FIN ADVOCATEN FISCALISTEN
Debbemeerstraat 14
2131 HE Hoofddorp
info@finaf.nl
023 3030730
www.finaf.nl

HANDBOEK AVG SPRINTWERKT B.V.

Hoofddorp, 9 juli 2018

Opgesteld door:

FIN ADVOCATEN FISCALISTEN

I. Algemeen

De Algemene Verordening Gegevensbescherming (AVG) vormt de nieuwe privacywetgeving, die op 25 mei 2018 van kracht wordt in de EU. De belangrijkste veranderingen die de AVG met zich meebrengt zijn de versterking en uitbreiding van privacyrechten van uw klanten en relaties, meer verantwoordelijkheden voor organisaties en stevige bevoegdheden voor alle Europese privacytoezichthouders.

II. Belangrijkste punten AVG

Hierna zullen de belangrijkste punten en onderwerpen van de AVG worden toegelicht. Dit handboek dient als naslagwerk voor alle informatie omtrent de AVG die uw onderneming nodig heeft.

1. Verwerking persoonsgegevens

a. Register verwerking persoonsgegevens

Voor grote(re) ondernemingen met meer dan 250 werknemers geldt de plicht om een verwerkingsregister bij te houden. Voor kleinere ondernemingen, zoals uw onderneming, geldt niet het vereiste van een dergelijk verwerkingsregister, maar u heeft wel een verantwoordingsplicht. Dat betekent dat u te allen tijde dient te kunnen verantwoorden welke persoonsgegevens* u verzamelt, met welke reden, met welk doel en voor welke periode. Het gaat voor uw onderneming dan om zowel gegevens van klanten als om gegevens van uw werknemers. In deze verantwoording dient u ook te omschrijven welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ten aanzien van deze persoonsgegevens. Voorbeelden van dergelijke maatregelen zijn autorisaties en versleuteling van computerbestanden of fysieke beveiliging (sloten of beveiligingscodes) op fysieke documenten.

> ***Persoonsgegevens in het kader van de AVG zijn**:
>
> Naam, adresgegevens, telefoonnummer, geboortedatum, BSN, bankgegevens, IP-adres, foto's, persoonlijk werke-mailadres, persoonlijk werktelefoonnummer, etc.

b. Grondslagen

Het is u niet toegestaan om zonder reden persoonsgegevens te verwerken. Het verwerken van persoonsgegevens mag alleen geschieden op grond van één van de zes in de AVG genoemde grondslagen.

Het gaat om de volgende zes grondslagen:

1. Toestemming;
   → Leg dit schriftelijk vast
2. Uitvoering van een overeenkomst;
   → Indien overeenkomst niet kan worden uitgevoerd zonder persoonsgegevens
3. Wettelijke verplichting;
   → Bijvoorbeeld verplichting om facturen 7 jaar te bewaren
4. Vitaal belang;
   → Bijvoorbeeld wanneer sprake is van een levensbedreigende situatie
5. Algemeen belang;
   → Bijvoorbeeld voor de uitoefening van openbaar gezag
6. Gerechtvaardigd belang
   → Noodzakelijk voor belangen verwerkings-verantwoordelijke tenzij privacyrechten betrokkene zwaarder wegen

Bij het opstellen van de verantwoording persoonsverwerkingsgegevens als genoemd onder sub a, dient daarom ook te worden vermeld op welk van deze grondslagen de verwerking gerechtvaardigd wordt. Dit kopje is dan ook opgenomen in ons model van het verwerkingsregister.

c. Verwerkersovereenkomst

De AVG stelt het verplicht dat u een zogenaamde "verwerkersovereenkomst" sluit, indien een ander bedrijf of persoon de persoonsgegevens van uw organisatie voor u verwerkt of opslaat. Dit kan al aan de orde zijn als u uw boekhouding uitbesteedt aan een derde. Deze derde krijgt dan persoonsgegevens onder ogen, waarop de AVG van toepassing is.

