STAPPENPLAN AVG

IN 12 STAPPEN KLAAR VOOR DE NIEUWE PRIVACYWET

DIRK SMIT | FUN2DESIGN
Prinses Beatrixstraat 26
5151 GT DRUNEN

INHOUDSOPGAVE

INLEIDING

Per 25 mei 2018 zal de Algemene Verordening Gegevensbescherming (AVG) de huidige Wet bescherming persoonsgegevens (Wbp) vervangen en is de AVG in de gehele Europese Unie van toepassing. Dit betekent dat je bedrijf vanaf die datum aan de bepalingen in de AVG dient te voldoen.

De AVG brengt een aantal grote wijzigingen met zich mee. Zo zullen betrokkenen meer privacy rechten hebben en krijgen de organisaties die persoonsgegevens verwerken meer verplichtingen waar zij aan dienen te voldoen.

Daarnaast krijgt de Autoriteit Persoonsgegevens de mogelijkheid om een forse boete op te leggen op het moment dat een organisatie de bepalingen uit de AVG niet naleeft. Deze boete kan oplopen tot wel € 20 miljoen of 4% van de wereldwijde jaaromzet van een organisatie.

Gelet op de verplichtingen in de AVG en de stevige boetes die de Autoriteit Persoonsgegevens kan opleggen, is het voor jou van groot belang acties en maatregelen te treffen zodat je bedrijf eind mei voldoet aan de AVG.

Dit zijn de te nemen stappen:

1. Creëer bewustwording
2. Breng in kaart
3. Wat is het doel?
4. Stel een privacyverklaring op
5. Verdiep je in nieuwe rechten
6. Leg toestemming vast
7. Raak vertrouwd met nieuw begrippen
8. Voer een DPIA uit
9. Stel een functionaris aan
10. Bepaal toezichthouder
11. Stel overeenkomsten op
12. Registreer en documenteer

STAP 1. CREËER BEWUSTWORDING

Een van de belangrijkste onderdelen van de AVG is bewustwording. Bewustwording creëer je op een aantal manieren. Dit kan bijvoorbeeld door het inplannen van overleggen of workshops.

Je moet alleen wel weten wat de inhoud van de bewustwording moet zijn. Want wanneer je de AVG succesvol wil implementeren moeten alle medewerkers op de hoogte zijn van de veranderingen.

DE BELANGRIJKSTE WIJZIGINGEN OP EEN RIJ

- ✓ Activiteiten en gegevens vallen sneller onder de privacywet. Naast namen en adressen vallen nu ook IP-adressen, MAC-adressen, alle cookies en dergelijke onder de privacywetgeving.

- ✓ Regels m.b.t. transparantie van privacyverklaringen zijn aangescherpt. Wat wordt gedaan met privacygevoelige gegevens, waaronder ook interesseprofielen van websitebezoekers en klanten? Hoe kan men deze gegevens inzien, wijzigen of verwijderen moet duidelijk worden vermeld.

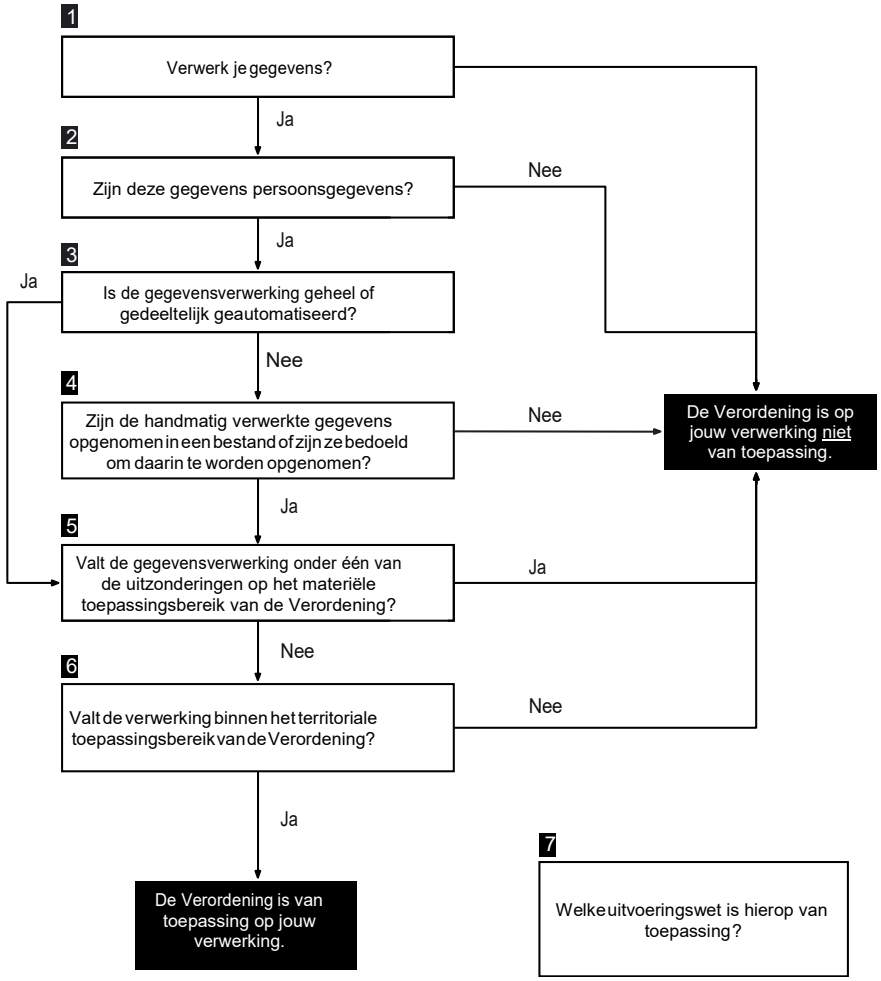
- ✓ Een verwerkersovereenkomst met data verwerkende partners en leveranciers is verplicht. Met alle leveranciers en partners aan wie privacygevoelige informatie wordt verstrekt, bijv. van websitebezoekers, dient een verwerkersovereenkomst te worden gesloten. Voor deze verstrekking van gegevens dient tevens toestemming te zijn gegeven.

- ✓ De wijze van gegevensverwerking moet worden gedocumenteerd. Alle verwerkingen van privacygevoelige gegevens dienen te worden gedocumenteerd, van de personeelsadministratie tot de abonnees op een nieuwsbrief.

- ✓ Eisen aan het gebruik van interesseprofielen worden strenger. Wanneer van bijv. bezoekers of klanten interesseprofielen worden bijgehouden, moet worden uitgelegd hoe dit gebeurt en met welk doel. Dit geldt ook voor het gebruik van cookies voor advertentiedoeleinden.

- ✓ De boetes bij overtreding worden gigantisch Bij overtreding van de AVG riskeert jouw organisatie boetes van 20 miljoen euro of max. 4% van de wereldwijde jaaromzet.

SCHEMA: IS DE VERORDENING OP JOU VAN TOEPASSING?



Bron van schema: Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid)

