Ministerie van Justitie en Veiligheid

De Algemene verordening gegevensbescherming

wat betekent deze Europese wet voor jou als ondernemer?

Inleiding

De AVG geldt voor alle ondernemers.

Heb je een klantenbestand of een personeelsadministratie? Dan verwerk je persoonsgegevens. En als je persoonsgegevens verwerkt, moet je je houden aan de Algemene verordening gegevensbescherming (AVG). Deze nieuwe Europese wet regelt de bescherming van persoonsgegevens. De wet bepaalt wat je allemaal mag doen met persoonsgegevens en hoe je deze gegevens moet beschermen.

Doe je iets met persoonsgegevens? Volgens de AVG ben je ze dan ook bijna altijd aan het verwerken. Denk aan het verzamelen, opslaan, wijzigen, aanvullen of doorsturen van gegevens. Zelfs als je gegevens anoniem maakt of verwijdert, ben je ze aan het verwerken!

Gegevens zijn persoonsgegevens als ze gaan over personen die je kunt onderscheiden van alle andere personen. Dat noemen we een geïdentificeerde persoon. Je hebt een persoon bijvoorbeeld geïdentificeerd als je zijn voornaam en achternaam weet. Heb je iemand nog niet geïdentificeerd, maar kun je dat wel zonder al te veel moeite doen? Dan is die persoon 'identificeerbaar'. Denk daarbij bijvoorbeeld aan klantnummers die je kunt koppelen aan accountgegevens. Of een telefoonnummer waarvan je eenvoudig kunt achterhalen van wie het is. Ook dit zijn persoonsgegevens.

De AVG geldt voor verwerkingen die helemaal automatisch gaan, of voor een deel. Bijvoorbeeld verwerkingen in een computer of database. Maar de AVG geldt ook voor persoonsgegevens die in een bestand zitten of daarin komen, zoals papieren dossiers. De AVG geldt niet voor een enkele losse handgeschreven aantekening waar toevallig een naam van een persoon in staat.

Verwerkingen van persoonsgegevens die veel voorkomen: een klantenbestand of een personeelsadministratie bijhouden en gerichte mailings versturen per post of email (direct marketing).

De persoon van wie je persoonsgegevens verwerkt heet de betrokkene. Dat kan een klant, werknemer of contactpersoon zijn. Gegevens over bedrijven zijn geen persoonsgegevens, gegevens over eenmanszaken of van ZZP'ers daartegen wel.

Belangrijk!
Met deze beknopte brochure leggen we uit wat de AVG voor jou als ondernemer betekent. We leggen je uit wat de regels zijn en hoe je je eraan kunt houden. Wil je er zeker van zijn dat je voldoet aan de AVG? Verdiep je dan verder in de AVG of vraag een specialist om advies. Dit is vooral belangrijk als jouw verwerkingen ingewikkeld zijn. Of als je gevoelige of risicovolle persoonsgegevens verwerkt, zoals het burgerservicenummer (BSN) of medische gegevens. Onder het kopje 'Wil je meer weten?' vind je links naar websites en organisaties die je verder helpen.

Aan welke regels moet je je houden?

Aan welke regels moet je je precies houden? Dat hangt af van de rol die je hebt bij het verwerken.

- Bepaal jij dat er persoonsgegevens verwerkt gaan worden? Dan ben je een verwerkingsverantwoordelijke. De meeste regels van de AVG gelden voor jou.
- Verwerk je persoonsgegevens in opdracht van een ander? Dan ben je een verwerker.

Je kunt voor dezelfde verwerking niet tegelijkertijd verwerkingsverantwoordelijke én verwerker zijn.

Ben je verwerkingsverantwoordelijke of verwerker?

Bepaal je zelf hoe en waarom je persoonsgegevens verwerkt? Dan ben je de verwerkingsverantwoordelijke. Je besluit bijvoorbeeld om personeel aan te nemen en je houdt daarom een personeelsadministratie bij. Of je registreert klanten via een website.

Verwerkt jouw organisatie persoonsgegevens in opdracht van anderen? Doe je bijvoorbeeld de salarisadministratie van een ander bedrijf? Of bied je ruimte aan voor websites (hosting)? Dan ben je een verwerker.

Let op! Je kunt tegelijk verwerker en verwerkingsverantwoordelijke zijn. Niet van dezelfde verwerking, maar wel van verschillende verwerkingen. Doe je bijvoorbeeld de loonadministratie voor een ander bedrijf, dan ben je voor deze verwerking een verwerker. En heb je daarnaast je eigen personeelsadministratie, dan ben je daarvoor de verwerkingsverantwoordelijke.

Regels voor de verwerkingsverantwoordelijke

De AVG stelt de volgende belangrijke eis aan de verwerkingsverantwoordelijke:

Je mag alleen persoonsgegevens verwerken als dat rechtmatig, behoorlijk en transparant is.

Een verwerking kan alleen rechtmatig zijn als je je daarbij houdt aan deze twee regels:

- Je hebt duidelijk beschreven met welk doel je de gegevens verwerkt.
- Dat doel valt binnen één van de zes grondslagen die de AVG noemt. Deze grondslagen vind je op pagina 13 van deze brochure, onder 'Wanneer is je verwerking rechtmatig?'

