag kunt aanvoeren uw verwerking nog steeds moet voldoen aan de eisen van proportionaliteit en subsidiariteit.

In de volgende sub-paragrafen worden de zes rechtsgrondslagen nader toegelicht.

4.3.1 Toestemming

Persoonsgegevens mogen worden verwerkt als de betrokkene hiervoor toestemming heeft gegeven. Om te spreken van geldige toestemming, moet de toestemming aan een aantal voorwaarden voldoen.

Vrij

Ten eerste moet de toestemming vrij gegeven zijn. Dit houdt in dat iemand daadwerkelijk de keuze moet hebben om te weigeren, zonder dat hier negatieve consequenties aan verbonden zijn. Met name wanneer er sprake is van een afhankelijkheidsrelatie, bijvoorbeeld in de arbeidssfeer of in de relatie overheid-burger, zal toestemming niet snel vrij zijn gegeven. Dit betekent dat u in dergelijke situaties de verwerking van persoonsgegevens niet op deze grondslag kan baseren.

Wanneer u de uitvoering van een overeenkomst afhankelijk maakt van het geven van toestemming voor een andere verwerking die niet noodzakelijk is voor de uitvoering van de overeenkomst ('bundelen'), dan dient ten strengste rekening te worden gehouden met de vraag of deze toestemming vrijelijk gegeven kan worden. Wanneer bijvoorbeeld een bank aan haar klanten met een betaalrekening vraagt om toestemming voor de verwerking van deze gegevens voor bepaalde direct marketingdoeleinden, en de weigering van deze toestemming leidt tot het niet meer leveren van betaaldiensten, het sluiten van de betaalrekening of hogere kosten voor de betaalrekening, dan wordt de toestemming veronderstelt niet vrij te zijn gegeven.

Specifiek en geïnformeerd
Ten tweede moet toestemming specifiek zijn en geïnformeerd. U moet dus als verwerkingsverantwoordelijke duidelijke informatie verschaffen over de redenen waarom u de persoonsgegevens gaat verwerken (het doel), maar ook over andere zaken die van belang zijn om te zorgen dat de betrokkene voldoende informatie heeft om een goed geïnformeerd besluit te nemen. Denk dan dus ook aan informatie over de manier waarop u de persoonsgegevens verwerkt, met wie u de persoonsgegevens gaat delen, hoe lang u ze gaat bewaren en of ze naar landen buiten de Europese Unie worden doorgegeven.

Ondubbelzinnig
Tenslotte moet toestemming ondubbelzinnig zijn. Er mag geen twijfel bestaan over het feit dat de betrokkene toestemming heeft gegeven. Toestemming kan blijken uit een ondubbelzinnige wilsuiting of uit een ondubbelzinnige, actieve handeling van de betrokkene. Vaak wordt hiervoor de term *opt in* gehanteerd. *Opt out* – het gebruik maken van de optie om je van toestemming te onthouden – is geen toestemming. Wanneer de betrokkene bijvoorbeeld een vinkje zet in een vakje om zijn akkoord aan te geven, dan is er sprake van ondubbelzinnige toestemming (*opt in*). Wanneer echter hetzelfde vakje al aangekruist is en de betrokkene vinkt het niet uit (*opt out*), dan is er geen ondubbelzinnige toestemming tot stand gekomen. Het is namelijk niet duidelijk wat de echte wil van de betrokkene is (deze kan bijvoorbeeld het vakje over het hoofd hebben gezien). Met andere woorden, het afleiden van toestemming uit het feit dat iemand niet handelt of niet protesteert (wat de Engelsen *implied consent* noemen), is niet toegestaan.

Naast de vereisten zijn er nog enkele aanvullende voorwaarden voor toestemming geformuleerd in de Verordening. Deze worden in paragraaf 4.4 behandeld.

4.3.2 Noodzakelijk voor de uitvoering van een overeenkomst

Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor de uitvoering van een overeenkomst. Als u met iemand een overeenkomst hebt gesloten, mag u de persoonsgegevens van deze persoon verwerken voor zover dit noodzakelijk is om de overeenkomst uit te kunnen voeren. Dit moet dan wel een overeenkomst zijn waarbij de betrokkene zelf ook partij is. De overeenkomst hoeft overigens niet gericht te zijn op het verwerken van persoonsgegevens, maar de verwerking moet wel een noodzakelijk uitvloeisel van de overeenkomst zijn. Wanneer een consument bijvoorbeeld in uw webwinkel een boek bestelt dan mag u de NAW-gegevens van deze consument verwerken, omdat u de consument het boek moet kunnen sturen.

Persoonsgegevens mogen ook worden verwerkt als dit noodzakelijk is om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. In deze zogenoemde precontractuele fase kan het verwerken van persoonsgegevens namelijk noodzakelijk zijn. Denk dan bijvoorbeeld aan een betrokkene die bij een bank om een offerte vraagt voor een hypotheek. Voor het berekenen van het maximale leenbedrag, zal de bank bepaalde persoonsgegevens nodig hebben, voordat er daadwerkelijk sprake is van een overeenkomst.

4.3.3 Noodzakelijk om te voldoen aan een wettelijke plicht

U mag ook persoonsgegevens verwerken als dit noodzakelijk is om te voldoen aan een wettelijke plicht. Om verwerkingen van persoonsgegevens op deze grondslag te kunnen baseren, moet het niet mogelijk zijn om aan de plicht te voldoen zonder dat er persoonsgegevens worden verwerkt.

De wettelijke plicht moet een grondslag hebben in het recht van de Europese Unie of in het recht van de lidstaat, waarin ook het doel van de verwerking wordt bepaald. Een verplichting kan nooit voortvloeien uit

het recht van een niet-EU lidstaat. Als verantwoordelijke moet u daarnaast daadwerkelijk onderworpen zijn aan dit recht om een verwerking van persoonsgegevens op deze grondslag te kunnen baseren.

Een voorbeeld van een verwerking van persoonsgegevens die op deze grondslag kan worden gebaseerd is de wettelijke plicht op werkgevers om een kopie of scan van het identiteitsbewijs van uw personeel op te nemen in uw loonadministratie in navolging van de Wet op de loonbelasting.

4.3.4 Noodzakelijk om de vitale belangen te beschermen

Als dit noodzakelijk is om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen, mogen persoonsgegevens worden verwerkt. Denk dan bijvoorbeeld aan een situatie waarin hulpverleners persoonsgegevens moeten verwerken om acuut dringend noodzakelijke medische hulp aan de betrokkene te verlenen.

Het verwerken van persoonsgegevens op basis van deze grondslag is alleen toegestaan indien het niet op basis van een andere grondslag kan worden gebaseerd. Alleen als het dus écht niet mogelijk is een andere grondslag, zoals toestemming, te gebruiken, bijvoorbeeld omdat iemand buiten bewustzijn is, kan deze grondslag worden gebruikt voor de verwerking van persoonsgegevens.

4.3.5 Noodzakelijk voor een taak in het algemeen belang of voor de uitoefening van het openbaar gezag

Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor de vervulling van een taak in het algemeen belang of als het noodzakelijk is voor de uitoefening van het openbaar gezag dat aan de verantwoordelijke is opgedragen. De verwerking moet in deze gevallen altijd een grondslag hebben in het recht van de Europese Unie of dat van de betreffende lidstaat, waarin ook het doel van de verwerking moet staan. Hierbij is wel van belang dat in de wetgeving van de Europese Unie of de lidstaat waarin de taak is omschreven, of waarmee het openbaar gezag wordt opgedragen, moet zijn vastgesteld wie deze taak uitvoert of aan wie het openbaar gezag is opgedragen. Dit kunnen zowel publiekrechtelijke als privaatrechtelijke organisaties zijn.

De Raad voor de Kinderbescherming heeft bijvoorbeeld de wettelijke taak om zorg te dragen voor de kinderbescherming in Nederland. De grondslag voor de verwerking van persoonsgegevens in dit kader door de Raad kan dan worden gevonden in de uitoefening van het openbaar gezag.

4.3.6 Noodzakelijk voor de behartiging van het gerechtvaardigde belang

Persoonsgegevens mogen tenslotte worden verwerkt als dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verwerkingsverantwoordelijke of een derde, mits de belangen, rechten en vrijheden van de betrokkene(n) niet zwaarder wegen.

Om verwerkingen op deze grondslag te kunnen baseren moet u een zorgvuldige beoordeling maken om te bepalen of er sprake is van een gerechtvaardigd belang, maar ook om te bepalen of de betrokkene, gelet op het moment en de context van de verzameling van de persoonsgegevens, redelijkerwijs mag verwachten dat zijn persoonsgegevens voor dit doel worden verwerkt.

Verwerkingen van persoonsgegevens die strikt noodzakelijk zijn voor het voorkomen van fraude of ten behoeve van direct marketing kunnen bijvoorbeeld worden gezien als gerechtvaardigde belangen van de verantwoordelijke en mogen dus op basis van deze grondslag worden verwerkt.

U zult uw gerechtvaardigde belangen uitdrukkelijk moeten afwegen tegen de rechten, vrijheden en belangen van de betrokkene. In deze afweging spelen de gevoeligheid van de verwerkte persoonsgegevens en de maatregelen die u heeft genomen een belangrijk rol. Hoe gevoeliger de persoonsgegevens zijn, hoe zwaarder de rechten, vrijheden en belangen van de betrokkene zullen wegen. Aan de andere kant, hoe sterker de (beveiligings)maatregelen zijn die u heeft getroffen, hoe eerder u de verwerkingen kan baseren op deze grondslag.

Wanneer u een verwerking baseert op uw gerechtvaardigde belang, dan moet u transparant zijn over dit gerechtvaardigde belang. U moet dan onder andere duidelijk maken voor welke doelen u persoonsgegevens verwerkt, welke persoonsgegevens u verwerkt, of u de gegevens deelt met andere partijen en hoe lang u de persoonsgegevens bewaart. Ook moet u de door u nagestreefde gerechtvaardigde belangen benoemen.

Betrokkenen moeten ten slotte altijd de mogelijkheid hebben om bezwaar aan te tekenen tegen het verwerken van persoonsgegevens wanneer dit op grond van het gerechtvaardigde belang gebeurt. Dit bezwaar moet wel betrekking hebben op de specifieke situatie van de betrokkene. U dient dan de verwerkingen te staken, tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de rechten, vrijheden en belangen van de betrokkene. Ook als u de persoonsgegevens moet verwerken voor het instellen, uitoefenen of onderbouwen van een rechtsvordering, kunt u de persoonsgegevens blijven verwerken. Zie hiervoor verder hoofdstuk 7.

Als de betrokkene bezwaar aantekent tegen verwerkingen voor direct marketing doeleinden, dan mogen de persoonsgegevens niet meer voor dit doel worden verwerkt.

Nota bene
Vanwege het feit dat de wetgever de rechtsgrond bepaalt voor de verwerking van persoonsgegevens door overheidsinstanties, is de rechtsgrond ‘gerechtvaardigd belang’ niet van toepassing op verwerkingen door overheidsinstanties in het kader van de uitvoering van hun taken.

Lees meer:
Artikelen 6 lid 1-3 AVG | Overwegingen 42 – 47 (rechtmatigheid van de verwerking)

4.4 Welke voorwaarden worden aan de toestemming gesteld?

Op het moment dat verwerkingen zijn gebaseerd op de toestemming van de betrokkene, zijn er enkele aanvullende voorwaarden van toepassing, in aanvulling op de algemene vereisten zoals beschreven in paragraaf 4.3.1.

Allereerst ligt de bewijslast voor het aantonen dat toestemming is verkregen bij u als verwerkingsverantwoordelijke. U zult dus moeten aantonen dat u van de betrokkene toestemming heeft gekregen voor het verwerken van zijn persoonsgegevens.

Als toestemming wordt gegeven in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, moet u op een begrijpelijke en gemakkelijke manier en in duidelijke en eenvoudige taal het onderscheid aangeven tussen dat waarvoor de betrokkene toestemming geeft en de andere aangelegenheden.

De betrokkene mag te allen tijde zijn toestemming intrekken. Deze intrekking heeft geen invloed op de legitimiteit van de verwerkingen vóór intrekking, maar vanaf het moment dat iemand zijn toestemming intrekt, mogen de persoonsgegevens niet meer worden verwerkt. U dient de betrokkene van deze mogelijkheid op de hoogte te stellen voordat de betrokkene zijn toestemming heeft verleend. Het intrekken van toestemming moet ook net zo gemakkelijk zijn als het geven ervan. Als u bijvoorbeeld toestemming vraagt door middel van een vinkje op uw website, zou het intrekken ervan op een vergelijkbare manier moeten kunnen.

Wanneer toestemming wordt gevraagd in het kader van diensten van de informatiemaatschappij (online diensten zoals webwinkels en sociale media) en de betrokkene is nog geen 16 jaar oud, dan moeten de ouders of degene met ouderlijke verantwoordelijkheden toestemming geven. U moet redelijke inspanningen leveren, waarbij u de beschikbare technologie in acht neemt, om te controleren dat de toestemming inderdaad door de ouder of degene met het ouderlijk gezag is gegeven.

Lees meer:
Artikel 7 AVG | Overwegingen 42-43 (voorwaarden voor toestemming)
Artikel 8 AVG | Overweging 38 (voorwaarden voor toestemming van kinderen bij het gebruik van diensten van de informatiemaatschappij)
Artikel 5 UAVG | (Toestemming van de wettelijk vertegenwoordiger)

Groep Gegevensbescherming Artikel 29, *Guidelines on consent under Regulation 2016/679*. Adopted on 28 November 2017, 17/EN/WP259

4.5 Mag ik bijzondere categorieën van persoonsgegevens verwerken?

In beginsel niet. Op het verwerken van bijzondere categorieën van persoonsgegevens rust gezien hun gevoelige aard een algemeen verwerkingsverbod (zie hoofdstuk 3). Hierop is echter wel een beperkt aantal uitzonderingen geformuleerd. Een deel van de uitzonderingen is geregeld in de Verordening en is van toepassing op alle bijzondere categorieën van persoonsgegevens. De Uitvoeringswet bevat daarnaast specifieke uitzonderingen per categorie.

Nota bene
Als één van de uitzonderingen op uw verwerking van toepassing is, dan betekent dit nog niet dat u de gegevens ook daadwerkelijk mag verwerken. Naast het feit dat uw verwerking past binnen één van deze uitzonderingsgronden moet de verwerking ook nog gerechtvaardigd zijn en voldoen aan de andere eisen die de Verordening stelt. Met andere woorden, de verwerking moet gebaseerd kunnen worden op één van de zes grondslagen uit de Verordening en u moet uw verantwoordingsplicht invullen (zie Checklist 1).

Een voorbeeld om dit te illustreren. Eén van de uitzonderingen op het verbod van verwerking van bijzondere categorieën van persoonsgegevens is dat de betrokkene deze zelf kennelijk openbaar heeft gemaakt. Dit is het geval wanneer iemand zijn medische gegevens open en bloot op het internet zet. Het enkele feit dat deze gegevens openbaar zijn gemaakt en dus binnen de uitzondering vallen, betekent nog niet dat u ze mag verwerken omdat het verbod niet van toepassing is. Uw verwerking moet nog steeds noodzakelijk zijn in het licht van een gerechtvaardigd doel.

Uiteraard geldt net als bij de 'gewone' persoonsgegeven dat wanneer u bijzondere categorieën van persoonsgegevens mag verwerken, u onverkort moet voldoen aan de regels in de Verordening, de Uitvoeringswet en andere toepasselijke regelgeving.

4.5.1 Welke uitzonderingen kent de Verordening op het verbod op het verwerken van bijzondere categorieën van persoonsgegevens?

De Verordening biedt tien verschillende algemene uitzonderingsgronden op het verwerkingsverbod op bijzondere categorieën persoonsgegevens. U mag ondanks het verwerkingsverbod toch bijzondere categorieën van persoonsgegevens verwerken wanneer:

- de betrokkene uitdrukkelijke toestemming heeft gegeven;
- de verwerking noodzakelijk is in het kader van de uitvoering van regels op het gebied van arbeids- en sociale zekerheidsrecht;
- de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon;
- de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

- de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsprekende bevoegdheid;
- de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten;
- de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid,
- de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Alle bovengenoemde uitzonderingen kennen specifieke voorwaarden, regels en beperkingen die nader zijn uitgewerkt in de Uitvoeringswet. De uitzonderingen op het verwerkingsverbod zijn onderverdeeld in algemene uitzonderingen en specifieke uitzonderingen.

4.5.2 Wat zijn de algemene uitzonderingsgronden op het verwerkingsverbod van bijzondere categorieën van persoonsgegevens?

De Nederlandse Uitvoeringswet onderscheidt de volgende algemene uitzonderingsgronden op basis van de Verordening en ons nationaal recht.

Uitdrukkelijke toestemming
Bijzondere categorieën persoonsgegevens mogen worden verwerkt voor één of meer welbepaalde doelen, als de betrokkene hiervoor zijn uitdrukkelijke toestemming heeft gegeven. De eis van uitdrukkelijke toestemming is strenger dan de eis van ondubbelzinnige toestemming bij het verwerken van niet-bijzondere categorieën van persoonsgegevens. Als u bijvoorbeeld genetische gegevens wilt verwerken voor een erfelijkheidsonderzoek op basis van toestemming, moet u de uitdrukkelijke toestemming hiervoor hebben gekregen. Er mag dan dus geen enkele twijfel over bestaan of de persoon in kwestie toestemming heeft gegeven. U kunt als richtsnoer aanhouden dat de handeling waarmee uitdrukkelijke toestemming gegeven wordt, specifiek moet zijn gericht op het geven van toestemming.

Vitale belangen
Wanneer een betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven, bijvoorbeeld omdat hij niet bij bewustzijn is, maar het verwerken van persoonsgegevens noodzakelijk is voor de bescherming van zijn vitale belangen, mogen bijzondere categorieën persoonsgegevens worden verwerkt. Het eerder gebruikte voorbeeld van een medische noodzaak is hier ook een goed voorbeeld, waarbij de medici naast ‘gewone’ persoonsgegevens ook bijvoorbeeld gezondheidsgegevens mogen verwerken.

Verwerkingen door instanties actief op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied
Instanties zonder winstoogmerk (stichtingen, verenigingen) die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam zijn, mogen in het kader van hun gerechtvaardigde activiteiten bijzondere categorieën van persoonsgegevens verwerken van hun leden, voormalige leden en personen die in verband met de doelen van de instantie regelmatig contact met de instantie onderhouden. Denk hierbij bijvoorbeeld aan de ledenadministratie van een vakbond of politieke partij. De persoonsgegevens mogen niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt.

Gegevens die kennelijk openbaar zijn gemaakt
In het geval de betrokkene zelf de bijzondere categorieën van persoonsgegevens kennelijk openbaar heeft gemaakt, mogen deze worden verwerkt als uitzondering op het algemene verwerkingsverbod. Denk dan bijvoorbeeld aan iemand die zich verkiesbaar stelt voor een politiek ambt en hiertoe met zijn politieke opvattingen naar buiten treedt. Dit zijn nog steeds bijzondere categorieën van persoonsgegevens, maar u mag ze onder deze omstandigheden wel verwerken, aangezien de betrokkene de persoonsgegevens zelf duidelijk openbaar heeft gemaakt.

Instelling, uitoefening of onderbouwing van een rechtsvordering
Het kan voorkomen dat u in een gerechtelijke procedure bent verwikkeld en hiervoor bijzondere categorieën van persoonsgegevens moet verwerken, bijvoorbeeld van uw wederpartij. In dergelijke gevallen is het toegestaan de persoonsgegevens te verwerken voor dit doel. Ditzelfde geldt voor de gerechten die de zaken moeten beoordelen.

Volkenrechtelijke verplichting
Het verbod op het verwerken van bijzondere categorieën van persoonsgegevens is niet van toepassing als dit noodzakelijk is om te kunnen voldoen aan een volkenrechtelijke verplichting.

Verwerking door de Autoriteit Persoonsgegevens of ombudsman
Wanneer dit noodzakelijk is voor de uitvoering van de aan hen opgedragen wettelijke taken mogen bijzondere categorieën van persoonsgegevens worden verwerkt door de Autoriteit Persoonsgegevens of een ombudsman.

Verwerking in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard
De verwerking is noodzakelijk in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard. Van deze uitzondering kan echter alleen gebruikt worden gemaakt ten behoeve van de doelen waarvoor de persoonsgegevens van strafrechtelijke aard worden verwerkt.

Wetenschappelijk onderzoek, historisch onderzoek, statistische doeleinden
Bijzondere categorieën van persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor wetenschappelijk of historisch onderzoek of statistische doeleinden. Dit mag echter alleen als het onderzoek een algemeen belang dient, het vragen van uitdrukkelijke toestemming onmogelijk blijkt en voldoende waarborgen zijn getroffen om zo min mogelijk risico's voor de persoonlijke levenssfeer van de betrokkene te creëren.

Lees meer:
Artikel 9 AVG |Overwegingen 51 - 56 (verwerking van bijzondere categorieën van persoonsgegevens)
Artikel 22 UAVG | (Verwerkingsverbod bijzondere categorieën van persoonsgegeven en algemene uitzonderingen in de verordening)
Artikel 23 UAVG | (Nationaalrechtelijke algemene uitzonderingen)
Artikel 24 UAVG | (Uitzonderingen voor wetenschappelijk of historisch onderzoek of statistische doeleinden)

4.5.3 Specifieke uitzonderingen
Naast de algemene uitzonderingen op het verwerkingsverbod op bijzondere categorieën van persoonsgegevens, biedt de Uitvoeringswet enkele specifieke uitzonderingen per categorie van bijzondere persoonsgegevens.

Ras en etnische afkomst
Persoonsgegevens waaruit ras of etnische afkomst blijkt, mogen worden verwerkt in twee specifieke situaties. Allereerst mogen deze persoonsgegevens worden verwerkt met het oog op de identificatie van de betrokkene, maar alleen maar voor zover dit onvermijdelijk is om het gestelde doel te bereiken. Dit is bijvoorbeeld het geval wanneer iemands paspoortgegevens worden verwerkt ten behoeve van identificatie-doeleinden. Persoonsgegevens waaruit ras of etnische afkomst blijkt, mogen daarnaast worden verwerkt met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen of feitelijke nadelen op te heffen. In dit geval mogen deze persoonsgegevens alleen maar worden verwerkt als dit noodzakelijk is voor het te behalen doel, die gegevens slechts betrekking hebben op het geboorteland van de betrokkene, diens ouders of grootouders en de betrokkene hier geen schriftelijk bezwaar tegen heeft gemaakt.

Verwerking gegevens waaruit politieke opvattingen blijken voor vervulling openbare functies
Deze uitzondering op het verwerkingsverbod voor persoonsgegevens waaruit politieke opvattingen blijken geldt voor situaties waarbij deze gegevens relevant zijn voor de vervulling van functies in bestuursorganen of adviescolleges. Dit speelt met name een rol bij benoemingen in bepaalde openbare functies, zoals bijvoorbeeld burgemeestersbenoemingen.

Verwerking van gegevens van religieuze of levensbeschouwelijke aard in het kader van geestelijke verzorging
Deze uitzondering op het verwerkingsverbod voor persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken is bedoeld voor de geestelijke verzorging in of ten behoeve van het leger, gevangenissen, ziekenhuizen, verpleeghuizen en andere instellingen. Omdat deze instellingen zelf geen religieuze doelstelling hebben is een specifieke uitzondering gecreëerd.

