Dit stappenplan hoort bij de brochure De AVG - wat betekent deze Europese wet voor jou als ondernemer?

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 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.

1.6 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?'

Stap 2: Zet je verwerkingen in een register

2.1

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!

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.

3.3

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.

3.4

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*