Heb je het doel duidelijk beschreven en valt dat binnen één van de zes grondslagen in de AVG? Dan mag je de persoonsgegevens gebruiken, maar wel alleen voor dat doel. Dat heet doelbinding.

Een verwerking moet niet alleen rechtmatig, maar ook behoorlijk en transparant zijn. Daarom moet je je ook nog aan de regels houden die hieronder staan. Hoe je dat precies doet, lees je in het stappenplan op pagina 4.

Wat moet je altijd doen?

- Hou een overzicht bij van alle verwerkingen. Dat heet registerplicht.
- Vertel de betrokkene altijd dat jouw bedrijf zijn of haar persoonsgegevens verzamelt en verder verwerkt en leg uit welke rechten en plichten daarbij horen.
- Zorg ervoor dat de gegevens juist zijn.
- Zorg ervoor dat je niet méér gegevens verwerkt dan nodig. Dat noemen we dataminimalisatie.
- Beveilig de gegevens goed.
- Bepaal vooraf hoelang je de verwerkte persoonsgegevens gaat bewaren.
- Respecteer de rechten van de betrokkenen. Zie ook pagina 16: 'Welke rechten hebben betrokkenen?'
- Maak schriftelijke afspraken met je verwerker. Zie ook pagina 14: 'Huur ik wel of niet een verwerker in?'
- Denk bij het ontwerp van je product of dienst al na over de privacy van de betrokkenen en zorg dat de privacy altijd zo goed mogelijk beschermd is (privacy by design). Verzamel nooit meer gegevens dan nodig en stel een programma bijvoorbeeld standaard in op de hoogste privacybescherming (privacy by default).
- Je mag persoonsgegevens in principe alleen binnen de EU opslaan en verwerken. Zie ook pagina 16: 'Mag je gegevens naar het buitenland sturen?'
- Je moet met bewijzen en argumenten kunnen uitleggen hoe je aan de AVG voldoet.

Wat moet je doen in bepaalde gevallen?

- Zijn er data gelekt? Dan moet je dat melden bij de Autoriteit Persoonsgegevens en bij de betrokkene. Op pagina 7 vind je meer informatie over datalekken.
- Kan het zijn dat jouw verwerking een hoog risico oplevert voor de privacy van betrokkenen? Dan moet je daar eerst onderzoek naar doen. Zo'n onderzoek heet een Data Protection Impact Assessment (DPIA).
- Moet je een grote groep mensen observeren of bijzondere gegevens (zie pagina 14) van een grote groep mensen verwerken? Dan moet je een funtionaris gegevensbescherming (FG) aanstellen.
- Als je verwerkingen daar aanleiding toe geven, bijvoorbeeld omdat ze heel risicovol zijn, dan moet je een privacybeleid opstellen. In het beleid laat je zien hoe je aan de regels voor gegevensbescherming voldoet. Ook wanneer je niet verplicht bent om een privacybeleid op te stellen, is het verstandig een privacybeleid te hebben. Dan weet iedereen in je bedrijf hoe ze met persoonsgegevens om moeten gaan.

Regels voor de verwerker

Als verwerker verwerk je persoonsgegevens in opdracht van een verwerkingsverantwoordelijke. Dit betekent onder meer dat je je moet houden aan de schriftelijke instructies van de verwerkingsverantwoordelijke. Alle afspraken die de verwerkingsverantwoordelijke met je maakt, staan in de verwerkersovereenkomst. Zie ook pagina 16 Als verwerker moet je je aan die afspraken houden.

Verder gelden voor jou voor een deel dezelfde regels als voor de verwerkingsverantwoordelijke. Hoe je je aan deze regels kunt houden, vind je in het stappenplan op pagina 10 Dit zijn de regels:

Wat moet je altijd doen?

- Houd een overzicht bij van alle verwerkingen die je doet voor de verwerkingsverantwoordelijke. Dat noemen we registerplicht.
- Beveilig de persoonsgegevens goed.
- Je mag alleen andere verwerkers inschakelen als de verwerkingsverantwoordelijke je daar vooraf toestemming voor gegeven heeft.
- Je mag persoonsgegevens in principe alleen binnen de EU opslaan en verwerken.

Wat moet je doen in bepaalde gevallen?

- Zijn er data gelekt? Dan moet je dat zo snel mogelijk laten weten aan de verwerkingsverantwoordelijke.
- Vraagt de Autoriteit Persoonsgegevens je om ergens aan mee te werken? Dan moet je dat ook doen.
- Moet je een grote groep mensen observeren of bijzondere gegevens van een grote groep mensen verwerken? Dan moet je een functionaris gegevensbescherming (FG) aanstellen.

Aan de slag! Stappenplan voor de **verwerkingsverantwoordelijke.**

Bepaal je zelf hoe en waarom je persoonsgegevens verwerkt? Dan ben je de verwerkingsverantwoordelijke. De meeste regels uit de AVG gelden voor de verwerkingsverantwoordelijke. Volg het onderstaande stappenplan om te kunnen voldoen aan deze regels.