Genetische gegevens
De uitzondering op het gebruik van genetische gegevens kent twee categorieën: het persoonlijk gebruik en het bovenpersoonlijk gebruik.

De uitzondering van het persoonlijk gebruik ziet op het gebruik van genetische gegevens van een betrokkene wanneer deze door de betrokkene zelf zijn geleverd. Deze uitzondering kan dus niét gebruikt worden om verwerkingen van genetisch materiaal te legitimeren die gericht zijn op andere personen in dezelfde genetische lijn. Het doel is om te voorkomen dat mogelijke erfelijke informatie (bijvoorbeeld genetische defecten) buiten de betrokken persoon om gebruikt worden.

Bovenpersoonlijk gebruik is enkel toegestaan als een zwaarwegend geneeskundig belang prevaleert of de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek dat een algemeen belang dient of ten behoeve van statistiek. Hierbij is de voorwaarde wel dat de betrokkene uitdrukkelijke toestemming heeft gegeven en bij de uitvoering is voorzien in passende waarborgen voor de bescherming van de persoonlijke levenssfeer. Alleen wanneer het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt dan kan deze achterwege blijven.

Biometrische gegevens
Het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken is niet van toepassing indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Wanneer u deze uitzondering wilt gebruiken moet u dus afwegen of het te beveiligen belang van een dusdanige aard is dat hiervoor biometrie de geëigende methode is.

Gezondheidsgegevens
De Uitvoeringswet kent vijf specifieke uitzonderingsgronden op het verwerkingsverbod voor gezondheidsgegevens.

Ten eerste mogen gezondheidsgegevens worden verwerkt door bestuursorganen, pensioenfondsen, werkgevers of instellingen die voor hen werkzaam zijn, voor zover de verwerking noodzakelijk is voor:
a. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene; of
b. de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

Ten tweede mogen gezondheidsgegevens worden verwerkt door scholen wanneer dit noodzakelijk is voor de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheid.

Ten derde mogen gegevens door reclasseringsinstellingen, bijzondere reclasseringsambtenaren, de Raad voor de kinderbescherming, gecertificeerde instellingen in de zin van de Jeugdwet en specifiek aangewezen rechtspersonen in het kader van de uitvoering van de Vreemdelingenwet 2000 worden verwerkt wanneer dit

noodzakelijk is voor de uitvoering van de aan hen opgedragen wettelijke taken. Verder mogen gezondheidsgegevens worden verwerkt door de Minister voor zover de verwerking in verband met de tenuitvoerlegging van vrijheidsbenemende maatregelen noodzakelijk is.

Ten vierde is het verbod niet van toepassing op hulpverleners en instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, wanneer de verwerking noodzakelijk is voor de goede behandeling of verzorging van de betrokkene of het beheer van de betreffende instelling of beroepspraktijk.

Tenslotte is het verbod niet van toepassing op verzekeraars en financiële dienstverleners die bemiddelen in verzekeringen voor zover de verwerking noodzakelijk is voor de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of de uitvoering van verzekeringsovereenkomst dan wel het assisteren bij het beheer en de uitvoering van de verzekering.

Alle verwerkingen van gezondheidsgegevens die plaatsvinden op basis van de uitzonderingen in de Uitvoeringswet, zijn gehouden aan een geheimhoudingsplicht, ook waar dit niet voortvloeit uit andere wetten waar de dienstverlener aan onderworpen is.

Lees meer:
Artikel 25 UAVG | (Uitzonderingen inzake verwerking van persoonsgegevens waaruit ras of etnische afkomst blijkt)
Artikel 26 UAVG | (Uitzonderingen inzake verwerking persoonsgegevens waaruit politieke opvattingen blijken voor vervulling openbare functies)
Artikel 27 UAVG | (Uitzonderingen inzake verwerking persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken voor geestelijke verzorging)
Artikel 28 UAVG | (Uitzonderingen inzake genetische gegevens)
Artikel 29 UAVG | (Uitzonderingen inzake biometrische gegevens)
Artikel 30 UAVG | (Uitzonderingen inzake gegevens over gezondheid)

4.6 Mag ik persoonsgegevens van strafrechtelijke aard verwerken?

Persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag (‘persoonsgegevens van strafrechtelijke aard’), mogen alleen worden verwerkt op basis van een gerechtvaardigde grondslag onder toezicht van de overheid en voor zover toegestaan in de Uitvoeringswet. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid. Strafbladen bijvoorbeeld mogen alleen worden bijgehouden door overheidsorganen die hiermee belast zijn.

De Verordening zelf biedt geen uitzonderingen of afwijking van de hoofdregel, maar bepaalt wel dat deze persoonsgegevens mogen worden verwerkt als dit is toegestaan op basis van het recht van de EU of de lidstaat en in deze wet- of regelgeving passende waarborgen zijn genomen voor het beschermen van de rechten en vrijheden van betrokkenen. In de Uitvoeringswet is in navolging hiervan meer in detail bepaald wanneer persoonsgegevens van strafrechtelijke aard mogen worden verwerkt.

De algemene uitzonderingsgronden op het verbod om persoonsgegevens van strafrechtelijke aard te verwerken zijn vergelijkbaar met die voor de bijzondere categorieën van persoonsgegevens. Het gaat om:
- de uitdrukkelijke toestemming van de betrokkene;
- situaties waar de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een andere natuurlijke persoon (indien de betrokkene fysiek of juridisch niet in staat is toestemming te geven);
- situaties waar de verwerking heeft betrekking op gegevens die door de betrokkene openbaar zijn gemaakt;

- situaties waar de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een vordering;
- gerechten die handelen in het kader van hun rechtsbevoegdheid;
- situaties waar de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- situaties waar de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden en is voldaan aan alle toepasselijke voorwaarden uit de Verordening (zie paragraaf 4.5.2).

Daarnaast kent de Uitvoeringswet specifieke uitzonderingsgronden voor de verwerking van persoonsgegevens van strafrechtelijke aard. Het gaat om de volgende situaties:
- verwerkingen door verwerkingsverantwoordelijken die zijn belast met de toepassing van het strafrecht, of door verwerkingsverantwoordelijken die de gegevens op grond van de Wet politiegegevens of de Wet Justitiële en strafvorderlijke gegevens hebben gekregen.
- verwerkingen door publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken wanneer dit noodzakelijk is voor de uitvoer van hun taken en passende waarborgen zijn getroffen.

Onder omstandigheden mag u als verwerkingsverantwoordelijke ook persoonsgegevens van strafrechtelijke aard ten eigen behoeve verwerken of ten behoeve van een derde.

U mag allereerst persoonsgegevens van strafrechtelijke aard verwerken wanneer dit nodig is voor de beoordeling van een verzoek van een betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren. Een voorbeeld is een screening in het kader van een sollicitatieprocedure voor een integriteitsfunctie. Onder omstandigheden mogen voor een dergelijk doel persoonsgegevens van strafrechtelijke aard worden verwerkt.

Daarnaast mag u persoonsgegevens van strafrechtelijke aard verwerken ter bescherming van uw eigen belangen, als strafbare feiten jegens u zijn gepleegd of worden verwacht te zullen worden gepleegd. Denk dan bijvoorbeeld aan camerabeelden waarop een diefstal te zien is. Dit zijn persoonsgegevens van strafrechtelijke aard, omdat er een strafbare handeling op te zien is die direct aan een persoon is te relateren. Deze persoonsgegevens mag u ten behoeve van uzelf wel verwerken in afwijking van de hoofdregel, maar mag u niet zonder meer openbaar maken.

Nota Bene:
Het is alleen toegestaan om persoonsgegevens van strafrechtelijke aard over uw medewerkers te verwerken, indien dit geschiedt overeenkomstig regels die zijn vastgesteld in overeenstemming met de procedure bedoeld in de Wet op de ondernemingsraden.

Het is tenslotte mogelijk om persoonsgegevens van strafrechtelijke aard ten behoeve van een derde te verwerken (bijvoorbeeld een ander bedrijf). Dit is alleen toegestaan in de volgende gevallen:
- u heeft een vergunning op grond van de Wet op de particuliere beveiligingsorganisaties en recherchebureaus; of
- u verwerkt rechtmatig gegevens van medewerkers ten behoeve van een groepsmaatschappij (bijvoorbeeld een dochterorganisatie); of
- indien de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang van een derde, passende waarborgen zijn getroffen ter bescherming van de persoonlijke levenssfeer van de betrokkene én de Autoriteit Persoonsgegevens u een vergunning heeft verleend voor de verwerking.

Lees meer:
Artikel 10 AVG | (Gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten)
Artikel 31 UAVG | (Uitzonderingen op de verplichting tot verwerking onder overheidstoezicht)
Artikel 32 UAVG | (Algemene uitzonderingen inzake persoonsgegevens van strafrechtelijke aard)

Artikel 33 UAVG | (Overige uitzonderingsgronden inzake persoonsgegevens van strafrechtelijke aard)
Richtlijn 2016/680/EG (Richtlijn politie- en justitiegegevens)
Wet politiegegevens (Wpg)
Wet justitiële en strafvorderlijke gegevens (Wjsg)
Wet op de ondernemingsraden

Website Autoriteit Persoonsgegevens, Onderwerp Werk en Uitkering (*www.autoriteitpersoonsgegevens.nl*)
Website Autoriteit Persoonsgegevens: Onderwerp zwarte lijst (*www.autoriteitpersoonsgegevens.nl*)

4.7 Wat wordt bedoeld met 'specifieke verwerkingssituaties'?

Ten aanzien van een aantal specifieke situaties waarin persoonsgegevens worden verwerkt, zijn in de Verordening specifieke bepalingen opgenomen. In een aantal van deze bepalingen zijn in de Verordening zelf afwijkingen, uitzonderingen of aanvullingen geformuleerd. In andere bepalingen draagt de Verordening aan de lidstaten op om voor die specifieke situatie nadere wet- of regelgeving aan te nemen, waar dat van toepassing is.

Deze specifieke situaties betreffen het verwerken van persoonsgegevens in relatie tot:
- de vrijheid van meningsuiting, waaronder journalistieke doeleinden;
- de toegang tot officiële documenten;
- het gebruik van het nationaal identificatienummer;
- verwerkingen in de arbeidsverhouding;
- verwerking voor historische en wetenschappelijke onderzoeksdoeleinden, statistische doeleinden en archiveringsdoeleinden in het algemeen belang; en
- voor verwerkingen door kerken of religieuze verenigingen bepaalde regelingen treffen.

Deze situaties worden hieronder kort behandeld.

4.7.1 Verwerken van persoonsgegevens en vrijheid van meningsuiting

Bij de uitoefening van het recht op de vrijheid van meningsuiting en van informatie worden in veel gevallen persoonsgegevens verwerkt. Hieronder vallen ook verwerkingen van persoonsgegevens voor journalistieke doeleinden of voor academische, artistieke of literaire uitingen. De Verordening geeft lidstaten de opdracht om dit recht op vrijheid van meningsuiting en van informatie in overeenstemming te brengen met het recht op de bescherming van persoonsgegevens. Concreet betekent dit dat voor journalistieke doeleinden en academische, artistieke en literaire uitdrukkingsvormen specifieke uitzonderingsgronden zijn opgenomen in de Uitvoeringswet. Zo zijn er uitzonderingen gemaakt op de toepassing van de hoofdstukken 3 tot en met 7 van Verordening en is ook een groot deel van de bepalingen uit de Uitvoeringswet niet van toepassing.

4.7.2 Toegang tot officiële documenten

Uit het recht van de Europese Unie of van de lidstaat kan voortvloeien dat overheidsinstanties of -organen, en in sommige gevallen ook particuliere organisaties, documenten openbaar moeten maken. Dit zijn bijvoorbeeld documenten die voor de uitvoering van een taak van algemeen belang in het bezit zijn van de betreffende organisatie. Deze openbaarmakingsplicht vloeit vaak voort uit het recht van burgers om toegang te hebben tot officiële documenten (bijvoorbeeld op basis van de Wet openbaarheid van bestuur). Het publiek maken van dergelijke documenten moet in overeenstemming gebeuren met het recht op bescherming van persoonsgegevens. Dit betekent dat bij de openbaarmaking van documenten, voldoende aandacht moet worden besteed aan het beschermen van de persoonsgegevens (waaronder die van derden) die mogelijk in de documenten staan.

4.7.3 Nationaal identificatienummer

De Verordening geeft lidstaten de mogelijkheid om voorwaarden te stellen aan het verwerken van een nationaal identificatienummer. Een dergelijk nummer mag alleen gebruikt worden als passende waarborgen zijn getroffen voor de bescherming van de rechten en vrijheden van de betrokkenen.
De Uitvoeringswet vult deze bepaling aan door te bepalen dat nationale identificatienummers die zijn voorgeschreven bij wet, zoals het burgerservicenummer (BSN), slechts mogen worden gebruikt ter uitvoering van de betreffende wet of voor de doelen die bij wet zijn bepaald. Door middel van een algemene maatregel van bestuur (amvb) kunnen gevallen worden aangewezen wanneer het identificatienummer mag worden verwerkt. U mag dus alleen identificatienummers zoals het BSN verwerken als dit bij wet of amvb is bepaald.

4.7.4 Arbeidsverhouding

Lidstaten kunnen bij wet of via een collectieve overeenkomst, zoals een CAO, nadere regels vaststellen die zien op de bescherming van persoonsgegevens van werknemers in het kader van de arbeidsverhouding. Deze nadere regels kunnen bijvoorbeeld zien op het werven van mensen, het uitvoeren van een overeenkomst of het beheer, de planning en de organisatie van arbeid, alsook op de gelijkheid en diversiteit op de werkvloer.

Als nadere regels worden vastgesteld door een lidstaat, moeten deze ook passende en specifieke maatregelen omvatten om de menselijke waardigheid en om de rechten van betrokkenen te waarborgen. Deze maatregelen moeten dan met name zien op de transparantieverplichting richting werknemers en de doorgifte van persoonsgegevens binnen het concern of groep van ondernemingen. De Nederlandse wetgever heeft hiervoor vooralsnog niet gekozen.

4.7.5 Wetenschappelijk en historisch onderzoek, statistiek en archivering in algemeen belang

Verwerkingen voor wetenschappelijk en historisch onderzoek, statistische doeleinden en archivering in het algemeen belang worden altijd verenigbaar geacht met het oorspronkelijke verzameldoel. Maar ook als het geen verdere verwerkingen zijn, mogen persoonsgegevens worden verwerkt voor deze doeleinden, mits aan de vereisten in de Verordening wordt voldaan. De Verordening eist dat voor de bescherming van de rechten en vrijheden van betrokkenen passende waarborgen worden getroffen. Die waarborgen moeten er onder andere voor zorgen dat technische en organisatorische maatregelen zijn getroffen om zo min mogelijk persoonsgegevens te verwerken, zoals pseudonimiseren of anonimiseren.

Het recht van de Europese Unie of de lidstaat mag daarnaast afwijkingen creëren voor verwerkingen voor deze doeleinden ten aanzien van de rechten van de betrokkene, zoals het inzagerecht, het recht op rectificatie, het recht op beperking van persoonsgegevens en het recht van bezwaar. In de Uitvoeringswet is er voor gekozen om verwerkingsverantwoordelijken die persoonsgegevens verwerken voor onderzoeksdoeleinden de mogelijkheid te geven om het recht op inzage, wijziging en beperking te weigeren. Voor archiefbescheiden in de zin van de Archiefwet 1995 die berusten in een archiefbewaarplaats is het recht op inzage, wijziging, beperking en dataportabiliteit beperkt. In zijn algemeenheid heeft de betrokkene wel het recht op inzage in archiefbescheiden, tenzij de verzoeken zodanig ongericht zijn dat ze niet in redelijkheid kunnen worden ingewilligd. Wanneer onjuiste persoonsgegevens in het archief zijn opgenomen, dan heeft de betrokkene het recht om zijn eigen lezing aan de betreffende archiefbescheiden toe te voegen.

4.7.6 Kerken en religieuze verenigingen

In sommige lidstaten zijn er op het moment van inwerkingtreding van de Verordening specifieke regels ten aanzien van de verwerking van persoonsgegevens door kerken of religieuze verenigingen of gemeenschappen. Als dit het geval is, mogen die regels van toepassing blijven, maar moeten ze wel in overeenstemming met de Verordening worden gebracht. Het is daarnaast toegestaan dat er een onafhankelijke toezichthouder toezicht houdt op de verwerkingen door deze organisaties, zolang deze maar voldoet aan de wettelijke vereisten die zijn gesteld in de Verordening aan de toezichthoudende autoriteiten.

4.7.7 Openbare registers

De rechten op inzage, wijziging, verwijdering, beperking en bezwaar zijn niet van toepassing op bij de wet ingestelde openbare registers wanneer deze registers voorzien in een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van de gegevens.

Lees meer:

Artikel 85 AVG | Overweging 153 (verwerking en vrijheid van meningsuiting en van informatie)
Artikel 86 AVG | Overweging 154 (verwerking en recht van toegang tot officiële documenten)
Artikel 87 AVG (verwerking van het nationaal identificatienummer)
Artikel 88 AVG | Overweging 155 (verwerking in het kader van de arbeidsverhouding)
Artikel 89 AVG | Overwegingen 156-163 (waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden)
Artikel 91 AVG | Overweging 165 (bestaande gegevensbeschermingsregels van kerken en religieuze verenigingen)
Artikel 43 UAVG | (Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen)
Artikel 44 UAVG | (Uitzonderingen inzake wetenschappelijk onderzoek en statistiek)
Artikel 45 UAVG | (Uitzonderingen inzake archivering in het algemeen belang)
Artikel 46 UAVG | (Verwerking nationaal identificatienummer)
Artikel 47 UAVG | (Uitzonderingen op rechten betrokkene bij openbare registers)

5 Wat zijn mijn plichten als verwerkings-verantwoordelijke?

Als verwerkingsverantwoordelijke bent u verantwoordelijk voor de rechtmatige en zorgvuldige omgang met persoonsgegevens. Dit betekent dat u:
- de plichten uit de Verordening moet naleven; en
- dat u de goede naleving van deze plichten kunt aantonen.

Deze verantwoordingsplicht (in het Engels *accountability*) staat centraal in de Verordening en geldt te allen tijden. Als verwerkingsverantwoordelijke bent u verplicht passende en effectieve maatregelen te nemen om te zorgen dat de verwerkingen in lijn met de Verordening plaatsvinden. Bij het nemen van maatregelen moet u rekening houden met de aard, de omvang, de context en het doel van de verwerking en de risico's die uw verwerking voor de rechten en vrijheden van de betrokkene kunnen hebben. Oftewel, de maatregelen die u neemt moeten in verhouding staan tot de verwerking. Wanneer het risico laag is, dan kunt u met minder verstrekkende maatregelen toe dan wanneer u zeer risicovolle verwerkingen doet. Zo zal bijvoorbeeld een ziekenhuis dat medische gegevens verwerkt strengere maatregelen moeten treffen dan een voetbalvereniging waar alleen een ledenlijst wordt bijgehouden. U dient zelf te bepalen wat passende en effectieve maatregelen zijn. Deze zogenaamde 'risico-gebaseerde benadering' komt in diverse plichten terug.

5.1 Wat zijn mijn plichten als verwerkingsverantwoordelijke?

Op grond van de Verordening heeft u de plicht om de gegevens in overeenstemming met de beginselen voor de verwerking van persoonsgegevens te verwerken (zie hoofdstuk 2). De Verordening bepaalt niet hoe u deze verantwoordingsplicht concreet moet invullen, anders dan dat u rekening moet houden met de aard, de omvang, de context en het doel van de verwerking en de daarmee gepaard gaande risico's voor de betrokkene. Stelregel is dat naarmate uw verwerking een hoger risico voor de betrokkenen met zich meebrengt, u meer en/of striktere maatregelen moet nemen ter bescherming van de gegevens en dat u ook een uitgebreidere verantwoordingsplicht heeft.

Om concreet invulling te kunnen geven aan deze eis moet u op grond van de Verordening (afhankelijk van uw concrete verwerkingen) tenminste de volgende maatregelen nemen:
- u dient een register van verwerkingsactiviteiten bij te houden ('de registerplicht');
- u dient onder bepaalde omstandigheden een functionaris voor gegevensbescherming aan te stellen;
- u dient voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling uit te voeren;
- u dient de Autoriteit Persoonsgegevens onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit te raadplegen ('de voorafgaande raadpleging');
- u dient bij het inrichten van verwerkingen rekening te houden met het principe van privacy door ontwerp en standaardinstellingen ('privacy by design & default');
- u dient passende beveiligingsmaatregelen te treffen met het oog op de bescherming van persoonsgegevens;
- u dient in het geval van een datalek melding te doen bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden betrokkenen daarover te informeren;
- u dient afspraken te maken met verwerkers.

Het is raadzaam om deze maatregelen in te bedden binnen een gegevensbeschermingsbeleid. In dit beleid bepaalt u bijvoorbeeld welke technische en organisatorische maatregelen genomen moeten worden, hoe deze maatregelen vorm krijgen in de praktijk (processen, procedures et cetera) en belegt u de rollen en verantwoordelijkheden voor de uitvoer ervan. Afhankelijk van de aard en de omvang van de verwerkingsactiviteiten kan een dergelijk gegevensbeschermingsbeleid verplicht zijn.

5.2 Hoe toon ik aan dat ik aan mijn verplichtingen voldoe?

Het is op grond van de Verordening niet voldoende dat u maatregelen neemt om te waarborgen dat uw verwerkingen in overeenstemming met de Verordening plaatsvinden, u moet dit ook kunnen aantonen (*accountability* in het Engels).

In het kader van uw 'aantoonplicht' moet u de volgende maatregelen nemen:
- een register van verwerkingsactiviteiten bijhouden;
- indien dit in verhouding staat tot de verwerkingsactiviteiten, het op schrift stellen van een passend gegevensbeschermingsbeleid;
- het documenteren van uw gegevensbeschermingseffectbeoordelingen;
- documenteren van de passende waarborgen die worden gehanteerd bij de overdracht van gegevens buiten de Europese Unie (zie hoofdstuk 8);
- informatievoorziening aan de betrokkenen op schrift stellen (bijvoorbeeld in de vorm van een *privacy statement*);
- wanneer u de grondslag toestemming hanteert, het vastleggen van de wijze waarop u toestemming vraagt;
- wanneer u de grondslag toestemming hanteert, het bewijs dat deze toestemming daadwerkelijk is gegeven documenteren;
- wanneer u de grondslag 'gerechtvaardigd belang' hanteert, uw gerechtvaardigde belang documenteren;
- het documenteren van uw processen en procedures ter waarborging van de rechten van de betrokkenen;
- verwerkersovereenkomsten conform de eisen uit de Verordening opstellen voor elke inzet van verwerkers;
- uw procedures voor de omgang met datalekken documenteren;
- een registratie van datalekken die zich in uw organisatie hebben voorgedaan bijhouden;
- de maatregelen die u neemt om invulling te geven aan de uitgangspunten van gegevensbescherming door ontwerp en door standaardinstellingen (zie hoofdstuk 5).

Hulp bij en aanwijzingen voor het naleven van uw verantwoordingsplicht kunnen – wanneer u deze heeft aangesteld – worden gegeven door de functionaris voor gegevensbescherming (zie paragraaf 5.4). Daarnaast kunt u zich aansluiten bij goedgekeurde gedragscodes of certificeringsmechanismen (zie paragraaf 5.11) om aan te tonen dat u uw verplichtingen als verwerkingsverantwoordelijke nakomt.