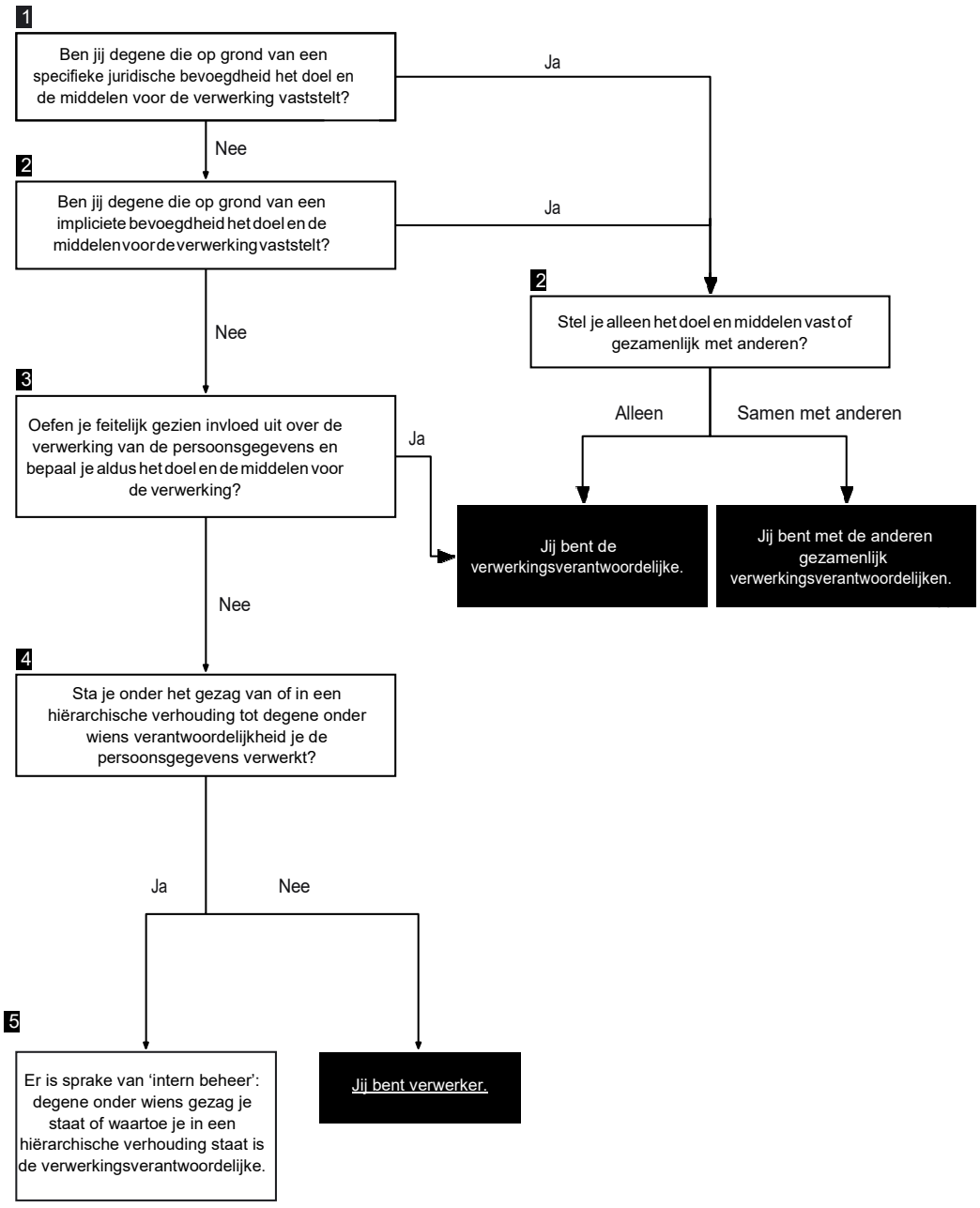
SCHEMA: WELKE UITVOERINGSWET IS VAN TOEPASSING?

Onderstaande schema laat voor veelvoorkomende situaties zien welke uitvoeringswetgeving van toepassing is (de Nederlandse Uitvoeringswet Algemene Verordening Gegevensbescherming of de uitvoeringswetgeving van een andere EU-lidstaat). Houd er 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

Bron van schema: Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid)

SCHEMA: BEN JIJ VERWERKINGSVERANTWOORDELIJKE OF VERWERKER?



Bron van schema: Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid)

STAP 2. BRENG IN KAART

Het is belangrijk om de persoonsgegevens die binnen je bedrijf worden verwerkt, in kaart te brengen, zodat je een start kunt maken met een zorgvuldige verwerking van deze persoonsgegevens.

De informatie die je deze stap verzamelt, vormt als het ware de basis voor de uitvoering van de stappen die nog volgen. Daarom is het van belang de volgende vragen te beantwoorden:

- Welke persoonsgegevens verwerk je binnen je bedrijf?
- Verwerk je bijzondere persoonsgegevens?
- Van welke categorie betrokkenen verwerk je persoonsgegevens?
- Met welk doel verwerk je persoonsgegevens? (zie stap 3)
- Door wie worden de persoonsgegevens verwerkt?
- Met wie deel je de persoonsgegevens en met welk doel deel je deze persoonsgegevens?
- Verschaf je informatie aan de betrokkene met betrekking tot de gegevensverwerking? (zie stap 6)
- Welke processen en protocollen gericht op de privacywetging zijn al binnen je bedrijf ingevoerd?
- Heb je al beveiligingsmaatregelen getroffen? (zie stap 4)
- Houd je al rekening met Privacy by design en Privacy by default? (zie stap 7)

Aan het eind van dit document vind je een lijst, waarin uitleg wordt gegeven over de genoemde begrippen.

STAP 3. WAT IS HET DOEL?

Stel vast wat het doel is en wat de grondslag is voor de gegevensverwerking

In de AVG zijn de navolgende voorwaarden opgenomen waaraan voldaan moet zijn om rechtmatig persoonsgegevens te verwerken:

Gerechtvaardigd doel

Allereerst moet je beschikken over een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel voor gegevensverwerking. De voorwaarde 'welbepaald' houdt in dat de doelomschrijving duidelijk moet zijn. Het moet tijdens het verzamelproces een kader bieden waaraan getoetst kan worden of de gegevens wel of niet nodig zijn voor dat doel.

Besteed zorgvuldig aandacht aan de doelomschrijving en vraag je bij iedere gegevensverwerking af of het verwerken van de persoonsgegevens noodzakelijk is voor het doel.

Nadat je gegevens hebt verzameld voor een bepaald doel, mag je deze gegevens ook gebruiken voor een ander doel dan waarvoor je heeft verzameld. Let op, je mag dat niet doen op een wijze die onverenigbaar is met het doel waarvoor de gegevens zijn verzameld.

Grondslag verwerking

Daarnaast moet je beschikken over één van de in de AVG genoemde grondslagen. Kort weergegeven zijn dit:

- Toestemming van de betrokkene
- Uitvoering van een overeenkomst

  Je mag de gegevens verwerken die noodzakelijk zijn voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of om maatregelen te nemen op verzoek van de betrokkene vóór de sluiting van een overeenkomst.

  Zo kan een online webshop geen pakket bezorgen conform de koopovereenkomst bij een klant zonder zijn naam en adres. Ook kan een werkgever het salaris van een werknemer conform de arbeidsovereenkomst niet uitbetalen zonder zijn bankrekeningnummer.
- Wettelijke verplichting

  Het is toegestaan ter uitvoering van een wettelijke verplichting persoonsgegevens te verwerken als dit noodzakelijk is. Een voorbeeld hiervan is dat de werkgever verplicht is op grond van de Wet op de Loonbelasting een kopie van het identiteitsbewijs van een werknemer in zijn administratie op te slaan.
- Vitaal belang

  Je mag persoonsgegevens verwerken als dit noodzakelijk is ter bescherming van de gezondheid van de betrokkene of een ander persoon. Zo mag een arts op de eerste hulp medische gegevens verwerken, voordat een behandelingsovereenkomst is gesloten.
- Algemeen belang

  Ter 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, mogen persoonsgegevens worden verwerkt. Voor het verwerken van persoonsgegevens vanuit deze grondslag dient een wettelijk doel te bestaan.

