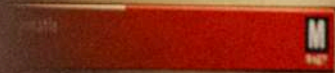




ICTRECHT



FACTSHEET

AVG

Factsheet AVG

Persoonsgegevens spelen een centrale rol in de digitale samenleving. Organisaties ervaren echter obstakels bij het zorgvuldig en rechtmatig verwerken van deze gegevens. Om deze obstakels weg te nemen biedt de Algemene verordening gegevensbescherming (AVG) regels voor rechtmatige verwerking, transparantie en beveiliging. De verwerking van persoonsgegevens kan risico's met zich meebrengen voor de persoonlijke levenssfeer van betrokkenen, variërend van ongewenste profilering en datalekken tot een gebrek aan controle over eigen gegevens. Tegelijkertijd bestaat bij organisaties vaak onduidelijkheid over de reikwijdte en toepassing van de regels, mede door de complexiteit van het juridische kader en de snelle technologische ontwikkelingen.



De AVG bevat een samenhangend stelsel van regels voor de verwerking van persoonsgegevens. De AVG stelt eisen aan de rechtmatigheid, transparantie en beveiliging van gegevensverwerkingen en beoogt betrokkenen meer controle te geven over hun persoonsgegevens, terwijl tegelijkertijd het vrije verkeer van gegevens binnen de interne markt wordt gewaarborgd.

De opbouw van de AVG is als volgt. De reikwijdte en actoren zijn vastgelegd aan het begin van de verordening en gelden voor de gehele AVG. Daarnaast is de AVG onderverdeeld in hoofdstukken over onder meer de kernbeginselen en grondslagen voor verwerking, de rechten van betrokkenen, de verplichtingen voor organisaties en het toezicht en de handhaving. In deze factsheet worden de belangrijkste onderwerpen nader toegelicht.

In deze factsheet wordt de AVG benaderd vanuit een praktische en systematische invalshoek voor organisaties. De opbouw volgt een logische volgorde die aansluit bij de vragen die organisaties zich in de praktijk stellen: wanneer is de AVG van toepassing, welke kernregels gelden, welke rechten hebben betrokkenen en welke verplichtingen rusten op organisaties?

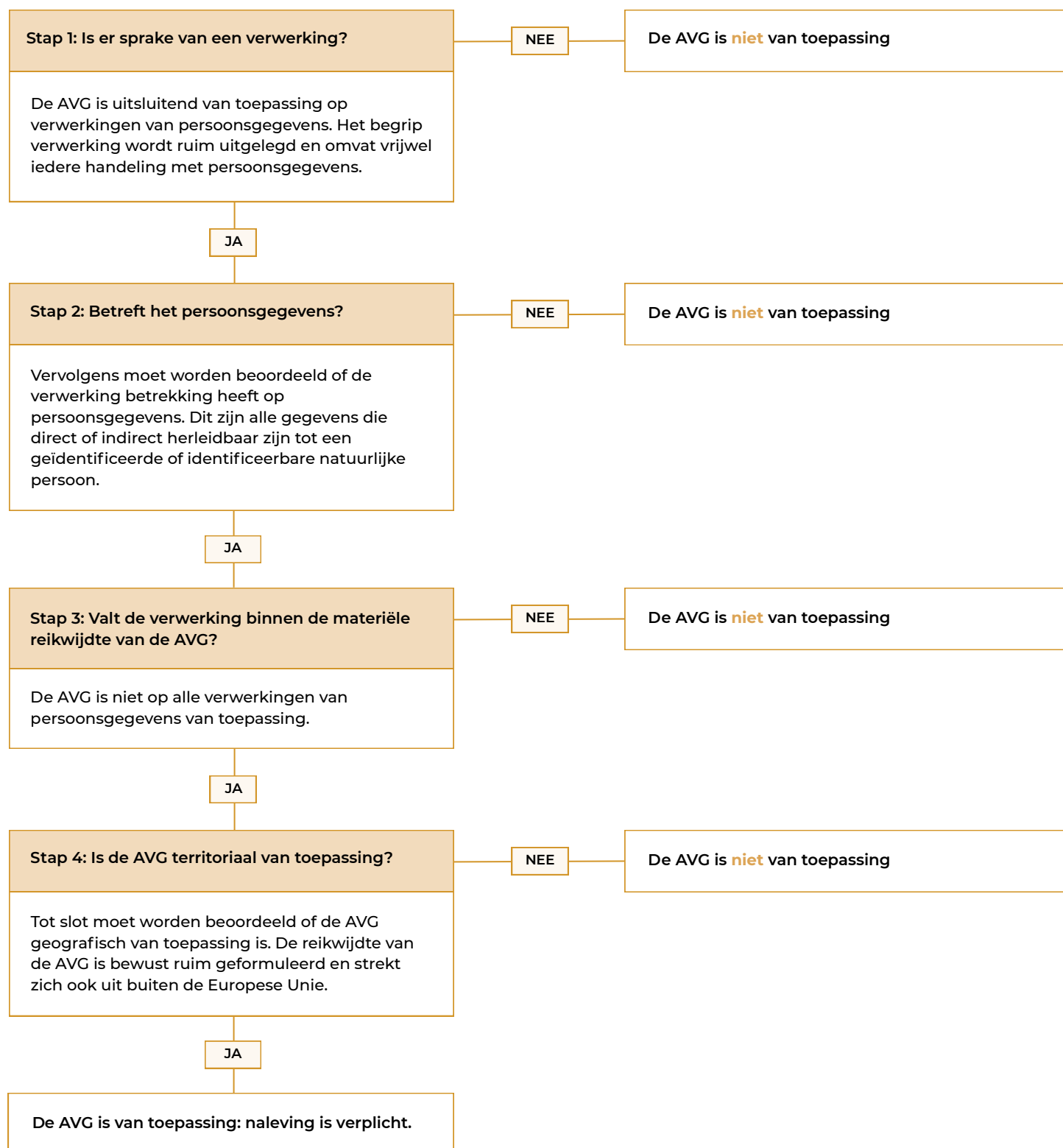
De factsheet behandelt achtereenvolgens:

- de **toepasselijkheid van de AVG**, aan de hand van een stappenplan waarmee kan worden vastgesteld of sprake is van verwerking van persoonsgegevens binnen de reikwijdte van de verordening;
- de **kernregels van de AVG**, waaronder de beginselen van gegevensverwerking en de grondslagen die een verwerking rechtmatig maken;
- de **rechten van betrokkenen** en de wijze waarop organisaties deze rechten praktisch kunnen waarborgen;
- de **rollen en verantwoordelijkheden** van verwerkingsverantwoordelijken en verwerkers, inclusief de bijbehorende verplichtingen zoals beveiliging, documentatie en risicobeoordeling;
- de regels omtrent **uitwisseling van persoonsgegevens en samenwerking**, waaronder verwerkersovereenkomsten en afspraken tussen partijen;
- de vereisten voor **doorgifte van persoonsgegevens** naar derde landen;
- en tot slot het **toezicht en de handhaving**, inclusief de rol van de toezichthouder en mogelijke sancties.

Deze factsheet is zodanig ingericht dat deze niet alleen dient als toelichting op de AVG, maar ook geldt als praktisch naslagwerk in combinatie met onze eerder verschenen [AVG-checklist](#). Per onderdeel wordt inzichtelijk gemaakt welke juridische eisen gelden en hoe organisaties hier concreet invulling aan kunnen geven. Daarmee biedt de factsheet een gestructureerd overzicht van de belangrijkste aandachtspunten voor AVG-compliance.

Toepasselijkheid van de AVG

Hoofdstuk I van de AVG bevat het onderwerp en doelstelling van de verordening en bepaalt wanneer organisaties vallen onder haar toepassingsgebied. Om dit vast te stellen, kan een organisatie het onderstaande stappenplan hanteren.



