



De Resultaatbepalers

Stappenplan AVG

Stap 1

Je begint het proces met het doorlezen van de gratis meegeleverde brochures en handleiding die beschikbaar zijn gesteld door de Autoriteit Persoonsgegevens. Verder lees je het [AVG in het mkb Informatieblad](#). Zo raken jij (en je medewerkers) bekend met de AVG. Het creëert bewustwording en je leert de rechten van betrokkenen kennen. Dit zijn de eerste 2 stappen binnen het door de Autoriteit Persoonsgegevens opgestelde 10 stappenplan. Vervolgens inventariseer je welke persoonsgegevens binnen je organisatie/bedrijf nu worden vastgelegd ('verwerkt') en waar, bijvoorbeeld aan de hand van de het document [AVG 0-meting](#). Ook kun je gebruik maken van de [AVG-Regelhulp](#) (klik) via website van de Autoriteit Persoonsgegevens. Maak aan de hand daarvan een [Verwerkingsregister](#). Neem daarin op hoe en door wie, waarvoor en met wie deze gegevens worden gedeeld en hoe lang de gegevens worden bewaard. Inventariseer ook de risico's en welke maatregelen er nu worden getroffen om die af te dekken. Het is belangrijk om het verwerkingsregister continu up-to-date te houden. Met het bijhouden van het verwerkingsregister voldoe je aan stap 3 van het 10 stappenplan van de Autoriteit Persoonsgegevens.

Stap 2

Op basis van het verwerkingsregister toets je per gegevensstroom of de bestaande gegevensverwerking voldoet aan de nieuwe privacyregels of dat er onacceptabele risico's bestaan. Voor veel bedrijven zal gelden dat stap 4 van het 10 stappenplan van de Autoriteit Persoonsgegevens, een Data protection impact assesment (DPIA) niet nodig is. Deze is alleen nodig bij beoogde gegevensverwerking met waarschijnlijk een hoog privacyrisico. Lees in dit geval het onderdeel [Data protection impact assesment](#) (klik) op de website van de Autoriteit Persoonsgegevens. Heb je het idee dat je wel een DPIA moet uitvoeren, schakel dan een AVG-specialist in voor begeleiding.

Stap 3

Stel vast of en zo ja, welke aanpassingen er nodig zijn binnen de bestaande verwerkingsprocessen. Maak hiervoor een plan van aanpak. Op basis van dit plan van aanpak ga je aan de slag om de bestaande verwerkingsprocessen te verbeteren. Zorg er voor dat ze passen binnen de AVG. Op deze manier rond je stap 5 van het 10 stappenplan van de Autoriteit Persoonsgegevens af. Vervolgens stel je vast of er een functionaris voor de gegevensbescherming (FG) benodigd is binnen je organisatie/bedrijf. Voor veel bedrijven zal een FG niet nodig zijn. Bezoek de website van de Autoriteit Persoonsgegevens [Functionaris voor de gegevensbescherming](#) (klik) om dit voor jezelf te bevestigen.

Stap 4

Stel een [privacy- en beveiligingsbeleid](#) op en bespreek dit met eventuele medewerkers. Informeer eventuele medewerkers ook door bijvoorbeeld de brochures en handleidingen en/of het AVG in het mkb Informatieblad toe te sturen. Het is van belang dat je organisatie/bedrijf gaat handelen volgens de AVG.

Stap 5

Informeer klanten, leveranciers en dienstverleners van wie persoonsgegevens worden verwerkt en stel een privacyverklaring op. Plaats de privacyverklaring op je website en verwijst bij nieuwe overeenkomsten en opdrachten naar de privacyverklaring van jouw organisatie/bedrijf. Gebruik je algemene voorwaarden. Ga dan na of deze ook een update nodig hebben. Daarnaast is het van belang om het cookiebeleid op je website te laten plaatsen. Laat de documenten doornemen en plaatsen door je website beheerder.

Stap 6

Informeer ook eventuele medewerkers over hun rechten als werknemer. Neem dit op in een apart protocol. Wanneer dit voor jouw organisatie/bedrijf aan de orde is overleg je dit met de organisatie die de loonadministratie verwerkt. Het privacy- en beveiligingsbeleid met betrekking tot werknemers wordt op deze wijze onderdeel van het arbeidscontract.

Stap 7

Stel een Instructie meldplicht datalekken op en zorg er voor dat een datalekregister (een (digitale) map met ingevulde formulieren) wordt bijgehouden. Wanneer er sprake is van een datalek, gebruik dan het Formulier registratie datalek om dit te registreren. Hiermee voldoe je aan stap 7 van het 10 stappenplan van de Autoriteit Persoonsgegevens.

Stap 8

Stel vast of je organisatie/bedrijf een verwerker is voor opdrachten. Kortom, verwerk je persoonsgegevens voor een andere organisatie of bedrijf. Stel in dat geval een verwerkersovereenkomst op en stuur deze aan opdrachtgevers. Zorg er voor dat deze getekend retour worden gezonden.

Stap 9

Jouw organisatie/bedrijf zal ook leveranciers hebben die persoonsgegevens van jouw organisatie/bedrijf verwerken. Stel een verwerkersovereenkomst op met deze eventuele externe partijen (de verwerkers of soms sub-verwerkers) die worden ingeschakeld. Met derden die geen verwerker zijn maar wel inzage hebben in de persoonsgegevens regel je een geheimhoudingsverklaring voor leveranciers. Zo voldoe je aan stap 8 van het 10 stappenplan van de Autoriteit Persoonsgegevens.

Stap 10

Als laatste stap beoordeel je of jouw organisatie/bedrijf is gevestigd in meerdere EU-landen of in meerdere EU-landen impact heeft. Is dat het geval dan zoek je uit onder welke toezichthouder je valt. Voor de meeste organisaties/bedrijven zal dit de Autoriteit Persoonsgegevens zijn. Dit is onderdeel van stap 9 van het 10 stappenplan van de Autoriteit Persoonsgegevens. Verder stel je voor je organisatie/bedrijf vast of je toestemming nodig hebt voor de gegevensverwerkingen van je betrokkenen. De AVG stelt namelijk strengere eisen aan deze toestemming. Je evalueert of de manier waarop je toestemming vraagt, krijgt en registreert toereikend is. Het is verplicht om aan te kunnen tonen dat je geldige toestemming hebt van betrokkenen om de persoonsgegevens te verwerken. Tot slot evalueer je jaarlijks het privacybeleid, voer je waar nodig aanpassingen door en actualiseer je indien nodig het verwerkingsregister. Hiermee voldoe je aan de laatste stap van het 10 stappenplan van de Autoriteit Persoonsgegevens.

Benodigde documenten

- AVG 0-meting
- Verwerkingsregister
- Privacy- en beveiligingsbeleid
- Cookiebeleid website
- Privacyverklaring, privacy- en beveiligingsbeleid website
- Formulier registratie datalek
- Instructie melden datalek
- Geheimhoudingsverklaring voor leveranciers
- Verwerkersovereenkomst