Lees meer:

Artikel 5, lid 1, AVG | Overwegingen 11-17 AVG (beginselen)
Artikel 5, lid 2, AVG | Overwegingen 74, 77, 82 (verantwoordingsplicht en register)
Artikel 24 AVG | Overwegingen 74-77, 83 (verantwoordelijkheid van de verwerkingsverantwoordelijke)
Artikel 40 AVG | Overwegingen 98, 99 (gedragscodes)
Artikel 42 AVG | Overweging 100 (certificering)

5.3 Wat is de registerplicht?

Om aantoonbaar te maken dat u aan de verplichtingen uit de Verordening voldoet, dient u een register bij te houden van de verwerkingsactiviteiten waarvoor u verwerkingsverantwoordelijke bent.

5.3.1 Wat is een register van verwerkingsactiviteiten?

Het register van verwerkingsactiviteiten is een opsomming van de belangrijkste informatie over uw verwerkingen van persoonsgegevens. U (of uw vertegenwoordiger) dient dit register bij te houden. Wanneer u een verwerker bent, dan moet u ook een register bijhouden (zie paragraaf 6.4). Hoewel het bijhouden van verwerkingsactiviteiten strikt genomen niet onder de verantwoordelijkheid van de functionaris voor gegevensbescherming valt, mag deze taak aan hem worden toebedeeld door de verwerkingsverantwoordelijke respectievelijk de verwerker.

5.3.2 Is er een vormvereiste aan het register?

U dient het register in schriftelijke vorm op te stellen. Hieronder is ook begrepen het bijhouden van een register in elektronische vorm. Er zijn geen andere vormvereisten. Het register mag dus worden opgemaakt in een tekstverwerkingsbestand, een spreadsheet, speciaal daartoe bestemde software of elke andere schriftelijke vorm.

5.3.3 Moet ik altijd een register bijhouden?

Ja. Alleen wanneer uw onderneming of organisatie minder dan 250 personen in dienst heeft, dan bent u niet verplicht om een register bij te houden, tenzij:

- De verwerking waarschijnlijk een risico voor betrokkenen met zich meebrengt (zie hoofdstuk 5); of
- de verwerking niet-incidenteel is; of
- er sprake is van de verwerking van bijzondere categorieën van persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

Bij een niet-incidentele verwerking kunt u denken aan elke verwerking met een zekere bestendigheid. Denk hierbij bijvoorbeeld aan het bijhouden van een klantendatabase of een personeelsadministratie. Aangezien veruit de meeste verwerkingen niet-incidenteel zijn, zal in de praktijk slechts in een beperkt aantal gevallen een beroep op deze uitzondering kunnen worden gedaan.

5.3.4 Wat moet ik in het register opnemen?

In het register dient u de volgende onderdelen op te nemen:

- uw naam en contactgegevens, of indien van toepassing die van uw vertegenwoordiger;
- waar van toepassing de naam en contactgegevens van partijen waarmee u gezamenlijk verwerkingsverantwoordelijke bent;
- de contactgegevens van uw functionaris voor gegevensbescherming als u die heeft aangesteld;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie. Daarbij dient u ook de documenten inzake de passende waarborgen te vermelden;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Nota bene:
In het register neemt u niét de daadwerkelijke persoonsgegevens van betrokkenen op! Het register geeft slechts door middel van een beschrijving inzicht in de verwerkingsactiviteiten. Het register bevat dus een beschrijving van de verwerkingsactiviteiten en niét de persoonsgegevens zelf.

5.3.5 Wat moet ik doen als ik mijn verwerkingsactiviteiten wijzig?

Als u uw verwerkingsactiviteit wijzigt, moet u het register daarop aanpassen. Wanneer u bijvoorbeeld persoonsgegevens die u al verwerkt en in het register hebt beschreven, voor een nieuw doel gaat gebruiken, dan moet u deze nieuwe verwerkingsactiviteit registreren. Maar ook wanneer u de verwerkingsactiviteiten voor dezelfde doeleinden voortzet, alleen met méér of andere gegevens, dan moet u deze nieuwe categorieën persoonsgegevens in het register toevoegen. Het register dient kort gezegd altijd een volledig en actueel overzicht van de hierboven genoemde informatie te bevatten.

5.3.6 Wie moet ik toegang geven tot het register?

Wanneer de Autoriteit Persoonsgegevens daarom vraagt moet u haar het register ter beschikking stellen. Ook dient de functionaris voor gegevensbescherming wanneer u die hebt aangesteld, toegang te krijgen tot het register. Het register is voor de functionaris voor gegevensbescherming een middel om zijn taken rondom het toezicht op de naleving van de Verordening te vervullen en de organisatie te informeren en adviseren over de gegevensverwerkingen die plaatsvinden.

5.3.7 Hoe lang moeten mijn verwerkingsactiviteiten in het register blijven staan?

U moet de verwerkingen in het register bijhouden die op dat moment plaatsvinden. Of u ook verplicht verwerkingen moet bijhouden die in het verleden hebben plaatsgevonden wordt niet geheel duidelijk uit de Verordening. Wel is het verstandig met het oog op uw bewijspositie, om wijzigingen in verwerkingen en gestaakte verwerkingen te archiveren.

Lees meer:

Artikel 30 AVG | Overweging 13, 39 en 82 (register van de verwerkingsactiviteiten)
Artikel 38 AVG | Overweging 82 (positie van de functionaris voor gegevensbescherming)

Groep Gegevensbescherming Artikel 29, *Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)*. Goedgekeurd op 13 december 2016. Laatstelijk herzien en goedgekeurd op 5 april 2017, 16/NL WP 243 rev.01

5.4 Wat is een functionaris voor gegevensbescherming?

De Verordening kent een belangrijke rol toe aan de functionaris voor gegevensbescherming (in het Engels *data protection officer*, afgekort *DPO*). De functionaris voor gegevensbescherming (FG) houdt intern toezicht op en adviseert over de toepassing en naleving van de Verordening door uw organisatie. Ook is de FG het aanspreekpunt voor de betrokkene. In een aantal gevallen is het aanstellen van een FG verplicht.

5.4.1 Wanneer moet ik verplicht een functionaris voor gegevensbescherming aanstellen?

U moet een FG aanstellen als uw organisatie aan ten minste één van de volgende drie voorwaarden voldoet:

1. *U bent een overheidsinstantie of overheidsorgaan*

Onder de Verordening is iedere overheidsinstantie of -orgaan verplicht een FG aan te stellen. Denk hierbij aan bijvoorbeeld de rijksoverheid, gemeenten en provincies. Gerechten hoeven voor gegevensverwerkingen in het kader van de uitvoering van hun taak geen FG aan te stellen.

Instanties of organen binnen de overheid mogen één gezamenlijke FG aanwijzen. Daarbij moeten zij wel rekening houden met hun organisatiestructuur en omvang.

2. *U bent hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen*

U moet als verwerkingsverantwoordelijke een FG aanstellen wanneer u hoofdzakelijk belast bent met verwerkingen die bestaan uit het op regelmatige basis stelselmatig observeren van betrokkenen op grote schaal. *Hoofdzakelijk belast* heeft betrekking op uw kernactiviteiten. De Groep Gegevensbescherming Artikel 29 (de 'Artikel 29-werkgroep'), het samenwerkingsverband van Europese toezichthouders, definieert

'kernactiviteiten' als processen die essentieel zijn om de doelen van de organisatie te bereiken, of die tot de hoofdtaken van de organisatie horen. Zo is de verwerking van gegevens over de gezondheid een kernactiviteit van een ziekenhuis. Maar de verwerking van persoonsgegevens die ondersteunend is aan de bedrijfsvoering, zoals de salarisadministratie, valt dan buiten de kernactiviteiten.

Over het algemeen is er sprake van *regelmatige en stelselmatige observatie* wanneer u betrokkenen over een bepaalde periode volgt en persoonsgegevens over hen vastlegt, bijvoorbeeld om profielen van die betrokkenen op te stellen.

De Verordening laat in het midden wat een verwerking op *grote schaal* is. U moet dit zelf bepalen en deze beoordeling is afhankelijk van de concrete situatie. Of er sprake is van verwerking op grote schaal kunt u vaststellen aan de hand van (onder andere) de volgende criteria:
- het aantal betrokkenen (hetzij als een specifiek aantal, hetzij als deel van de relevante populatie);
- de hoeveelheid gegevens die u verwerkt;
- de duur of het permanente karakter van de gegevensverwerking;
- de geografische omvang van de verwerking.

Voorbeelden van grootschalige verwerkingen zijn: verwerking van patiëntgegevens in een ziekenhuis (maar niet die van een individuele arts), reisgegevens die worden bijgehouden door een openbaar vervoersorganisatie, verwerking van klantgegevens door een verzekeringsmaatschappij en het verwerken van zoekgegevens door een zoekmachine-aanbieder.

3. *U bent hoofdzakelijk belast met verwerkingen die de grootschalige verwerking van bijzondere categorieën van persoonsgegevens en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten behelzen.*

Ook wanneer uw kernactiviteiten bestaan uit het grootschalig verwerken van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard, dient u een FG aan te stellen. Dit is bijvoorbeeld het geval bij ziekenhuizen of onderzoeksinstellingen die gebruik maken van gezondheidsgegevens.

In deze categorie gaat het ook om kernactiviteiten en grootschalige verwerkingen. De verwerkingen behoeven echter niet *regelmatig en stelselmatig* plaats te vinden.

5.4.2 Kan ik ook vrijwillig een functionaris voor gegevensbescherming aanstellen?

Ja, dat kan. Ook organisaties die niet onder één van hierboven genoemde situaties vallen mogen een FG aanstellen. Dit wordt met name aangeraden voor private organisaties die een publieke of semi-publieke taak uitvoeren, zoals bijvoorbeeld energie- en waterleidingbedrijven. Bij het inrichten van de functie moet u rekening houden met de aard van de verwerkingsactiviteiten en de daarbij behorende risico's voor de betrokkenen.

Wanneer u ervoor kiest vrijwillig een FG aan te stellen, dient u er rekening mee te houden dat deze FG in dat geval dezelfde taken, bevoegdheden, verantwoordelijkheden en positie heeft als wanneer deze verplicht zou moeten worden aangesteld. Wanneer u een met de FG vergelijkbare rol instelt (bijvoorbeeld een *privacy officer* of een medewerker gegevensbescherming), dan moet het binnen en buiten de organisatie duidelijk zijn dat deze persoon niet de formele rol van FG bekleedt.

5.4.3 Welke eisen worden gesteld aan een functionaris voor gegevensbescherming?

De functie van FG moet worden vervuld door een deskundige persoon. Het benodigde niveau van kennis en expertise moet in verhouding staan tot de gevoeligheid, complexiteit en hoeveelheid persoonsgegevens die een organisatie verwerkt. De FG dient deskundig te zijn op het gebied van nationale en Europese wetgeving en de praktijk rondom de bescherming van persoonsgegevens, waaronder een diepgaand begrip van de Verordening en de Uitvoeringswet. Verder dient hij voldoende persoonlijke kwaliteiten te bezitten om zijn taken op grond van de Verordening goed te kunnen vervullen. Dergelijke kwaliteiten zien onder meer op integriteit en professionele ethiek.

De FG hoeft volgens de Artikel 29-werkgroep niet alle deskundigheden zelf te bezitten. Het is voldoende als deze deskundigheden in zijn team beschikbaar zijn.

5.4.4 Kan ik een functionaris voor gegevensbescherming extern aanstellen of inhuren?

Ja. Het is niet noodzakelijk dat de FG bij u in loondienst is. De FG mag ook op basis van een dienstverleningsovereenkomst met een externe organisatie worden aangesteld. Ook kunnen meerdere organisaties dezelfde FG delen. Zo kunnen bijvoorbeeld meerdere gemeenten één FG delen.

5.4.5 Welke taken heeft een functionaris voor gegevensbescherming?

De FG heeft de volgende taken op grond van de Verordening:

1. *De FG informeert en adviseert over uw verplichtingen op grond van de Verordening*

De FG heeft allereerst een informerende en adviserende rol binnen uw organisatie. U dient de FG te zien als deskundige die u en uw medewerkers adviseert over de wijze waarop uw organisatie aan haar verplichtingen op grond van de Verordening, de Uitvoeringswet en andere relevante nationale of Europese regelgeving met betrekking tot de bescherming van persoonsgegevens kan voldoen.

2. *De FG ziet toe op de naleving van de Verordening en uw interne gegevensbeschermingsbeleid*

De FG moet toezien op de naleving van de Verordening en andere nationale of Europese regelgeving met betrekking tot de bescherming van persoonsgegevens en op het door u vastgestelde beleid voor de bescherming van persoonsgegevens. Dit toezicht ziet onder meer op de vraag of u voldaan heeft aan uw verplichtingen omtrent:

- het toewijzen van verantwoordelijkheden;
- het bewustmaken en opleiden van het bij de verwerking betrokken personeel; en
- het uitvoeren van audits;

De FG verzamelt ten behoeve van het toezicht informatie binnen uw organisatie om verwerkingsactiviteiten te identificeren, te analyseren en te beoordelen. Op grond daarvan voorziet de FG u van informatie, advies en aanbevelingen rondom de naleving van de Verordening bij de verwerkingsactiviteiten door uw organisatie.

3. *De FG moet op uw verzoek adviseren over de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan*

Op uw verzoek dient de FG u te adviseren over de gegevensbeschermingseffectbeoordeling. Het gaat dan om:

- de noodzakelijkheid van het uitvoeren van een gegevensbeschermingseffectbeoordeling;
- de methodologie;
- of u de beoordeling zelf kunt uitvoeren of dit beter door een externe partij kan worden gedaan;
- of een gegevensbeschermingseffectbeoordeling goed is uitgevoerd;
- of op basis van de uitkomsten nakoming van de Verordening is gewaarborgd wanneer de voorgenomen verwerking wordt gestart en of de Autoriteit Persoonsgegevens moet worden geraadpleegd;
- welke maatregelen en waarborgen bij die verwerking dienen te worden genomen.

4. *Samenwerken met en optreden als contactpunt voor de Autoriteit Persoonsgegevens*

De FG is de schakel tussen uw organisatie en de Autoriteit Persoonsgegevens. Hoewel de FG gehouden is tot geheimhouding dan wel vertrouwelijkheid met betrekking tot de uitvoering van zijn taken, belet dat deze niet om met de Autoriteit Persoonsgegevens overleg te plegen en advies te vragen omtrent de uitleg van bepaalde onderdelen van de Verordening.

Verder treedt de FG op als contactpunt voor de Autoriteit Persoonsgegevens in het geval u een voorafgaande raadpleging heeft aangevraagd (zie paragraaf 5.6).

Ook dient de FG als contactpunt op te treden wanneer de Autoriteit Persoonsgegevens toegang vordert tot documenten of informatie ten behoeve van haar toezichthoudende taken en in de uitoefening van haar bevoegdheden.

5. *De FG rapporteert over de uitvoering van zijn taken*

De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende binnen uw organisatie. Daarnaast kan de FG ook jaarlijks een verslag uitbrengen van de door hem uitgevoerde activiteiten en deze ter beschikking stellen aan het hoogste management.

5.4.6 Wat is de positie van een functionaris voor gegevensbescherming?

Om de rol van FG goed te kunnen uitvoeren, dient de FG goed gepositioneerd te zijn binnen de organisatie. Dit betekent het volgende:

1. De FG moet tijdig en behoorlijk worden betrokken

U dient de FG *tijdig* en *naar behoren* te betrekken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Bij het uitvoeren van een gegevensbeschermingseffectbeoordeling (zie paragraaf 5.5) dient de FG bijvoorbeeld in een vroeg stadium te worden betrokken.

Om te waarborgen dat de FG inderdaad op tijd en in voldoende mate wordt betrokken, dient u erop toe te zien dat:

- de FG regelmatig wordt uitgenodigd om aan vergaderingen van het hoger management en het middenmanagement deel te nemen.
- aan de mening van de FG altijd passende waarde wordt gehecht. Bij geschillen is het raadzaam om vast te leggen waarom het advies van de FG niet gevolgd is.
- de FG onmiddellijk wordt geraadpleegd indien zich een datalek of ander incident voordoet.

Verder is het aan te bevelen de FG uit te nodigen wanneer beslissingen met gevolgen voor gegevensbescherming worden genomen. Tenslotte dient alle relevante informatie tijdig aan de FG te worden verstrekt. U kunt door middel van het opstellen en kenbaar maken van intern beleid medewerkers informeren over wanneer en bij welke aangelegenheden de FG dient te worden geraadpleegd.

2. De FG moet ondersteund worden in de uitvoering van zijn taken

U moet de FG ondersteunen bij de uitvoering van de hierboven besproken taken. Dit betekent onder andere dat u de FG toegang moet verschaffen tot persoonsgegevens en verwerkingsactiviteiten opdat deze zelf kan onderzoeken welke verwerkingsactiviteiten plaatsvinden en of deze voldoen aan de vereisten van de Verordening. Ook dient u de middelen ter beschikking te stellen die de FG nodig heeft om zijn taken te vervullen. Deze middelen zijn bijvoorbeeld:

- voldoende tijd om zijn taken uit te voeren;
- financiële middelen;
- faciliteiten zoals een werkplek, elektronische middelen en indien nodig personeel;
- officiële interne berichtgeving over aanstelling van de FG;
- toegang tot andere diensten binnen de organisatie, zodat de FG de nodige ondersteuning, inbreng en informatie kan verkrijgen vanuit die diensten.

Verder dient u de FG in staat te stellen zijn deskundigheid op peil te houden. Dit houdt bijvoorbeeld in dat de FG periodiek bijscholing moet kunnen krijgen om op de hoogte te blijven van ontwikkelingen op het gebied van gegevensbescherming.

Wanneer binnen uw organisatie tegen het advies van de FG in besluiten worden genomen die naar zijn oordeel in strijd zijn met de Verordening, dient de FG de mogelijkheid te hebben om zijn advies voor te leggen aan het hoogste management binnen de organisatie.

3. De FG dient onafhankelijk zijn rol te kunnen vervullen

De FG vervult binnen uw organisatie een belangrijke rol met het oog op de naleving van de Verordening en de Uitvoeringswet en dient daarom deze rol *onafhankelijk* te kunnen vervullen. Dit houdt onder andere in dat u de FG geen instructies mag geven, bijvoorbeeld met het oog op het beoogde resultaat van een onderzoek, hoe een klacht dient te worden afgehandeld, of omtrent het betrekken van de Autoriteit Persoonsgegevens. Ook dient de FG zich een onafhankelijke visie te kunnen vormen over de uitleg van de Verordening.

De FG heeft ook een vorm van ontslagbescherming: de FG kan niet ontslagen of gestraft worden voor de uitvoering van zijn taken.

4. Betrokkenen moet contact op kunnen nemen met de FG
Betrokkenen moeten zich kunnen wenden tot de FG voor alle aangelegenheden die verband houden met de Verordening, in het bijzonder daar waar het de uitoefening van hun rechten op grond van de Verordening betreft.

5. De FG is gehouden tot geheimhouding
De FG is gehouden tot geheimhouding voor wat betreft de uitvoering van zijn taken. In het bijzonder is de FG gehouden tot geheimhouding van hetgeen hem op grond van klachten of verzoeken van de betrokkene ter ore komt, tenzij de betrokkene instemt met bekendmaking.

6. De FG mag geen conflicterende belangen hebben
Het is mogelijk dat de FG geen voltijd positie vervult binnen uw organisatie. De persoon die de rol van FG vervult mag dan ook met andere taken en plichten binnen uw organisatie worden belast. Daarbij is wel van belang dat die andere taken en plichten niet conflicteren met diens taken als FG. Zo mag de FG niet ook een functie vervullen waarbij deze het doel en de middelen voor gegevensverwerkingen vaststelt. Zo is bijvoorbeeld de functie van HR directeur onverenigbaar met de functie van FG, omdat de HR directeur besluiten neemt over het verwerken van gegevens van medewerkers.

5.4.7 Is een functionaris voor gegevensbescherming eindverantwoordelijk voor de naleving van de Verordening?

Nee. De verwerkingsverantwoordelijke blijft eindverantwoordelijk (*accountable*) voor de goede naleving van de Verordening. De FG wordt geraadpleegd (*consulted*) en houdt toezicht, maar is niet de degene die uiteindelijk de beslissing neemt over het al dan niet verwerken van persoonsgegevens of het nemen van maatregelen.

Lees meer:

Artikel 37 AVG | Overweging 97 (aanwijzing van de functionaris voor gegevensbescherming)
Artikel 38 AVG | Overweging 97 (positie van de functionaris voor gegevensbescherming)
Artikel 39 AVG | Overweging 97 (taken van de functionaris voor gegevensbescherming)
Artikel 35, lid 2, AVG | (Betrekken van de functionaris bij gegevensbeschermingseffectbeoordelingen)
Artikel 39 UAVG | (Geheimhoudingsplicht)

Groep Gegevensbescherming Artikel 29, *Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)*, Goedgekeurd op 13 december 2016. Laatstelijk herzien en goedgekeurd op 5 april 2017, 16/NL WP 243 rev.01

Autoriteit Persoonsgegevens, "Functionaris voor de gegevensbescherming", te raadplegen via: *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg*

5.5 Wat is een gegevensbeschermingseffectbeoordeling?

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dan dient u voorafgaand aan de verwerking een zogenaamde gegevensbeschermingseffectbeoordeling uit te voeren. Een gegevensbeschermings-effectbeoordeling, in de praktijk ook wel *Privacy Impact Assessment (PIA)* of *Data Protection Impact Assessment (DPIA)* genoemd, is een beoordeling van de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. Een gegevensbeschermingseffect-beoordeling is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of te verkleinen. Ook toont u met een gegevensbeschermingseffectbeoordeling aan dat u aan de vereisten van de Verordening hebt voldaan voor die verwerkingsactiviteit.

5.5.1 Wanneer moet ik een gegevensbeschermingseffectbeoordeling uitvoeren?

U bent verplicht een gegevensbeschermingseffectbeoordeling uit te voeren voor verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen (de betrokkenen). Voor verwerkingen waarbij een dergelijk hoog risico waarschijnlijk niet aanwezig is, hoeft u géén gegevensbeschermingseffectbeoordeling uit te voeren.

De rijksoverheid is daarnaast verplicht een gegevensbeschermingseffectbeoordeling uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien. Dit is staand beleid. Zie hiervoor de Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA).

5.5.2 Wanneer is er sprake van een 'hoog risico'?

Volgens de Verordening is er in ieder geval sprake van een hoog risico wanneer u:

- geautomatiseerd systematisch en uitgebreid persoonlijke aspecten evalueert, waaronder begrepen profilering, en op basis daarvan besluiten neemt met rechtsgevolgen voor de betrokkene, of die de betrokkene anderszins in aanzienlijke mate treffen (zie hoofdstuk 7);
- op grote schaal bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard verwerkt;
- grootschalig en stelselmatig mensen volgt in openbaar toegankelijke ruimten (bijvoorbeeld door middel van cameratoezicht).

Dit is echter geen uitputtende lijst. Hoewel de Verordening deze drie situaties specifiek noemt, dient voor alle situaties met een mogelijk hoog risico voor betrokkenen een gegevensbeschermingseffectbeoordeling te worden uitgevoerd. Om te bepalen of er mogelijk sprake is van een hoog risico hanteren de toezichthouders de onderstaande vuistregel.