Stap 1: Bepaal hoe je persoonsgegevens verwerkt

1.1 Waar binnen je organisatie verwerk je persoonsgegevens?

Kijk naar alle processen en systemen in je bedrijf. Welke persoonsgegevens worden waar verwerkt? Bepaal dat voor jezelf. In een klantenbestand zitten bijvoorbeeld vaak NAW-gegevens, de aankoopgeschiedenis en financiële gegevens. Bepaal ook van wie je de gegevens gekregen hebt en aan wie je ze doorstuurt.

1.2 Voor welk doel verwerk je de persoonsgegevens?

Stel per verwerking het doel vast. Houd er rekening mee dat je één bestand voor meer doelen kunt gebruiken. Een klantenbestand gebruik je bijvoorbeeld niet alleen om contact te houden met je klanten. Je gebruikt het misschien ook om ze commerciële aanbiedingen te doen. Zorg dat je je doelen duidelijk omschrijft, zodat de betrokkene snapt wat je doet met de gegevens.

1.3 Hebben alle verwerkingen een wettelijke basis (een 'grondslag')?

Stel voor elk verwerkingsdoel een grondslag uit de AVG vast. Deze grondslagen vind je op pagina 13: 'Wanneer is het doel van je verwerking rechtmatig?'. Kun je geen grondslag vinden? Dan mag je de gegevens niet verwerken en moet je je bedrijfsprocessen aanpassen of stoppen met de verwerking. Kijk ook steeds of je wel écht alle gegevens nodig hebt voor je doel. Heb je bepaalde gegevens niet nodig? Dan moet je ze weggooien.

1.4 Hoelang mag je de gegevens bewaren?

Zijn de persoonsgegevens niet meer nodig voor je doelen? Ook dan moet je ze weggooien. Bepaal vooraf hoelang je persoonsgegevens bewaart. Sommige verwerkingen moet je binnen een wettelijke termijn verwijderen, bijvoorbeeld een personeelsdossier. Maar meestal moet je de termijn zelf bepalen.

1.5 Wil je gegevens naar het buitenland sturen?

Wil je de gegevens aan iemand doorgeven buiten de Europese Unie? Controleer dan eerst of dat mag. Zie hiervoor pagina 16: 'Mag je gegevens naar het buitenland sturen?'

1.6 Aan wie geef je de gegevens allemaal door?

Bepaal ook aan wie je de gegevens allemaal doorgeeft. Dat kunnen verwerkers zijn, die voor jou werken. Het kunnen ook andere verwerkingsverantwoordelijken zijn, die hun eigen doelen hebben met de persoonsgegevens.

Stap 2: Zet je verwerkingen in een register

Alles wat je hierboven hebt uitgezocht en beschreven, zet je in een register van verwerkingen. Hierin schrijf je in ieder geval per verwerking het volgende op:

- *je verwerkingsdoel*
- *de categorie personen van wie je gegevens verwerkt: klanten, werknemers en alle andere contacten*
- *de gegevens die je verwerkt*
- *aan wie je de gegevens allemaal doorgeeft*
- *hoelang je de gegevens bewaart*
- *wat je allemaal doet om de gegevens te beveiligen*

Met dit register houd je overzicht over alles wat er gebeurt met persoonsgegevens binnen je bedrijf. Zorg er daarom voor dat het register actueel blijft!

2.1

Stap 3: Zorg voor een zorgvuldige verwerking

3.1

Zorg goed voor de kwaliteit van de persoonsgegevens

Zorg ervoor dat de gegevens juist zijn en blijven. Dat doe je bijvoorbeeld door ze regelmatig te controleren.

3.2

Informeer de betrokkenen

Informeer alle betrokkenen van wie je persoonsgegevens verwerkt. Dat kun je bijvoorbeeld doen via een privacyverklaring die makkelijk te vinden is. Wil je betrokkene toestemming vragen voor de verwerking van zijn persoonsgegevens, informeer hem dan vooraf duidelijk over onder meer het doel en de verwerking waarvoor je toestemming vraagt, en meld ook dat hij zijn toestemming kan intrekken.

Beveilig de persoonsgegevens

Kijk welke risico's jouw verwerkingen kunnen veroorzaken voor betrokkenen. En pas je beveiliging daarop aan. Niet alleen je digitale beveiliging, maar ook de fysieke beveiliging van iemands bedrijf. Daarmee bedoelen we bijvoorbeeld controle bij de deur, kluisjes en andere beveiliging van gebouwen en ruimtes.

3.3

3.4

Meld datalekken

Zijn er persoonsgegevens gestolen? Ben je een laptop met persoonsgegevens kwijtgeraakt? Dan zijn er data gelekt. Een datalek moet je binnen 72 uur melden bij de Autoriteit Persoonsgegevens. Dat kun je doen via: datalekken.autoriteitpersoonsgegevens.nl. Soms moet je ook de betrokkenen informeren over het lek. Maak een duidelijk actieplan, zodat iedereen binnen het bedrijf weet wat hij of zij moet doen als er een datalek is.