Stap 1: Verwerking

Allereerst moet sprake zijn van een **verwerking** van persoonsgegevens. Het begrip verwerking wordt in de AVG zeer ruim uitgelegd en omvat in wezen iedere handeling die met gegevens wordt verricht. Daaronder vallen niet alleen het actief verzamelen of delen van gegevens, maar ook het vastleggen, ordenen, structureren en opslaan daarvan. Hetzelfde geldt voor het bijwerken, wijzigen, opvragen en raadplegen van gegevens, evenals het gebruiken, doorzenden, verspreiden of beschikbaar stellen aan derden. Ook het samenbrengen van gegevens, het met elkaar in verband brengen, afschermen, wissen en vernietigen kwalificeren als verwerking.

In de praktijk betekent dit dat vrijwel iedere omgang met gegevens binnen een organisatie kwalificeert als verwerking. Denk aan het bijhouden van klantgegevens, het versturen van nieuwsbrieven of het opslaan van personeelsdossiers. De reikwijdte is bewust breed geformuleerd, vanuit het oogpunt om betrokkenen de hoogst mogelijke bescherming te kunnen bieden.

Stap 2: Persoonsgegevens

De AVG is uitsluitend van toepassing op een verwerking van **persoonsgegevens**. Onder persoonsgegevens wordt verstaan alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het begrip is bewust ruim geformuleerd en omvat niet alleen direct identificerende gegevens zoals een naam, adres of e-mailadres, maar ook gegevens die indirect tot een persoon te herleiden zijn. Te denken valt aan klantnummers, IP-adressen, locatiegegevens en zelfs gedrags- en beoordelingsprofielen die in onderlinge combinatie slechts betrekking kunnen hebben op één persoon.

Dat het om gegevens van een natuurlijke persoon moet gaan, betekent dat gegevens over rechtspersonen of ondernemingen in beginsel buiten de AVG vallen. Dit ligt anders wanneer de onderneming feitelijk samenvalt met één persoon, zoals bij een eenmanszaak of zzp'er. In dat geval zeggen bedrijfsgegevens zoals omzet of omzetcijfers direct iets over het inkomen van de eigenaar, waardoor deze gegevens alsnog als persoonsgegevens kwalificeren.

Pseudonimisering en anonimisering

Een belangrijk aandachtspunt is hier weggelegd voor gepseudonimiseerde en volledig anonieme gegevens. Bij pseudonimisering worden gegevens zodanig verwerkt dat zij niet meer direct aan een specifieke persoon kunnen worden gekoppeld, maar heridentificatie met behulp van apart bewaarde aanvullende gegevens nog wel mogelijk blijft.



Gepseudonimiseerde gegevens blijven daarom persoonsgegevens waarop de AVG onverkort van toepassing is. Pseudonimisering is wel een waardevolle maatregel om risico's voor betrokkenen te beperken en kan organisaties helpen bij het naleven van hun verplichtingen inzake gegevensbescherming.

Alleen wanneer gegevens **volledig anoniem** zijn en op **geen enkele** wijze meer tot een **persoon** kunnen worden **herleid**, valt de verwerking buiten het toepassingsbereik van de AVG.

In de praktijk betekent dit dat organisaties kritisch moeten beoordelen welke gegevens zij verwerken. Het bijhouden van bedrijfsnamen in een leveranciersbestand valt mogelijk buiten de AVG, maar zodra contactpersonen, e-mailadressen of andere identificerende gegevens van externe partijen of medewerkers worden verwerkt, is de verordening van toepassing.

Stap 3: Uitzonderingen op het materiële toepassingsgebied

Ook indien sprake is van verwerking van persoonsgegevens, kan de AVG buiten toepassing blijven indien een van de **wettelijke uitzonderingen** geldt. De belangrijkste uitzondering betreft verwerkingen die plaatsvinden in het kader van een zuiver persoonlijke of huishoudelijke activiteit. Daarnaast is de AVG niet van toepassing op verwerkingen door bevoegde autoriteiten in het kader van opsporing en nationale veiligheid, waarvoor andere specifieke regelgeving geldt.

Daarnaast geldt dat de AVG alleen van toepassing is indien de verwerking geheel of gedeeltelijk geautomatiseerd plaatsvindt, of wanneer de gegevens zijn opgenomen in een bestand of bestemd zijn om daarin te worden opgenomen.

Klantgegevens die een medewerker op een post-it noteert en vervolgens weggooit, vallen hier **niet** onder. Worden diezelfde gegevens echter later ingevoerd in een CRM-systeem, opgenomen in een digitaal klantenbestand of toegevoegd aan een fysiek dossier, dan is de AVG **wel** van toepassing.

Deze uitzonderingen moeten terughoudend worden toegepast. In een zakelijke of professionele context zal doorgaans geen beroep op deze uitzonderingen mogelijk zijn.



Stap 4: Territoriaal toepassingsgebied

Als laatste stap dient te worden beoordeeld of de AVG **territoriaal** van toepassing is. De verordening kent een ruime geografische reikwijdte, beperkt zich **niet** tot organisaties die binnen de Europese Unie zijn gevestigd en is van toepassing in de volgende situaties:

- de verwerking vindt plaats in het kader van een **vestiging binnen de EU**;
- een organisatie buiten de EU **biedt goederen of diensten aan** personen binnen de EU;
- een organisatie buiten de EU **monitort het gedrag** van personen binnen de EU.

Ook organisaties zonder vestiging in de EU kunnen onder de AVG vallen wanneer zij zich richten op de Europese markt of gedrag van personen binnen de EU volgen.

Een organisatie buiten de EU valt onder de AVG wanneer zij goederen of diensten aanbiedt aan personen in de EU of hun gedrag monitort, zoals bij een Amerikaanse webshop die levert aan Nederlandse klanten of een buitenlandse app die surfgedrag volgt. In dat geval is zij op grond van artikel 27 AVG verplicht een vertegenwoordiger in de EU aan te wijzen. Deze vertegenwoordiger, gevestigd in een lidstaat waar betrokkenen zich bevinden, fungeert als aanspreekpunt voor toezichthouders en betrokkenen, zoals bijvoorbeeld een Nederlandse vertegenwoordiger voor een Britse softwareleverancier na de Brexit.

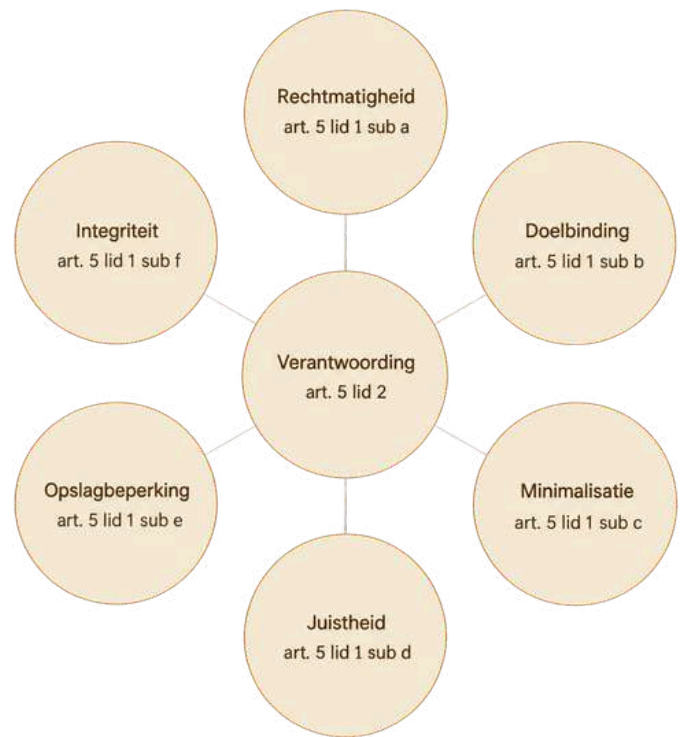


Kernregels van de **AVG**

Hoofdstuk II van de AVG bevat een samenhangend stelsel van regels waaraan elke verwerking van persoonsgegevens moet voldoen. Dit hoofdstuk behandelt achtereenvolgens de verwerkingsbeginselen en de grondslagen voor rechtmatige verwerking.