- Gerechtvaardigd belang

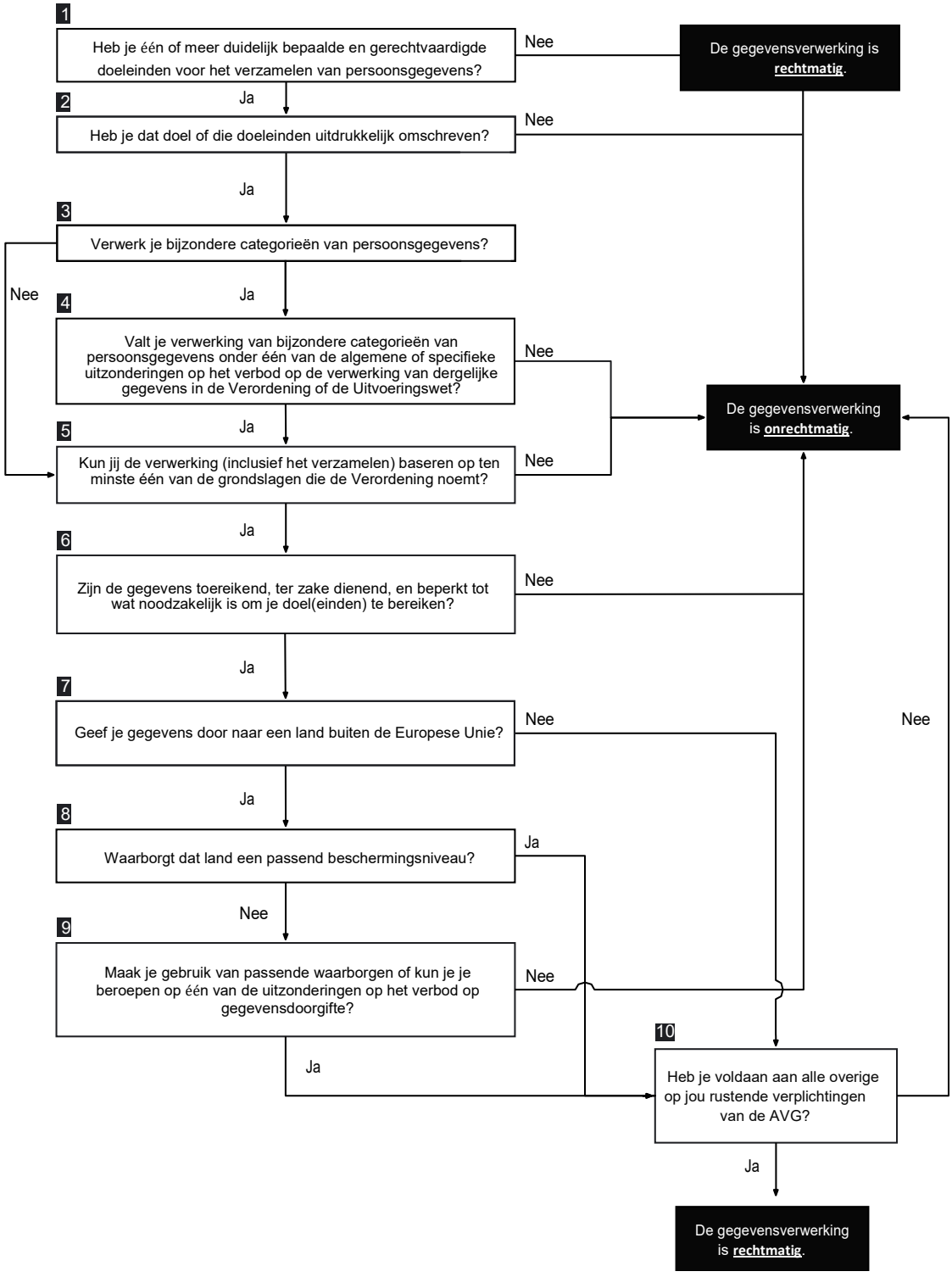
  Persoonsgegevens mogen worden verwerkt ter behartiging van een gerechtvaardigd belang, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene prevaleren. Bij het bepalen of sprake is van een dergelijk gerechtvaardigd belang, spelen de volgende criteria een rol:

  - het belang moet rechtmatig zijn;
  - het belang moet voldoende zeker en specifiek zijn;
  - het mag gaan om een algemeen belang of een specifiek commercieel belang;
  - de impact en risico's van de beslissingen die op basis van de data worden genomen en de emotionele impact daarvan, zoals irritatie, angst en chilling effect;
  - de aard van de data;
  - de manier en schaal van verwerking;
  - de redelijke verwachtingen van de betrokkene;
  - de status/aard van de betrokkene en de verantwoordelijke en/of
  - de waarborgen die je neemt voor het verwerken van persoonsgegevens.

Let op: voor de verwerking van bijzondere persoonsgegevens gelden aanvullende vereisten.

Gebruik deze informatie om het register verwerkingsactiviteiten op de juiste manier in te kunnen vullen.

SCHEMA: IS DE GEGEVENSVERWERKING GERECHTVAARDIGD



Bron van schema: Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid)

STAP 4. STEL EEN PRIVACYVERKLARING OP

Je moet de betrokkene heldere informatie geven over de persoonsgegevens die je verwerkt en voor welk(e) doel(en) je deze gegevens verwerkt. Dit wordt ook wel de informatieplicht genoemd.

De AVG verplicht je om de volgende informatie aan de betrokkene te verstrekken:

- de naam en contactgegevens van de verantwoordelijke;
- de contactgegevens van de FG (Functionaris Gegevensbescherming);
- het doel en de rechtsgrond van de verwerking van de persoonsgegevens;
- verwerk je de persoonsgegevens op grond van een gerechtvaardigde belang, dan moet je vermelden wat dit gerechtvaardigd belang is;
- de ontvangers of categorieën van ontvangers van de persoonsgegevens, als persoonsgegevens worden doorgegeven;
- de passende waarborgen die zijn genomen om de privacy in een ander land te waarborgen, als de persoonsgegevens buiten de Europese Unie worden doorgegeven;
- de bewaartermijn of de criteria ter bepaling van die termijn;
- de rechten van betrokkene, zoals het recht op inzage, wissen en rectificatie van de persoonsgegevens of beperking van de verwerking ervan;
- is de verwerking gebaseerd op toestemming van de betrokkene, dan dient de betrokkene op zijn recht, om de toestemming te allen tijde in te kunnen trekken, te worden gewezen;
- de mogelijkheid van de betrokkene om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn van niet-verstrekking van de gegevens en
- het bestaan van geautomatiseerde besluitvorming (inclusief ‘profiling’) en nuttige informatie over logica, belang en gevolgen daarvan voor de betrokkene.

Al deze informatie moet je in principe verstrekken op het moment dat de persoonsgegevens worden verzameld. Om aan deze informatieplicht te voldoen, kun je een privacyverklaring (ook wel privacy statement genoemd) opstellen. Deze privacyverklaring kun je bijvoorbeeld op je website plaatsen.

STAP 5. VERDIEP JE IN NIEUWE RECHTEN

Het opstellen van een privacybeleid, ook wel gegevensbeschermingsbeleid genoemd, is in bepaalde gevallen verplicht. Je bent verplicht een privacybeleid op te stellen als dat in verhouding staat tot je verwerkingsactiviteiten.

Bij deze beoordeling moet je rekening te houden met de:

- aard,
- de omvang,
- de context en
- het doel van de gegevensverwerking.

Ziekenhuizen, gemeenten en social mediabedrijven zijn vaak verplicht om een gegevensbeschermingsbeleid op te stellen.

Bent je niet verplicht om een privacybeleid op te stellen, dan kan het waardevol zijn om dit toch te doen. Onder de AVG heb je namelijk ook een verantwoordingsplicht. Dit betekent dat op jou de verantwoordelijkheid rust om te kunnen aantonen dat je organisatie zich aan de wet houdt. Door het opstellen van een privacybeleid, kunt je makkelijker aan de verantwoordingsplicht voldoen.

De AVG geeft niet precies aan wat in een privacybeleid dient te worden opgenomen.

De volgende onderdelen kunt je in het privacybeleid opnemen:

1. Dataminimalisatiebeleid

Met de komst van de AVG worden de beginselen Privacy by design en Privacy by default geïntroduceerd. Om te waarborgen dat binnen je bedrijf wordt gehandeld in overeenstemming met Privacy by design en Privacy by default, is het aan te raden om een dataminimalisatiebeleid te hanteren en hierin te omschrijven hoe je aan deze beginselen voldoet.

2. Beveiligingsbeleid

In dit deel beschrijf je welke beveiligingsmaatregelen je neemt om de persoonsgegevens te beveiligen.

3. Beleid datalekken

Het is belangrijk om te bepalen hoe je omgaat met een datalek.

Bepaal daarvoor:

1. welke stappen je neemt op het moment dat je bedrijf wordt geconfronteerd met een datalek,
2. welke informatie je moet verzamelen, vastleggen en/of melden en
3. wie binnen je bedrijf verantwoordelijk is voor de uitvoering van het beleid.

4. Beleid omtrent de rechten van betrokkenen

Onder de AVG krijgen betrokkenen verschillende rechten die zij kunnen uitoefenen. Het is belangrijk dat je je hierop voorbereidt, zodat je op tijd en op de juiste manier op een verzoek kan reageren. In dit deel van het beleid omschrijf je hoe je omgaat met een verzoek van een betrokkene om een van zijn rechten uit te oefenen.

Betrokkene beschikken over de volgende rechten:

Recht op informatie

De betrokkene dient op de hoogte te worden gesteld van onder andere het feit dat de verwerking van zijn persoonsgegevens plaatsvindt.