3.5

Maak duidelijke afspraken met je verwerkers

Controleer of je een verwerkersovereenkomst hebt gesloten met je verwerkers. Heb je dat niet? Doe dat dan zo snel mogelijk. Wil je bepalen wie van jouw zakenpartners verwerkers zijn? Ga dan naar pagina 14, onder het kopje 'Huur ik wel of niet een verwerker in?'

3.6

Stel een functionaris voor gegevensbescherming (FG) aan

Moet je een grote groep mensen observeren of bijzondere gegevens van een grote groep mensen verwerken? Dan moet je een functionaris gegevensbescherming in dienst nemen of inhuren. Deze persoon heet ook wel een Data Protection Officer (DPO). Hij of zij adviseert je organisatie over de AVG en controleert of iedereen zich eraan houdt.

3.7

Onderzoek de risico's voor de privacy

Ontwikkel je een nieuwe dienst of een nieuw product? En verwerk je daarbij persoonsgegevens? Dan moet je vooraf inschatten welke risico's er zijn voor de privacy van betrokkenen. Voorbeelden van verwerkingen met een hoog risico zijn:

- *verwerking van medische gegevens van een grote groep mensen*
- *toezicht met camera's*
- *verwerkingen die je doet met nieuwe technologieën.*

Is het risico voor de privacy hoog? Dan moet je daar onderzoek naar doen met een Data Protection Impact Assessment (DPIA). Dit heet ook wel een Privacy Impact Assessment (PIA). In dat onderzoek schat je de risico's in voor de betrokkenen. En je bedenkt maatregelen om deze risico's te beperken.

3.8

Houd al bij het ontwerp rekening met privacy

Ontwikkel je een product of dienst? Of koop je een nieuw systeem? Bepaal dan altijd wat je moet doen om de privacy van personen te beschermen. Houd bijvoorbeeld in het ontwerp al rekening met de beveiliging en zorg er voor dat je gegevens niet direct koppelt aan een persoon als dat niet hoeft (pseudonimidering). Deze acties vallen onder privacy by design. Denk verder goed na welke gegevens je écht nodig hebt en zorg standaard voor privacybeschermende instellingen. Dat noemen we ook wel privacy by default. Laat je systemen kopen of bouwen? Schrijf deze eisen dan op als je om een offerte vraagt.

3.9

Organiseer een systeem om goed met verzoeken van betrokkenen om te gaan

Betrokkenen hebben onder andere recht op inzage, correctie en verwijdering van hun gegevens zie pagina 16: 'Welke rechten hebben betrokkenen?'. Organiseer een werkproces in je bedrijf waarmee je uitvoering kan geven aan deze rechten. Bepaal bij wie de verzoeken binnenkomen, wie ze behandelt en wie ze beantwoordt. Zorg ervoor dat deze medewerkers weten welke rechten betrokkenen hebben en hoe ze daarmee om moeten gaan.

3.10

Maak een document waarin het privacybeleid staat

Hoewel het niet altijd verplicht is, is het verstandig om voor je bedrijf een document te maken waarin staat hoe je omgaat met privacy en gegevensbescherming. Dat noemen we het privacybeleid. Schrijf daarin onder andere het volgende op:

- *Aan welke regels moeten de medewerkers zich houden?*
- *Wie neemt de beslissingen over het verwerken van persoonsgegevens?*
- *Wie controleert of iedereen zich aan de regels houdt?*

3.11

Vertel het personeel over de AVG

Zorg dat je personeel weet wat er in het privacybeleid en de AVG staat. Train alle medewerkers om persoonsgegevens te herkennen en leer ze de belangrijkste regels uit de AVG. Die regels vind je op pagina 2, onder 'Regels voor de verwerkingsverantwoordelijke'. Maak de medewerkers duidelijk waarom privacy zo belangrijk is. En leer ze waar ze zelf verantwoordelijk voor zijn als ze persoonsgegevens verwerken.

3.12

Zorg dat je verantwoording kunt afleggen

Je moet met bewijzen en argumenten kunnen uitleggen hoe je aan de AVG voldoet. Schrijf daarom op hoe je precies omgaat met persoonsgegevens. Leg in ieder geval het volgende vast:

- *al je verwerkingen (de registerplicht)*
- *rapporten van Data Protection Impact Assessments (DPIA)*
- *een overzicht van alle datalekken de toestemming die je hebt gekregen van betrokkenen*

Aan de slag! Stappenplan voor de **verwerker.**

Verwerk jij persoonsgegevens in opdracht van een andere organisatie? Dan ben je een verwerker. Volg het onderstaande stappenplan om je te houden aan de AVG.

Stap 1: Bepaal hoe je persoonsgegevens verwerkt

1.1

Welke persoonsgegevens verwerk je?

Kijk eerst goed welke persoonsgegevens van klanten je precies verwerkt, en hoe je dat doet.

1.2

Stuur je ook gegevens naar het buitenland?

Kijk ook of je al je gegevens binnen de Europese Unie opslaat of verwerkt. Wil je ook gegevens doorsturen naar iemand buiten de Europese Unie? Controleer dan eerst of dat mag. Zie hiervoor pagina 16: ‘Mag je gegevens naar het buitenland sturen?’