Er is sprake van een hoog risico wanneer uw voorgenomen verwerking aan twee of meer van de onderstaande negen criteria voldoet:
1. evaluatie van personen of scoretoekenning;
2. geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. stelselmatige monitoring;
4. gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. op grote schaal verwerkte gegevens;
6. matching of samenvoeging van datasets;
7. gegevens met betrekking tot kwetsbare betrokkenen;
8. innovatieve toepassing van nieuwe technologsiche of organisatorische oplossing;
9. blokkering van een recht, dienst of contract.

De toezichthouders moeten lijsten publiceren met daarop verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling noodzakelijk is. De toezichthouders mogen lijsten publiceren met verwerkingen waarvoor geen gegevensbeschermingseffectbeoordeling verplicht is. Deze lijsten worden gepubliceerd op de website van de Autoriteit Persoonsgegevens.

5.5.3 Moet ik voor elke verwerking een gegevensbeschermingseffectbeoordeling uitvoeren?

U hoeft niet voor iedere afzonderlijke verwerking met een hoog risico een gegevensbeschermingseffectbeoordeling uit te voeren. Indien verschillende verwerkingen vergelijkbaar zijn en vergelijkbare risico's bevatten, kunnen deze verwerkingen door middel van dezelfde gegevensbeschermingseffectbeoordeling beoordeeld worden. Het besluit om meerdere verwerkingen te combineren dient u te motiveren.

5.5.4 Wat houdt het uitvoeren van een gegevensbeschermingseffectbeoordeling in?

Door middel van een gegevensbeschermingseffectbeoordeling dient u met name de oorsprong, aard, het specifieke karakter en de ernst van risico's voor de bescherming van de rechten en vrijheden van betrokkene te analyseren. Daarbij moet u de specifieke waarschijnlijkheid en de ernst van de risico's voor de persoonlijke levenssfeer van betrokkenen beoordelen. Wanneer bijvoorbeeld met behulp van een smartwatch gezondheidsgegevens worden vastgelegd om persoonlijke fitprofielen op te stellen, dan is het risico voor betrokkenen bij deze verwerking hoog. Een dergelijke toepassing dient dan ook met voldoende waarborgen te zijn omkleed.

Bij de beoordeling van de risico's voor de betrokkene dient u de volgende omstandigheden mee te nemen:
- de aard van de voorgenomen gegevensverwerking;
- de omvang, context en doelen van de verwerking; en
- de bronnen van de risico's.

De focus van de gegevensbeschermingseffectbeoordeling ligt daarin dat u onderzoekt of de geplande maatregelen, waarborgen en mechanismen om de belangen van betrokkene te beschermen voldoende zijn, dan wel of hier nog verbeteringen in kunnen worden doorgevoerd waarmee de risico's voor betrokkene verder worden beperkt. Het is daarom van belang dat een gegevensbeschermingseffectbeoordeling in een zo vroeg mogelijk stadium wordt gestart. Ook omdat u alleen dan goed invulling kunt geven aan de eisen van gegevensbescherming en standaardinstellingen (*privacy by design* and *privacy by default*). Indien een goedgekeurde gedragscode op de verwerking van toepassing is, wordt deze meegenomen in de beoordeling.

5.5.5 Wat moet ik met de resultaten van de gegevensbeschermingseffect-beoordeling doen?

De gegevensbeschermingseffectbeoordeling dient te resulteren in:
- een beschrijving van de beoogde verwerking en de doelen voor die verwerking;
- een oordeel over de noodzakelijkheid en evenredigheid van de verwerking met het oog op het vastgestelde doel;
- een oordeel over de risico's voor betrokkenen;
- de beoogde maatregelen in de zin van waarborgen, veiligheidsmaatregelen en mechanismen om die risico's weg te nemen of te beperken.

De resultaten van de gegevensbeschermingseffectbeoordeling dient u mee te nemen wanneer u de maatregelen gaat vaststellen om de belangen van betrokkene te beschermen en om aan te tonen dat u de Verordening bij uw verwerkingsactiviteit naleeft. Wanneer u de hoge risico's voor betrokkenen niet met redelijke maatregelen kunt beperken, moet u de voorgenomen verwerking, voordat u aan die verwerking begint, voorleggen aan de Autoriteit Persoonsgegevens (zie paragraaf 5.6).

U dient de resultaten van de gegevensbeschermingseffectbeoordeling regelmatig te evalueren met het oog op veranderde omstandigheden, met name wanneer de verwerkingsactiviteit anders wordt ingericht, bijvoorbeeld door het gebruik van andere of nieuwere technologieën.

Verder mag u (delen van) de resultaten van de gegevensbeschermingseffectbeoordeling openbaar maken. Dit is geen verplichting op grond van de Verordening, maar wordt aangeraden met het oog op transparantie en verantwoording.

5.5.6 Kan een functionaris voor gegevensbescherming de gegevensbeschermingseffectbeoordeling uitvoeren?

De verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren is opgelegd aan de verwerkingsverantwoordelijke, niet aan de FG. Wel kan de FG betrokken worden bij het uitvoeren van de gegevensbeschermingseffectbeoordeling. De FG dient hiertoe tijdig betrokken te worden, opdat deze zijn taken met het oog op het informeren, adviseren over en toezien op de naleving van de Verordening kan uitvoeren (zie ook paragraaf 5.4.5).

De FG brengt in het kader van de gegevensbeschermingseffectbeoordeling een advies uit. Wanneer u als verwerkingsverantwoordelijke het niet eens bent met dit advies, dan dient bij het registreren van de gegevensbeschermingseffectbeoordeling schriftelijk te worden gemotiveerd waarom het advies niet is meegenomen in het oordeel, dan wel waarom het advies niet is opgevolgd. Op grond van het model gegevensbeschermingseffectbeoordeling rijksdienst (PIA) dient de FG binnen de rijksoverheid zijn advies op te nemen in het rapport.

Lees meer:
Artikel 35 | Overweging 75, 84, 89, 90, 91, 92 en 93 (gegevensbeschermingseffectbeoordeling)

Groep Gegevensbescherming Artikel 29, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679*. Vastgesteld op 4 april 2017, zoals laatstelijk gewijzigd en vastgesteld op 4 oktober 2017, 17/NL WP 248 rev.01

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Justitie en Veiligheid, *Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)*; Kamerbrief minister Plasterk (BZK) van 29 september 2017 over nieuw Model gegevensbeschermingseffectbeoordeling rijksdienst.

Autoriteit Persoonsgegevens: "*Privacy Impact Assessments*", te raadplegen via:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/privacy-impact-assessment-pia?qa=PIA

5.6 Wat is een 'voorafgaande raadpleging'?

Wanneer uit de gegevensbeschermingseffectbeoordeling blijkt dat een voorgenomen verwerking een hoog risico voor betrokkenen inhoudt, en dat dit risico niet wordt weggenomen door het treffen van risicobeperkende maatregelen, dan moet u de voorgenomen verwerking voorleggen aan de Autoriteit Persoonsgegevens.

Indien u deel uitmaakt van de rijksoverheid moet u ook een voorafgaande raadpleging aanvragen bij het opstellen van wet- en regelgeving die ziet op de verwerking van persoonsgegevens.

U mag niet beginnen met uw verwerkingsactiviteit zolang de Autoriteit Persoonsgegevens geen positief oordeel heeft uitgebracht.

5.6.1 Welke informatie moet ik aan de toezichthouder verstrekken bij een voorafgaand raadpleging?

Bij de aanvraag van een voorafgaande raadpleging moet u de toezichthouder de volgende informatie verstrekken:
- de doelen en middelen van de voorgenomen verwerking;
- de maatregelen en waarborgen die worden getroffen voor de naleving van de Verordening;
- de uitkomsten van de gegevensbeschermingseffectbeoordeling.

Daarnaast moet u, indien van toepassing, de volgende informatie verstrekken:
- uw respectievelijke verantwoordelijkheden, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor verwerkingen binnen een concern;
- de contactgegevens van uw functionaris voor gegevensbescherming;
- alle andere informatie waar de toezichthoudende autoriteit om verzoekt.

5.6.2 Wanneer krijg ik antwoord van de Autoriteit Persoonsgegevens?

U krijgt in beginsel binnen acht weken antwoord van de Autoriteit Persoonsgegevens. Deze termijn kan onder omstandigheden worden verlengd, bijvoorbeeld als de voorgenomen verwerking zeer complex is.

5.7 Wat houdt 'privacy door ontwerp en standaardinstellingen' in?

Een nieuw uitgangspunt in de Verordening is het beginsel van privacy door ontwerp en door standaardinstellingen, in de praktijk vaak aangeduid met de Engelse benamingen *Privacy by Design* en *Privacy by Default*. Privacy door ontwerp en door standaardinstellingen houdt kort gezegd in dat u privacy en gegevensbescherming meeneemt als eisen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt. U dient er zorg voor te dragen dat u een zo klein mogelijke inbreuk op de persoonlijke levenssfeer maakt bij uw verwerkingsactiviteiten, bijvoorbeeld door het toepassen van pseudonimisering en het inbouwen van andere technische waarborgen. Het uitgangspunt van privacy door ontwerp en door standaardinstellingen is in de Verordening neergelegd als een concrete plicht voor de verwerkingsverantwoordelijke.

Welke technische en organisatorische maatregelen u moet nemen om invulling te geven aan het uitgangspunt van privacy door ontwerp en door standaardinstellingen is afhankelijk van het concrete geval. Bij het bepalen van de verwerkingsmiddelen en de verwerking moet u rekening houden met de volgende elementen:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking;
- de risico's voor de betrokkene.

Deze elementen bepalen gezamenlijk welke technische en organisatorische maatregelen u moet nemen om de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in te bouwen ter naleving van de eisen uit de Verordening. Met andere woorden: de maatregelen die u neemt moeten in verhouding staan tot de risico's en redelijk zijn met het oog op de stand van de techniek en de uitvoeringskosten die u moet maken om de maatregelen te implementeren.

Bij het ontwerpen van uw systemen en processen kunt u volgende ontwerpstrategieën hanteren:

Data georiënteerde ontwerp strategieën	
Minimaliseer	Beperk zoveel mogelijk de verwerking van gegevens. Selecteer voor het verzamelen. Verwijder wanneer mogelijk.
Scheid	Scheid persoonsgegevens zoveel mogelijk van elkaar en werk zo gedistribueerd mogelijk.
Abstraheer	Aggregeer tot het hoogst mogelijke niveau. Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.
Bescherm/maak onherleidbaar	Voorkom dat gegevens openbaar worden. Beveilig gegevens. Verbreek waar mogelijk de link tussen personen en gegevens (anonimiseer en pseudonimiseer).

Proces georiënteerde ontwerp strategieën	
Informeer	Informeer gebruikers over de verwerking van hun persoonsgegevens.
Geef controle	Geef gebruikers controle over de verwerking van hun persoonsgegevens.
Dwing af	Stel een privacybeleid op en dwing dit af met technische en organisatorische middelen.
Toon aan	Toon aan dat op een privacyvriendelijke wijze persoonsgegevens worden verwerkt. Verzamel logs, doe audits en rapporteer.

Privacy door ontwerp en door standaardinstellingen voor producenten

Wanneer u een producent bent van een product, dienst of toepassing die is gebaseerd op de verwerking van persoonsgegevens, dient u bij de ontwikkeling en uitwerking van die producten, diensten en toepassingen rekening te houden met het recht op bescherming van persoonsgegevens. Met inachtneming van de stand van de techniek moet u erop toezien dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming.

Privacy door ontwerp en door standaardinstellingen bij aanbestedingen
Overheidsinstellingen moeten er verder rekening mee houden dat ook bij openbare aanbestedingen de beginselen van privacy door ontwerp en door standaardinstellingen in aanmerking worden genomen.

5.7.1 Hoe maak ik aantoonbaar dat ik met deze uitgangspunten rekening heb gehouden?

U dient aantoonbaar te maken dat u bij de ontwikkelingen van nieuw beleid of het ontwerp van nieuwe systemen er zorg voor hebt gedragen dat de inbreuk op de bescherming van persoonsgegevens voor betrokkenen zo klein mogelijk is. Dit doet u door interne beleidsmaatregelen te nemen en technische maatregelen toe te passen. Hieronder volgt een aantal mogelijke maatregelen:

- het minimaliseren van de verwerking van persoonsgegevens;
- het zo spoedig mogelijk pseudonimiseren van persoonsgegevens;
- transparantie met betrekking tot de functies en de verwerking van persoonsgegevens;
- het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking; en
- beveiligingskenmerken creëren en verbeteren.

U kunt ook door middel van certificeringsmechanismen aantonen dat u aan deze beginselen hebt voldaan (zie paragraaf 5.11).

Lees meer:
Artikel 25 AVG | Overweging 78 (privacy door ontwerp en door standaardinstellingen)

European Union Agency for Network and Information Security (2015), *Privacy and Data Protection by Design – from policy to engineering*

Colesky, Hoepman & Hillen (2016), *A critical analysis of privacy by design strategies*, in: Security and Privacy Workshops (SPW), 2016 IEEE

5.8 Aan welke beveiligingseisen moeten mijn verwerkingen voldoen?

De Verordening verplicht u de persoonsgegevens die u verwerkt te beveiligen. U dient hiertoe passende technische en organisatorische maatregelen te treffen, die een op het risico afgestemd beschermingsniveau waarborgen. Deze maatregelen omvatten bijvoorbeeld:

- pseudonimisering en versleuteling van de persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- 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.

Technische maatregelen zijn bijvoorbeeld het toepassen van encryptie, het opzetten van een firewall of het opslaan van gegevens in beveiligde omgevingen. Bij organisatorische maatregelen kunt u denken aan het beperken van de toegang tot gegevens tot bepaalde medewerkers (autorisatiebeleid).

5.8.1 Hoe stel ik vast welke beveiligingsmaatregelen ik moet treffen?

1. Stel het risico vast voor de betrokkenen
Bij het vaststellen van de juiste beveiligingsmaatregelen dient u allereerst het risico voor de betrokkene bij de gegevensverwerkingen vast te stellen. Het beveiligingsniveau dient immers op dat risisco afgestemd te zijn. Risico's voor betrokkenen doen zich met name voor in situaties waar er sprake is van verlies, vernietiging, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens. Bij risico's voor betrokkenen moet gedacht worden aan lichamelijke, materiële of immateriële schade.

Van dergelijke risico's is voornamelijk sprake wanneer de verwerking kan leiden tot:
- discriminatie;
- identiteitsdiefstal of -fraude;
- financiële verliezen;
- reputatieschade;
- verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- ongeoorloofde ongedaanmaking van pseudonimisering;
- enig ander aanzienlijk economisch of maatschappelijk nadeel.

Een verhoogd risico wordt in ieder geval aangenomen wanneer:
- de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;
- wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt;
- bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
- wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

U dient dit risico objectief vast te stellen. Dit houdt in dat iedereen, niet alleen u als subjectief persoon, dit risico zo zou vaststellen. Uit uw oordeel dient te blijken of de verwerking gepaard gaat met een risico of met een hoog risico.

2. Neem passende maatregelen

De beveiliging van persoonsgegevens dient *passend* te zijn. U hoeft dus niet persé de zwaarst mogelijke beveiligingsmaatregelen te treffen, maar maatregelen die in verhouding staan tot de gegevens en de bijbehorende risico's voor de betrokkenen. Hoe groter het risico voor betrokkenen, des te zwaarder de beveiligingsmaatregelen die u moet treffen. Wanneer u bijvoorbeeld op grote schaal bijzondere categorieën van persoonsgegevens verwerkt, dan dient u zwaardere beveiligingsmaatregelen te treffen dan wanneer u kleinschalig NAW-gegevens verwerkt.

Verder dient u bij het vaststellen van passende beveiligingsmaatregelen rekening te houden met:
- de stand van de techniek;
- de uitvoeringskosten;
- de aard van de verwerking;
- de omvang van de verwerking;
- de context van de verwerking;
- de verwerkingsdoeleinden;
- de ernst van de vastgestelde risico's; en
- de waarschijnlijkheid dat de vastgestelde risico's zich zullen verwezenlijken.

3. Evalueer tussentijds de maatregelen

De beveiligingsmaatregelendie u treft dienen gedurende de gehele looptijd van de verwerking passend te zijn. Dit betekent dat u, met name bij verwerkingen die langere tijd voortduren, periodiek dient te evalueren of de genomen beveiligingsmaatregelen nog steeds passend zijn.

Wanneer bijvoorbeeld door technische ontwikkelingen cybercriminelen nieuwe methoden tot hun beschikking krijgen om uw beveiligingsmaatregelen te ondermijnen, dan moet u uw beveiliging hierop aanpassen.

5.8.2 Kan ik mij certificeren of bij een gedragscode aansluiten om aan deze verplichting te voldoen?

Door u aan te sluiten bij een goedgekeurde gedragscode of door het gebruik van een goedgekeurd certificeringsmechanisme kunt u aantonen dat u aan uw beveiligingsverplichtingen voldoet (zie hiervoor paragraaf 5.11). De Verordening moedigt het opstellen van gedragscodes door organisaties van verwerkingsverantwoordelijken sterk aan.

Lees meer:

Artikel 32 AVG | Overweging 83, 74, 75, 76, 77 (beveiliging van de verwerking)

Autoriteit Persoonsgegevens, *CBP Richtsnoeren Beveiliging van persoonsgegevens*

5.9 Wat is de verplichting om een inbreuk in verband met persoonsgegevens mede te delen?

De Verordening bevat een verplichting om onder omstandigheden een inbreuk in verband met persoonsgegevens (een datalek) mede te delen aan de Autoriteit Persoonsgegevens en de betrokkene. Deze 'meldplicht datalekken' bestond sinds 1 januari 2016 reeds in Nederland onder de Wbp. Een datalek kan voor betrokkenen grote gevolgen hebben, waaronder verlies van controle over hun persoonsgegevens, de beperking van hun rechten, discriminatie, identiteitsdiefstal of financiële verliezen. Het is dan ook van belang dat een datalek tijdig en op passende wijze wordt aangepakt. De verplichte mededeling aan de Autoriteit Persoonsgegevens en in voorkomende gevallen aan de betrokkene is daar een uitwerking van.

5.9.1 Wanneer is er sprake van een inbreuk in verband met persoonsgegevens?

Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Het is voor de kwalificatie als 'inbreuk in verband met persoonsgegevens' niet relevant dat er boos opzet in het spel is. Hoewel een *hack* van uw systemen waarbij persoonsgegevens worden buitgemaakt een schoolvoorbeeld is van een datalek, kunnen ook gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk openstaat ook kwalificeren als een datalek.

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou *kunnen* leiden tot een beveiligingsincident. Er heeft zich *daadwerkelijk* een beveiligingsincident voorgedaan, en de preventieve maatregelen die u eventueel heeft getroffen waren niet toereikend om dit te voorkomen.

5.9.2 Moet ik ieder datalek melden aan de Autoriteit Persoonsgegevens?

Ja. In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht.

5.9.3 Wanneer moet ik aan de betrokkene mededelen dat er een inbreuk heeft plaatsgevonden?

Wanneer u heeft vastgesteld dat de inbreuk op de persoonsgegevens een *hoog* risico voor betrokkenen inhoudt, dient u ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens.

U hoeft de betrokkene niet te informeren wanneer:

- u passende technische en organisatorische beschermingsmaatregelen heeft genomen, bijvoorbeeld in de vorm van versleuteling van de gegevens;
- u achteraf maatregelen heeft genomen waarmee de vastgestelde risico's voor betrokkenen zijn weggenomen;

- de mededeling aan betrokkenen u onevenredig veel inspanning zou kosten. In dat geval kunt u volstaan met een openbare mededeling, bijvoorbeeld door de onder paragraaf 5.9.5 vereiste informatie te publiceren op uw website.

Verder hoeft u het datalek niet te melden bij de betrokkene wanneer het achterwege blijven van die melding noodzakelijk is ter waarborging van:
- de nationale veiligheid;
- de landsverdediging;
- de openbare veiligheid;
- de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, en de tenuitvoerlegging van straffen;
- andere belangrijke doelstellingen van algemeen belang van de Europese Unie of een lidstaat;
- de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
- een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
- de inning van civielrechtelijke vorderingen.

Voor de financiële sector geldt de meldplicht aan de betrokkene op grond van de Verordening niet. Voor deze sector geldt op grond van de Wet op het financieel toezicht dat een melding aan de betrokkene moet worden gedaan op grond van de zorgplicht.

Nota bene:
Wanneer u betrokkenen niet heeft geïnformeerd en de Autoriteit Persoonsgegevens is van mening dat dit alsnog moet gebeuren, dan kan zij haar handhavende bevoegheden inzetten.

5.9.4 Wanneer moet ik het datalek melden?

U dient de Autoriteit Persoonsgegevens binnen 72 uur na ontdekking in kennis te stellen over het datalek. Het is goed mogelijk dat u de onder paragraaf 5.9.5 vermelde informatie niet binnen 72 uur volledig in beeld heeft. In die gevallen dient u zo veel mogelijk informatie binnen 72 uur te verstrekken en kunt u de overige informatie zonder onredelijke verdere vertraging in fasen aanleveren. De eerste kennisgeving dient in die gevallen vergezeld te gaan van een verklaring voor de vertraging.

Daarnaast dient u, wanneer kennisgeving aan betrokkenen vereist is, deze *onverwijld* te informeren. Het onverwijld melden houdt in dat u, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek om vast te stellen of u betrokkenen moet informeren. Wat in een concreet geval als ‘onverwijld’ moet worden aangemerkt zal afhangen van de omstandigheden van het geval. U moet daarbij rekening houden met het feit dat de betrokkene naar aanleiding van uw melding tijdig in staat moet zijn gesteld mogelijke maatregelen te nemen om de nadelige gevolgen van het datalek zo veel mogelijk te beperken of te voorkomen.

5.9.5 Welke informatie moet ik bij de melding verstrekken?

Welke informatie u moet verstrekken is afhankelijk van de vraag aan wie u de mededeling moet doen: de Autoriteit Persoonsgegevens of de betrokkenen.

Mededeling aan de Autoriteit Persoonsgegevens
U dient de Autoriteit Persoonsgegevens bij het doen van de melding in ieder geval van de volgende informatie te voorzien:
- de aard en omvang van de inbreuk;

- waar mogelijk de categorieën van betrokkenen, de persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die u heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Mededeling aan betrokkenen
Wanneer u betrokkenen moet informeren over de inbreuk, dient die kennisgeving in ieder geval de volgende elementen te bevatten:
- een omschrijving van de aard van de inbreuk;
- de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
- de maatregelen die u heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

U dient de kennisgeving aan betrokkenen in duidelijke en eenvoudige taal op te stellen.

5.9.6 Wat moet ik verder met de mededeling doen?
U dient het datalek te documenteren in een overzicht van datalekken die zich in uw organisatie hebben voorgedaan. In dit overzicht dient u ten minste de feiten omtrent de inbreuk en de gevolgen ervan te documenteren. Verder is het verstandig met het oog op het verantwoordingsbeginsel en uw bewijspositie om de door u genomen corrigerende maatregelen ook te documenteren.