Recht op inzage

De betrokkene heeft allereerst het recht om te weten of je persoonsgegevens van hem verwerkt. Is dit het geval, dan heeft de betrokkene recht om inzage te verkrijgen in die persoonsgegevens (alsmede een kopie) en inzage te verkrijgen in bepaalde informatie, zoals:

- de verwerkingsdoeleinden;
- de betrokken categorieën van persoonsgegevens en
- aan wie de persoonsgegevens zijn of zullen worden verstrekt.

Recht op rectificatie ofwel correctie

De betrokkene heeft recht op rectificatie van hem betreffende onjuiste persoonsgegevens dan wel het recht een aanvullende verklaring te verstrekken wanneer de verwerking plaatsvindt op basis van onvolledige gegevens.

Recht op vergetelheid ofwel gegevenswissing

Dit houdt in dat je bedrijf in een aantal gevallen persoonsgegevens moet wissen als de betrokkene daarom vraagt. In de volgende situaties heeft de betrokkene recht op vergetelheid:

- als de persoonsgegevens niet meer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of verwerkt;
- als de betrokkene zijn eerder gegeven toestemming voor het gebruik van zijn gegevens intrekt;
- als de betrokkene bezwaar maakt tegen de verwerking;
- als de persoonsgegevens onrechtmatig zijn verwerkt;
- als je wettelijk verplicht bent om de gegevens na een bepaalde tijd te wissen en
- als de betrokkene jonger is dan 16 jaar en de persoonsgegevens zijn verzameld via bijv. een app of website.

Recht op beperking van de verwerking

De betrokkene heeft in bepaalde gevallen het recht om een beperking van de verwerking te verkrijgen. Een beperking van de verwerking houdt in dat de persoonsgegevens niet verwerkt en gewijzigd mogen worden.

Recht op gegevensoverdraagbaarheid ofwel dataportabiliteit

Dataportabiliteit kun je ook gegevensoverdraagbaarheid noemen. Onder de AVG hebben personen het recht hun persoonsgegevens over te dragen van de ene naar de andere organisatie. Dit houdt allereerst in dat de betrokkene het recht heeft om de persoonsgegevens die je van hem hebt in een gestructureerd, gangbaar en machineleesbaar formaat te verkrijgen (bijvoorbeeld CSV). Daarnaast biedt dit recht de betrokkene de mogelijkheid om op een eenvoudige manier zijn persoonsgegevens van de ene IT-omgeving naar de andere te verplaatsen, te kopiëren of door te sturen. Denk hierbij aan het overstappen naar een andere zorgverzekeraar of bank. Heeft u na het vertrek de persoonsgegevens van uw vertrekkende klant niet meer nodig? Dan dient u deze uiteraard in het kader van dataminimalisatie te verwijderen.

STAP 6. LEG TOESTEMMING VAST

Hoe vraag, krijg en registreer je toestemming?

Een van de grondslagen op basis waarvan je bedrijf persoonsgegevens kan verwerken is ‘toestemming’ van de betrokkene. De AVG stelt strenge eisen aan deze grondslag. Zo dient een toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig te zijn gegeven. Daarom is het van belang dat je de manier evalueert waarop je deze toestemming vraagt, krijgt en registreert. Controleer vervolgens of je aan de eisen in de AVG voldoet en pas zo nodig de werkwijze aan.

Toestemming kan worden gegeven door middel van een verklaring of een actieve handeling. Bij een actieve handeling kun je denken aan het ‘aanvinken’ van een leeg hokje op uw website. Let wel dat de toestemming niet geldig is als de betrokkene een op voorhand aangevinkt hokje op je website niet ‘uitzet’.

Een toestemming is ‘vrij’ gegeven als de betrokkene zijn toestemming kan weigeren of intrekken zonder (de vrees) dat dit nadelige gevolgen voor hem heeft. Volgens de AVG is geen sprake van ‘vrij gegeven toestemming’ als tussen jou en de betrokkene een machtsverhouding bestaat. Dit kan zich bijvoorbeeld voordoen in arbeidsrelaties. Bovendien is geen sprake van ‘vrij gegeven toestemming’ als de betrokkene alleen gebruik kan maken van een bepaalde dienst, als hij toestemming geeft voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

Voorbeeld

Een persoon wil op internet een leesboek bestellen. De boekhandel vraagt deze persoon toestemming te geven om naast zijn naam en adresgegevens, tevens informatie over bijvoorbeeld wie zijn werkgever is en hoe lang de persoon daar in dienst is te verwerken. In principe wordt deze toestemming geacht niet rechtsgeldig te zijn gegeven.

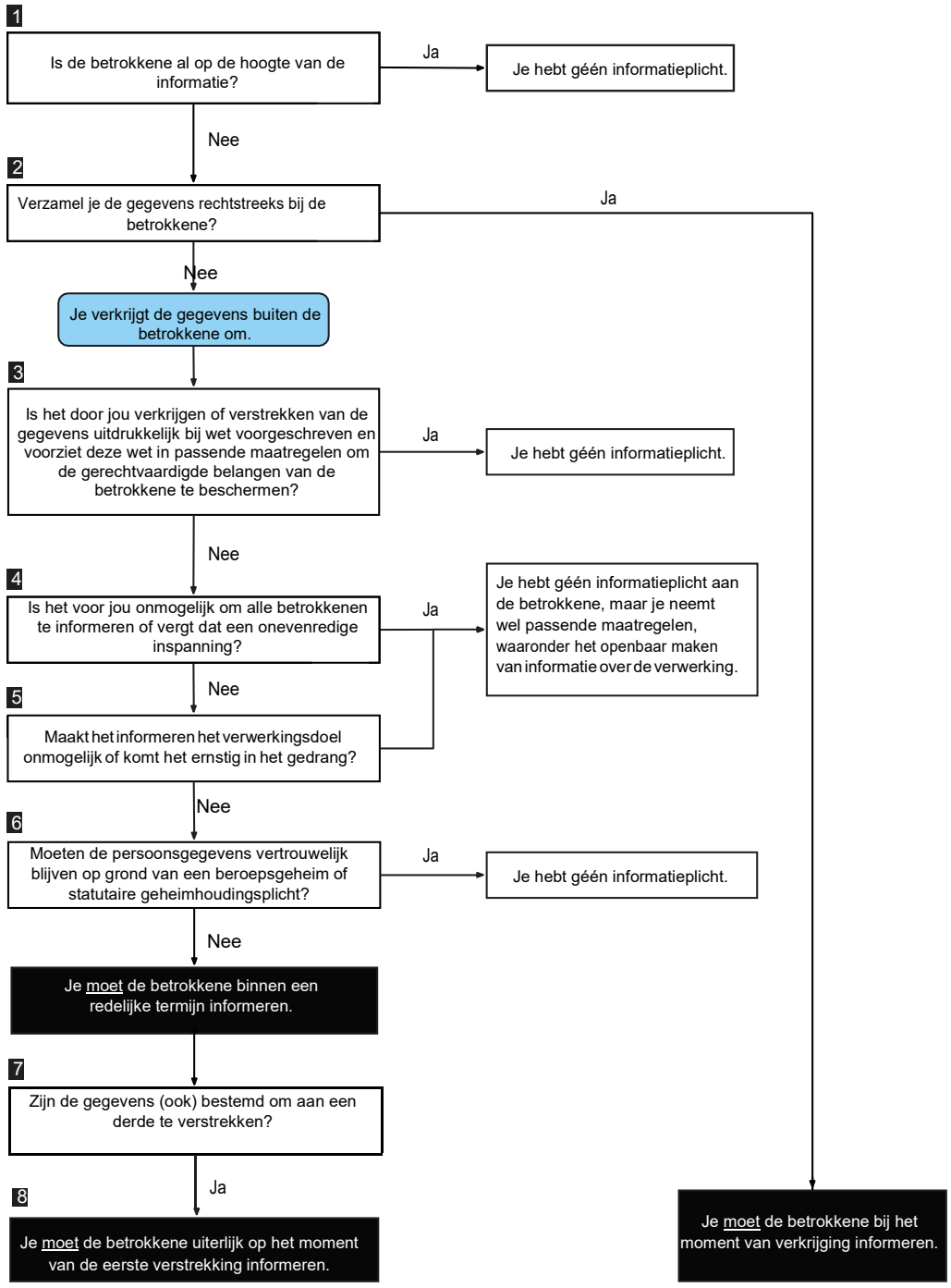
Een toestemming is ‘specifiek’ gegeven als duidelijk is voor welke specifieke verwerking(en), van welke persoonsgegevens en voor welk doel de toestemming is verleend.