Stap 2: Zet je verwerkingen in een register

2.1

Zet je verwerkingen in een register. Schrijf het volgende op:

- *alle klanten voor wie je gegevens verwerkt*
- *alle verwerkingen die je doet voor deze klanten*
- *wat je allemaal doet om de gegevens te beveiligen*
- *of de gegevens binnen de Europese Unie blijven of niet*

Stap 3: Zorg voor een zorgvuldige verwerking

3.1

Beveilig de persoonsgegevens

Kijk hoe gevoelig de gegevens zijn die je verwerkt. En pas je beveiliging daarop aan. Niet alleen de digitale beveiliging, maar ook de fysieke beveiliging. Daarmee bedoelen we bijvoorbeeld controle bij de deur, kluisjes en andere beveiliging van gebouwen en ruimtes. Voor meer informatie zie ‘Wil je meer weten?’ op pagina 17. Kun je bepaalde gegevens niet goed beveiligen? Is er iets mis met de beveiliging? Of is er een datalek? Zeg dat dan meteen tegen de verwerkingsverantwoordelijke.

Sluit verwerkersovereenkomsten af

Controleer of je met elke klant een verwerkersovereenkomst hebt gesloten. Heb je dat niet gedaan? Doe dat dan zo snel mogelijk.

3.2

3.3

Maak afspraken met sub-verwerkers

Hoe voer je de verwerkingen precies uit? Werken er nog andere organisaties aan mee? Dan zijn dat sub-verwerkers. Ook met sub-verwerkers moet je schriftelijke afspraken maken. Zij moeten de gegevens van jouw klanten net zo goed beschermen als jij.

Stel een functionaris voor gegevensbescherming (FG) aan

Moet je een grote groep mensen observeren of bijzondere persoonsgegevens van hen verwerken? Dan moet je een functionaris voor gegevensbescherming (FG) in dienst nemen of inhuren. Deze persoon heet ook wel een Data Protection Officer (DPO). Hij of zij adviseert je organisatie over de AVG en controleert of iedereen zich eraan houdt. Je kunt een FG ook inhuren via een dienstverlener.

3.4

Maak een document waarin het privacybeleid staat

Maak voor je bedrijf een document waarin staat hoe je omgaat met privacy en gegevensbescherming. Dat noemen we het privacybeleid. Je bent als verwerker niet verplicht zo'n beleid te hebben, maar het is wel verstandig. Schrijf in het privacybeleid onder andere het volgende op:

- *Aan welke regels moeten de medewerkers zich houden?*
- *Wie neemt de beslissingen over de verwerking van persoonsgegevens?*
- *Wie controleert of iedereen zich aan de regels houdt?*

3.5

3.6

Vertel het personeel over de AVG

Zorg dat het personeel weet wat er in het privacybeleid en de AVG staat. Train alle medewerkers om persoonsgegevens te herkennen en leer ze de belangrijkste regels uit de AVG. Maak de medewerkers duidelijk waarom privacy zo belangrijk is. En leer ze waar ze zelf verantwoordelijk voor zijn als ze persoonsgegevens verwerken.

Wanneer is het doel van je verwerking rechtmatig?

Ben je verwerkingsverantwoordelijke? Dan moet je ervoor zorgen dat het doel van de verwerking rechtmatig is. En dat is alleen zo als je je houdt aan deze twee regels:

- *Je hebt duidelijk beschreven met welk specifiek doel je de gegevens verwerkt.*
- *Dat doel valt binnen één van de zes "wettelijke basissen" (grondslagen) die de AVG noemt.*

Dit zijn de zes grondslagen die de AVG noemt:

1. Je hebt de toestemming van de betrokkene.
Als je vooraf toestemming vraagt aan de betrokkene dan mag je de gegevens verwerken. Je moet wel heel duidelijk omschrijven waar je toestemming voor vraagt en dit moet goed zichtbaar zijn voor de betrokkene. De toestemming mag je bijvoorbeeld niet verstoppen in de algemene voorwaarden. Ook moet de betrokkene volledig vrij zijn om toestemming te geven. Een werknemer kan bijvoorbeeld in de meeste gevallen niet vrij toestemming geven, omdat hij of zij afhankelijk is van de werkgever. Houd er rekening mee dat de betrokkene de toestemming altijd kan intrekken! Je moet dan stoppen met de verwerking. Het intrekken van de toestemming moet net zo makkelijk zijn voor de betrokkene als het geven.

2. Je moet gegevens verwerken om een contract dat je hebt met de betrokkene uit te voeren.
Als je een contract sluit met de betrokkene en je moet daarvoor gegevens verwerken, dan kun je deze grondslag hanteren. Wanneer je bijvoorbeeld online boeken verkoopt dan heb je de adresgegevens van kopers nodig, anders kun je de boeken niet leveren.

3. Je bent wettelijk verplicht om de gegevens te verwerken.
Als de wet je verplicht om persoonsgegevens te verwerken, dan kun je deze grondslag gebruiken. De belastingwetgeving bijvoorbeeld verplicht je om persoonsgegevens van je personeel vast te leggen.