Beginselen inzake verwerking van persoonsgegevens

Elke verwerking van persoonsgegevens moet voldoen aan de beginselen uit artikel 5 AVG. Deze beginselen vormen het fundament van de gegevensbescherming en gelden cumulatief. Om organisaties te helpen bij de praktische toepassing van deze beginselen, worden zij hieronder uiteengezet aan de hand van kernvragen die elke organisatie zichzelf dient te stellen.



Rechtmatigheid, behoorlijkheid en transparantie

(art. 5 lid 1 sub a AVG)

Kernvraag

Hebben wij een rechtmatige grondslag, is de verwerking behoorlijk en zijn betrokkenen adequaat geïnformeerd?

Toelichting

Elke verwerking vereist een geldige grondslag uit artikel 6 AVG. Daarnaast dient de verwerking behoorlijk te zijn: persoonsgegevens mogen niet worden gebruikt op een manier die nadelig, discriminerend of onverwacht is voor de betrokkene. Tot slot moeten betrokkenen weten dat hun persoonsgegevens worden verwerkt. Voor natuurlijke personen dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt. Dit gebeurt doorgaans via een privacyverklaring met informatie over de verwerkte persoonsgegevens, doeleinden, grondslagen en rechten van betrokkenen.

Doelbinding

(art 5 lid 1 sub b AVG)

Kernvraag

Wat is ons doel en gebruiken wij persoonsgegevens alleen daarvoor?

Toelichting

Persoonsgegevens mogen alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Stel het doel dus vast vóórdat de gegevens worden verzameld.

Minimale gegevensverwerking

(art. 5 lid 1 sub c AVG)

Kernvraag

Verzamelen we enkel de persoonsgegevens die noodzakelijk zijn?

Toelichting

Persoonsgegevens dienen toereikend te zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Verwerk niet meer gegevens dan nodig om het vastgestelde doel te bereiken.

Juistheid

(art. 5 lid 1 sub d AVG)

Kernvraag

Kloppen onze persoonsgegevens nog of zijn ze verouderd?

Toelichting

Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist. Richt processen in om gegevens periodiek te controleren.

Kernvraag

Bewaren wij persoonsgegevens niet langer dan nodig?

Toelichting

Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens en voor een periodieke toetsing ervan. Soms volgt de bewaartermijn uit de wet, zoals de fiscale bewaarplicht. Zo niet, stel dan zelf een passende termijn vast.

Kernvraag

Zijn onze persoonsgegevens adequaat beveiligd?

Toelichting

De verwerkingsverantwoordelijke en de verwerker dienen, met oog voor de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doelen van de verwerking, passende technische en organisatorische maatregelen te nemen. Het doel daarvan is om een beveiligingsniveau te realiseren dat past bij de risico's. Denk daarbij, waar dat zinvol is, bijvoorbeeld aan het pseudonimiseren en versleutelen van persoonsgegevens.

Kernvraag

Kunnen wij aantonen dat wij aan alle beginselen voldoen?

Toelichting

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van bovenstaande beginselen en moet kunnen aantonen dat hieraan wordt voldaan. Dit vereist documentatie, zoals een verwerkingsregister met daarin onder meer de verwerkingsdoeleinden, categorieën betrokkenen en persoonsgegevens, categorieën ontvangers, bewaartermijnen en beveiligingsmaatregelen.

Grondslagen

Grondslag	Vereiste	Voorbeeld	Aandachtspunten
Toestemming (art. 6 lid 1 sub a jo. art. 7)	De betrokkene heeft vrije, specifieke, geïnformeerde en ondubbelzinnige toestemming gegeven voor een of meer specifieke doeleinden. Daarnaast heeft de betrokkene te allen tijde het recht zijn/haar toestemming in te trekken.	Een webshop vraagt bezoekers actief om toestemming voor het ontvangen van een nieuwsbrief via een niet-vooraf aangevinkt vakje.	In machtsverhoudingen (zoals op de werkvloer of met de overheid) geldt toestemming zelden als geschikte grondslag wegens de afhankelijkheids- en ondergeschiktheidsrelatie tussen werkgever en werknemer. De betrokkene moet toestemming te allen tijde kunnen intrekken, waarna de verwerking moet stoppen.
Overeenkomst (art. 6 lid 1 sub b)	De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.	Een webshop deelt de adresgegevens van een klant met een bezorgdienst om de bestelde producten te kunnen afleveren.	Beperk de verwerking strikt tot wat noodzakelijk is voor de uitvoering van de overeenkomst. Marketingactiviteiten of het opstellen van klantprofielen vallen hier niet onder. Vermijd het "oprekken" van deze grondslag.
Wettelijke verplichting (art. 6 lid 1 sub c)	De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.	In sommige gevallen moet je persoonsgegevens verwerken, simpelweg omdat hier een wettelijke opdracht toe is. Denk hierbij bijvoorbeeld aan het bewaren van bepaalde persoonsgegevens voor de Belastingdienst voor de loonadministratie.	Controleer welke persoonsgegevens noodzakelijk zijn om aan de wettelijke verplichting te voldoen.
Vitaal belang (art. 6 lid 1 sub d)	De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen.	Een BHV'er deelt medische informatie van een bewusteloze medewerker met hulpdiensten bij een bedrijfsongeval.	Deze grondslag is uitsluitend bedoeld voor acute, levensbedreigende situaties en kan niet worden ingezet voor structurele gegevensverzameling. Gebruik deze grondslag alleen wanneer de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd.
Algemeen belang (art. 6 lid 1 sub e)	De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.	Een gemeente verwerkt persoonsgegevens in het kader van handhaving of vergunningverlening.	Deze grondslag is voor het overgrote deel gericht op overheden. Echter, ook niet-overheden kunnen zich hierop beroepen. Zo worden ook aan liefdadigheidsinstellingen dergelijke taken toegewezen.
Gerechtvaardigd belang (art. 6 lid 1 sub f)	De verwerking is noodzakelijk voor de behartiging van gerechtvaardigde belangen, mits de belangen van de betrokkene niet zwaarder wegen.	Een werkgever plaatst cameratoezicht op de werkvloer ter beveiliging van bedrijfseigendommen en de veiligheid van medewerkers.	Voer altijd een gedocumenteerde belangenafweging uit. De belangen, grondrechten en fundamentele vrijheden van de betrokkene kunnen zwaarder wegen, met name bij kinderen. Deze grondslag is niet beschikbaar voor overheden bij de uitoefening van hun publieke taken.

Rechten van betrokkenen

Hoofdstuk III van de AVG geeft betrokkenen rechten om controle te houden over hun persoonsgegevens. Organisaties moeten deze rechten faciliteren.

Let op: het is van belang bedacht te zijn op de relevante termijnen: één maand om te reageren op een verzoek van een betrokkene tot uitoefening van zijn/haar rechten. Bij complexe of veelvuldige verzoeken kan deze termijn met maximaal twee maanden worden verlengd. Betrokkenen dienen binnen de eerste maand over de verlenging te worden geïnformeerd.