Tot slot moet de toestemming ‘geïnformeerd’ zijn gegeven. Hierbij is het allereerst van belang dat de toestemming van betrokkene is gebaseerd op een juiste en volledige voorstelling van zaken. Daarnaast is van belang dat het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm wordt aangeboden en in een duidelijke en eenvoudige taal.

Verwerk je persoonsgegevens op basis van toestemming, dan moet je er rekening mee te houden dat de betrokkene op ieder moment zijn toestemming weer kan intrekken. Het intrekken van de toestemming moet voor de betrokkene net zo gemakkelijk zijn als het geven van toestemming. Bovendien moet je de betrokkene over dit recht informeren.

Ook moet je er op bedacht te zijn dat je op ieder moment moet kunnen aantonen dat je een geldige toestemming van de betrokkene heeft ontvangen om diens persoonsgegevens te mogen verwerken. Zorg er daarom voor dat je een verleende toestemming op een overzichtelijke wijze vastlegt.

SCHEMA: WANNEER MOET JE DE BETROKKENE INFORMEREN OVER EEN VERWERKING VAN PERSOONSGEGEVENS?



Bron van schema: Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid)

STAP 7. RAAK VERTROUWD MET NIEUWE BEGRIPPEN

Maak je bedrijf vertrouwd met de verplichte uitgangspunten van Privacy by Design en Privacy by Default. Ga na hoe je deze beginselen in je bedrijf kunt invoeren.

Privacy by default

Privacy by default houdt in dat je technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat je alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken. Met andere woorden, de standaardinstellingen op je website of in je applicatie dienen zo privacyvriendelijk mogelijk te zijn.

Een voorbeeld hiervan is dat je op je website het vakje 'ja, ik wil aanbiedingen ontvangen', niet vóóraf aanvinkt. Je moet de gebruiker het vakje actief laten aanvinken.

Privacy by design

Privacy by design houdt allereerst in dat je tijdens de ontwikkeling van producten en diensten aandacht besteed aan privacy verhogende maatregelen.

Bijvoorbeeld door extra (technische) maatregelen te nemen om de persoonsgegevens te beschermen, zoals anonimisering en pseudonimisering. De aandacht voor privacy dient tijdens de gehele levensduur van het systeem te blijven bestaan.

Daarnaast moet je rekening houden met dataminimalisatie. Dit betekent dat je zo min mogelijk persoonsgegevens verwerkt en alleen die gegevens verwerkt die noodzakelijk zijn voor het doel van de verwerking. Tevens moet je beoordelen hoe lang de gegevens bewaard mogen blijven.

In de praktijk betekent dit dat je allereerst dient te beoordelen of het verwerken van de persoonsgegevens écht nodig is voor het leveren van het product of de dienst. Vraag dus niet zomaar aan een klant naar de geboortedatum, maar sta stil bij de vraag of verkrijging van dit persoonsgegeven noodzakelijk is. Besluit je het persoonsgegeven toch te verwerken, dan is het van belang dat je beoordeelt hoe lang de verwerkte gegevens moeten worden bewaard. Denk tot slot na over privacy bevorderende maatregelen die je kunt nemen.

STAP 8. VOER EEN DPIA UIT

Wanneer een DPIA uitvoeren?

Bepaal of je verplicht bent om privacyrisico's van een gegevensverwerking in kaart te brengen d.m.v. een DPIA.

DPIA staat voor Data Protection Impact Assessment (DPIA). Een DPIA is een hulpmiddel om vooraf de privacyrisico's van een bepaalde gegevensverwerking in kaart te brengen en deze risico's vervolgens te verkleinen door maatregelen te treffen.

Niet voor elke gegevensverwerking hoef je een DPIA uit te voeren. Een DPIA is slechts verplicht als je gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. Je dient in ieder geval een DPIA uit te voeren op het moment dat je:

- systematisch en uitgebreid persoonlijke aspecten van personen beoordeelt, op grond waarvan besluiten worden genomen en waaraan voor de persoon rechtsgevolgen zijn verbonden. Daarbij kan gedacht worden aan profilering;
- op grote schaal bijzondere persoonsgegevens verwerkt;
- op grote schaal en stelselmatig mensen volgt in een openbare ruimte (bijvoorbeeld aan de hand van cameratoezicht).

Zijn bovenstaande punten niet op jouw situatie van toepassing, dan bepaal je zelf of je gegevensverwerking een hoog privacyrisico oplevert. Hierbij kun je als uitgangspunt nemen dat je een DPIA moet uitvoeren wanneer je verwerking aan twee of meer van de onderstaande negen criteria voldoet:

1. Je beoordeelt mensen op basis van persoonlijke kenmerken. Bijvoorbeeld een bank die de kredietwaardigheid van klanten bepaalt op basis van een kredietreferentiedatabank of een bedrijf dat gedrags- of marketingprofielen opstelt op basis van het gebruik van of de navigatie op zijn website.
2. Je neemt geautomatiseerde beslissingen die voor de betrokkene een rechtsgevolg of wezenlijk gevolg hebben. Bijvoorbeeld een besluit dat ervoor zorgt dat mensen worden uitgesloten of gediscrimineerd.
3. Er is sprake van stelselmatige en grootschalige monitoring van personen.
4. Je verwerkt bijzondere persoonsgegevens.
5. Je verwerkt op grote schaal persoonsgegevens.
6. Je koppelt of combineert verschillende databases met elkaar.
7. Je verwerkt gegevens van kwetsbare personen. Vraag je je af of er een machtsverhouding bestaat met degene van wie je gegevens verzameld, zoals kinderen, werknemers, geesteszieken en bejaarden.
8. Je maakt gebruik van een nieuwe technologie. Bijvoorbeeld het combineren van het gebruik van vingerafdrukken en gezichtsherkenning voor een toegangscontrole.
9. Je blokkeert door de gegevensverwerking een recht, dienst of contract van betrokkene. Een voorbeeld hiervan is een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand wil verstrekken.

Voorbeeld toepassing van bovenstaande criteria

Stel, je bedrijf monitort stelselmatig de activiteiten van haar werknemers, inclusief hun werkplek en interactiviteiten. In dat geval zijn mogelijk relevante criteria: ‘stelselmatige monitoring’ en ‘gegevens over kwetsbare betrokkene’. Dit betekent dat een DPIA gewenst is.

Inhoud DPIA

Een DPIA dient in ieder geval het volgende te bevatten:

- een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Beroep je je op een gerechtvaardigd belang als grondslag voor de verwerking, dan moet je dit belang ook opnemen in de beschrijving;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen. Dat houdt in dat je:
    - dient te beoordelen of het verwerken van persoonsgegevens op deze manier noodzakelijk is om je doel te bereiken en
    - of de inbreuk op de privacy van de betrokkenen niet onevenredig is in verhouding tot het doel.
- een beoordeling van de privacyrisico’s voor de betrokkenen;
- de beoogde maatregelen om:
    - de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en
    - aan te tonen dat je aan de AVG voldoet.

STAP 9. STEL EEN FUNCTIONARIS AAN

Verplichte of vrijwillige functionaris gegevensbescherming?

Onder de AVG kan het zijn dat je verplicht bent om een functionaris voor de gegevensbescherming (FG) aan te stellen. De FG wordt gezien als een functionaris die binnen je bedrijf toezicht houdt op de toepassing en naleving van de AVG.

Het aanstellen van een FG is verplicht als je:

- een overheidsinstantie of publieke organisatie bent. Denk hierbij aan de rijksoverheid en zorg- en onderwijsinstellingen;
- vanuit je kerntaak op grote schaal individuen regelmatig en stelselmatig observeert;
- je vanuit je kerntaak bezighoudt met het op grote schaal verwerken van bijzondere persoonsgegevens.

Val je niet onder de verplichtstelling, dan kun je vrijwillig een FG aanstellen. Dit kan interessant zijn voor je bedrijf, omdat een FG je organisatie ondersteuning biedt bij bijvoorbeeld het in kaart brengen van de risico's bij het verwerken van persoonsgegevens.

Een vrijwillig aangestelde FG moet zich aan dezelfde regels en kaders te houden als een verplichte FG. Dit betekent onder andere dat de vrijwillig ingestelde FG hetzelfde takenpakket heeft als de verplichte FG.