4. Je moet gegevens verwerken omdat dat van (acuut) levensbelang is voor de betrokkene of iemand anders.
Is het noodzakelijk om gegevens te werken om bijvoorbeeld iemands leven te redden? Dan kun je van deze grondslag gebruik maken. In de praktijk kun je deze grondslag bijna nooit voor gewone verwerkingen gebruiken.

5. Je moet gegevens verwerken om een taak van algemeen belang of openbaar gezag goed uit te kunnen voeren.
Deze grondslag is met name bedoeld voor overheden en organisaties met een publieke functie. De meeste bedrijven kunnen deze grondslag niet gebruiken.

6. Je moet gegevens verwerken voor je eigen belang en dat belang weegt zwaarder dan de privacy van de betrokkene.
Wil je deze grondslag gebruiken? Dan moet je jouw bedrijfsbelang beschrijven en onderbouwen waarom dat belang zwaarder weegt dan het privacybelang van de betrokkene. Beveiliging en fraudebestrijding kunnen bijvoorbeeld gerechtvaardigde belangen zijn.

Valt het doel van je verwerking binnen één van deze grondslagen? Dan mag je de persoonsgegevens verwerken (als je ook aan de overige eisen uit de AVG voldoet uiteraard).

Houd er rekening mee dat je de gegevens alleen mag gebruiken voor het doel waarvoor je ze hebt verzameld. Als je bijvoorbeeld iemands adres hebt gekregen voor de levering van een boek, dan mag je dat adres niet verkopen aan een ander bedrijf, want dat is niet het doel waarvoor je het adres verzameld hebt. Ook mag je niet meer gegevens verzamelen dan nodig om het doel te bereiken.

Let op!
Controleer goed of je verwerking echt past binnen één van de bovenstaande grondslagen. Verdiep je in wat die grondslagen precies inhouden. Meer hierover kun je vinden onder het kopje 'Wil je meer weten?' op pagina 17.

Bijzondere persoonsgegevens, strafrechtelijke gegevens en het burgerservicenummer (BSN)

Bijzondere persoonsgegevens zijn zéér gevoelig en daarom extra beschermd. Het gaat om de volgende gegevens:

- gegevens waaruit iemands ras of etnische afkomst blijkt
- gegevens waaruit iemands politieke voorkeur blijkt
- gegevens waaruit iemands godsdienst of levensovertuiging blijkt
- gegevens over iemands lidmaatschap van een vakbond
- iemands genetische gegevens
- iemands lichamelijke kenmerken, bijvoorbeeld iemands vingerafdruk of gezichtsscan.
- iemands medische gegevens
- gegevens over iemands seksueel gedrag of seksuele voorkeur

Het is verboden om deze bijzondere persoonsgegevens te verwerken. Maar er is wel een aantal uitzonderingen. Je mag bijvoorbeeld wel bijzondere persoonsgegevens verwerken als de betrokkene daar zelf duidelijk toestemming voor gegeven heeft of het wettelijk geregeld is.

Binnen bedrijven worden bijzondere persoonsgegevens met name verwerkt binnen de personeelsadministratie en de verzuimregistratie. De regels hiervoor veranderen met de AVG niet. Voor meer informatie zie ‘Wil je meer weten?’ op pagina 17.

Strafrechtelijke gegevens

Naast de bijzondere persoonsgegevens zijn ook strafrechtelijke gegevens zeer gevoelig. Ook deze gegevens zijn extra beschermd en mag je niet zomaar verwerken.

Het burgerservicenummer (BSN)

Voor het BSN gelden speciale regels. Dit nummer mag je alleen verwerken als je er wettelijk toe verplicht bent. Voor de loonbelasting moet je bijvoorbeeld verplicht het BSN van je medewerkers opslaan. Je kunt geen andere grondslagen aanvoeren om het BSN te verwerken dan de wettelijke plicht! Zelfs als de betrokkene toestemming heeft gegeven mag je het BSN niet verwerken als je daar niet wettelijk toe verplicht bent.

Verwerk je bijzondere persoonsgegevens, strafrechtelijke gegevens of het BSN? Gaat het niet om gangbare verwerkingen zoals bijvoorbeeld de personeelsadministratie of verzuimregistratie? Dan is het verstandig gespecialiseerd juridisch advies in te winnen.