Lees meer:
Artikel 33 AVG | Overweging 75, 85, 87, 88 (melding van een datalek aan de toezichthoudende autoriteit)
Artikel 34 AVG | Overweging 75, 86, 87, 88 (melding van een datalek aan de betrokkene
Artikel 23 AVG | Overweging 73 (beperkingen)
Artikel 42 UAVG | (Uitzondering op meldplicht datalekken aan de betrokkene)

Groep Gegevensbescherming Artikel 29, *Guidelines on Personal data breach notification under Regulation 2016/679*, aangenomen 3 oktober 2017, 17/EN WP250

5.10 Afspraken met verwerkers

De Verordening bepaalt dat u, indien u gebruik maakt van verwerkers, de verwerking door die verwerker moet regelen in een overeenkomst of anderszins bindende rechtshandeling (zie voor de definitie van verwerker hoofdstuk 3).

De verwerkersovereenkomst dient in schriftelijke vorm, waaronder elektronische vorm, te worden opgesteld.

5.10.1 Moet ik een verwerkersovereenkomst sluiten?
Als u een verwerker inschakelt voor uw gegevensverwerkingen dan moet u met deze verwerker een verwerkersovereenkomst sluiten. In deze overeenkomst dient u ten minste de volgende zaken te regelen:
- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Verder dient in de overeenkomst te worden bepaald dat de verwerker:

- de persoonsgegevens alleen verwerkt onder uw schriftelijke instructies, onder andere voor wat betreft de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht);
- waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- minimaal hetzelfde niveau van beveiliging van de persoonsgegevens hanteert als u doet;
- u alle mogelijke ondersteuning biedt bij het nakomen van uw verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen (zie hoofdstuk 7);
- u bijstaat bij het nakomen van uw verplichtingen op het gebied van beveiliging van persoonsgegevens en de meldplicht datalekken;
- na beëindiging van de overeenkomst tussen u en verwerker, de in uw opdracht verwerkte persoonsgegevens wist of aan u teruggeeft, en bestaande kopieën verwijdert;
- u alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de Verordening rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- afspraken met betrekking tot sub-verwerkers maakt (zie paragraaf 5.10.2).

U mag in plaats van een individuele overeenkomst ook kiezen om de afspraken tussen u en uw verwerker te regelen door middel van door de Europese Commissie of Autoriteit Persoonsgegevens vastgestelde standaardcontractbepalingen.

5.10.2 Mag mijn verwerker zomaar andere partijen inschakelen bij het uitvoeren van mijn verwerkingen?

Nee. De verwerker mag alleen een andere partij inschakelen bij de uitvoering van de verwerking (een sub-verwerker) wanneer u daar toestemming voor heeft gegeven.

Lees meer:
Artikel 28 AVG | Overweging 81 (de verwerker)

5.11 Wat zijn goedgekeurde gedragscodes en certificeringsmechanismen?

De Verordening stimuleert het opstellen van gedragscodes die de goede uitvoering en naleving van de Verordening bevorderen. Goedgekeurde gedragscodes worden daarom bij verschillende verplichtingen uit de Verordening als mogelijkheid aangehaald voor de verwerkingsverantwoordelijke of de verwerker om aan te tonen dat zij aan die verplichtingen voldoen. Daarnaast stimuleert de Verordening het instellen van certificeringsmechanismen, gegevensbeschermingszegels en -merktekens, met name ter bevordering van de transparantie van gegevensverwerkingen.

5.11.1 Door wie kan een gedragscode of certificeringsmechanisme worden opgesteld?

Gedragscodes worden opgesteld, gewijzigd of uitgebreid door verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen. Zij moeten bij het opstellen van een gedragscode overleg plegen met belanghebbenden zoals betrokkenen, en rekening houden met bijdragen en standpunten die uit dat overleg voortvloeien. De Autoriteit Persoonsgegevens neemt een besluit over de goedkeuring, wijziging of uitbreiding van een gedragscode naar aanleiding van een uniforme openbare voorbereidingsprocedure.

Certificeringen worden uitgegeven door geaccrediteerde certificeringsorganen of door de Autoriteit Persoonsgegevens.

5.11.2 Is iedere gedragscode toereikend om naleving van de Verordening aan te tonen?

Nee, alleen gedragscodes die goedgekeurd en openbaar zijn gemaakt door de Autoriteit Persoonsgegevens kunnen worden gebruikt om naleving van (onderdelen) van de Verordening en de Uitvoeringswet aan te tonen.

5.11.3 Ontslaat het onderschrijven van een gedragscode of certificering mij van verdere naleving van de Verordening?

Nee, u blijft verplicht de Verordening en de Uitvoeringswet na te leven. Ook mag de toezichthouder nog steeds haar taken en bevoegdheden blijven uitoefenen, ongeacht of u een certificaat heeft met het oog op gegevensbescherming of aangesloten bent bij een gedragscode.

Lees meer:

Artikel 40 AVG | Overweging 98, 99 (gedragscodes)
Artikel 41 AVG | (Toezicht op goedgekeurde gedragscodes)
Artikel 42 AVG | Overweging 100 (certificering)
Artikel 14 UAVG | (Taken en bevoegdheden Autoriteit Persoonsgegevens)
Artikel 21 UAVG | (Aanwijzing accrediterende instantie)

6 Wat zijn mijn plichten als verwerker?

De verwerkingsverantwoordelijke bepaalt het doel en middelen voor de verwerking en om die reden is ook het merendeel van de verplichtingen uit de Verordening aan de verwerkingsverantwoordelijke gericht. In de rolverdeling tussen de verwerkingsverantwoordelijke en de verwerker betekent dit dat de verwerker handelt op basis van de instructies van de verwerkingsverantwoordelijke. Ook moet de verwerker de verwerkingsverantwoordelijke helpen bij het uitvoeren van sommige van de plichten, zoals bijvoorbeeld de invulling van de rechten van de betrokkene, het uitvoeren van gegevensbeschermingseffectbeoordelingen en het melden van datalekken.

Daarnaast zijn er enkele plichten die (ook) zelfstandig gericht zijn aan de verwerker. Het gaat dan om de beveiliging van gegevens, het bijhouden van een register van verwerkingsactiviteiten en het aanstellen van een functionaris voor gegevensbescherming.

6.1 Moet ik de verwerkingsverantwoordelijke garanties bieden?

Een verwerkingsverantwoordelijke mag alleen verwerkers inschakelen die afdoende garanties met betrekking tot de naleving van de Verordening kunnen bieden. Deze garanties zien met name op uw deskundigheid als verwerker, uw betrouwbaarheid en de middelen om ervoor te zorgen dat de technische en organisatorische maatregelen die u treft of heeft getroffen, voldoende zijn om naleving van de Verordening te garanderen. Deze maatregelen zien bijvoorbeeld op de beveiliging van persoonsgegevens.

Om aan te tonen dat u als verwerker inderdaad voldoende garanties biedt met betrekking tot de naleving van de Verordening, kunt u aansluiten bij goedgekeurde gedragscodes of certificeringsmechanismes (zie hoofdstuk 5).

6.2 Moet ik als verwerker verplicht een verwerkersovereenkomst tekenen?

Ja. U dient afspraken te maken met de verwerkingsverantwoordelijke over de wijze waarop u persoonsgegevens namens de verwerkingsverantwoordelijke verwerkt. U kunt uiteraard onderhandelen over de inhoud van de overeenkomst met de verwerkingsverantwoordelijke. Wel is het maken van afspraken over een aantal onderwerpen verplicht. Zie voor de vereisten die aan deze afspraken worden gesteld hoofdstuk 5.

6.3 Mag ik andere partijen inzetten bij het verwerken van persoonsgegevens?

Wanneer u als verwerker zelf een andere verwerker (sub-verwerker) wilt inschakelen voor de verwerking van persoonsgegevens die een verwerkingsverantwoordelijke aan u heeft opgedragen, dan dient u hiervoor voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke te krijgen.

Wanneer u een algemene schriftelijke toestemming heeft om bepaalde verwerkers in dienst te nemen, dient u de verwerkingsverantwoordelijke te informeren over wijzigingen in de inzet van die verwerkers, bijvoorbeeld wanneer u een verwerkingsactiviteit weghaalt bij een verwerker, dan wel wanneer u nieuwe verwerkers inschakelt.

6.4 Welke afspraken moet ik maken met sub-verwerkers?

Wanneer u een sub-verwerker inschakelt voor de gegevensverwerkingen, dient u door middel van een overeenkomst of een andere rechtshandeling deze sub-verwerker te verplichten minimaal hetzelfde niveau van gegevensbescherming te bieden als uzelf biedt ten opzichte van de verwerkingsverantwoordelijke.

Houd er rekening mee dat u als verwerker ten opzichte van de verwerkingsverantwoordelijke volledig aansprakelijk blijft met betrekking tot de gegevensbescherming, ook voor de naleving van de verplichtingen door de sub-verwerker.

Lees meer:
Artikel 28 AVG | Overwegingen 81, 171 (de verwerker)

6.5 Moet ik mijn verwerkingsactiviteiten registreren?

Ja. Ook als verwerker dient u een register van verwerkingsactiviteiten bij te houden. Dit register dient alle categorieën van verwerkingsactiviteiten te bevatten die u ten behoeve van een verwerkingsverantwoordelijke heeft verricht.

6.5.1 Wanneer hoef ik geen register bij te houden?

U hoeft geen register bij te houden als uw onderneming of organisatie minder dan 250 personen in dienst heeft, tenzij de verwerkingen die u voor de verwerkingsverantwoordelijke uitvoert waarschijnlijk een hoog risico voor betrokkenen met zich meebrengen, of niet-incidenteel van aard zijn (zie paragraaf 5.3.3).

6.5.2 Wat moet ik in het register opnemen?

U dient in ieder geval de volgende elementen op te nemen in het register:

- uw naam en contactgegevens;
- contactgegevens van alle verwerkingsverantwoordelijken namens wie u gegevensverwerkingen uitvoert;
- indien van toepassing, de contactgegevens van uw vertegenwoordiger en/of de contactgegevens van de vertegenwoordiger van de verwerkingsverantwoordelijke;
- de contactgegevens van de functionaris voor gegevensbescherming indien u deze heeft aangesteld;
- de categorieën van verwerkingen die u voor de afzonderlijke verwerkingsverantwoordelijken uitvoert;
- indien van toepassing, de doorgiften van persoonsgegevens aan derde landen of internationale organisaties, welke derde landen of internationale organisaties dat betreft en indien van toepassing de documenten waarmee de passende waarborgen die worden getroffen inzichtelijk zijn;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

6.5.3 In welke vorm moet ik het register opstellen?

U dient het register in schriftelijke vorm, waaronder begrepen elektronische vorm, op te stellen.

6.5.4 Wie moet ik toegang geven tot het register?

U dient het register op verzoek aan de Autoriteit Persoonsgegevens ter beschikking te stellen.

Lees meer:
Artikel 30 AVG | Overweging 13, 39, 82 (register van verwerkingsactiviteiten)

6.6 Moet ik een functionaris voor gegevensbescherming aanstellen?

Ook verwerkers dienen onder omstandigheden een FG aan te stellen. De vereisten die aan die FG worden gesteld, alsook diens taken en positie in de organisatie zijn gelijk aan de vereisten die de Verordening aan een FG bij verwerkingsverantwoordelijken stelt. Zie hiervoor hoofdstuk 5.

Lees meer:

Artikel 37 AVG | Overweging 97 (aanwijzing van de functionaris voor gegevensbescherming)
Artikel 38 AVG | Overweging 97 (aanwijzing van de functionaris voor gegevensbescherming)
Artikel 39 AVG | Overweging 97 (taken van de functionaris voor gegevensbescherming)

Groep Gegevensbescherming Artikel 29, *Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)*. Goedgekeurd op 13 december 2016 Laatstelijk herzien en goedgekeurd op 5 april 2017, 16/NL WP 243 rev.01

Website Autoriteit Persoonsgegevens, Onderwerp: AVG - Nieuwe Europese privacywetgeving, (*www.autoriteitpersoonsgegevens.nl*)

6.7 Hoe moet ik de beveiligingseis invullen?

In beginsel is de verplichting om persoonsgegevens te beschermen opgelegd aan de verwerkingsverantwoordelijke. Als verwerker bent u echter onder de Verordening zelfstandig verplicht om passende beveiligingsmaatregelen te treffen voor de gegevensverwerkingen die u in opdracht van de verwerkingsverantwoordelijke uitvoert. Zie voor de wijze waarop u vaststelt welke beveiligingsmaatregelen u dient te treffen hoofdstuk 5.

Verder dient u ervoor zorg te dragen dat eenieder die onder uw gezag handelt en toegang heeft tot de persoonsgegevens, deze enkel in opdracht van de verwerkingsverantwoordelijke verwerkt en vertrouwelijk behandelt.

Lees meer:

Artikel 32 AVG | Overweging 74-77, 83 (beveiliging van de verwerking)

6.8 Wat moet ik doen bij een inbreuk in verband met persoonsgegevens?

De meldplicht datalekken bij de Autoriteit Persoonsgegevens en eventueel aan betrokkenen zoals besproken in hoofdstuk 5 is de verantwoordelijkheid van de verwerkingsverantwoordelijke. Wel moet u de verwerkingsverantwoordelijke zonder onredelijke vertraging in kennis stellen van r een inbreuk in verband met persoonsgegevens. Bij het vaststellen of er sprake is van een inbreuk in verband met persoonsgegevens dient u dezelfde afwegingen te maken als de verwerkingsverantwoordelijke.

Lees meer:

Artikel 33 AVG | Overweging 75, 85, 87 en 88 (melding van een inbreuk van persoonsgegevens aan de toezichthoudende autoriteit)

6.9 Moet ik meewerken met de Autoriteit persoonsgegevens?

U dient als verwerker volledige medewerking te verlenen aan de Autoriteit Persoonsgegevens bij het vervullen van haar taken. Ook als dit tegen de zin van de verwerkingsverantwoordelijke is.

Lees meer:
Artikel 31 AVG (Medewerking met de toezichthoudende autoriteit)

6.10 Wat moet ik doen als de verwerkingsverantwoordelijke de verwerkingsactiviteiten beëindigt?

Wanneer de verwerking van persoonsgegevens niet langer ten behoeve van de verwerkingsverantwoordelijke plaatsvindt, dient u de betrokken persoonsgegevens te wissen of terug te geven aan de verwerkingsverantwoordelijke, tenzij een andere wettelijke bepaling u verplicht die gegevens langer te bewaren.

Lees meer:
artikel 28 AVG | Overweging 81 (de verwerker)

7 Hoe ga ik om met de rechten van de betrokkene?

7.1 Welke rechten hebben betrokkenen?

Om een eerlijke verwerking van persoonsgegevens te waarborgen geeft de Verordening diverse rechten aan de betrokkene. De betrokkene kan deze rechten uitoefenen tegen de verwerkingsverantwoordelijke. De betrokkene heeft:

- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens en 'het recht om vergeten te worden';
- het recht op beperking van de gegevensverwerking;
- het recht op verzet tegen de gegevensverwerking;
- het recht op overdracht van zijn gegevens (dataportabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

7.1.1 Ben ik verplicht gehoor te geven aan verzoeken van de betrokkene?

Ja. U moet als verwerkingsverantwoordelijke gehoor geven aan deze rechten, tenzij de verzoeken van de betrokkene kennelijk ongegrond of buitensporig zijn (bijvoorbeeld wanneer de betrokkene heel vaak achter elkaar exact hetzelfde vraagt). De risico-gebaseerde benadering geldt niet voor de rechten van de betrokkene, u moet altijd de rechten van de betrokkene respecteren.

U moet de uitvoering van deze rechten faciliteren en u mag de uitoefening ervan niet bemoeilijken. U kunt het voor betrokkenen makkelijk maken om hun rechten uit te oefenen door bijvoorbeeld de mogelijkheid te bieden een verzoek digitaal in te dienen of door een standaardformulier voor het indienen van een verzoek te verstrekken.

U mag geen kosten in rekening brengen voor het uitoefenen van deze rechten, tenzij het gaat om ongegronde of buitensporige verzoeken (welke u dus ook mag weigeren).

Uiteraard moet u wel met voldoende zekerheid vaststellen dat degene die het verzoek doet daadwerkelijk de betrokkene is.

7.1.2 Hoe snel moet ik reageren op verzoeken van de betrokkene?

U moet binnen een maand na ontvangst van het verzoek de betrokkene informeren over de uitvoering van het verzoek. Ook wanneer u geen gehoor geeft aan het verzoek van de betrokkene moet u dit binnen een maand kenbaar maken. U moet een weigering motiveren en de betrokkene wijzen op het klachtrecht bij de toezichthouder. U mag twee maanden extra de tijd nemen indien het gaat om veel verzoeken of complexe verzoeken. Als u van deze extra tijd gebruik maakt dan moet u de betrokkene hierover ook binnen een maand na ontvangst van het verzoek informeren.

7.1.3 Aan welke vormvereisten moet de invulling van deze rechten voldoen?

Wanneer u de betrokkene informeert, dan moet u dit in duidelijke en eenvoudige taal doen. Verder moet de informatie in gemakkelijke, toegankelijke vorm worden aangeboden en beknopt, transparant en begrijpelijk zijn. Ditzelfde geldt voor communicatie in het kader van het uitvoeren van een verzoek van de betrokkene (bijvoorbeeld het gehoor geven aan een inzageverzoek). Wanneer u zich tot een kind richt, dan moet u extra rekening houden met de bovenstaande eisen.

De informatie moet schriftelijk of met andere (elektronische) middelen worden verstrekt. Indien de betrokkene daarom verzoekt, kunt u de informatie ook mondeling meedelen, maar dan moet u wel met voldoende zekerheid de identiteit van de betrokkene hebben vastgesteld.

7.1.4 Zijn er beperkingen op de rechten van de betrokkenen?

Ja. In specifieke situaties hoeft u geen gehoor te geven aan de rechten van de betrokkenen. Deze situaties doen zich voor wanneer het beperken van de rechten van de betrokkenen *noodzakelijk* is voor de waarborging van:

- de nationale veiligheid, landsverdediging of openbare veiligheid;
- de voorkoming, onderzoek, opsporing en vervolging van strafbare feiten, of tenuitvoerlegging van straffen;
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepenschendingen van de beroepscodes van gereglementeerde beroepen;
- andere belangrijke doelstellingen van algemeen belang van Nederland of de Europese Unie;
- de bescherming van de onafhankelijkheid van rechters en rechterlijke procedures; en
- taken op het gebied van toezicht, inspectie of regelgeving op de hierboven genoemde gebieden.

Verder is het mogelijk de rechten van de betrokkenen te beperken wanneer dit noodzakelijk is ter waarborging van:

- de bescherming van de betrokkene of van de rechten of vrijheden van anderen; of
- de inning van civielrechtelijke vorderingen.

Wanneer u als verwerkingsverantwoordelijke een uitzondering maakt op de rechten van de betrokkenen (waaronder begrepen het informeren van de betrokkene over de verwerking van persoonsgegevens en eventuele datalekken) op basis van de bovenstaande situaties, dan moet u daarbij de aard van de verwerkingen, de risico's voor de rechten en vrijheden van de betrokkene en het recht van de betrokkene om op de hoogte te worden gesteld van deze beperkingen meewegen. Meer specifiek moet u rekening houden met de volgende elementen:

- de doeleinden van de verwerking of van de categorieën van verwerking;
- de categorieën van persoonsgegevens;
- het toepassingsgebied van de ingevoerde beperkingen;
- de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
- de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
- de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
- de risico's voor de rechten en vrijheden van de betrokkenen; en
- het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

7.1.5 Wat kan er gebeuren als de betrokkene het niet eens is met mijn besluit over zijn rechten?

Wanneer een betrokkene zijn rechten inroept en u besluit daar als verwerkingsverantwoordelijke al dan niet gehoor aan te geven, dan kan het natuurlijk zijn dat de betrokkene het niet eens is met dit besluit of de uitvoering ervan. De betrokkene heeft dan de mogelijkheid om naar de rechter te stappen. De rechter kan u dan bevelen alsnog uitvoering te geven aan het verzoek van de betrokkene. Wanneer u als bestuursorgaan een schriftelijke beslissing neemt in het kader van de uitoefening van de rechten van de betrokkene, dan geldt dit als een besluit in de zin van de Algemene wet bestuursrecht en staan daarmee de gangbare rechtsmiddelen open tegen uw besluit.

Daarnaast kan de betrokkene zich wenden tot de Autoriteit Persoonsgegevens met een verzoek om te bemiddelen in een geschil met de verwerkingsverantwoordelijke over de uitoefening van zijn rechten. Wanneer de verwerkingsverantwoordelijke is aangesloten bij een goedgekeurde gedragscode, dan kan van de in de gedragscode beschreven geschillenbeslechtingsregeling gebruik worden gemaakt.

Tenslotte kan de betrokkene zich richten tot de Autoriteit Persoonsgegevens met een verzoek tot handhaving.

Lees meer:
Artikel 57 AVG | (Taken van de toezichthoudende autoriteit)
Artikel 34 UAVG | (Toepasselijkheid Algemene wet bestuursrecht bij beslissing van bestuursorganen)
Artikel 35 UAVG | (Toepasselijkheid burgerlijk recht bij beslissing van niet-bestuursorganen)
Artikel 36 UAVG | (Geschilbeslechting door Autoriteit Persoonsgegevens of via gedragscode)
Artikel 41 UAVG | (Uitzonderingen op rechten betrokkene en plichten verwerkingsverantwoordelijke)

7.2 Wat houdt het recht op informatie in?

Als verwerkingsverantwoordelijke heeft u de plicht om het publiek te informeren over uw gegevensverwerkingen. Meer specifiek hebben betrokkenen het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de waarborgen en de manier waarop zij hun rechten met betrekking tot de verwerking van gegevens kunnen uitoefenen.

7.2.1 In welke gevallen moet ik de betrokkene informeren?

Uitgangspunt is dat u altijd een informatieplicht heeft wanneer u persoonsgegevens verwerkt. Met betrekking tot het informeren van de betrokkene maakt de Verordening een onderscheid tussen twee situaties:

- de gegevens worden bij de betrokkene zelf verzameld; en
- de gegevens worden buiten de betrokkene om verkregen.

In de meeste gevallen zult u de gegevens rechtstreeks bij de betrokkene verzamelen: een consument meldt zich aan op uw website, u stuurt een enquête naar uw klanten, u registreert de gegevens van uw medewerkers enzovoorts. Maar u kunt ook gegevens buiten de betrokkene om verkrijgen, bijvoorbeeld via andere personen of organisaties of omdat ze op het internet staan. Het onderscheid dat de Verordening maakt tussen deze twee situaties is van belang, omdat de invulling van de informatieplicht en de uitzonderingen op die plicht in beide gevallen verschillen.

Ook als u de gegevens voor een ander doel gaat gebruiken dan waar u ze oorspronkelijk voor heeft verzameld, dan moet u de betrokkene informeren.

7.2.2 Wanneer hoef ik de betrokkene niet te informeren?

Uitgangspunt is dat de betrokkene altijd geïnformeerd moet worden. In een aantal gevallen hoeft de u de betrokkene niet te informeren. Welke uitzonderingen van toepassing zijn is afhankelijk van de manier waarop u de gegevens heeft verkregen (zie Schema 5).