De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van betrokkenen uit hoofde van de artikelen 15 tot en met 22, welke hieronder worden besproken. Om als organisatie op adequate wijze te kunnen voldoen aan deze rechten, is het noodzakelijk om vooraf de juiste documenten en procedures in te richten. Intern dient een procedure te worden ingericht zodat duidelijk is:

- wie de verzoeken van betrokkenen beoordeelt;
- hoe de verzoeken naar deze persoon worden doorgezet;
- hoe deze persoon de verzoeken afhandelt.

Deze procedure geldt voor alle rechten die in dit hoofdstuk worden besproken. Voorafgaand verifieert de organisatie de identiteit van de verzoeker om te voorkomen dat persoonsgegevens met de verkeerde persoon worden gedeeld. Wanneer de verwerkingsverantwoordelijke redenen heeft om te twijfelen aan de identiteit, kan hij om aanvullende informatie vragen (art. 12 lid 6 AVG). Nadat het verzoek is beoordeeld, volgt de afhandeling. Wanneer een verzoek elektronisch is ingediend, wordt de informatie indien mogelijk ook elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt (art. 12 lid 3 AVG).

Recht op informatie (art. 13 en 14 AVG)

Het recht op informatie vormt het fundament van alle overige rechten van betrokkenen. Zonder adequate informatie over de verwerking van hun

persoonsgegevens zijn betrokkenen immers niet in staat om hun overige rechten effectief uit te oefenen. De betrokkene heeft het recht om te weten dat zijn gegevens worden verwerkt, voor welke doeleinden dit gebeurt en aan wie de persoonsgegevens worden verstrekt.

De betrokkene dient ten minste te worden geïnformeerd over het recht om inzage te verkrijgen in en rectificatie of verwijdering van persoonsgegevens, het recht op beperking van de verwerking, het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid. Wanneer de verwerking op toestemming is gebaseerd, heeft de betrokkene het recht om deze te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan. Ook heeft de betrokkene het recht om een klacht in te dienen bij een toezichthoudende autoriteit.

Praktische invulling aan dit recht wordt doorgaans gegeven via een duidelijke en toegankelijke [privacyverklaring](#) en een intern privacybeleid. Beide documenten dienen te worden gepubliceerd op respectievelijk de website en het intranet. Tevens dient naar de privacyverklaring te worden verwezen bij elk contactmoment waarop persoonsgegevens worden verzameld.

Recht op inzage (art. 15 AVG)

Het recht op inzage stelt betrokkenen in staat om te vernemen of hun persoonsgegevens worden verwerkt en, als dat het geval is, welke gegevens dit betreft. De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitend te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen in die persoonsgegevens.

Bij een [inzageverzoek](#) verstrekt de organisatie informatie over de verwerkingsdoeleinden, de betrokken categorieën van persoonsgegevens, de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of

internationale organisaties, en indien mogelijk de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen.

Indien mogelijk moet de verwerkingsverantwoordelijke op afstand toegang kunnen geven tot een beveiligd systeem waarop de betrokkene direct zijn persoonsgegevens kan inzien.

Het inzagerecht mag geen afbreuk doen aan de rechten of vrijheden van anderen, met inbegrip van het zakengeheim of de intellectuele eigendom en met name aan het auteursrecht dat software beschermt. Hieronder valt ook het recht op gegevensbescherming van andere betrokkenen. Wanneer de verwerkingsverantwoordelijke een grote hoeveelheid persoonsgegevens verwerkt, kan hij de betrokkene voorafgaand aan de informatieverstrekking verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.

Voor de verificatie van de identiteit van de verzoeker wordt verwezen naar de algemene procedure aan het begin van dit hoofdstuk.

Recht op rectificatie (art. 16 AVG)

Het recht op rectificatie biedt betrokkenen de mogelijkheid om onjuiste persoonsgegevens te laten corrigeren of onvolledige gegevens te laten aanvullen. Dit recht is nauw verbonden met het beginsel van juistheid dat voorschrijft dat persoonsgegevens correct en actueel moeten zijn.

Gedacht kan worden aan een updateproces waarmee betrokkenen op eenvoudige wijze wijzigingen kunnen doorgeven.

Indienen van een verzoek

Er kan op verschillende manieren invulling worden gegeven aan het recht op rectificatie, bijvoorbeeld via een online portaal waarin betrokkenen zelfstandig hun persoonsgegevens kunnen aanpassen of middels een verzoek tot rectificatie per e-mail of telefonisch.

Verwerking van de correctie

Wanneer een correctie wordt doorgevoerd, dient de wijziging in alle systemen te worden verwerkt waarin de gegevens zijn opgeslagen. Vervolgens ontvangt de betrokkene een bevestiging van de wijziging.

Recht op verwijdering (art. 17 AVG)

Het recht op verwijdering, ook wel het recht om vergeten te worden genoemd, stelt betrokkenen in staat om onder bepaalde omstandigheden hun persoonsgegevens te laten verwijderen. Dit recht geldt bijvoorbeeld wanneer de persoonsgegevens niet langer noodzakelijk zijn voor de doeleinden waarvoor zij werden verzameld, wanneer de betrokkene zijn toestemming intrekt, of wanneer de betrokkene bezwaar maakt tegen de verwerking.

Recht op beperking van de verwerking (art. 18 AVG)

Het recht op beperking van de verwerking biedt betrokkenen de mogelijkheid om te verzoeken dat de verwerking van hun persoonsgegevens tijdelijk wordt stopgezet. Dit kan bijvoorbeeld aan de orde zijn wanneer de betrokkene de juistheid van de gegevens betwist en de organisatie tijd nodig heeft om dit te verifiëren, of wanneer de betrokkene bezwaar heeft gemaakt en de afweging van belangen nog moet plaatsvinden.

Met een heldere workflow kunnen gegevens tijdelijk worden "bevroren" wanneer dat nodig is. Markeer de betreffende gegevens in de systemen en houd de betrokkene op de hoogte van de voortgang. Zodra de situatie is opgehelderd, informeer dan de betrokkene voordat de beperking wordt opgeheven.

Recht op overdraagbaarheid van gegevens (art. 20 AVG)

Het recht op overdraagbaarheid van gegevens stelt betrokkenen in staat om de persoonsgegevens die zij aan een organisatie hebben verstrekt in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. Betrokkenen kunnen deze gegevens vervolgens overdragen aan een andere verwerkingsverantwoordelijke.

Dit recht is van toepassing wanneer de verwerking berust op toestemming of een overeenkomst, en de verwerking geautomatiseerd plaatsvindt.

Door een gebruiksvriendelijke exportfunctie aan te bieden in gangbare formaten wordt het voor betrokkenen gemakkelijk om hun gegevens te ontvangen. Waar technisch mogelijk, kunnen de persoonsgegevens ook rechtstreeks naar een andere partij worden overgedragen. Dit draagt vaak bij aan een positieve klantervaring.

Recht van bezwaar (art. 21 AVG)

Het recht van bezwaar hangt nauw samen met de grondslag gerechtvaardigd belang (art. 6 lid 1 sub f AVG). Bij deze grondslag dient de verwerkingsverantwoordelijke voorafgaand aan de verwerking een belangenafweging te maken. Het recht van bezwaar biedt de betrokkene de mogelijkheid om deze afweging opnieuw te laten beoordelen op basis van zijn specifieke situatie.

Wanneer een betrokkene bezwaar maakt, staakt de verwerkingsverantwoordelijke de verwerking van de persoonsgegevens, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene (art. 21 lid 1 AVG).

Het is aan te bevelen om als organisatie een afwegingskader te ontwikkelen om bezwaren te beoordelen. Door de afweging en de uitkomst te documenteren, kan de organisatie voldoen aan de verantwoordingsplicht.