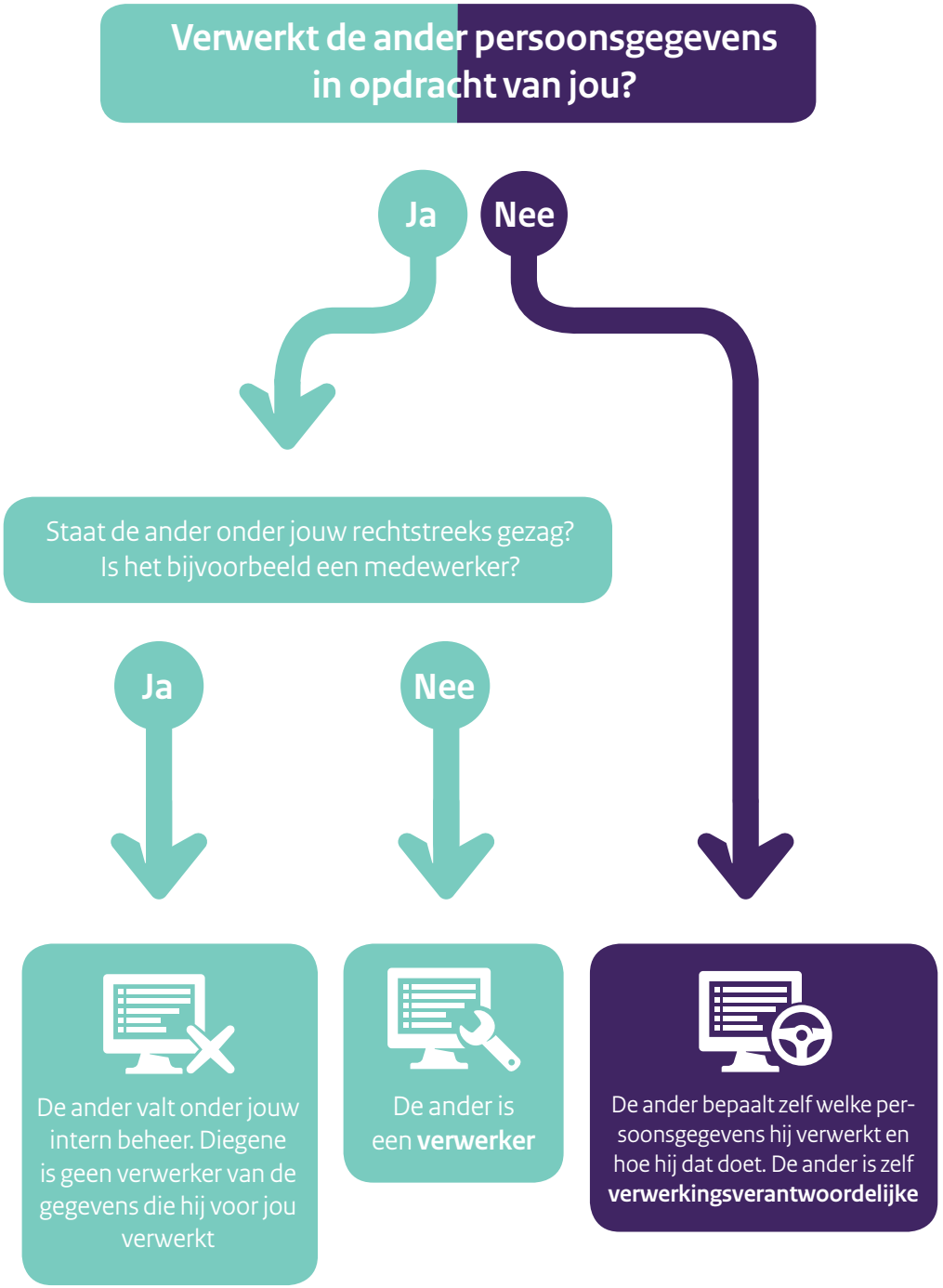
Huur ik wel of niet een verwerker in?

Doe je zaken met andere bedrijven of organisaties? En verwerken zij persoonsgegevens voor jou? Of stuur je persoonsgegevens aan hen door? Dan moet je bepalen of deze organisaties zelf verwerkingsverantwoordelijken zijn, of verwerkers voor jou.

Houd er rekening mee dat een ander alleen een verwerker kan zijn als hij niet onder jouw rechtstreeks gezag staat. Medewerkers bijvoorbeeld zijn geen verwerkers omdat zij onder jouw gezag staan.

Gebruik het schema hiernaast om te bepalen welke rol de ander heeft.

Het is niet altijd makkelijk om te bepalen of je zaken doet met een verwerkingsverantwoordelijke of met een verwerker. Wil je hulp om hierin de juiste keuze te maken? Ga dan naar pagina 17 van deze brochure. Onder het kopje ‘Wil je meer weten?’ vind je een paar handige links.



De verwerkersovereenkomst

De verwerkingsverantwoordelijke en de verwerker moeten hun afspraken schriftelijk vastleggen in een verwerkersovereenkomst. Daarin moet onder andere het volgende staan:

- De verwerker mag alleen iets doen op basis van schriftelijke instructies van de verwerkingsverantwoordelijke.
- De verwerker gebruikt een bepaald niveau van beveiliging.
- De gegevens blijven vertrouwelijk.
- De verwerker mag niet zomaar andere partijen (sub-verwerkers) inzetten voor zijn werk. Dat mag alleen als hij daar toestemming voor gekregen heeft.

Mag je gegevens naar het buitenland sturen?

Je mag persoonsgegevens niet doorgeven aan iemand buiten de Europese Unie (EU). Je mag gegevens bijvoorbeeld niet buiten de EU opslaan of ze daarnaar toe sturen. Wil je dit toch doen? Dan moet de EU dat land speciaal hebben aangewezen als een 'adequaat land'. Of je moet speciale bepalingen zetten in het contract met die buitenlandse organisatie. Meer weten? Kijk dan op pagina 17, onder het kopje 'Wil je meer weten?' of vraag advies aan een gespecialiseerd jurist.