Uitzonderingen op de informatieplicht wanneer u de gegevens bij de betrokkene zelf verzamelt.
Wanneer u de gegevens bij de betrokkene zelf verzamelt dan hoeft u deze niet te informeren wanneer deze al over de benodigde informatie beschikt. U moet weten dat de betrokkene de betreffende informatie al heeft, een vermoeden is onvoldoende. U mag hiervan uitgaan als u, naar objectieve maatstaven, uit een gedraging of verklaring van betrokkene kon afleiden dat betrokkene inderdaad op de hoogte was. Dit is bijvoorbeeld het geval als u de informatie eerder aan betrokkene heeft verstrekt door middel van een e-mail gericht aan een door betrokkene zelf opgegeven e-mailadres.

Uitzonderingen op de informatieplicht wanneer u de gegevens buiten de betrokkene om verkrijgt.
Wanneer u de persoonsgegevens buiten de betrokkene om heeft verkregen, dan hoeft u de betrokkene net als wanneer u de gegevens bij hem zelf verzamelt, niet te informeren wanneer de betrokkene reeds over de informatie beschikt. Dit is bijvoorbeeld het geval wanneer de betrokkene al geïnformeerd is door de oorspronkelijke verantwoordelijke dat de gegevens naar u doorgestuurd worden.

Daarnaast zijn er voor deze situatie nog drie specifieke uitzonderingsgronden:
- de informatieverstrekking aan de betrokkene blijkt onmogelijk, of vergt een onevenredige inspanning; of
- de verkrijging of verstrekking van de persoonsgegevens is uitdrukkelijk bij wet voorgeschreven en in die wet zijn de gerechtvaardigde belangen van de betrokkene gewaarborgd; of
- de persoonsgegevens moeten vertrouwelijk blijven in verband met een beroepsgeheim.

Indien u de gegevens niet van betrokkene zelf heeft gekregen, kan het in de praktijk onmogelijk blijken of onevenredig veel inspanning van u vergen om alle betrokkenen afzonderlijk te informeren. Voor die gevallen laat de Verordening ruimte om de informatieplicht achterwege te laten, op voorwaarde dat de informatie zoals hierboven beschreven wél openbaar wordt gemaakt. Dit kan bijvoorbeeld door het publiceren van de informatie op uw website. Dit geldt in het bijzonder wanneer u de persoonsgegevens verwerkt met het oog op archivering in het algemeen belang of als u een instelling of dienst voor wetenschappelijk onderzoek of statistiek bent. Wilt u van deze uitzondering gebruik kunnen maken, dan moet u wel voldoende maatregelen hebben getroffen om te verzekeren dat de persoonsgegevens alleen voor dat wetenschappelijk onderzoek of statistisch doel worden verwerkt.

7.2.3 Welke informatie moet ik aan de betrokkene verstrekken?

De Verordening geeft aan welke informatie u tenminste moet verstrekken. Ook hierbij is het weer relevant of u de gegevens bij de betrokkene zelf verzamelt, of buiten de betrokkene om verkrijgt.

U verzamelt de gegevens bij de betrokkene zelf

Wanneer u de gegevens bij de betrokkene zelf verzamelt, dan moet u de volgende informatie verstrekken:
- uw identiteit en uw contactgegevens, of de contactgegevens van uw vertegenwoordiger;
- indien u een functionaris voor gegevensbescherming hebt aangesteld, de contactgegevens van deze functionaris;
- de doelen waarvoor u persoonsgegevens verwerkt;
- de grondslag waarop u de verwerking baseert;
- wanneer u de verwerking baseert op de grondslag ‘gerechtvaardigd belang’: wat uw gerechtvaardigd belang is;
- de eventuele ontvangers of categorieën ontvangers van de gegevens;
- in geval van verstrekking aan derde landen:
  - of er een adequaatheidsbesluit van de Commissie bestaat,
  - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd;
- de bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan;
- de rechten van de betrokkene (beschreven in dit hoofdstuk);
- in het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken;
- dat de betrokkene het recht heeft een klacht in te dienen over uw verwerking bij de Autoriteit Persoonsgegevens;
- of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die gegevens voor de betrokkene;
- ingeval van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene.

Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen. U moet zelf bepalen welke aanvullende informatie naast deze verplichte elementen het eventueel zou betreffen.

Als u de persoonsgegevens voor andere doelen verder gaat verwerken, moet u de betrokkene opnieuw informeren over dat nieuwe doel en opnieuw alle hierboven genoemde informatie verstrekken, behalve voor zover de betrokkene al van die informatie op de hoogte is.

U verkrijgt de gegevens buiten de betrokkene om
Wanneer u gegevens verzamelt buiten de betrokkene om, dan moet u in beginsel dezelfde informatie verstrekken als wanneer u de gegevens van de betrokkene zelf heeft gekregen. Het enige dat u moet toevoegen is de bron waaruit persoonsgegevens zijn verkregen. Als de bron van de informatie niet kan worden vastgesteld, bijvoorbeeld omdat de informatie uit verschillende bronnen is samengesteld, dient u algemene informatie over de herkomst te verstrekken.

7.2.4 Op welk moment moet ik de betrokkene informeren?

Het tijdstip waarop u de betrokkene moet informeren hangt ook af van het antwoord op de vraag van wie u de persoonsgegevens heeft verkregen.

U verzamelt de gegevens bij de betrokkene zelf
Wanneer u de gegevens bij de betrokkene zelf verzamelt, dan moet u de betrokkene informeren bij het moment van de verkrijging van de gegevens.

U verkrijgt de gegevens buiten de betrokkene om
Als u de gegevens niet van betrokkene zelf hebt gekregen, dan moet u de betrokkene binnen een redelijke termijn na ontvangst van de gegevens informeren. De Verordening stelt dat dit in ieder geval niet langer dan één maand na ontvangst van de gegevens is.

7.2.5 Mag ik gebruik maken van icoontjes om de betrokkene te informeren?

Ja. De informatie mag worden verstrekt met behulp van gestandaardiseerde iconen. De iconen moeten een betrokkene een nuttig overzicht geven en goed zichtbaar, begrijpelijk en leesbaar zijn. Wanneer u de iconen elektronisch weergeeft (bijvoorbeeld op uw website of in een app), dan moeten ze 'machineleesbaar' zijn. Dat wil zeggen dat een computer ze moet kunnen herkennen en begrijpen.

Nota bene:
Er moet sprake zijn van gestandaardiseerde iconen. De Europese Commissie kan nadere regels stellen voor wat betreft de inhoud van de iconen en het bijbehorende standaardisatieproces. U kunt dus om invulling te geven aan uw informatieplicht niet volstaan met zelf verzonnen iconen, het moet gaan om 'officieel' goedgekeurde iconen. U kunt dus wel eigen iconen en andere visualisaties gebruiken ter ondersteuning of verduidelijking van uw (schriftelijke) informatievoorziening, maar niet ter vervanging.

Lees meer:
Artikel 13 AVG | Overweging 58, 60-62 (informatieverstrekking bij verzameling bij de betrokkene zelf)
Artikel 14 AVG | Overweging 58, 60-62 (informatieverstrekking bij verzameling buiten de betrokkene om)
Artikel 89 AVG | Overwegingen 156-163 (waarborgen en afwijkingen bij archivering, onderzoek en statistiek)
Artikel 41 UAVG | (Uitzonderingen op rechten betrokkene en plichten verwerkingsverantwoordelijke)
Artikel 43 UAVG | (Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen)

Groep Gegevensbescherming Artikel 29, *Guidelines on transparency under Regulation 2016/679*, 17/EN/WP260

7.3 Wat houdt het recht op inzage in?

Iedere betrokkene heeft het recht om de persoonsgegevens die van hem verzameld zijn in te zien. Een betrokkene mag daarom met redelijke tussenpozen aan u vragen of, en zo ja welke, persoonsgegevens u van hem verwerkt. U bent verplicht om gehoor te geven aan dergelijke verzoeken en de beschikbare informatie te verstrekken.

7.3.1 Welke informatie moet ik aan de betrokkene verstrekken?

Het overzicht dat u biedt aan de betrokkene moet tenminste de volgende informatie bevatten:

- de doelen waarvoor u de gegevens verwerkt;
- de categorieën persoonsgegevens die u van de betrokkene verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven, met name ontvangers in derde landen of internationale organisaties;
- indien mogelijk hoe lang u de gegevens bewaart, of indien dat niet mogelijk is, de criteria om de bewaartermijn te bepalen;
- het op recht op wijziging, verwijdering, beperking of bezwaar;
- het recht om een klacht in te dienen bij de toezichthouder;
- wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens; en
- het bestaan van geautomatiseerde besluitvorming waaronder profilering, en indien dit het geval is, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer u de persoonsgegevens doorstuurt naar een land zonder passend beschermingsniveau (zie hoofdstuk 8), dan bent u ook verplicht om de passende waarborgen mee te delen die u gebruikt om de gegevensexport te legitimeren.

7.3.2 Moet ik ook een kopie van de gegevens aan de betrokkene verstrekken?

Ja, als de betrokkene daarom verzoekt moet u een kopie van de gegevens verstrekken, dan wel de betrokkene op afstand toegang bieden tot de gegevens in een beveiligde omgeving (zoals bijvoorbeeld een persoonlijk account). U mag voor de kopie van de gegevens geen kosten in rekening brengen. Wanneer de betrokkene meerdere kopieën wil ontvangen, dan mag u daarvoor op basis van administratieve kosten wel een redelijke vergoeding vragen. U moet de kopie schriftelijk (waaronder begrepen in elektronische vorm) aanbieden. Wanneer de betrokkene zijn verzoek elektronisch indient (bijvoorbeeld per e-mail) dan moet u de kopie in een gangbare elektronische vorm verstrekken, tenzij de betrokkene om een andere regeling vraagt.

U moet bij het verstrekken van de informatie en de kopie van de gegevens ook rekening houden met de bescherming van persoonsgegevens van andere personen. Verstrek dus bijvoorbeeld niet per ongeluk ook hun gegevens aan de betrokkene.

7.3.3 Hoe weet ik zeker dat degene die het verzoek doet wel de betrokkene is?

Wanneer u een inzageverzoek krijgt, dan moet u er zich van vergewissen dat degene die het inzageverzoek doet, daadwerkelijk degene is op wie de gegevens betrekking hebben. Hiertoe moet u de identiteit van de betrokkene vaststellen. Dit geldt in het bijzonder bij online diensten.

7.4 Wat houdt het recht op rectificatie in?

Wanneer u persoonsgegevens verwerkt, dan moet u zorgen dat deze gegevens accuraat zijn en blijven. Toch kan het voorkomen dat u persoonsgegevens verwerkt die niet (meer) kloppen. De betrokkene heeft dan het recht u op te dragen deze gegevens te corrigeren. Ook heeft de betrokkene het recht om de gegevens aan te laten vullen wanneer deze incompleet zijn, bijvoorbeeld door een aanvullende verklaring aan u als verwerkingsverantwoordelijke te verstrekken.

7.4.1 Moet ik ontvangers van de gegevens ook informeren over de wijzigingen?

Ja. Wanneer u de gegevens heeft gedeeld met andere partijen, dan moet u deze partijen op de hoogte stellen van de wijzigingen. U hoeft dit alleen niet te doen wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning van u vergt.

Of iets een onevenredige inspanning vergt moet u bepalen door de belangen van de betrokkene te wegen tegen de inspanningen (kosten, tijd et cetera) die u moet leveren om de ontvangers te informeren.

7.5 Wat houdt het recht op verwijdering en het recht om vergeten te worden in?

Onder bepaalde omstandigheden hebben betrokkenen het recht om hun gegevens door de verwerkingsverantwoordelijke te laten verwijderen, bijvoorbeeld wanneer de verwerking onrechtmatig is. Daarnaast heeft de betrokkene het recht om 'vergeten te worden'. Dit recht is met name in het leven geroepen zodat mensen op het internet niet voor altijd (ten onrechte) met hun verleden worden geconfronteerd.

7.5.1 Wanneer kan de betrokkene zijn gegevens laten wissen?

De betrokkene heeft het recht om zijn gegevens zo snel mogelijk door u te laten wissen, maar alleen in één van de volgende gevallen:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene trekt zijn toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking berust of kan berusten;
- de betrokkene heeft gegrond bezwaar gemaakt tegen de verwerking (zie paragraaf 7.7)
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op u rust;
- de persoonsgegevens zijn verzameld in verband met een rechtstreeks aanbod van internetdiensten aan een kind.

7.5.2 Wat houdt het 'recht om vergeten te worden' in?

Naast het recht op verwijdering heeft de betrokkene onder bepaalde omstandigheden ook het recht om 'vergeten te worden'. Dit recht ligt in het verlengde van het recht op verwijdering van gegevens. Het gaat dan om situaties waarbij u als verwerkingsverantwoordelijke persoonsgegevens van de betrokkene openbaar heeft gemaakt (bijvoorbeeld door ze online te zetten) en de betrokkene u gevraagd heeft de gegevens te wissen. Naast het wissen van de gegevens uit uw eigen systemen moet u redelijke technische en organisatorische maatregelen nemen om andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene vergeten wil worden. Dit betekent dat iedere koppeling naar en kopie of reproductie van de gegevens gewist moet worden.

Het recht op verwijdering en het recht om vergeten te worden gelden voor iedereen, maar wegen in het bijzonder zwaar bij de verwerking van gegevens van kinderen. Ook wanneer een betrokkene die als kind toestemming heeft gegeven voor een verwerking inmiddels volwassen is, dient dit zwaar te worden gewogen. Dit omdat de betrokkene zich waarschijnlijk destijds nog niet volledig bewust was van de verwerkingsrisico's.

7.5.3 Moet ik altijd de gegevens verwijderen of zijn er uitzonderingen?

Het recht op verwijdering en het recht om vergeten te worden zijn niet absoluut, maar moeten gewogen worden tegen andere rechten en belangen. Het recht op verwijdering en het recht om vergeten te worden zijn niet op u als verwerkingsverantwoordelijke van toepassing wanneer de verwerking nodig is voor:

- het uitoefenen van uw recht op vrijheid van meningsuiting en informatie;
- het nakomen van een wettelijke verwerkingsverplichting die op u rust;
- het vervullen van een taak van algemeen belang die op u rust;
- het uitoefenen van het openbaar gezag waarmee u bent bekleed;
- om redenen van algemeen belang op het gebied van volksgezondheid;
- archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wanneer verwijdering van de gegevens de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
- de instelling, uitoefening of onderbouwing van een rechtsvordering.

7.5.4 Moet ik ontvangers van de gegevens ook informeren over de verwijdering?

Wanneer u de gegevens heeft gedeeld met andere partijen, dan moet u deze partijen op de hoogte stellen van het feit dat de gegevens zijn verwijderd op verzoek van de betrokkene. U hoeft dit alleen niet te doen wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning van u vergt.

Of iets een onevenredige inspanning vergt moet u bepalen door de belangen van de betrokkene te wegen tegen de inspanningen (kosten, tijd et cetera) die u moet leveren om de ontvangers te informeren.

7.6 Het recht op beperking

Het recht op beperking van de verwerking van persoonsgegevens houdt in dat betrokkenen de mogelijkheid krijgen om de verwerking van hun persoonsgegevens tijdelijk 'stil te laten zetten'. De gegevens mogen dan alleen nog worden verwerkt in de volgende gevallen:

- met de toestemming van de betrokkene;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- ter bescherming van de rechten van anderen of om gewichtige redenen van algemeen belang voor de Europese Unie of voor een lidstaat.

7.6.1 Wanneer heeft de betrokkene recht op beperking van de verwerking?

Een betrokkene kan zijn recht op beperking van de verwerking inroepen in de volgende situaties:

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt om de juistheid van de persoonsgegevens te controleren;
- de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

7.6.2 Wat moet ik doen om de gegevensverwerking te beperken?

Hoe u technisch en organisatorisch de beperking van gegevens vormgeeft mag u zelf bepalen. De Verordening stelt dat -in beginsel met technische middelen- moet worden gezorgd voor een zodanige beperking van de verwerking dat de persoonsgegevens niet verder kunnen worden verwerkt. Het feit dat de verwerking van persoonsgegevens beperkt is, moet duidelijk zijn aangegeven in de gegevens (bijvoorbeeld met *tags* of *labels*).

De Verordening geeft de volgende voorbeelden hoe een verantwoordelijke gegevensverwerkingen kan beperken:

- de geselecteerde persoonsgegevens tijdelijk overbrengen naar een ander verwerkingssysteem;
- de geselecteerde gegevens voor gebruikers tijdelijk onbeschikbaar maken;
- de gepubliceerde gegevens tijdelijk van een website halen.

Wanneer u de beperking opheft, dan moet u de betrokkene hiervan vooraf in kennis stellen.

7.7 Het recht op verzet

Een betrokkene kan onder omstandigheden bezwaar maken tegen de (verdere) verwerking van zijn gegevens en zijn recht op verzet inroepen. U moet dan als verwerkingsverantwoordelijke de verwerkingen staken.

7.7.1 Wanneer kan de betrokkene zijn recht op verzet inroepen?

De betrokkene kan zijn recht op verzet in een drietal situaties inroepen:

De betrokkene kan allereerst vanwege persoonlijke omstandigheden bezwaar maken tegen verwerkingen die gebaseerd zijn op de grondslagen:
- noodzakelijk voor de uitoefening van een taak van algemeen belang of openbaar gezag; of
- het gerechtvaardigd belang van de verwerkingsverantwoordelijke.

U moet dan de verwerking staken tenzij er dwingende, gerechtvaardigde gronden zijn waardoor uw verwerkingsbelang groter is dan het belang van de betrokkene om de verwerking te laten staken.

Ten tweede kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens met het oog op direct marketing. Dit recht op verzet is absoluut, u moet hier dus altijd gehoor aan geven.

Ten derde kan de betrokkene bezwaar maken tegen de verwerking van zijn gegevens voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden op grond van specifiek met zijn situatie verband houdende redenen. U moet aan dit bezwaar gehoor geven, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

7.8 Het recht op overdraagbaarheid van gegevens (dataportabiliteit)

Het recht op overdraagbaarheid van persoonsgegevens geeft de betrokkene het recht om een kopie te krijgen van de persoonsgegevens die hij aan u heeft verstrekt. De kopie moet in een gestructureerde, gangbare en machineleesbare vorm (CSV, JSON, XML et cetera) worden verstrekt. Het doel van het recht op gegevensoverdraagbaarheid is de zeggenschap van de betrokkene over zijn gegevens te vergroten. Het achterliggende idee is dat de betrokkene zijn gegevens mee kan nemen naar bijvoorbeeld een andere aanbieder en daardoor minder gebonden is aan de oorspronkelijke verwerkingsverantwoordelijke.

7.8.1 Welke gegevens moet ik overdragen?

Het recht op overdraagbaarheid geldt alleen voor *verstrekte* gegevens die *geautomatiseerd* worden verwerkt op basis van de volgende grondslagen:
- de ondubbelzinnige dan wel uitdrukkelijke toestemming van de betrokkene;
- de noodzakelijkheid voor de uitoefening van de overeenkomst.

Het recht op overdraagbaarheid geldt dus niet wanneer de verwerking op een andere rechtsgrond dan een toestemming of een overeenkomst geschiedt.

Onder verstrekte gegevens worden door de Artikel 29-werkgroep niet alleen de gegevens verstaan die de betrokkene zelf actief invult in bijvoorbeeld een webformulier, maar ook de gegevens die van de betrokkene worden *geobserveerd*. Denk hierbij bijvoorbeeld aan locatiegegevens die worden vastgelegd door een fitness app tijdens het hardlopen. Afgeleide gegevens (interpretaties of conclusies die de verwerkingsverantwoordelijke op basis van de gegevens trekt) vallen niet onder het recht op overdraagbaarheid. Het is hierbij van belang om aan te tekenen dat het hier gaat om de interpretatie van de Artikel 29-werkgroep en niet per se de mening van de Europese wetgever.

7.8.2 Ben ik verplicht om overgedragen gegevens te accepteren?

Nee. Wanneer een betrokkene bij u aanklopt met zijn overgedragen gegevens dan bent u niet verplicht om de gegevens te accepteren. Ook bent u niet verplicht om technisch compatibele systemen voor gegevensverwerking op te zetten of te onderhouden. Wel moedigt de Verordening verwerkingsverantwoordelijken aan om interoperable gegevensformaten te ontwikkelen die de overdraagbaarheid van gegevens vergemakkelijken en daarmee het recht op overdraagbaarheid faciliteren.

7.9 Het recht niet onderworpen te worden aan geautomatiseerde individuele besluitvorming waaronder profilering

7.9.1 Wat is geautomatiseerde individuele besluitvorming?

Wanneer persoonsgegevens worden gebruikt om tot een bepaalde beslissing te komen en deze beslissing is *uitsluitend* gebaseerd op geautomatiseerde verwerking van persoonsgegevens, dan is er sprake van geautomatiseerde individuele besluitvorming. Met andere woorden, bij geautomatiseerde individuele besluitvorming is er géén sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomsten kunnen worden gecorrigeerd.

7.9.2 Wat is profilering?

Profilering (*profiling*) is het indelen van personen in categorieën (profielen) op basis van hun persoonsgegevens. Op basis van deze profielen kunnen vervolgens (geautomatiseerde) individuele besluiten worden genomen, zoals bijvoorbeeld het verlenen van krediet door een financiële instelling.

Profilering kan op de volgende drie manieren worden ingezet:
1) algemene profilering (nog zonder besluitvorming);
2) besluitvorming gebaseerd op profilering;
3) *geautomatiseerde* individuele besluitvorming gebaseerd op profilering.

Het verschil in toepassing 2 en 3 zit hem in de menselijke tussenkomst. Onder toepassing 2 is er nog sprake van noemenswaardige menselijke tussenkomst. Het profiel dient slechts ter ondersteuning van de besluitvorming. Terwijl onder 3 het besluit geautomatiseerd wordt genomen en er geen sprake meer is van noemenswaardige menselijke tussenkomst.

7.9.3 Wat houdt het recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming waaronder profilering in?

Betrokkenen hebben het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking, (waaronder profilering), gebaseerd besluit, wanneer dit:
- rechtsgevolgen heeft voor hen; of
- het hen anderszins in aanzienlijke mate treft.

Hoewel deze bepaling in de Verordening is geformuleerd als een recht van de betrokkene, gaat het in feite om een verbod voor de verwerkingsverantwoordelijke.

Een voorbeeld van een verboden geautomatiseerde individuele besluitvorming met een rechtsgevolg is de opzegging van een arbeidscontract, enkel omdat de computer aangeeft dat de werknemer een risico vormt voor de organisatie.

Voor wat betreft profilering gaat het om de inzet van profilering op de wijze besproken onder punt 3 in de vorige paragraaf. Een vorm van profilering die mensen in aanzienlijke mate treft, is het opstellen van bijvoorbeeld een kredietwaardigheidsprofiel en enkel op basis van dit profiel geautomatiseerd besluiten om iemand geen lening te geven.

7.9.4 Zijn er uitzondering op verbod van geautomatiseerde individuele besluitvorming?

Ja. Niet alle vormen van geautomatiseerde individuele besluitvorming zijn verboden, ook al hebben zij rechtsgevolgen voor betrokkenen of treffen zij hen in aanzienlijke mate.

In de volgende situaties is het mogelijk om gebruik te maken van geautomatiseerde individuele besluitvorming, waaronder ook profilering:
1. wanneer dit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;

2. wanneer de betrokkene zijn uitdrukkelijke toestemming heeft gegeven;
3. wanneer dit is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. (Voor profilering is dit niet geregeld in nationaal recht.)