Als alternatief voor het instellen van een vrijwillige FG is het ook mogelijk:

- een werknemer in dienst te nemen of
- een adviseur in te huren die zich met de bescherming van persoonsgegevens bezighoudt.

Heeft deze persoon een andere functienaam, positie en takenpakket dan de FG, dan gelden de wettelijke regels voor de FG niet.

Taken van de functionaris gegevensbescherming

De FG heeft een aantal taken die hij verplicht dient uit te voeren. Allereerst informeert en adviseert de FG je bedrijf over je verplichtingen uit de AVG en andere privacywetgeving en houdt de FG toezicht op de naleving en toepassing van die verplichtingen. Daarnaast adviseert de FG je over het uitvoeren van een Data Protection Impact Assessment (DPIA). Meer informatie over het DPIA komt aan bod in stap 8. Ook is de FG de contactpersoon voor je bedrijf bij de Autoriteit Persoonsgegevens en werkt de FG samen met de Autoriteit Persoonsgegevens.

Je kunt met de FG afspreken dat hij ook andere werkzaamheden verricht zoals het:

- maken van inventarisaties van gegevensverwerkingen;
- bijhouden van meldingen betreffende datalekken;
- afhandelen van vragen en klachten van mensen binnen en buiten de organisatie en
- ontwikkelen van intern beleid.

Bevoegdheden van de functionaris gegevensbescherming

Een FG kan geen sancties opleggen. De FG heeft echter wel bepaalde bevoegdheden. Zo moet je de FG tijdig betrekken bij alle aangelegenheden die te maken hebben met de bescherming van persoonsgegevens. Dit betekent bijvoorbeeld dat je de FG onmiddellijk dient te raadplegen op het moment dat zich een datalek heeft voorgedaan.

Daarnaast moet je de FG toegang geven tot persoonsgegevens en verwerkingsactiviteiten. Het is dus belangrijk dat de FG ruimtes mag betreden, zaken mag onderzoeken en informatie en inzage krijgt.

Tot slot is het van belang dat je de FG de benodigde middelen ter beschikking stelt voor het vervullen van zijn taken. Denk hierbij aan het verschaffen van voldoende financiële middelen en tijd, zodat hij zijn taken naar behoren kan uitvoeren.

Waarborgen: geen instructies en geen ontslag voor de functionaris gegevensbescherming

Allereerst mag je de FG bij de uitvoering van de taken geen instructies geven over hoe hij bepaalde aangelegenheden moet behandelen. Bijvoorbeeld hoe de FG een klacht dient te onderzoeken en wanneer de FG de Autoriteit Persoonsgegevens moet raadplegen.

Hoe stelt u een functionaris gegevensbescherming aan?

De AVG stelt verschillende eisen aan de FG. Het is belangrijk dat u bij het aanstellen van de FG controleert of aan de volgende eisen wordt voldaan.

1. de FG dient voldoende deskundig te zijn en over voldoende professionele kwaliteiten te beschikken om zijn taken uit te kunnen voeren. Dit betekent dat de FG onder andere:
    - ervaring en kennis heeft van de AVG en andere privacywetgeving;
    - verstand heeft van IT en beveiliging van gegevens en ook
    - kennis heeft van de organisatie en de sector waarin hij actief is.
2. Het is van belang dat de FG geen conflicterend belang heeft. Een conflicterend belang doet zich bijvoorbeeld voor als de FG binnen de organisatie een functie in het hogere management uitvoert (bijvoorbeeld: hoofd van Human Resources, hoofd van de IT-afdeling en Chief Executive).

In principe mag je ieder personeelslid dat voldoet aan de eisen van de AVG tot FG benoemen. Laat diegene dan wel een opleiding tot FG volgen om zo de juiste kennis op te doen.

Je kunt echter ook een externe FG inhuren en met diegene een dienstverleningsovereenkomst overeenkomen.

Heb je een FG aangesteld, neem de contactgegevens van de FG dan op in een privacyverklaring. Meer informatie over de privacyverklaring volgt in stap 4. Maak daarnaast de contactgegevens van de FG bekend bij de Autoriteit Persoonsgegevens.

STAP 10. BEPAAL TOEZICHTHOUDER

De AVG gaat uit van de zogeheten onestopshop-regel. Dit houdt in dat als je een grensoverschrijdende gegevensverwerking uitvoert, je maar met één privacytoezichthouder zaken hoeft te doen. Deze toezichthouder wordt de ‘’leidend toezichthouder’’ genoemd.

Is het relevant om te bepalen wie leidend toezichthouder is?

Het bepalen van de leidend toezichthouder is alleen relevant als je een grensoverschrijdende verwerking van persoonsgegevens uitvoert.

In de navolgende twee gevallen is sprake van een grensoverschrijdende verwerking:

1. Als je bedrijf gegevens verwerkt in verschillende landen. Dit betekent bijvoorbeeld dat wanneer je bedrijf een vestiging heeft in Nederland en Duitsland en in het kader van haar activiteiten in beide landen persoonsgegevens verwerkt, dit als grensoverschrijdende verwerking wordt gezien;
2. Als de verwerking die je bedrijf uitvoert voor de betrokkene wezenlijke gevolgen heeft in meer dan één lidstaat (of dat dit waarschijnlijk is).

Welk leidend toezichthouder?

De leidend toezichthouder is in principe de toezichthouder van de lidstaat waar je bedrijf is gevestigd. Heb je meerdere vestigingen in de EU, dan moet je bepalen welke vestiging je hoofdvestiging is.

Voor de verwerkingsverantwoordelijke is de hoofdvestiging de plaats waar je centrale administratie in de EU is gelegen. Dit is anders als de beslissingen over het doel en de middelen van verwerkingen van persoonsgegevens worden genomen in een andere vestiging. Dan is dit de hoofdvestiging.

Voor de verwerker is de hoofdvestiging de plaats waar je centrale administratie in de EU is gelegen. Heb je geen centrale administratie, dan is de hoofdvestiging de vestiging waar de voornaamste verwerkingsactiviteiten plaatsvinden.

Er kunnen zich gevallen voordoen waarin er meer dan een leidend toezichthouder is. Dit is bijvoorbeeld het geval wanneer je bedrijf verschillende grensoverschrijdende gegevensverwerkingen uitvoert en de beslissingen daarover in verschillende landen worden genomen.

STAP 11. STEL OVEREENKOMSTEN OP

Verwerkingsovereenkomsten

Met de komst van de AVG wijzigen de definities:

- ‘bewerker’ in ‘verwerker’ en
- ‘bewerkersovereenkomst’ in ‘verwerkersovereenkomst’.

Een verwerker is een derde die ten behoeve van je bedrijf persoonsgegevens verwerkt. Hierbij kun je denken aan het bedrijf dat je salarisadministratie verzorgt. Je bent verplicht om met de verwerker een overeenkomst aan te gaan.

In deze overeenkomst moet je in ieder geval de volgende informatie opnemen:

- Algemene beschrijving

  De verwerkersovereenkomst bevat een algemene beschrijving van onder meer de volgende punten:

  a. de inhoud,

  b. de duur,

  c. de aard en het doel van de verwerking,

  d. het soort persoonsgegevens,

  e. de categorieën van betrokkenen en

  f. de rechten en verplichtingen van de verwerkingsverantwoordelijke.

- Instructies verwerking

  De verwerking van persoonsgegevens door de verwerker mag slechts plaatsvinden op basis van schriftelijke instructies van de verwerkingsverantwoordelijke.

- Geheimhoudingsplicht

  Aan de verwerker moet een geheimhoudingsplicht worden opgelegd.

- Beveiliging

  De verwerker moet passende technische en organisatorische maatregelen treffen om de verwerking te beveiligen. Voorbeelden hiervan zijn:

  a. pseudonimisering en versleuteling van persoonsgegevens,

  b. permanente informatiebeveiliging,

  c. herstel van beschikbaarheid,

  d. toegang tot gegevens bij incidenten en

  e. regelmatige beveiligingstesten.

- Subverwerkers

  De verwerker mag geen subverwerker(s) inschakelen zonder voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. De verwerker legt in een verwerkersovereenkomst dezelfde verplichtingen op aan de subverwerker, als de verplichtingen die de verwerker heeft richting de verwerkingsverantwoordelijke.