Welke rechten hebben betrokkenen?

De personen van wie je gegevens verwerkt, noemen we betrokkenen. Dat kunnen klanten of zakelijke contacten zijn, maar het kunnen bijvoorbeeld ook je eigen medewerkers zijn. Betrokkenen hebben volgens de AVG verschillende privacyrechten:

Je moet een betrokkene altijd laten weten dat je persoonsgegevens van hem of haar verzamelt. Dit kun je bijvoorbeeld doen door een privacyverklaring op je website te zetten.

Heb je gegevens van een betrokkene verzameld? Dan mag de betrokkene jou vragen om de volgende dingen te doen:

- De persoonsgegevens laten zien die je van hem of haar verwerkt.
- De gegevens te verbeteren of aan te vullen.
- De gegevens te verwijderen. De betrokkene heeft in bepaalde gevallen het recht om vergeten te worden.
- Tijdelijk niets te doen met de persoonsgegevens. Houd ze alleen opgeslagen. Dit heet het recht op beperking.
- De gegevens digitaal door te sturen naar hem of haar, of naar een andere verwerkingsverantwoordelijke. Doe dat in een door de computer leesbaar formaat. Dit recht heet dataportabiliteit.
- Vind jij dat je een gerechtvaardigd belang hebt om persoonsgegevens te verwerken en de betrokkene is het daar niet mee eens? Dan mag de betrokkene daar bezwaar tegen maken.
- Maakt de betrokkene bezwaar tegen verwerkingen die je doet voor direct marketing? Dan moet je meteen met die verwerkingen stoppen.

Vraagt een betrokkene je iets op basis van zijn rechten? Dan ben je verplicht om binnen één maand te reageren. Alle communicatie met betrokkenen moet kort, begrijpelijk en in eenvoudige taal zijn.

Geautomatiseerde besluitvorming en profilering

Je moet oppassen met besluiten die volledig door de computer worden genomen, zonder dat daar nog een mens aan te pas komt. Denk bijvoorbeeld aan profilering. Dat is een techniek waarbij de computer mensen op basis van hun kenmerken indeelt in een bepaald profiel en op basis van dat profiel beslissingen neemt. Heeft zo'n automatisch besluit grote gevolgen voor iemands leven? Kun je iemand zo bijvoorbeeld afwijzen voor een lening of een baan? Dan mag je deze techniek niet zomaar gebruiken.

Wil je meer weten?

Meer over de AVG?

Twijfel je ergens over? Of wil je meer weten? Bijvoorbeeld over het doel van je verwerking? Of over het verschil tussen de verwerkingsverantwoordelijke en de verwerker? Dan kun je meer lezen op de volgende websites:

Website van de Rijksoverheid over de AVG: *www.rijksoverheid.nl/avg*

Website van de Autoriteit Persoonsgegevens over de AVG: *hulpbijprivacy.nl*

Jouw branchevereniging

Ben je lid van een branchevereniging? Dan kun je daar informatie en hulpmiddelen vinden voor jouw sector. Ook kun je daar vragen stellen over de AVG. Voor een overzicht van brancheverenigingen kun je terecht op de websites van MKB-Nederland en VNO-NCW: *www.mkb.nl/leden* *www.vno-ncw.nl/leden-vno*

Wil je je verder verdiepen in de AVG en wat de wet voor jou betekent? Lees dan de Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming.:*www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming*

Meer over beveiliging & meldplicht datalekken?

In de volgende dossiers en standaarden lees je meer over beveiliging van persoonsgegevens en meldplicht bij datalekken:

Dossier beveiliging van de Autoriteit Persoonsgegevens: *www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging*

De ISO 27001 en 27002 standaarden voor informatiebeveiliging: *www.nen.nl/NEN-Shop/Informatiebeveiliging-1.htm*

Dossier Meldplicht datalekken van de Autoriteit Persoonsgegevens: *www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken*

Meer over de functionaris voor gegevensbescherming?

Wil je meer informatie over de functionaris voor gegevensbescherming? Lees dan het Dossier functionaris voor gegevensbescherming van de Autoriteit Persoonsgegevens: *www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming*

Meer over gegevens naar het buitenland?

Wil je meer weten over gegevens versturen naar het buitenland? Lees dan het Dossier Internationaal gegevensverkeer van de Autoriteit Persoonsgegevens: *www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer*

Wil je weten welke landen 'adequaat' zijn? Kijk dan op deze website: *ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_nl*

Meer over het verwerken van gegevens van personeel?

Wil je meer weten over het verwerken van gegevens van het personeel en het gebruik van bijzondere persoonsgegevens, strafrechtelijke gegevens en het BSN? Lees dan het Dossier Werk en Uitkering van de Autoriteit Persoonsgegevens: *www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering*

Aan de inhoud van deze brochure kunt u geen rechten ontlenen.

Dit is een publicatie van
Ministerie van Justitie en Veiligheid

Tot stand gekomen met medewerking van
VNO-NCW en MKB-Nederland.

© 2018 Ministerie van Justitie en Veiligheid
Auteursrechten voorbehouden

Mei 2018| 104969