Kosten en weigering

Het afhandelen van verzoeken is in beginsel kosteloos voor de betrokkene. Dit benadrukt het belang dat de AVG hecht aan toegankelijke rechten voor iedereen. Alleen wanneer verzoeken kennelijk ongegrond of buitensporig zijn, bijvoorbeeld vanwege een repetitief karakter, mag de verwerkingsverantwoordelijke een redelijke vergoeding vragen of het verzoek weigeren. Het is aan de verwerkingsverantwoordelijke om dit aan te tonen.

Benader verzoeken van betrokkenen met een servicegerichte instelling. Wanneer in uitzonderlijke gevallen een verzoek niet kan worden ingewilligd, leg dan vriendelijk en transparant uit waarom dit zo is en welke alternatieven er eventueel zijn. Een respectvolle communicatie draagt bij aan het vertrouwen in jouw organisatie.



Rollen en verantwoordelijkheden

Hoofdstuk IV van de AVG bevat artikelen over de verplichtingen voor de verwerkingsverantwoordelijke en de verwerker onder de AVG. Hieronder vallen bijvoorbeeld algemene verplichtingen, beveiligingsverplichtingen, DPIA's en de FG.

AVG-rollen

Onder de AVG kwalificeert een organisatie die persoonsgegevens verwerkt als een verwerkingsverantwoordelijke of een verwerker. Het correct vaststellen van deze rol is essentieel, omdat dit de verhouding tot andere partijen en de toepasselijke verplichtingen onder de AVG bepaalt.



Verwerkingsverantwoordelijke	Verwerker
Artikel 4 onder 7 AVG.	Artikel 4 onder 8 AVG.
Bepaalt het <i>doel</i> en de <i>middelen</i> voor de verwerking van persoonsgegevens.	Verwerkt persoonsgegevens <i>ten behoeve van</i> de verwerkingsverantwoordelijke.
Waarom en hoe worden de persoonsgegevens verwerkt?	Worden persoonsgegevens alleen in opdracht van een andere organisatie verwerkt en niet voor eigen doeleinden?
Bijv. webshops, werkgevers, overheidsinstanties, zorginstellingen.	Bijv. IT-dienstverleners, softwareleveranciers.

Let op:

Één organisatie kan meerdere rollen hebben. De rol wordt namelijk vastgesteld per verwerking. Zo is een softwareleverancier verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens van haar eigen werknemers, maar verwerker voor de persoonsgegevens die klanten in de software zetten.



Verwerkingsverantwoordelijken en verwerkers hebben onder de AVG verschillende verantwoordelijkheden. Hieronder zijn de verantwoordelijkheden uit hoofdstuk IV van de AVG schematisch weergegeven:

Onderwerp	Verplichting	Toelichting
Beveiliging	Treffen passende technische en organisatorische maatregelen (art. 24, 28 lid 1 en 32 AVG)	De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te nemen om te waarborgen en aan te tonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd. Artikel 32 AVG kleurt dit verder in. Zowel de verwerkingsverantwoordelijke als de verwerker dient passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Welk risico dit is zal verschillen per organisatie. De AVG geeft hierbij aan dat rekening gehouden dient te worden met de stand van de techniek en de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden. Tot slot dient ook de waarschijnlijkheid en ernst van de risico's voor de betrokkenen meegewogen te worden. Voor het verwerken van medische gegevens zal een ander beveiligingsniveau passend zijn dan voor NAW-gegevens. Artikel 28 lid 1 AVG maakt duidelijk dat de verwerkingsverantwoordelijke enkel verwerkers in mag schakelen die afdoende garanties bieden met betrekking tot het toepassen van bovengenoemde technische en organisatorische maatregelen.
	Data protection by design and default (art. 25 AVG)	Verwerkingsverantwoordelijken dienen rekening te houden met gegevensbescherming door ontwerp en door standaardinstellingen. Kort gezegd komt dit erop neer dat gegevensbescherming al een rol speelt vanaf het moment dat een product of dienst waarbij persoonsgegevens worden verwerkt, wordt ontworpen. Bijvoorbeeld door het automatisch pseudonimiseren van persoonsgegevens. Daarnaast dient de applicatie of dienst zo privacyvriendelijk mogelijk te worden ingesteld. Ook hierbij geldt een op het risico gebaseerde aanpak. Hoewel de AVG de verplichting oplegt aan verwerkingsverantwoordelijken , zal in de praktijk vaak de hulp van een verwerker worden ingeschakeld. Het is daarom aan te raden voor verwerkers om bijvoorbeeld bij de bouw van software/websites/apps rekening te houden met deze verplichting
Datalekken	Meldplicht Autoriteit Persoonsgegevens (art. 33 AVG)	De AVG spreekt van een 'inbreuk in verband met persoonsgegevens' (datalek) wanneer een inbreuk op de beveiliging leidt tot het verlies, of het ongeoorloofd wijzigen, verstrekken, inzien of anderszins verwerken van persoonsgegevens. Er is iets gebeurd met de persoonsgegevens terwijl dat niet de bedoeling was.

Onderwerp	Verplichting	Toelichting
		Voorbeelden van datalekken: • Een hacker verkrijgt toegang tot persoonsgegevens. • Het versturen van een e-mailbericht waarin alle e-mailadressen in het CC-veld staan, in plaats van het BCC-veld. • Een werknemer heeft per ongeluk de salarisstrook van een andere werknemer ontvangen. Niet elk datalek hoeft gemeld te worden bij de Autoriteit Persoonsgegevens (AP). Een datalek moet aan de toezichthouder gemeld worden indien er sprake is van een risico voor de rechten en vrijheden van betrokkenen. Een datalek kan een risico teweegbrengen als het een grote hoeveelheid persoonsgegevens betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig), of een combinatie daarvan. Denk bijvoorbeeld aan financiële gegevens, medische informatie of kopieën van identiteitsbewijzen. Het datalek dient zo snel mogelijk, maar in ieder geval binnen 72 uur na ontdekking van het datalek, via de website van de AP gemeld te worden door de verwerkingsverantwoordelijke. Deze termijn start op het moment dat de verwerkingsverantwoordelijke op de hoogte raakt van het datalek. Hierdoor zijn heldere afspraken met verwerkers essentieel.
	Mededeling betrokkenen (art. 34 AVG)	Indien het datalek een hoog risico oplevert voor de rechten en vrijheden van betrokkenen moet het datalek door de verwerkingsverantwoordelijke zowel aan de toezichthouder als aan de betrokkene(n) gemeld worden. Een datalek brengt een hoog risico voor betrokkenen teweeg wanneer het privéleven van betrokkenen waarschijnlijk door het lek wordt geschaad. Gevolgen die dan kunnen ontstaan zijn bijvoorbeeld: • Identiteitsfraude • Discriminatie • Reputatieschade Wanneer gevoelige gegevens zijn gelekt, is er eigenlijk vrijwel altijd sprake van een hoog risico. Dan moet het datalek dus ook vrijwel altijd worden gemeld aan de getroffen personen.
	Interne registratie (art. 33 lid 5 AVG)	Van belang is om elk datalek intern te registreren in een datalekregister. Ook als het datalek niet aan de AP of, bij een hoog risico, aan betrokkenen gemeld hoeft te worden. In het datalekregister staat alle informatie over een of meerdere datalekken die zich hebben voorgedaan bij de verwerkingsverantwoordelijke (of bij de verwerker van de organisatie). Het is gebruikelijk om in ieder geval onderstaande informatie in het datalekregister op te nemen:

Onderwerp	Verplichting	Toelichting
		• Omschrijving van het datalek • Categorieën persoonsgegevens en betrokkenen • Mogelijke gevolgen • Partijen die betrokken zijn bij het datalek • Is het datalek wel/niet gemeld aan de Autoriteit Persoonsgegevens en betrokkenen en waarom wel/niet?
Verwerkingsregister	Bijhouden verwerkingsregister (art. 30 AVG)	De hoofdregel is dat organisaties die minstens 250 personen in dienst hebben, een verwerkingsregister moeten bijhouden. Organisaties die minder dan 250 personen in dienst hebben, moeten ook een verwerkingsregister bijhouden als er sprake is van een van onderstaande gevallen: • organisatie houdt zich bezig met risicovolle verwerkingen (zoals het opstellen van klantprofielen of het verwerken van grote hoeveelheden persoonsgegevens); • wanneer de verwerking structureel en dus niet incidenteel is; • organisatie verwerkt gevoelige gegevens (zoals gegevens over gezondheid en strafrechtelijke gegevens). Bij de verwerkingsverantwoordelijke bevat het verwerkingsregister de volgende informatie: • naam en contactgegevens van de verwerkingsverantwoordelijke, en van de functionaris gegevensbescherming (indien aanwezig); • verwerkingsdoeleinden; • categorieën betrokkenen (bijvoorbeeld klanten, websitebezoekers en medewerkers); • categorieën persoonsgegevens (bijvoorbeeld NAW-gegevens, contactgegevens, financiële gegevens); • categorieën ontvangers (bijvoorbeeld ICT-dienstverleners); • informatie over eventuele doorgifte van persoonsgegevens naar een derde land; • bewaartermijnen; • beveiligingsmaatregelen. Bij de verwerker is het register georganiseerd per verwerkingsverantwoordelijke. Verwerkers nemen de volgende informatie op in het verwerkingsregister: • naam en contactgegevens van de verwerker en de verwerkingsverantwoordelijke, en de functionaris gegevensbescherming (indien aanwezig); • categorieën verwerkingen; • informatie over eventuele doorgifte van persoonsgegevens naar een derde land; • beveiligingsmaatregelen.
Contact toezichthoudende autoriteiten	Medewerking toezichthoudende autoriteiten (art. 31 AVG)	Zowel de verwerkingsverantwoordelijke als de verwerker dienen desgevraagd samen te werken met de toezichthoudende autoriteit bij het vervullen van haar taken.

Onderwerp	Verplichting	Toelichting
Risicobeoordeling	Uitvoeren DPIA (art. 35 AVG)	Een DPIA wordt uitgevoerd door de verwerkingsverantwoordelijke. De verwerker dient de verwerkingsverantwoordelijke hierbij te helpen. In sommige gevallen voert een verwerker vrijwillig een DPIA uit. Aan de hand daarvan kan een verwerker namelijk aantonen dat bijvoorbeeld haar software/IT-systeem privacyvriendelijk is ingericht. Een DPIA is verplicht in situaties waarin de gegevensverwerking waarschijnlijk een hoog risico oplevert voor de privacy van betrokkenen. In de AVG zijn enkele voorbeelden opgenomen van situaties waarin een DPIA verplicht is: • grootschalige besluiten worden genomen gebaseerd op geautomatiseerde verwerkingen van persoonsgegevens, zoals bij profilering; • grootschalige verwerking van bijzondere persoonsgegevens of strafrechtelijke gegevens; • stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten. Daarnaast heeft de Autoriteit Persoonsgegevens een DPIA-lijst gepubliceerd waarin staat in welke situaties een DPIA verplicht is. In onderstaande gevallen dient jouw organisatie in ieder geval een DPIA uit te (laten) voeren: • Samenwerkingsverbanden waarin overheden met andere publieke of private organisaties bijzondere persoonsgegevens of gevoelige gegevens delen (bijv. gegevens over armoede, gezondheid, werkloosheid en sociale problematiek). • Stelselmatige monitoring, zoals door cameratoezicht of het gebruik van (tracking) cookies die de betrokken personen blijven volgen. • Grootschalige verwerkingen van (bijzondere) persoonsgegevens en/of stelselmatige monitoring in het kader van fraudebestrijding. • Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. • Combineren van databases en het uitvoeren van big data-analyses. • Ontwikkeling van een nieuw project of nieuwe software waarmee persoonsgegevens worden verwerkt.
	Voorafgaande raadpleging toezichthoudende autoriteit (art. 36 AVG)	Wanneer uit de DPIA volgt dat de verwerking een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, dient de organisatie voorafgaand aan de verwerking de Autoriteit Persoonsgegevens te raadplegen.

Gegevensuitwisseling & samenwerken

Organisaties delen veel persoonsgegevens met elkaar. Het is belangrijk om hier goede afspraken over te maken.

Verwerkersovereenkomst

Wanneer een verwerkingsverantwoordelijke en verwerker gegevens uitwisselen, moeten zij een verwerkersovereenkomst sluiten. In die overeenkomst maken partijen afspraken over hoe er wordt omgegaan met de persoonsgegevens.

Wat staat allemaal in een verwerkersovereenkomst?

1. Persoonsgegevens en doeleinden

De verwerker moet duidelijke instructies krijgen over welke persoonsgegevens er worden verwerkt, en voor welke doeleinden dat gebeurt.

2. Subverwerkers

In sommige gevallen maakt een verwerker weer gebruik van een andere verwerker, ook wel subverwerker genoemd. Dat mag niet zomaar. Daar moeten afspraken over worden gemaakt in een verwerkersovereenkomst.

3. Doorgifte van persoonsgegevens

Het is mogelijk dat de verwerker of subverwerker gevestigd is in een land buiten de Economische Ruimte (EER), een zogenaamd derde land. Denk bijvoorbeeld aan ICT-dienstverleners die gevestigd zijn in de Verenigde Staten. De persoonsgegevens mogen alleen worden doorgegeven als er passende waarborgen zijn getroffen. In een verwerkersovereenkomst regelen de verwerkingsverantwoordelijke en verwerker of, en zo ja onder welke voorwaarden, persoonsgegevens mogen worden doorgegeven aan een derde land.

4. Beveiligingsmaatregelen

Verhoog je weerbaarheid en aantoonbare compliance met risico-gestuurde beveiligingsmaatregelen zodat persoonsgegevens op de juiste wijze worden beveiligd. Het is gebruikelijk om deze keuzes vast te leggen in bijvoorbeeld een overzicht van beveiligingsmaatregelen in de verwerkersovereenkomst.

5. Datalekken

Gebeurt er iets met persoonsgegevens dat niet de bedoeling is, dan hebben we te maken met een datalek. Borg een snelle, zorgvuldige datalekafhandeling om de impact te beperken en vertrouwen te versterken. Een goede samenwerking tussen een verwerkingsverantwoordelijke en verwerker is hierbij essentieel.

6. Audits

Een verwerkingsverantwoordelijke heeft het recht om te (laten) controleren of de verwerker de werkzaamheden goed verricht. Aan de hand van een audit kan de werkwijze worden gecontroleerd.

7. Verzoeken van betrokkenen

Ontvangt een van de partijen een verzoek van een betrokkene, dan zal dat verzoek opgepakt moeten worden. In sommige situaties is de verwerkingsverantwoordelijke afhankelijk van de medewerking van de verwerker. Op welke manier verzoeken van betrokkenen worden afgehandeld volgt uit de verwerkersovereenkomst.

8. Verwijdering of vernietiging van de persoonsgegevens

Stopt de dienstverlening, dan heeft de verwerker de persoonsgegevens vaak niet meer nodig. Het is aan de verwerkingsverantwoordelijke om te bepalen wat er vervolgens met de persoonsgegevens gebeurt: dient de verwerker de gegevens te vernietigen of terug te leveren?