- Verplichtingen privacyrechten

  De verwerker zal de verwerkingsverantwoordelijke bijstand verlenen bij het vervullen van diens plicht, als betrokkenen hun privacyrechten willen uitoefenen. Het gaat om privacyrechten zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit.

- Nakomen verplichtingen verwerkingsverantwoordelijke

  De verwerker verleent de verwerkingsverantwoordelijke bijstand bij het uitoefenen van diens verplichtingen, zoals het melden van datalekken, het uitvoeren van een data protection impact assessment en bij een voorafgaande raadpleging.

- Gegevens verwijderen

  Eindigt de verwerkingsovereenkomst, dan dient de verwerker alle gegevens te verwijderen of aan de verwerkingsverantwoordelijke terug te bezorgen, tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.

- Audits

  De verwerker dient de verwerkingsverantwoordelijke alle informatie ter beschikking te stellen die nodig is om te controleren of hij zich als verwerker aan de hierboven genoemde verplichtingen houdt. Daarnaast dient de verwerker mee te werken aan audits.

Het is belangrijk dat jouw overeenkomsten aan bovenstaande punten voldoen. Breng daarom in kaart welke organisaties voor jou persoonsgegevens verwerken en of je met deze organisatie(s) een overeenkomst hebt gesloten. Controleer vervolgens of de overeenkomst voldoet aan de AVG en pas waar nodig de overeenkomst aan of sluit nieuwe verwerkingsovereenkomsten.

STAP 12. REGISTREER EN DOCUMENTEER

Register verwerkingsactiviteiten

In een aantal gevallen bent je verplicht een register van verwerkingsactiviteiten op te stellen. Of je een verwerkingsregister moet opstellen, hangt af van de omvang van je bedrijf en het type gegevens dat je verwerkt.

Organisatie of onderneming met 250 of meer medewerkers

Heb je 250 of meer medewerkers in dienst, dan moet je een register van de verwerkingsactiviteiten opstellen.

Organisatie of onderneming met minder dan 250 medewerkers

Heb je minder dan 250 medewerkers in dienst, dan hoef je in principe geen verwerkingsregister op te stellen. Behalve als je persoonsgegevens verwerkt:

- die een hoog risico inhouden voor de rechten en vrijheden van personen van wie je persoonsgegevens verwerkt en/of
- waarvan de verwerking niet incidenteel is en/of
- die vallen onder de categorie bijzondere persoonsgegevens, zoals godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Ook als je niet verplicht bent een register van verwerkingsactiviteiten op te stellen, kan het verstandig zijn dit wel te doen. De AVG legt namelijk de verantwoordelijkheid bij jou om aan te tonen dat je aan de privacyregels voldoet. Het opstellen van dit register biedt je ondersteuning bij het voldoen aan de verantwoordingsplicht.

Inhoud verwerkingsregister

De wet schrijft voor dat de volgende gegevens in het verwerkingsregister moeten worden opgenomen:

- De naam en de contactgegevens van:
  - je bedrijf of de vertegenwoordiger van je bedrijf;
  - eventuele gezamenlijke verwerkingsverantwoordelijken;
  - de functionaris voor gegevensbescherming.
- De verwerkingsdoeleinden.
- Een beschrijving van de categorieën van betrokkenen van wie je gegevens verwerkt.
- Een beschrijving van de categorieën van persoonsgegevens die je verwerkt.
- De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt.
- Deel je gegevens met een derde land of een internationale organisatie, dan moet je dit aangeven.
- Indien mogelijk, de datum waarop je de persoonsgegevens moet wissen.

  De AVG bepaalt dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is voor de doeleinden waarvoor het is verzameld. Een concrete bewaartermijn wordt in de AVG niet gegeven. In een aantal andere wetten, worden wel specifieke bewaartermijnen voorgeschreven. Een kopie van het ID-bewijs van een werknemer bijvoorbeeld, dient de werkgever vijf jaar te bewaren na einde dienstverband.

Ook bestaat er een aantal algemene richtlijnen. Zo mogen persoonsgegevens van sollicitanten in principe tot maximaal vier weken na het einde van de sollicitatieprocedure worden bewaard en de arbeidsovereenkomsten van werknemers mogen in principe tot maximaal twee jaar na het einde van het dienstverband worden bewaard.

- Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die je hebt genomen om persoonsgegevens die je verwerkt te beveiligen.

VOORBEELD: OVERZICHT VERWERKINGSACTIVITEITEN

	Verwerkingsactiviteit		Activiteit identificatie:	xxxxxx
Beschrijving van de activiteit				
Naam verwerkingsactiviteit				
Activiteit identificatie	xxxxxx			
Aanmaakdatum				
Datum laatste wijziging				

Verantwoordelijken	Voor- en achternaam	Adres	Postcode	Woonplaats	Land	Email	Telefoon
Verwerkingsverantwoordelijke							
Functionaris gegevensbescherming							
Vertegenwoordiger verwerkingsverantwoordelijke							
Mede verwerkingsverantwoordelijke(n)							
Mede verwerkingsverantwoordelijke(n)							
Mede verwerkingsverantwoordelijke(n)							

Doel van de verwerking	
Primair doel	
Secundair doel 1	
Secundair doel 2	
Secundair doel 3	
Secundair doel 4	
Secundair doel 5	

Veiligheidsmaatregelen	
Technische maatregelen	
Organisatorische maatregelen	

Categorieën van persoonsgegevens	Omschrijving	Opslaglocatie(s)	Toegangsrechten	Grondslag	Bewaartermijn
Burgerlijke staat, identiteit, identificatie van gegevens, foto's					
Het persoonlijke leven (lifestyle, gezinssituatie, etc.)					
Economische en financiële informatie (inkomen, financiële status, fiscale status, etc.)					
Digitale gegevens (IP adres, logs, enz.)					
Locatiegegevens (reizen, GPS-gegevens, GSM, etc.)					

Categorieën bijzondere gegevens (gevoelig)	Omschrijving	Opslaglocatie(s)	Toegangsrechten	Grondslag	Bewaartermijn
Gegevens waaruit de raciale of etnische afkomst blijkt					
Informatie omtrent politieke opvattingen					
Gegevens waaruit de godsdienstige of levensbeschouwelijke overtuiging blijkt					
Vakbondsgegevens					
Genetische gegevens					
Biometrische gegevens					
Medische gegevens / gezondheid					
Gegevens met betrekking tot seksleven of seksuele geaardheid					
Gegevens met betrekking tot strafrechtelijke veroordelingen of delicten					
Uniek nationaal identificatienummer (BSN nummer)					

Categorieën van betrokkenen	Omschrijving
Betrokkenen	
Betrokkenen	
Betrokkenen	
Betrokkenen	

Categorieën van ontvangers binnen de EU	Omschrijving	Type ontvanger	Land	Garanties (contract en versie)	Locatie van contract
Ontvanger					
Ontvanger					
Ontvanger					
Ontvanger					

Categorieën van ontvangers buiten de EU	Omschrijving	Type ontvanger	Land	Garanties (contract en versie)	Locatie van contract
Ontvanger					
Ontvanger					
Ontvanger					
Ontvanger					

Register datalekken

Er is sprake van een datalek op het moment dat er een inbreuk plaatsvindt op de beveiliging van persoonsgegevens. Dat is onder andere het geval als iemand toegang krijgt tot persoonsgegevens of persoonsgegevens openbaar toegankelijk worden zonder dat dit de bedoeling is.