Wanneer u gebruik wilt maken van de eerste twee uitzonderingen, dan moet u voor passende maatregelen zorgen ter bescherming van de rechten van de betrokkene. Dit geldt eens te meer als het kinderen betreft. Deze maatregelen moeten tenminste het volgende omvatten:
- het recht op menselijke tussenkomst;
- het recht voor de betrokkene om zijn standpunt kenbaar te maken; en
- het recht om het besluit aan te vechten.

Geautomatiseerde individuele besluitvorming is toegestaan zolang er geen sprake is van profilering (derde uitzondering). Wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of het noodzakelijk is voor de vervulling van een taak van algemeen belang. In dergelijke gevallen moet de verwerkingsverantwoordelijke wel passende maatregelen treffen die strekken tot de bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. Dit is voor verwerkingsverantwoordelijken die geen bestuursorgaan zijn in ieder geval zo wanneer er een recht op menselijke tussenkomst is, de betrokkene zijn standpunt kenbaar kan maken en het recht heeft om het besluit aan te vechten.

Wanneer u een bestuursorgaan bent, dan zijn de gebruikelijke waarborgen uit de Algemene wet bestuursrecht van toepassing, zoals het zorgvuldigheids- en evenredigheidsbeginsel en de mogelijkheid van betrokkene om bezwaar aan te tekenen.

Verder mogen de geautomatiseerde individuele besluiten niet gebaseerd worden op bijzondere categorieën van persoonsgegevens tenzij daarvoor uitdrukkelijke toestemming is van de betrokkene, of het gebruik noodzakelijk is met het oog op een zwaarwegend algemeen belang op grond van Unierecht of lidstatelijk recht. In beide gevallen moeten passende maatregelen worden getroffen ter bescherming van de gerechtvaardigde belangen van de betrokkene. In de eerste situatie treft de verwerkingsverantwoordelijke deze maatregelen zelf, in de tweede situatie worden deze bij wet voorgeschreven.

Lees meer:

Artikel 15 AVG | Overwegingen 63, 64 (recht van inzage van de betrokkene)
Artikel 16 AVG | Overweging 65 (recht op rectificatie)
Artikel 17 AVG | Overweging 65, 66 (recht op gegevenswissing (recht op vergetelheid))
Artikel 18 AVG | Overweging 67 (recht op beperking van de verwerking)
Artikel 19 AVG | (Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking)
Artikel 20 AVG | Overweging 68 (recht op overdraagbaarheid van gegevens)
Artikel 21 AVG | Overweging 69, 70 (recht van bezwaar)
Artikel 22 AVG | Overweging 71, 72 (geautomatiseerde individuele besluitvorming, waaronder profilering)
Artikel 23 AVG | Overweging 73
Artikel 40 UAVG | (Uitzonderingen op verbod geautomatiseerde individuele besluitvorming)
Artikel 41 UAVG | (Uitzonderingen op rechten betrokkene en plichten verwerkingsverantwoordelijke)
Artikel 42 UAVG | (Uitzondering op meldplicht datalekken aan de betrokkene)
Artikel 43 UAVG | (Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen)

Groep Gegevensbescherming Artikel 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Goedgekeurd 3 oktober 2017, 17 EN WP251

Groep Gegevensbescherming Artikel 29, *Richtlijnen inzake het recht op gegevensoverdraagbaarheid*. Goedgekeurd op dinsdag 13 december 2016. Laatstelijk herzien en goedgekeurd op 5 april 2017, 16/NL WP 242 rev.01

8 Onder welke voorwaarden mag ik gegevens naar het buitenland sturen?

Door de globalisering van de economie ontstaat er steeds meer één grote wereldmarkt. Daarnaast heeft het internet ervoor gezorgd dat landsgrenzen steeds makkelijker overschreden worden. Door deze ontwikkelingen is er steeds vaker sprake van doorgifte van gegevens naar landen buiten de Europese Unie. De Verordening stelt voorwaarden aan de doorgifte van persoonsgegevens naar dergelijke landen.

8.1 Mag ik gegevens naar het buitenland sturen?

Op het moment dat u persoonsgegevens naar landen buiten de Europese Unie stuurt, of vanuit deze landen toegang biedt tot uw gegevens, dan is er sprake van een doorgifte van persoonsgegevens. Voor het doorgeven van persoonsgegevens naar landen buiten de Europese Unie stelt de Verordening dat dit alleen mag als het door de Verordening geboden beschermingsniveau niet wordt ondermijnd. Dit is het geval als het land buiten de Europese Unie een adequaat niveau van gegevensbescherming kent, of als u aanvullende waarborgen biedt bij de doorgifte van gegevens.

Nota bene
Het is belangrijk te beseffen dat iedere doorgifte van persoonsgegevens ook een verwerking is in de zin van de Verordening. Dit betekent dat bij iedere doorgifte moet worden voldaan aan de vereisten uit de Verordening.

8.2 Welke landen buiten de Europese Unie bieden een adequaat niveau van gegevensbescherming?

Landen die een met de Verordening vergelijkbaar niveau van gegevensbescherming bieden in hun nationale wetgeving worden geacht een passend niveau van gegevensbescherming te bieden. De Europese Commissie stelt vast of dit het geval is en neemt dan een zogeheten 'adequaatheidsbeslissing'. Deze beslissingen kunnen een heel land betreffen, maar ook één of meerdere sectoren of regio's binnen een land. Indien er een adequaatheidsbeslissing is genomen, hoeven er voor doorgiftes naar dat land, die sector of regio, geen aanvullende waarborgen worden getroffen.

De Europese Commissie heeft een twaalftal adequaatheidsbeslissingen aangenomen, waaronder ten aanzien van Nieuw-Zeeland, Zwitserland en Canada (behalve Quebec). Ook voor de Verenigde Staten bestaat een adequaatheidsbeslissing, maar alleen voor zover de ontvangende partij zichzelf heeft verplicht zich te houden aan de principes zoals vastgelegd in deze beslissing, ook wel het *Privacy Shield* geheten.

Alle landen met een adequaatheidsbeslissing zijn te vinden op de website van de Europese Commissie: *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

8.2.1 Hoe zit het met de Europese Economische Ruimte?

Voor de landen die onderdeel uitmaken van de Europese Economische Ruimte (EER), te weten Noorwegen, Liechtenstein en IJsland, geldt dat zij via de Overeenkomst betreffende de Europese Economische Ruimte de Verordening volgen. Dit betekent dat u gegevens naar deze landen mag sturen. Houd er rekening mee, dat wanneer u vanuit deze landen gegevens doorgeeft naar derde landen buiten de EER/EU dezelfde regels gelden met betrekking tot de doorgifte als bij de doorgifte vanuit de Europese Unie.

8.2.2 Wat gebeurt er als een lidstaat de Europese Unie verlaat?

In de situatie waarin een lidstaat de Europese Unie verlaat (denk aan het vertrek van het Verenigd Koninkrijk uit de Europese Unie), zal het tot het moment dat dit feitelijk is gebeurd onderdeel blijven van het Europese rechtsgebied en daarmee een adequaat beschermingsniveau bieden. Op het moment echter dat de Europese Unie daadwerkelijk is verlaten, zal het land niet langer onderdeel zijn van de Europese Unie en zullen er aanvullende waarborgen moeten worden getroffen wanneer persoonsgegevens daarheen worden gestuurd in afwezigheid van een adequaatheidsbesluit.

Lees meer:
Artikel 44 AVG | Overwegingen 101-102 (algemeen beginsel inzake doorgiften)
Artikel 45 AVG | Overwegingen 102-107 (doorgiften op basis van adequaatheidsbesluiten)

8.3 Welke passende beschermingsmaatregelen moet ik treffen wanneer ik gegevens buiten de EU exporteer?

Als de Europese Commissie geen adequaatheidsbeslissing heeft genomen, dan dienen op een andere manier passende waarborgen te worden getroffen om een voldoende hoog beschermingsniveau te bieden.

Standaard contractbepalingen (*standard contractual clauses* in het Engels, afgekort *SCCs*), die zijn vastgesteld door de Europese Commissie of door de Autoriteit persoonsgegevens, kunnen bijvoorbeeld worden gebruikt door de contractpartijen om een passend beschermingsniveau te borgen voor de doorgifte van persoonsgegevens. Het is dan wel van belang dat deze standaard contractbepalingen ongewijzigd worden overgenomen. Uiteraard moeten de bepalingen in het contract dan ook worden nageleefd.

Als u bijvoorbeeld persoonsgegevens wilt doorgeven aan een partij in India, kunt u ervoor kiezen om deze standaard contractbepalingen te gebruiken om hiermee een passend beschermingsniveau te garanderen voor de persoonsgegevens die door u naar India worden gestuurd.

Andere manieren om een passend beschermingsniveau te bieden, zijn door gebruik te maken van goedgekeurde gedragscodes of via een certificeringsmechanisme. Voorwaarde is dan wel dat die samen moeten gaan met bindende en afdwingbare toezeggingen van de partij in het derde land om de passende waarborgen toe te passen.

Voor publieke organisaties is het ook mogelijk om passende waarborgen te treffen voor de doorgifte van persoonsgegevens door middel van een juridisch bindend en afdwingbaar instrument, zoals een overeenkomst of een verdrag.

Ten slotte kunnen ondernemingen in concernverband ook bindende bedrijfsvoorschriften vaststellen. Zie voor meer hierover de volgende paragraaf.

Lees meer:
Artikel 46 AVG | Overwegingen 108-109 AVG (doorgiften op basis van passende waarborgen)

8.4 Wat zijn bindende bedrijfsvoorschriften?

Om doorgifte naar landen buiten de Europese Unie te legitimeren kunnen ook bindende bedrijfsvoorschriften (*binding corporate rules* in het Engels, afgekort *BCRs*) worden gebruikt. BCRs zijn regels die juridisch bindend voor en handhaafbaar zijn door alle leden van een concern of een groep van ondernemingen die een gezamenlijke economische activiteit uitoefenen, waaronder ook de leden die zich buiten de Europese Unie bevinden.

De bindende bedrijfsvoorschriften moeten uitdrukkelijk afdwingbare rechten toekennen aan betrokkenen. Daarnaast moeten ze voldoen aan de in de Verordening gestelde vereisten, zoals bijvoorbeeld het vastleggen van de structuur en contactgegevens van het concern of de groep, het interne en extern juridisch bindende karakter en voorzien in een klachtenprocedure.

Bindende bedrijfsvoorschriften moeten zijn goedgekeurd door de bevoegde toezichthouder in de Europese Unie, willen ze daadwerkelijk als passende waarborgen dienen voor het beschermen van persoonsgegevens bij doorgiftes.

U kunt als concern of groep van ondernemingen dus zelf bindende bedrijfsvoorschriften opstellen, om deze vervolgens goedgekeurd te krijgen door de Autoriteit persoonsgegevens of een andere toezichthouder in de Europese Unie, afhankelijk van waar de hoofdvestiging van uw concern of groep zich bevindt. De Autoriteit Persoonsgegevens, of de andere toezichthouder, werkt zelf samen met de andere toezichthouders in de Europese Unie om Unie-brede goedkeuring te bewerkstelligen.

Lees meer:
Artikel 4 lid 18 | (Definitie onderneming)
Artikel 4 lid 19 | (Definitie concern)
Artikel 47 AVG | Overweging 110 AVG (bindende bedrijfsvoorschriften)

8.5 Wat als geen van bovenstaande manieren mogelijk zijn om passende waarborgen te treffen?

Komt u tot de conclusie dat er geen adequaatheidsbeslissing is genomen en het is niet mogelijk om standaard contractbepalingen, gedragscodes of een certificering te gebruiken, noch om bindende bedrijfsvoorschriften op te stellen, dan kunt u in een aantal specifieke situaties toch persoonsgegevens doorgeven. Het gaat dan om de volgende situaties:

- de verwerkingsverantwoordelijke heeft de uitdrukkelijke toestemming van de betrokkene;
- de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen;
- de doorgifte is noodzakelijk voor de sluiting of de uitvoering van een overeenkomst in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke of rechtspersoon;
- de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang;
- de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven;
- de doorgifte is verricht vanuit een bij wet ingesteld register dat bedoeld is om het publiek voor te lichten.

Mochten de bovenstaande situaties niet van toepassing zijn, dan kunt u alsnog gegevens doorgeven, maar alleen wanneer de gegevensdoorgifte:

- niet repetitief van aard is;
- slechts een beperkt aantal betrokkenen betreft;
- noodzakelijk is voor de dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke, die niet ondergeschikt zijn aan de belangen, rechten en vrijheden van de betrokkene; en
- wanneer passende waarborgen zijn getroffen.

Wanneer u gebruik maakt van deze uitzondering, dan moet u de Autoriteit Persoonsgegevens hierover informeren. Ook moet u de betrokkene informeren over de doorgifte en de door u nagestreefde dwingende gerechtvaardigde belangen.

Nota bene
Wanneer u gebruik wilt maken van de toestemming van de betrokkene moet u transparant zijn over de risico's die verbonden zijn aan de doorgifte bij gebrek aan een adequaatheidsbeslissing of passende waarborgen. Ook moet de toestemming specifiek zien op de doorgifte. Het simpele feit dat iemand akkoord is met het verwerken van zijn persoonsgegevens voor bijvoorbeeld marketingdoeleinden, betekent niet dat hij ook akkoord is met de doorgifte van zijn persoonsgegevens.

Lees meer:

Artikel 49 AVG | Overweging 111-116 AVG (afwijkingen voor specifieke situaties)

9 Hoe is het toezicht op de naleving geregeld en wat zijn de consequenties bij niet naleving?

Iedere natuurlijke- of rechtspersoon die onder de Verordening en de Uitvoeringswet valt, moet zich houden aan de hierin vastgelegde regels en verplichtingen. Per lidstaat van de Europese Unie zijn één of meer toezichthouders opgericht om naleving van de Verordening te stimuleren en om daar toezicht op te houden. Voor deze doeleinden hebben de toezichthouders een groot aantal taken en bevoegdheden gekregen. Daarnaast hebben betrokkenen ook direct de mogelijkheid om actie te ondernemen bij – vermeende – overtredingen van de Verordening en de relevante uitvoeringswetten.

9.1 Wie houdt toezicht op de naleving van de Verordening in Nederland?

De Verordening bepaalt dat iedere lidstaat van de Europese Unie één of meer toezichthouders moet oprichten, die belast zijn met het toezicht op de toepassing van de wet. In Nederland is dit de Autoriteit Persoonsgegevens. De meeste lidstaten hebben één nationale toezichthouder; Duitsland en Spanje hebben ook toezichthouders op regionaal niveau.

Deze Europese toezichthouders, waaronder de Autoriteit Persoonsgegevens, treden volledig onafhankelijk op bij de uitvoering van hun taken en de uitoefening van hun bevoegdheden. Dit betekent dat zij geen instructies mogen vragen of ontvangen van anderen en dat ze moeten beschikken over voldoende mensen en middelen om hun werk naar behoren te kunnen doen. De Autoriteit Persoonsgegevens bestaat uit één voorzitter en maximaal twee andere collegeleden en beschikt over een secretariaat dat wordt aangestuurd door een directie.

Lees meer:
Artikelen 51-59 AVG | Overwegingen 117-121 AVG (de onafhankelijke toezichthoudende autoriteit)
Hoofdstuk 2 UAVG | (De Autoriteit Persoonsgegevens)

9.2 Hoe is het toezicht op Europees niveau georganiseerd?

De Autoriteit Persoonsgegevens kan alleen haar taken uitvoeren en bevoegdheden uitoefenen op het Nederlandse territorium. Persoonsgegevens gaan echter steeds vaker de grens over, waardoor ook het toezicht steeds grensoverschrijdender wordt. Om te zorgen voor een coherente en consistente interpretatie van de Verordening, moeten de toezichthouders van de Europee Unie met elkaar samenwerken.

Deze samenwerking kent een aantal vormen. Toezichthouders moeten bijvoorbeeld met elkaar samenwerken in zaken die grensoverschrijdende gegevensverwerkingen betreffen. In de situatie waarin een concern meerdere vestigingen in de EU heeft, zullen de toezichthouders van de lidstaten waar deze vestigingen zijn of waar burgers worden geraakt door de gegevensverwerking, met elkaar moeten samenwerken teneinde tot een besluit te komen. Hierbij zal de toezichthouder van het land waar de hoofdvestiging is de leidende toezichthouder zijn en het enige aanspreekpunt voor het concern in kwestie.

Het uitgangspunt is dus wanneer u vestigingen heeft in meerdere lidstaten van de Europese Unie of als u goederen of diensten aanbiedt in meerdere lidstaten, u voor deze verwerkingen in beginsel met één toezichthouder te maken heeft, die samenwerkt met de andere toezichthouders. Welke toezichthouder uw leidende toezichthouder is, is afhankelijk van de locatie van de hoofdvestiging van uw concern.

Deze samenwerking tussen de autoriteiten in het zogenoemde één-loket-mechanisme – vaak aangeduid met de Engelse benaming *one stop shop* – met een leidende autoriteit is belangrijk onder de Verordening. Het is voor u dus zaak te weten welke autoriteit voor u de leidende autoriteit is. Dit is de autoriteit in de lidstaat waar uw hoofdvestiging zich bevindt. Dit is in beginsel de plaats waar de centrale administratie in de EU is gevestigd, tenzij de belangrijkste beslissingen over de verwerking van persoonsgegevens op een andere plaats worden genomen. Een organisatie zelf identificeert in eerste instantie waar haar hoofdvestiging is. De toezichthouder moet het daar echter wel mee eens zijn. Het is dus nuttig hierover met de toezichthouder te overleggen, indien uw organisatie in meerdere EU landen een vestiging heeft.

De toezichthouders moeten ook samenwerken om bijvoorbeeld EU-brede gedragscodes, bindende bedrijfsvoorschriften en modelbepalingen vast te stellen. Ten slotte zullen ze ook gezamenlijke richtsnoeren of aanbevelingen aan kunnen nemen en gezamenlijke onderzoeken kunnen uitvoeren ten aanzien van de specifieke onderwerpen. Dit gebeurt via het Europees Comité voor de gegevensbescherming.

9.2.1 Het Europees Comité voor de gegevensbescherming

Het Europees Comité voor de gegevensbescherming is ingesteld als orgaan van de Europese Unie. Het Comité bestaat uit de voorzitters van de toezichthouders van de lidstaten van de Europese Unie en de Europese toezichthouder (EDPS). Het is onafhankelijk in de uitvoering van haar taken. Het doel van het Comité is de consequente toepassing van de Verordening in de gehele EU.

Het Comité is de opvolger van de Artikel 29-Werkgroep en zal een belangrijke rol spelen bij het uniform uitleggen van de Verordening, vooral via het uitvaardigen van adviezen, richtsnoeren, aanbevelingen en *best practices*.

Het Comité speelt ook een rol in het toezicht in grensoverschrijdende zaken. Wanneer er een geschil is tussen toezichthouders, bijvoorbeeld over het besluit dat moet worden genomen in grensoverschrijdende zaken, wordt de zaak opgeschaald naar het Comité. Het Comité zal dan met twee derde meerderheid van stemmen een bindend besluit nemen in deze zaak. Het besluit van het Comité wordt aangehecht aan het definitieve besluit van de leidende toezichthouder jegens de organisatie in kwestie. Het definitieve besluit van de leidende toezichthouder en het besluit van het Comité zelf zijn beiden aanvechtbaar, respectievelijk bij de nationale en bij de Europese rechter.

Ook andere kwesties kunnen door de toezichthouder worden voorgelegd aan het Comité. Soms bestaat daartoe een verplichting voor de toezichthouder, zoals in het geval van gedragscodes of bindende bedrijfsvoorschriften. In andere gevallen is het een vrije keuze van de toezichthouder om het Comité in te schakelen. In beide situaties wordt gestemd met een gewone meerderheid van stemmen. Deze stemmingen leiden niet tot bindende besluiten, maar tot adviezen. In de regel zal de toezichthouder zich aan dit advies houden. Bovendien leidt een positief advies tot de goedkeuring van een gedragscode of van bindende bedrijfsvoorschriften.

Lees meer:

Artikelen 63-66 en 68-67 AVG | Overwegingen 139-140 AVG (samenwerking en coherentie)
Artikelen 55-56 en 60-62 en 67 AVG | Overwegingen 123-128 en 133-138 AVG (samenwerking en coherentie)

9.3 Welke taken en bevoegdheden heeft de toezichthouder?

Alle toezichthouders van de Europese Unie hebben onder de Verordening dezelfde taken en bevoegdheden. Het takenpakket is zeer uitgebreid. De belangrijkste taak is het monitoren en handhaven van de toepassing van de Verordening. Hiertoe verrichten zij onderzoeken en behandelen zij klachten van betrokkenen. Zij hebben ook tot taak organisaties bekend te maken met hun verplichtingen uit hoofde van de Verordening, de bekendheid bij het brede publiek over gegevensbescherming te bevorderen en te adviseren over wetgeving en beleid op dit terrein.

Voor het uitvoeren van hun taken hebben de toezichthouders verschillende soorten bevoegdheden gekregen onder de Verordening. Zo hebben ze een set aan onderzoeksbevoegdheden gekregen, waaronder de bevoegdheid om controles te verrichten en alle informatie te verkrijgen die voor het toezicht nodig is. Daarnaast hebben ze bevoegdheden gekregen tot het nemen van corrigerende maatregelen, bijvoorbeeld door waarschuwingen af te geven of verwerkingen stop te zetten.

De Autoriteit Persoonsgegevens heeft tal van bevoegdheden, zoals het kunnen vorderen van inlichtingen en het betreden van plaatsen. De Autoriteit Persoonsgegevens heeft naast een boetebevoegdheid ook de mogelijkheid om een last onder bestuursdwang op te leggen.

Tenslotte heeft de Autoriteit Persoonsgegevens enkele autorisatie- en adviesbevoegdheden, bijvoorbeeld voor gedragscodes en certificeringsmechanismen.

Lees meer:
Artikel 57 AVG | Overweging 123, 132 (taken)
Artikel 58 AVG | Overwegingen 129 (bevoegdheden)
Hoofdstuk 2 UAVG | (De Autoriteit Persoonsgegevens)
Afdeling 5.2 Algemene wet bestuursrecht (Awb)| (Bestuursdwang)

9.4 Ben ik verplicht mee te werken met de toezichthouder?

Ja. De toezichthouder heeft de bevoegdheid om een organisatie te gelasten om alle voor de uitvoering van haar taken vereiste informatie te verstrekken. Ook heeft de toezichthouder de bevoegdheid om toegang te verkrijgen tot alle persoonsgegevens en de middelen die worden gebruikt voor de verwerking van persoonsgegevens.

De Verordening vereist daarnaast expliciet dat organisaties desgevraagd mee moeten werken met de toezichthouder bij het vervullen van haar taken. Wanneer u dus een verzoek krijgt van de Autoriteit Persoonsgegevens, moet u hieraan alle medewerking verlenen.

Lees meer:
Artikel 31 AVG | Overweging 82 (medewerking met de toezichthoudende autoriteit)
Artikel 58 AVG | Overweging 129 (bevoegdheden)

9.5 Welke sancties staan er op het niet naleven van de Verordening?

In aanvulling op, of in plaats van, de bevoegdheden die hierboven zijn genoemd, kan de toezichthouder ook besluiten een administratieve boete op te leggen. Wanneer een toezichthouder hiertoe overgaat, moet zij borgen dat de boete doeltreffend, evenredig en afschrikwekkend is. Hierbij moeten onder andere de aard en de ernst van de overtreding, de opzettelijke of nalatige aard en de genomen maatregelen worden meegewogen.