Data-uitwisselingsovereenkomst

Wanneer beide partijen gezamenlijk verwerkingsverantwoordelijke zijn, dan maken zij afspraken in een data-uitwisselingsovereenkomst. Dit staat in artikel 26 AVG. Als partijen zelfstandig verwerkingsverantwoordelijke zijn, is zo'n overeenkomst niet verplicht, maar wel aan te raden. Dit om bijvoorbeeld te waarborgen dat de ontvanger de gegevens niet voor een ander doel verwerkt dan waarvoor ze verstrekt zijn.



Functionaris Gegevensbescherming (FG)

Sommige organisaties zijn wettelijk verplicht om een functionaris gegevensbescherming (FG) aan te stellen. De FG informeert en adviseert over de omgang met persoonsgegevens. Daarbij neemt de FG een onafhankelijke positie in.

Onderstaande organisaties zijn verplicht om een FG aan te stellen:

- Overheidsorganen
- Organisaties die belast zijn met stelselmatige observatie
- Organisaties die op grote schaal bijzondere persoonsgegevens verwerken

Ook voor organisaties die niet onder een van deze categorieën vallen, is het raadzaam om een FG aan te stellen. Dit om het recht op gegevensbescherming te waarborgen.

Doorgifte naar derde landen

Hoofdstuk 5 van de AVG bevat artikelen over de doorgifte van persoonsgegevens naar derde landen en internationale organisaties. De AVG biedt drie routes om dergelijke doorgiften rechtmatig te organiseren: via een adequaatheidsbesluit, via passende waarborgen of, in enkele gevallen, via specifieke uitzonderingen.

In een digitale en internationale bedrijfsvoering is doorgifte van persoonsgegevens buiten de EER vaak onvermijdelijk. Denk aan cloudoplossingen, internationale leveranciers of 24/7-supportdiensten. Juist deze doorgiften brengen verhoogde risico's met zich mee, omdat het beschermingsniveau in derde landen niet vanzelfsprekend gelijkwaardig is aan dat binnen de EU. Hieronder worden de verschillende routes kort toegelicht.



Adequaatheidsbesluit (art. 45 AVG)

De meest eenvoudige situatie doet zich voor wanneer de Europese Commissie heeft vastgesteld dat een land een passend beschermingsniveau biedt. In dat geval mogen persoonsgegevens zonder aanvullende contractuele maatregelen worden doorgegeven. Voor organisaties betekent dit vooral dat zij moeten controleren of een dergelijk besluit van toepassing is en blijft. Leg deze keuze vast in het verwerkingsregister en contractdossier en controleer periodiek of het besluit nog geldig is.

Een actueel en praktisch relevant voorbeeld is het **EU-VS Data Privacy Framework**. Dit adequaatheidsbesluit maakt doorgifte naar de Verenigde Staten mogelijk, mits de ontvangende organisatie zich heeft gecertificeerd onder dit framework. Voor organisaties betekent dit dat niet alleen moet worden gekeken naar het land, maar ook naar de specifieke ontvanger en diens certificeringsstatus.

Voorbeeld:

Een onderneming maakt gebruik van een Amerikaanse cloudprovider die gecertificeerd is onder het Data Privacy Framework. De organisatie controleert deze certificering, legt de doorgifte vast en monitort periodiek of de status actueel blijft.

Passende waarborgen (art. 46 AVG)

Ontbreekt een adequaatheidsbesluit, dan moeten organisaties zelf waarborgen treffen. In de praktijk gebeurt dit meestal via **Standard Contractual Clauses** (SCC's). Het sluiten van deze standaardcontracten zorgt ervoor dat persoonsgegevens ook buiten de EER volgens Europese normen worden beschermd. Het gebruik van SCC's is echter niet voldoende op zichzelf. Organisaties moeten aanvullend beoordelen of de wetgeving en praktijk in het ontvangende land deze bescherming niet ondermijnen.

Deze beoordeling vindt plaats via een zogeheten data transfer impact assessment (DTIA). Daarbij wordt gekeken naar risico's, zoals toegang door lokale autoriteiten, en naar de vraag of aanvullende technische, organisatorische en/of contractuele maatregelen nodig zijn. Denk aan versleuteling, pseudonimisering of het beperken van toegang tot gegevens.

Voorbeeld:

Een onderneming gebruikt een SaaS-oplossing buiten de EER. Zij sluit SCC's, voert een DTIA uit, versleutelt data en beperkt toegang tot specifieke accounts, waarbij alle toegang wordt gelogd.

Voor internationale concerns kunnen **Binding Corporate Rules** (BCR's) een alternatief bieden. Dit zijn interne regels die door toezichthouders worden goedgekeurd en geschikt zijn voor structurele gegevensstromen binnen een groep. De wachttijd voor goedkeuring is echter lang: ongeveer 5 jaar.

Voorbeeld:

HR-gegevens worden vanuit Europese vestigingen gedeeld met een zusteronderneming die als servicecentrum fungeert en buiten de EER gevestigd is. De organisatie gebruikt BCR's en controleert periodiek of deze correct worden nageleefd.

Uitzonderingen (incidenteel) (art. 49 AVG)

Alleen in specifieke situaties is doorgifte toegestaan zonder adequaatheidsbesluit of passende waarborgen, bijvoorbeeld wanneer de betrokkene uitdrukkelijk toestemming heeft gegeven of wanneer de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst. Deze route is nadrukkelijk bedoeld voor incidentele gevallen en niet voor structurele oplossingen.

Voorbeeld:

Bij een eenmalige samenwerking met een leverancier buiten de EER vraagt een organisatie expliciete toestemming voor het delen van contactgegevens.

Wat moet je organiseren?

Voor een zorgvuldige inrichting van internationale doorgiften is het essentieel dat organisaties hun datastromen volledig in kaart brengen: welke gegevens worden gedeeld, met wie en naar welk land. Vervolgens moet per situatie de juiste juridische route worden gekozen en contractueel worden vastgelegd. Indien geen adequaatheidsbesluit geldt, is een gedocumenteerde risicobeoordeling (DTIA) noodzakelijk, inclusief eventuele aanvullende maatregelen.

Daarnaast moeten deze keuzes worden geïntegreerd in bestaande processen, zoals vendor management en change management, zodat wijzigingen in datalocaties of leveranciers tijdig worden gesignaleerd. Tot slot is het van belang dat betrokken functies binnen de organisatie, zoals inkoop, legal en IT, voldoende bekend zijn met deze regels.

In het kort:

Doorgifte buiten de EER is goed mogelijk, mits deze bewust en gestructureerd wordt ingericht. Door per datastroom de juiste route te kiezen, passende waarborgen te treffen en dit zorgvuldig te documenteren, blijven persoonsgegevens ook internationaal adequaat beschermd en voldoet de organisatie aan de eisen van de AVG.



Toezicht en handhaving

In het laatste hoofdstuk van deze factsheet worden de meest relevante en belangrijkste onderwerpen met betrekking tot toezicht en handhaving van de AVG samengevoegd.

De AP als toezichthouder

De Autoriteit Persoonsgegevens (AP) is de Nederlandse toezichthouder op het gebied van gegevensbescherming. De AP houdt toezicht op de naleving van de AVG en kan adviseren, onderzoeken, handhaven en voorlichten. Een organisatie kan op verschillende manieren met de AP te maken krijgen.

Zo kan de AP optreden naar aanleiding van een klacht of tip, bijvoorbeeld wanneer een betrokkene vindt dat zijn verzoek niet of onvoldoende is afgehandeld. Daarnaast kan de AP ook uit eigen beweging een onderzoek starten. Tot slot beschikt de AP over de mogelijkheid van een interventie: zonder een formeel onderzoek te openen stuurt zij een brief of gaat zij met een organisatie in gesprek om een overtreding te stoppen.