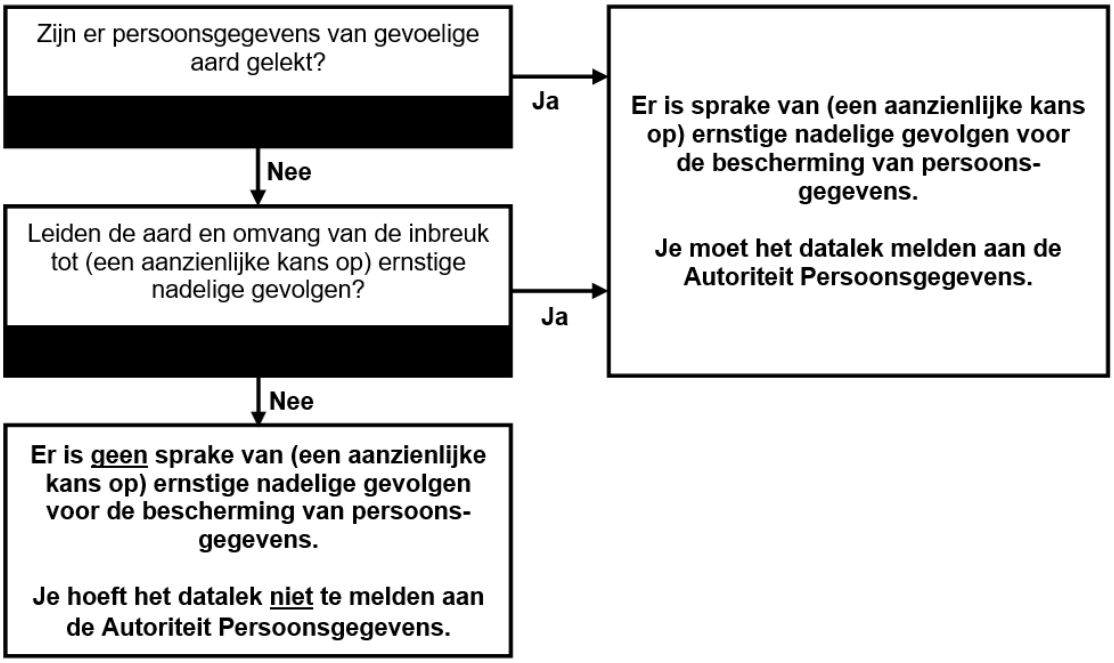
Als sprake is van een datalek, moet je dit zo spoedig mogelijk te melden aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De melding moet als het kan binnen 72 uur nadat u kennis heeft genomen van het datalek plaat te vinden. Is het niet mogelijk zijn om de melding binnen 72 uur te doen, dan moet je bij de melding aangeven waarom de melding langer heeft geduurd.

Op het moment dat het datalek waarschijnlijk ook resulteert in een hoog risico voor de rechten en vrijheden van de betrokkene, dan moet je de betrokkene ook op de hoogte te stellen.

Naast het melden van een datalek, moet je een datalek ook registreren. Het is van belang de volgende informatie per datalek op te nemen in het register:

- de feiten en gegevens over de aard van het datalek;
- de categorieën van de getroffen betrokkenen en persoonsgegevens en indien mogelijk het aantal betrokkenen;
- de gevolgen van het datalek;
- de genomen maatregelen om het datalek aan te pakken;
- of het datalek is gemeld aan de Autoriteit Persoonsgegevens en
- of het datalek is gemeld aan de betrokkene(n).

SCHEMA: MOET IK EEN DATALEK MELDEN?



BEGRIPPENLIJST

Sommige begrippen hebben net iets meer uitleg nodig:

Betrokkene
De betrokkene betreft degene op wie een persoonsgegeven betrekking heeft.

Bijzondere persoonsgegevens
In de AVG worden bepaalde persoonsgegevens als ‘bijzonder persoonsgegeven’ aangemerkt. Bijzondere persoonsgegevens zijn alle persoonsgegevens die informatie verschaffen over onder meer:

- iemands ras of etnische afkomst,
- politieke opvattingen,
- religieuze of levensbeschouwelijke overtuigingen,
- lidmaatschap van een vakbond,
- biometrische gegevens (denk aan vingerafdrukken),
- gezondheid en
- seksuele leven.

Categorie betrokkenen
Denk bijvoorbeeld aan werknemers, opdrachtgevers, klanten, bezoekers of patiënten.

Categorieën van persoonsgegevens
Bijvoorbeeld het Burgerservicenummer, NAW-gegevens, telefoonnummers, e-mailadressen, camerabeelden of IP-adressen.

Grote schaal
Kijk, om te bepalen of je bedrijf op grote schaal persoonsgegevens verwerkt, naar de volgende criteria:

- het aantal betrokkenen (de mensen van wie je gegevens verwerkt);
- de hoeveelheid gegevens die je verwerkt;
- de duur van de gegevensverwerking en
- de geografische reikwijdte van de verwerking.

Een voorbeeld van grootschalige gegevensverwerking is een vervoersmaatschappij die reisinformatie verwerkt van mensen die met het openbaar vervoer reizen. Ook kun je denken aan een ziekenhuis dat in het kader van de regelmatige bedrijfsvoering patiëntgegevens verwerkt.

Een voorbeeld van een verwerking die niet als grootschalig is aan te merken, is de verwerking van patiëntgegevens door een individuele arts.

Gezamenlijke verwerkingsverantwoordelijken

Wanneer je samen met een andere organisatie de doeleinden en middelen van de verwerking bepaalt, wordt je beide als verwerkingsverantwoordelijke aangemerkt.

Gezamenlijke verantwoordelijkheid voor gegevensverwerkingen komt bijvoorbeeld voor bij samenwerking tussen rechtspersonen binnen een concernverband.

Kerntaken

Tot de kerntaak van een organisatie vallen de belangrijkste handelingen die nodig zijn om de doelen van de organisatie te bereiken. Ook wanneer de verwerking van gegevens een onlosmakelijk onderdeel van de werkzaamheden van de onderneming is, kan er worden gesproken van een kerntaak.

Voorbeeld: de kerntaak van een ziekenhuis is het bieden van gezondheidszorg. Een ziekenhuis is echter niet in staat veilige en effectieve gezondheidszorg te bieden zonder medische gegevens, zoals de medische dossiers van patiënten, te verwerken. Daarom dient het verwerken van deze gegevens als één van de kerntaken van een ziekenhuis gezien te worden en moeten ziekenhuizen FG's aanwijzen.

Een ander voorbeeld is een beveiligingsbedrijf dat een aantal winkelcentra en openbare gelegenheden bewaakt. De kerntaak van het bedrijf is bewaking, wat onlosmakelijk is verbonden met het verwerken van persoonsgegevens. Derhalve dient ook dit bedrijf een FG aan te wijzen.

De verwerking van persoonsgegevens die ondersteunend is aan de bedrijfsvoering, zoals voor de salarisadministratie, valt buiten de kernactiviteiten en wordt gezien als nevenactiviteit.

Persoonsgegevens

Een persoonsgegeven is elk gegeven waarmee een natuurlijke persoon kan worden geïdentificeerd. Een natuurlijk persoon is iemand van vlees en bloed, die rechten en plichten heeft. Een persoonsgegeven gaat dus niet over gegevens betreffende een organisatie.

Voorbeelden van persoonsgegevens zijn:

- iemands naam,
- adres,
- woonplaats,
- telefoonnummer en
- functie.

Een e-mailadres is vaak (ook) een persoonsgegeven. Daarbij is het van belang dat een persoonsgegeven niet alleen informatie in geschreven tekst betreft, maar tevens in beeld en geluid. Denk hierbij aan cameratoezicht en geluidsopnames van telefoongesprekken.

Processen en protocollen

Denk onder andere aan een proces gericht op inzage of verwijdering van persoonsgegevens en een protocol datalekken.

Pseudonimisering

Voorbeeld: het vervangen van de voor- en achternaam van de betrokkene door een aan hem of haar toegewezen dossiernummer.

Rechtsgevolgen

Het gevolg dat door het recht aan bepaalde feiten of handelingen wordt verbonden.

Regelmatig en stelselmatig observeren

Dit omvat alle vormen van opsporing en profilering. Bijvoorbeeld:

- het beheren van een telecommunicatienetwerk,
- het uitvoeren van marketingactiviteiten op basis van persoonsgegevens en
- het profileren van mensen voor het maken van een risicobeoordeling.

Verwerker

Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Dit betekent dat de verwerker niet het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerkingsdoeleinden

De reden waarom je bepaalde persoonsgegevens verwerkt. Bijvoorbeeld het verzamelen van e-mailadressen met het doel: een nieuwsbrief verspreiden. Een ander voorbeeld is het registreren van een bankrekeningnummer om salaris over te maken.

Verwerkingsverantwoordelijke

Degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt

Verwerkt / verwerking

Een verwerking van persoonsgegevens betreft elke bewerking of een geheel van bewerkingen met betrekking tot een persoonsgegeven. Hieronder valt in ieder geval het:

- verzamelen,
- vastleggen,
- ordenen,
- bewaren,
- bijwerken,
- wijzigen,
- opvragen,
- raadplegen,
- gebruiken,
- verstrekken door middel van doorzending,
- verspreiding of enige andere vorm van terbeschikkingstelling,
- samenbrengen,
- met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.