Overtredingen van de bepalingen die zien op de (verantwoordings)plichten die rusten op organisaties, zoals het doen van een gegevensbeschermingseffectbeoordeling of het doen van een melding in geval van een datalek, kunnen worden gesanctioneerd met een administratieve boete van maximaal 10 miljoen euro of 2% van de wereldwijde jaaromzet, in het geval deze hoger is.

Overtredingen van de bepalingen over de principes, rechtsgrondslagen en rechten van betrokkenen, kunnen worden gesanctioneerd met een administratieve boete van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet, in het geval deze hoger is.

De Verordening voorziet – behalve in boetes – ook in een reeks sancties die erop gericht zijn overtredingen te beëindigen of nadelige gevolgen voorvloeiend uit een overtreding te herstellen.

Lees meer:
Artikel 83 AVG | Overweging 148, 150, 151 (algemene voorwaarden voor het opleggen van administratieve geldboeten)
Artikel 84 AVG | Overwegingen 149, 152 AVG (sancties)

9.6 Welke acties kan de betrokkene tegen mij ondernemen?

Betrokkenen kun ook zelf actie ondernemen als zij van mening zijn dat hun persoonsgegevens in strijd met de geldende wet- en regelgeving worden verwerkt. Hiertoe hebben ze verschillende mogelijkheden.

9.6.1 Recht op een klacht bij de toezichthouder

Ten eerste hebben betrokkenen het recht een klacht in te dienen bij de toezichthouder. De toezichthouder heeft tot taak de klacht of het verzoek te behandelen en hier een besluit over te nemen. Tegen dit besluit kan de betrokkene in bezwaar gaan bij de toezichthouder zelf. Is de betrokkene het niet eens met de beslissing op het bezwaar, dan kan deze zich tot de rechter wenden om beroep aan te tekenen. Als er sprake is van een spoedeisend belang, dan kan ook een voorlopige voorziening worden gevraagd bij de rechter. In beide gevallen moet de betrokkene zich wenden tot de rechter in het land waar de toezichthouder is gevestigd.

In Nederland mag een betrokkene daarnaast de Autoriteit Persoonsgegevens verzoeken te bemiddelen of te adviseren in zijn geschil met een verwerkingsverantwoordelijke.

Lees meer:
Artikelen 77 AVG | Overweging 141-142 AVG (recht om een klacht in te dienen bij de toezichthoudende autoriteit)
Artikel 78 AVG | Overwegingen 143-144 AVG (recht om een voorziening in rechte in te stellen tegen de toezichthoudende autoriteit)

9.6.2 Recht op een doeltreffende voorziening in rechte tegen de verwerkingsverantwoordelijke

Een betrokkene kan ook rechtstreeks (civielrechtelijk) een voorziening in rechte instellen tegen de organisatie in kwestie, indien hij van mening is dat de verwerking van zijn persoonsgegevens niet in overeenstemming met de geldende wet- en regelgeving heeft plaatsgevonden. Deze voorziening kan worden ingesteld in de lidstaat waar de betrokkene gewoonlijk verblijft, maar ook in de lidstaat waar de organisatie in kwestie is gevestigd. Wanneer de organisatie een publieke instantie betreft, moet het echter altijd in de lidstaat van de organisatie.

9.6.3 Recht op vertegenwoordiging

Een betrokkene mag een organisatie, orgaan of vereniging zonder winstoogmerk machtigen om namens hem een klacht in te dienen of de rechten uit te oefenen die hem gegeven zijn uit hoofde van de Verordening. Dit kan zowel bij de civiele rechter als bij de bestuursrechter. De organisatie, orgaan of vereniging moet als statutaire doelstelling het openbare belang dienen of actief zijn op het gebied van de bescherming van persoonsgegevens. Een voorziening in rechte kan dus ook namens de betrokkene worden ingesteld tegen een verwerkingsverantwoordelijke.

9.6.4 Recht op schadevergoeding

Als een betrokkene materiële of immateriële schade heeft geleden als gevolg van een overtreding van de Verordening, heeft hij het recht om een schadevergoeding te ontvangen voor de geleden schade. Als verwerkingsverantwoordelijke bent u aansprakelijk voor de geleden schade. Indien u gebruik maakt van een verwerker is deze slechts aansprakelijk als de verwerker niet heeft voldaan aan de op de verwerker rustende verplichtingen uit hoofde van de Verordening of als hij in strijd heeft gehandeld met de afspraken die zijn gemaakt met de verantwoordelijke.

Als meerdere organisaties bij dezelfde verwerking zijn betrokken (als verwerkingsverantwoordelijken of verwerkers), worden zij elk hoofdelijk aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk de schadevergoeding ontvangt. De partij die de gehele schade heeft vergoed, kan (een deel van) het betaalde bedrag verhalen op de andere betrokken organisaties.

Een verwerkingsverantwoordelijke of verwerker is niet aansprakelijk als hij kan bewijzen dat hij hier op geen enkele manier verantwoordelijk voor is.

Lees meer:

Artikel 79 AVG | Overweging 145 AVG (recht om een voorziening in rechte in te stellen tegen verwerkingsverantwoordelijke of verwerker)
Artikel 80 AVG | Overweging 142 AVG (vertegenwoordiging van betrokkenen)
Artikel 82 AVG | Overweging 146 AVG (recht op schadevergoeding en aansprakelijkheid)

Groep Gegevensbescherming Artikel 29, *Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker*. Goedgekeurd op dinsdag 13 december 2016. Laatstelijk herzien en goedgekeurd op 5 april 2017, 16/NL WP 244 rev.01

10 Bijlage

10.1 Implementatietabel UAVG

AVG artikel	Onderwerp	UAVG	Overweging uit AVG	Aanwezigheid en invulling van facultatieve bepalingen	Wbp artikel
Hoofdstuk I AVG – Algemene bepalingen					
1	Onderwerp en doelstellingen		ov. 1-14	-	-
2	Materiële toepassingsgebied van de AVG		ov. 14-21, 27	-	2
3	Territoriaal toepassingsgebied		ov. 22-25	-	4
4	Definities		ov. 26-38	-	1
5	Beginselen		ov. 39	-	6, 7, 9-11, 13, 15
Hoofdstuk II AVG – Beginselen voor verwerking					
6(1)	Grondslagen		ov. 40, 41, 44-50	-	8
6(2)	Specifiekere bepalingen inzake wettelijke plicht en taak van algemeen belang		-	Van deze mogelijkheid is in dit wetsvoorstel geen gebruik gemaakt.	-
6(3)	Bepalingen wettelijke plicht/taak van algemeen belang		ov. 45	Deze bepalingen zijn opgenomen in sectorspecifieke regelgeving.	-
6(4)	Verenigbaarheid		ov. 50	-	9
7	Voorwaarden voor toestemming		ov. 32, 33, 42, 43	-	1(i)
8	Voorwaarden voor toestemming in geval van kind bij internet- en mobieletelefoniediensten		ov. 38	Van de mogelijkheid uit lid 1, slotzin, om te voorzien in een lagere leeftijdsgrens dan 16 jaar is geen gebruik gemaakt.	5(1)
9(1)	Verbod verwerking bijzondere categorieën van persoonsgegevens	22(1) UAVG	ov. 34, 51	-	16
9(2) aanhef	Uitzonderingen		ov. 51-56		-
9(2)(a)	Uitdrukkelijke toestemming	22(2)(a) UAVG	ov. 33	Van de mogelijkheid om deze uitzonderingsgrond uit te sluiten, is geen gebruik gemaakt.	23(1)(a)
9(2)(b)	Socialezekerheidsrechtelijke verwerkingen	30(1) UAVG	ov. 52	Van deze uitzonderingsbepaling is gebruikgemaakt.	21(1)(f)
9(2)(c)	Vitale belangen	22(2)(b) UAVG	-	-	23(1)(d)
9(2)(d)	Instelling op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied	22(2)(c) UAVG	ov. 55, 56	-	17, 19, 20
9(2)(e)	Kennelijk openbaar gemaakte gegevens	22(2)(d) UAVG	-	-	23(1)(b)
9(2)(f)	Verdediging van een recht in rechte	22(2)(e) UAVG	ov. 52	-	23(1)(c)
9(2)(g)	Zwaarwegend belang	23, 25, 26, 27, 28, 29, 30(2) UAVG	-	Van deze uitzonderingsbepaling is gebruikgemaakt.	23(1)(e+g), 22(5), 18, 19(1)(b), 17(1)(c), 21(4), 21(1)(c,d,e)
9(2)(h)	Medische redenen en beheer van gezondheidsdiensten en sociale stelsels	30(3) UAVG	ov. 52-53	Van deze uitzonderingsbepaling is gebruikgemaakt.	21(1)(a+)

AVG artikel	Onderwerp	UAVG	Overweging uit AVG	Aanwezigheid en invulling van facultatieve bepalingen	Wbp artikel
9(2)(i)	Gezondheidszorg algemeen		ov. 52, 53, 54	Van deze uitzonderingsbepaling is gebruikgemaakt.	23(1)(f)
9(2)(j)	Archivering in alg. belang of wetenschappelijk of historisch onderzoek of statistische doeleinden	24 UAVG	-	Van deze uitzonderingsbepaling is gebruikgemaakt.	23(2)
9(3)	Geheimhouding	30(4) UAVG	-	-	21(2)
9(4)	Aanvullend recht genetische, biometrische of gezondheidsgegevens	28 UAVG	ov. 53	Van deze bepaling inzake aanvullende vereisten is gebruikgemaakt.	21(4)
10	Persoonsgegevens van strafrechtelijke aard	31-33 en 17 UAVG	-	Van de mogelijkheid tot uitzonderingen op deze grondslag is gebruikgemaakt.	16, 22
11	Geen identificatie vereist		ov. 57	-	-
Hoofdstuk III AVG – Rechten van de betrokkene					
12	Transparantie algemeen		ov. 58-59	-	33-42
13	Informatieverstrekking (bij direct verkregen persoonsgegevens)		ov. 60-62	-	33
14	Informatieverstrekking (bij indirect verkregen persoonsgegevens)		ov. 60-62	-	34
15	Inzagerecht		ov. 63-64	-	35
16	Correctierecht		-	-	36
17	Recht op gegevenswissing/'recht op vergetelheid'		ov. 65-66	-	36
18	Recht op beperking van de verwerking		ov. 67	-	-
19	Kennisgevingsplicht inzake rectificatie, wissing of beperking		ov. 66	-	38
20	Dataportabiliteit		ov. 68	-	-
21	Recht van bezwaar		ov. 69-70	-	40, 41
22	Geautomatiseerde besluitvorming	40 UAVG	ov. 71-72	De mogelijkheid tot uitzondering uit lid 2, onderdeel b, is gebruikt.	42
23	Uitzonderingen/beperkingen op 5, 12–12, 34 AVG	41, 42 en 47 UAVG	ov. 73	Van de mogelijkheid tot uitzonderingen is gebruikgemaakt.	43, 44 en 34a(11)
Hoofdstuk IV AVG – Verwerkingsverantwoordelijke en verwerker					
24	Reikwijdte verantwoordelijkheid van de verwerkingsverantwoordelijke		ov. 74-77	-	-
25	Privacy by design and default		ov. 78	-	-
26	Gezamenlijke verwerkingsverantwoordelijken		ov. 79	-	-
27	Vertegenwoordiger van niet in EU gevestigde verwerkingsverantwoordelijken of verwerkers		ov. 80	-	4(3)
28	Verwerker		ov. 81	-	14, 12
29	Verwerking onder gezag		-	-	12(1)
30	Register verwerkingen		ov. 82	-	-
31	Medewerkingsplicht met toezichthouder		ov. 82	-	61, 66 jo. 5:20 Awb
32	Beveiliging van verwerking		ov. 83	-	13, 14
33	Meldplicht datalekken aan toezichthouder		ov. 85, 87, 88	-	34a(1)

AVG artikel	Onderwerp	UAVG	Overweging uit AVG	Aanwezigheid en invulling van facultatieve bepalingen	Wbp artikel
34	Meldplicht datalekken aan betrokkene		ov. 86-88	-	34a(2)
35	PIA/GEB		ov. 84, 89-93	-	-
36(1–3)	Voorafgaande raadpleging toezichthouder		ov. 94, 95	-	31, 32
36(4)	Wetgevingsadvisering toezichthouder		ov. 96	-	51(2)
36(5)	Voorafgaande toestemming bij taak van algemeen belang		-	Van de mogelijkheid om in deze gevallen categorisch voorafgaande toestemming verplicht te stellen, is geen gebruik gemaakt.	31, 32
37	Aanwijzing functionaris gegevensbescherming		ov. 97	Van de mogelijkheid uit lid 4 om in meer gevallen dan genoemd in lid 1 te verplichten tot aanwijzing van fg's, is geen gebruik gemaakt.	62, 63(1)
38(1-4,6)	Positie functionaris gegevensbescherming		-	-	63
38(5)	Geheimhoudingsplicht functionaris gegevensbescherming	39 UAVG		-	63(4)
39	Taken functionaris gegevensbescherming		ov. 97	-	64
40	Gedragscodes	14(2) UAVG t.b.v. 40(5)AVG	ov. 98-99	-	25-26
41	Toezicht op goedgekeurde gedragscode		-	-	25-26
42	Certificering		ov. 100	-	-
43	Certificeringsorganen	21 UAVG		-	-
Hoofdstuk V AVG – Doorgifte aan derde landen en internationale organisaties					
44	Algemeen beginsel inzake doorgiften		ov. 101, 102	-	-
45	Doorgiften op basis van adequaatheidsbesluiten		ov. 103-107, 114	-	76, 78
46	Doorgiften op basis van passende waarborgen		ov. 108-109	-	77(1)(g) en 77(2)
47	Bindende bedrijfsvoorschriften		ov. 110	-	-
48	Niet bij EU-recht toegestane doorgiften of verstrekkingen		ov. 115	-	-
49	Afwijkingen voor specifieke situaties internationale doorgifte		ov. 111-115	Eerste lid, onderdeel d, jo. vierde lid: deze mogelijkheid om wegens gewichtige redenen van algemeen belang doorgifte toe te staan, zal in sectorspecifieke regelgeving moeten worden vastgesteld, indien passend. Eerste lid, onderdeel g: gegevensverwerkingen uit openbare registers zijn geregeld in de wetgeving ter zake.	77
50	Samenwerking toezichthouders		ov. 116	-	61(6)
Hoofdstuk VI AVG – Onafhankelijke toezichthoudende autoriteiten					
51	Instelling toezichthouder	6(1+2) en 15(1) UAVG	ov. 117, 123	Van de mogelijkheid om meer dan één toezichthouder aan te wijzen is geen gebruik gemaakt.	51
52(1–3)	Onafhankelijkheid toezichthouder	7-13 UAVG	ov. 118, 120	-	52(2), 59, 59a
52(4+5)	Lidstaat zorgt voor personele, technische en financiële middelen en voor door toezichthouder gekozen personeel	10 UAVG	ov. 120, 121	-	56

AVG artikel	Onderwerp	UAVG	Overweging uit AVG	Aanwezigheid en invulling van facultatieve bepalingen	Wbp artikel
52(6)	Financieel toezicht	Huidige Kaderwet zbo's	ov. 118	-	-
53	Voorwaarden leden toezichthouder, procedure	7(3) UAVG	ov. 121	-	53, 54, 55
54(1)(a)	Regels inzake instelling toezichthouder	6 UAVG	-	-	53, 59, 59a
54(1)(b)	Benoemingsvoorwaarden leden	7(4+2) UAVG	-	-	53(2)
54(1)(c)	Benoemingsprocedure leden	7(3) UAVG	-	-	53(3)
54(1)(d)	Ambtstermijn leden	7(5) UAVG	-	-	53(3)
54(1)(e)	Mogelijkheid herbenoeming leden	7(6) UAVG	-	Van de mogelijkheid tot herbenoeming is gebruikgemaakt	53(3)
54(1)(f)	Integriteitsregels	8 UAVG, huidig 13 Kaderwet zbo's en 61(4) ARAR	-	-	54
54(2)	Geheimhoudingsplicht	Huidig 125a(3) Ambtenarenwet	-	-	-
55	Competentie toezichthouder		ov. 20, 122, 123	-	60, 61
56	Competentie leidende toezichthouder en one stop shop mechanisme		ov. 124-128	-	-
57	Taken toezichthouder	14(1) UAVG	ov. 129	-	51
58(1–3)	Bevoegdheden toezichthouder	14(1) en 15(1) UAVG	ov. 122, 129	-	61, 65
58(4)	Waarborgen van toepassing op optreden toezichthouder	14(4) UAVG en huidige Awb, m.n. hfd 5 en 8		-	-
58(5)	In rechte optreden tegen inbreuken op AVG	20 UAVG	ov. 129	-	-
58(6)	Mogelijkheid voor lidstaten om toezichthouder bijkomende bevoegdheden te geven	15, 16 en 36 UAVG en huidige titel 5.2/ 5.3 Awb	-	Beleidsruimte gebruikt om Awb-bevoegdheden inzake toezicht op de naleving (titel 5.2 Awb) en last onder dwangsom en last onder bestuursdwang te behouden. Ook behoud van bevoegdheid betreden woning (huidig art. 61(2) Wbp).	47, 61, 65
59	Jaarverslag toezichthouder		-	-	58
Hoofdstuk VII AVG – Samenwerking en coherentie					
60	Samenwerking leidende toezichthouder en andere betrokken toezichthouders		ov. 130, 131, 138	-	-
61	Informatie en wederzijdse bijstand		ov. 133	-	61(6)
62	Gezamenlijke werkzaamheden toezichthouders		ov. 134	Lid 3: het betreft hier een algemene verwijzing naar het lidstatelijk recht dat voorziet in bevoegdheden voor de toezichthoudende autoriteit.	-
63	Coherentiemechanisme		ov. 135	-	-
64	Advies van het Comité		ov. 136	-	-
65	Geschillenbeslechting door het Comité		ov. 136	-	-
66	Spoedprocedure betrokken toezichthouder		ov. 137	-	-
67	Informatie-uitwisseling		-	-	-
68	Europees Comité voor gegevensbescherming		ov. 139	-	-
69	Onafhankelijkheid Comité		ov. 139	-	-

AVG artikel	Onderwerp	UAVG	Overweging uit AVG	Aanwezigheid en invulling van facultatieve bepalingen	Wbp artikel
70	Taken Comité		ov. 139	-	-
71	Jaarverslag Comité		-	-	-
72	Procedurevoorschriften Comité		-	-	-
73	Voorzitter Comité		-	-	-
74	Taken voorzitter Comité		ov. 139	-	-
75	Secretariaat Comité		ov. 140	-	-
76	Vertrouwelijkheid Comité		-	-	-
Hoofdstuk VIII AVG – Beroep, aansprakelijkheid en sancties					
77	Klachtrecht bij toezichthouder		ov. 141	-	60
78(1,3,4)	Voorziening in rechte tegen toezichthouder	Huidig hfd. 6-8 Awb	ov. 143	-	-
78(2)	Voorziening bij niet behandelen klacht	Huidig 4:13, 6:2 en 6:12 Awb	ov. 143	-	-
79	Voorziening in rechte tegen verwerkingsverantwoordelijke of verwerker	34/35/36 UAVG en huidig hfd. 8 Awb en Wetboek Burg. Rv	ov. 145	-	45-48
80	Vertegenwoordiging van betrokkenen	37 UAVG	ov. 142	Lid 2: er is geen behoefte aan de ruimte die dit artikel laat voor lidstatelijk recht.	50(2)
81	Schorsing procedure i.v.m. litispendentie		ov. 144	-	-
82	Recht op schadevergoeding en aansprakelijkheid	Huidige titel 8.4 Awb of civiele rechter	ov. 146-147	-	49, 50
83(1–6,9)	Voorwaarden aan opleggen van administratieve boetes	14(3) UAVG	ov. 148-152	-	65-71
83(7)	Mogelijkheid van regels over boetes aan overheden	18 UAVG	-	Van de mogelijkheid is gebruikgemaakt.	-
83(8)	Procedurele waarborgen	Huidige titel 5.4 en hfd 6-8 Awb	ov. 148	-	-
83(9)	Rechtsstelsel zonder administratieve boetes		ov. 151	-	
84	Andere sancties van nationaal recht	17 UAVG	-	-	65, 49, 50, 75
Hoofdstuk IX AVG – Specifieke verwerkingen					
85	Verwerking en vrijheid van meningsuiting en informatievrijheid	43 UAVG en 7(1) Grondw.	ov. 153	-	3
86	Verwerking en toegang tot officiële documenten	Huidig 10(1)(d) Wob	ov. 154	-	-
87	Verwerking nationaal identificatienummer	46 UAVG, huidige Wabb en Wet aanv. bep. verw. persoonsgegevens in de zorg	-	-	24
88	Verwerking in kader arbeidsverhouding		ov. 155	Van de mogelijkheid tot specifieke bepalingen over gegevenswerking in het kader van arbeidsverhoudingen is geen gebruik gemaakt.	-

AVG artikel	Onderwerp	UAVG	Overweging uit AVG	Aanwezigheid en invulling van facultatieve bepalingen	Wbp artikel
89	Archivering in het algemeen belang en wetenschappelijke, historische of statistische doeleinden	44 en 45 UAVG	ov. 156-163	De mogelijkheden uit lid 2 en 3 om uitzonderingen te maken, zijn gebruikt.	9(3), 10(2), 44
90	Geheimhoudingsplicht aanvullend nationaal recht	15(4) UAVG	ov. 164	De mogelijkheid van lid 1 van een uitzondering op geheimhoudingsplichten i.v.m. toezicht is gebruikt.	61(5)
91	Bestaande regels kerken en religieuze verenigingen		ov. 165	-	-
Hoofdstuk X AVG – Gedelegeerde handelingen					
92	Uitoefening van bevoegdheidsdelegatie		ov. 166, 167	-	-
93	Comitéprocedure		ov. 168-169	-	-
Hoofdstuk XI AVG – Slotbepalingen en overgangsrecht					
94	Intrekken richtlijn 95/46/EG		ov. 171	-	-
95	Verhouding tot richtlijn 2002/58/EG		ov. 173	-	-
96	Verhouding tot eerder gesloten overeenkomsten		-	-	-
97	Commissieverslagen		-	-	-
98	Toetsing andere EU-regels gegevensbescherming		-	-	-
99	Inwerkingtreding en toepassing		-	-	-

10.2 Organisaties en inhoudelijk deskundigen die waren vertegenwoordigd in de klankbordgroep Handleiding AVG

Artsenfederatie KNMG
Autoriteit Persoonsgegevens
Kennedy Van der Laan
Nederlands Genootschap van Functionarissen voor de Gegevensbescherming
Nederlandse Orde van Advocaten
Nederlandse Vereniging van Banken
Verbond van Verzekeraars
Vereniging van Samenwerkende Nederlandse Universiteiten
Vereniging van Nederlandse Gemeenten
VNO-NCW en MKB Nederland
Zorgverzekeraars Nederland
Prof. dr. mr. G.J. Zwenne, Hoogleraar Recht en de Informatiemaatschappij (op persoonlijke titel)

Dit is een publicatie van

Ministerie van Justitie en Veiligheid

januari 2018 | 108130