Boetes

De AP beschikt over verschillende handhavingsinstrumenten. Zo kan de AP een waarschuwing of berisping geven, een last onder dwangsom opleggen of een boete uitdelen.

Een van de bekendste maatregelen is de boete. De AVG noemt twee boetecategorieën: (i) overtredingen met een boete tot 10 miljoen euro, of tot 2% van de totale wereldwijde jaaromzet indien dat bedrag hoger is, en (ii) overtredingen met een boete tot 20 miljoen euro, of tot 4% van de wereldwijde jaaromzet indien dat bedrag hoger is. Onder de eerste categorie vallen bijvoorbeeld het niet hebben van een verwerkingsregister en het niet melden van een datalek aan de AP. Onder de tweede categorie vallen overtredingen van de

basisbeginselen (zie hoofdstuk 2 van deze factsheet) en de rechten van betrokkenen.

Naast een boete kan de AP een last onder dwangsom opleggen. Waar een boete een sanctie is voor een reeds begane overtreding, is een last onder dwangsom gericht op het beëindigen van een voortdurende overtreding: de organisatie krijgt een termijn om de overtreding te herstellen en betaalt een dwangsom indien zij hier niet aan voldoet.

Een boete is natuurlijk erg vervelend voor een organisatie, maar ook reputatieschade speelt een belangrijke rol. Boetebesluiten worden bijvoorbeeld vaak in het nieuws besproken, waardoor een organisatie ook langs die weg schade kan oplopen.

Optreden door betrokkenen

Ook betrokkenen kunnen op verschillende manieren optreden tegen (vermeende) overtredingen van de AVG door organisaties. Als organisatie is het goed om hiervan bewust te zijn.

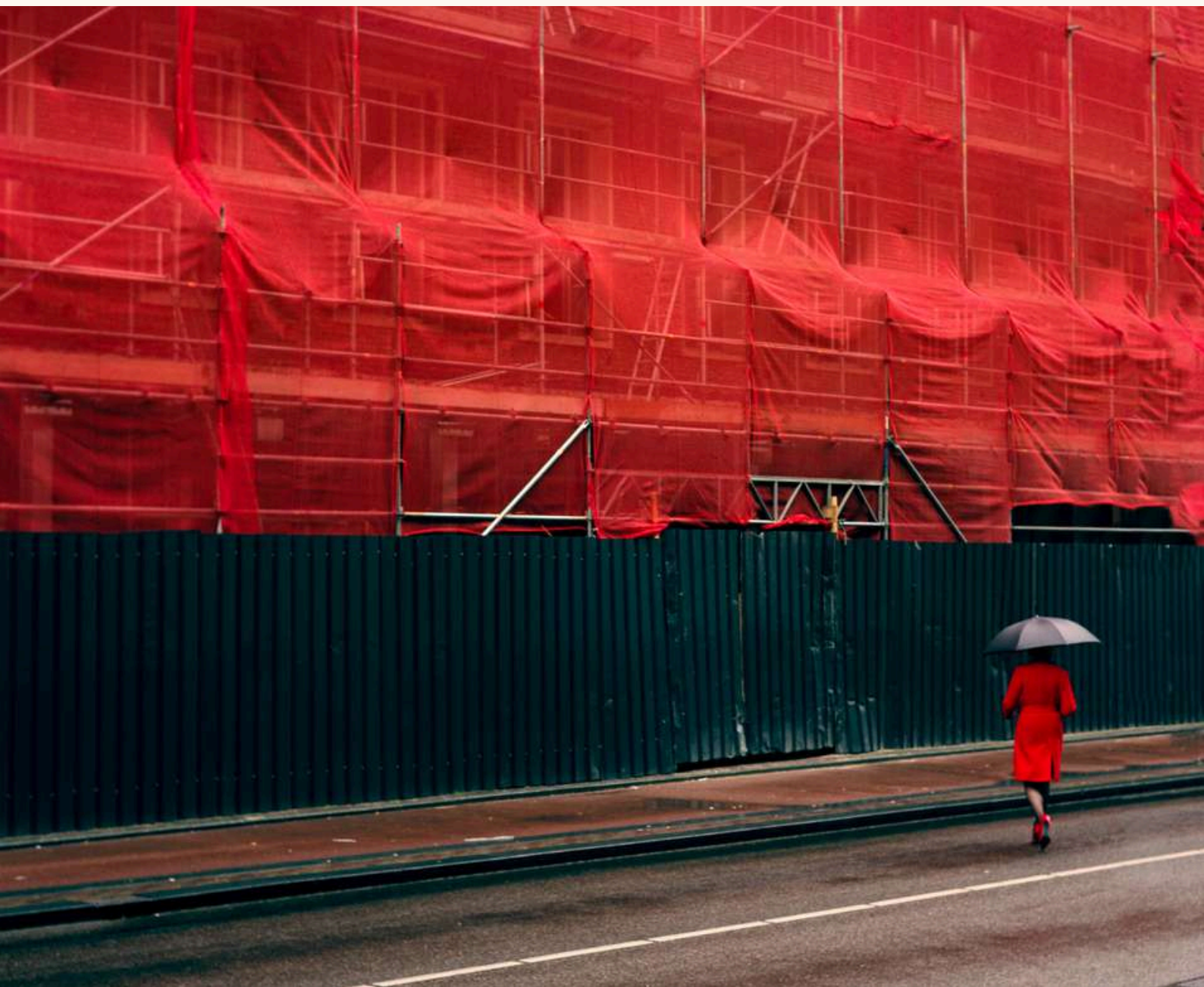
Zo hebben betrokkenen het recht om een klacht in te dienen bij de toezichthoudende autoriteit (art. 77), maar mag een betrokkene zich ook rechtstreeks tot de rechter wenden (art. 79). De betrokkene hoeft dit niet zelf te doen. De AVG biedt de mogelijkheid om te worden bijgestaan door bijvoorbeeld stichtingen of verenigingen. Collectieve acties behoren ook tot de mogelijkheid (art. 80).

Schadevergoeding en aansprakelijkheid

Op grond van artikel 82 AVG heeft een betrokkene recht om schadevergoeding te ontvangen voor de geleden schade door een inbreuk op de AVG. Dit geldt zowel voor materiële als immateriële schade. Bij inbreuken op het recht op gegevensbescherming zal vooral sprake zijn van immateriële schade. Het zal in de praktijk lastig zijn om de hoogte van dergelijke schade vast te stellen.

De verwerkingsverantwoordelijke en de verwerker zijn hoofdelijk aansprakelijk voor de geleden schade, voor zover zij beide bij dezelfde verwerking betrokken zijn. De partij die aansprakelijk is gehouden voor het geheel, kan het gedeelte van de schade waar de andere partij voor verantwoordelijk was verhalen op die partij (art. 82 lid 5).

Hierbij dient rekening gehouden te worden met artikel 82 lid 2 AVG: een verwerkingsverantwoordelijke is in beginsel verantwoordelijk voor schade die wordt veroorzaakt door een verwerking die inbreuk maakt op de AVG. Een verwerker is slechts aansprakelijk voor de schade wanneer hij niet heeft voldaan aan de verplichtingen uit de AVG die tot verwerkers gericht zijn, of als hij in strijd heeft gehandeld met de rechtmatige instructies van de verwerkingsverantwoordelijke. Tot slot geldt dat wanneer een verwerkingsverantwoordelijke of verwerker kan bewijzen dat hij op geen enkele wijze verantwoordelijk is voor de geleden schade, hij van aansprakelijkheid vrijgesteld wordt (art. 82 lid 3).



**Benieuwd wat wij
voor jouw organisatie
kunnen betekenen?**

Bezoek onze website voor
meer informatie.

www.ictrecht.nl/avg
020 - 663 1941