Met 7 stappen voldoe je aan de privacywet

Over de Algemene verordening gegevensbescherming (AVG) is al veel geschreven. De wet is sinds 25 mei van toepassing, maar veel ondernemingen hebben hun privacybeleid nog (lang) niet op orde. Franchiseadvocaat Remy Albers heeft een stappenplan gemaakt om aan de nieuwe regels te voldoen.

Tekst **Remy Albers**

In mijn praktijk sta ik veelal ondernemers en franchiseketens uit het mkb bij en de wijze waarop zij de AVG benaderen, varieert van aan de ene kant totale stress tot - en dit is verreweg de grootste groep - een 'het zal wel loslopen'-houding.

Hoewel de Autoriteit Persoonsgegevens vermoedelijk niet direct op de stoep zal staan bij de gemiddelde cafetariahouder, is het wel van belang dat ook u kunt aantonen dat u de privacy van uw klanten (en werknemers) serieus neemt. Om u daarbij te helpen, heb ik hieronder een stappenplan opgenomen.

1 Breng alle gegevensverwerkingen in kaart

Vermoedelijk zijn er al veel meer processen binnen je bedrijf waarbij je persoonsgegevens verwerkt, dan je op voorhand vermoedt. Enkele voorbeelden:

- Je hebt personeel in dienst.
- Je ontvangt gegevens van sollicitanten.
- Je geeft klantenkaarten uit of registreert op een andere wijze klantgegevens in het kader van loyaliteitsprogramma's.
- Je verstuurt een nieuwsbrief.
- Je neemt bestellingen aan op naam.
- Je bezorgt bestellingen.
- Je hebt een beveiligingscamera.

2 Stel de grondslagen voor de verwerkingen vast

Voor het verwerken van persoonsgegevens heb je een verwerkingsgrondslag nodig. Dat kunnen er zes zijn, waarbij de meest voorkomende zijn:

- Toestemming van de betrokkene.
- De verwerking van de gegevens is nodig voor het uitvoeren van de overeenkomst (bijvoorbeeld het bezorgen van een bestelling).

- Een wettelijke verplichting (bijvoorbeeld fiscale verplichtingen).

3 Stel bewaartermijnen vast

Bepaal hoe lang je de persoonsgegevens bewaart. Hiervoor bestaan geen harde normen, maar voor veel verwerkingen kan wel worden aangesloten bij het vrijstellingsbesluit in de vorige Wet bescherming persoonsgegevens. Enkele voorbeelden:

- Gegevens sollicitanten: 4 weken.
- Beelden beveiligingscamera's: 4 weken.
- Verzuimgegevens: 2 jaar.

Voor sommige gegevens gelden ook wettelijke bewaartermijnen, bijvoorbeeld:

- Salarisafspraken en arbeidsvoorwaarden: 7 jaar.
- Loonbelasting en identiteitsbewijzen: 5 jaar.
- Debiteuren- en crediteurenadministratie: 7 jaar.

4 Bepaal of je verwerkersovereenkomsten moet aangaan

Nadat je de gegevensverwerkingen in kaart hebt gebracht, is het van belang om vast te stellen of je in aanraking komt met verwerkers die in jouw opdracht persoonsgegevens verwerken. Denk aan boekhouders of leveranciers van (cloud) software, waaronder CRM- of kassasystemen, waarin persoonsgegevens worden verwerkt. Met verwerkers moet je een verwerkersovereenkomst sluiten waarin je onder meer afspraken maakt over de doeleinden van de verwerking, geheimhouding en de beveiliging van persoonsgegevens.

5 Stel een verwerkingsregister op

Vooralsnog zijn alleen ondernemingen boven 250 medewerkers verplicht een verwerkingsregister bij te houden, tenzij sprake is van risicovolle verwerkingen, verwerking van gevoelige persoonsgegevens of het verwerken van persoonsgegevens op structurele basis. Aan dit laatste criterium zal welhaast elke onderneming in het mbk voldoen, reden waarom zij (vooralsnog) verplicht zijn om een verwerkingsregister bij te houden.

Een register kan worden bijgehouden in een Excelbestand en daarin dient de volgende informatie worden opgeslagen:

- Identiteit en contactinformatie van de verwerkingsverantwoordelijke.
- De doeleinden voor gegevensverwerking.
- Een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens.
- De voorgenomen categorieën ontvangers.
- Een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie.
- De voorgenomen bewaartermijnen.
- Een algemene beschrijving van de beveiligingsmaatregelen.

> ER ZIJN VEEL MEER PROCESSEN WAARBIJ JE **PERSOONSGEGEVENS VERWERKT**, DAN JE OP VOORHAND VERMOEDT

6 Ontwikkel privacybeleid

Vorm een privacybeleid, mede aan de hand van de informatie die je in de bovenstaande stappen hebt verzameld. Stel ook protocollen op voor medewerkers. Zo is het voor medewerkers én de Autoriteit Persoonsgegevens duidelijk hoe je met privacy omgaat. Hiervoor gelden geen vormvereisten, maar het is aan te bevelen om diverse protocollen op te stellen. Op jou als verantwoordelijke rusten namelijk diverse verplichtingen waarbij je binnen een bepaalde termijn een handeling dient te verrichten. Bijvoorbeeld ten aanzien van je meldplicht in het kader van datalekken (binnen 72 uur) of je verplichtingen ten aanzien van de rechten van betrokken (binnen 4 weken). Daarom is het raadzaam dat de procedures voor jou en je medewerkers duidelijk zijn.

7 Informeer klanten

Informeer klanten hoe je met privacy omgaat door middel van een privacyverklaring, ook wel privacy statement genoemd. Op grond van de AVG moet je klanten hierover informeren op het moment dat je de persoonsgegevens verzamelt. Dat betekent dat je, bijvoorbeeld bij het plaatsen van een bestelling of een contactverzoek op je website, de klant moet wijzen op uw privacyverklaring.

In de privacyverklaring moet ten minste de volgende informatie zijn opgenomen:

- Identiteit en contactinformatie van de verwerkingsverantwoordelijke.
- Doel en de grondslag voor de verwerking.
- Informatie omtrent het doorsturen van de persoonsgegevens naar een land buiten de EU, indien van toepassing.
- De bewaartermijn, of de criteria waarmee de bewaartermijn bepaald wordt.
- De rechten van de betrokkene (inzage, verwijdering, beperking, rectificatie, bezwaar, dataportabiliteit).
- Je moet de betrokkene wijzen op het recht om zijn toestemming voor de verwerking in te trekken, indien de verwerking hierop is gebaseerd.
- Je moet de betrokkene wijzen op zijn recht om een klacht in te dienen bij de toezichthouder. **SK**

Remy Albers is franchiseadvocaat bij Ludwig & Van Dam Advocaten
albers@ludwigvandam.nl