In deze verwerkersovereenkomst worden specifieke afspraken gemaakt omtrent de wijze waarop de derde moet omgaan met deze persoonlijke gegevens. Een belangrijk aandachtspunt daarbij is dat, wanneer u diensten waarbij persoonsgegevens van een klant betrokken zijn uitbesteedt, u hiervoor toestemming dient te vragen aan de betreffende klant.

d. Dataportabiliteit - privacybeleid

Het is van belang dat u uw klanten inlicht over het feit dat zij recht hebben op inzage, correctie, verwijdering en het meenemen van eigen gegevens. Dit wordt ook wel 'dataportabiliteit' genoemd. Bovendien dient u uw klanten in te lichten over het feit dat zij recht hebben op het intrekken van de door hen verleende toestemming, en het feit dat zij recht hebben om een klacht hieromtrent in te dienen.

Voor uw onderneming is de eenvoudigste manier om dit te doen het opnemen van deze informatie in de privacyverklaring op uw website (zie hieronder bij alinea 2). Daarnaast kunt u in uw opdrachtbevestiging een clausule opnemen waarin u verwijst naar de vindbaarheid van deze privacyverklaring. Indien geen privacyverklaring op de website wordt opgenomen, dient u uw klanten op een andere manier te informeren over uw verwerking van persoonsgegevens, bijvoorbeeld door dit uitgebreid uiteen te zetten in uw opdrachtbevestiging. Voor (nieuwe) werknemers geldt dat wij aanraden om de privacyverklaring als addendum achter de arbeidsovereenkomst op te nemen. Alle huidige werknemers kunnen op de privacyverklaring worden gewezen door hen uitdrukkelijk te wijzen op de privacyverklaring op de website.

e. Dataminimalisatie

Voor de toekomst is belangrijk dat u bij het inrichten van uw systemen rekening houdt met het uitgangspunt van dataminimalisatie. In het bijzonder zijn daarbij de volgende punten van belang:

- *Privacy by Design* → u vraagt niet meer gegevens op dan u daadwerkelijk nodig heeft.
- *Privacy by Default* → bij het opvragen van persoonsgegevens dient de standaardinstelling van uw systemen zo privacyvriendelijk mogelijk te zijn. De persoon kan zelf gegevens achterlaten of dient een actieve handeling te verrichten om toestemming te geven.

De systemen van uw onderneming zoals de website dienen daarom te worden ingericht met dataminimalisatie in het achterhoofd. Indien u uw toestemming voor gegevensverzameling op uw website verkrijgt door het aanvinken van een hokje waarin de klant toestemming geeft, dan mag dit hokje bijvoorbeeld niet bij voorbaat al zijn aangevinkt. Het aanvinken is namelijk de actieve handeling

die door de klant dient te worden verricht. Daarnaast vraagt u bijvoorbeeld niet de adresgegevens van uw klant op, bij een invulformulier voor inschrijving voor een e-mailnieuwsbrief op uw website. Die gegevens heeft u immers niet nodig voor het versturen van de nieuwsbrief.

2. Privacyverklaring website

U dient uw klanten of bezoekers van uw website te informeren over het verzamelen van persoonsgegevens. Hiervoor stelt u een privacyverklaring op, die gemakkelijk te vinden is voor bezoekers van uw website. In deze privacyverklaring dient onder meer informatie te worden opgenomen omtrent cookies, doeleinden gegevensverwerking en informatie over inzage en correctie door klanten of bezoekers. Zoals hiervoor aangestipt, kunt u deze privacyverklaring van toepassing verklaren op al uw werkzaamheden, bijvoorbeeld in uw opdrachtbevestiging.

3. Datalekken

a. Datalekken

Met de invoering van de AVG wordt het verplicht om alle datalekken intern te documenteren, ook degene die niet behoeven te worden gemeld aan de toezichthouder. Het is daarom van belang dat u op de hoogte bent van wanneer sprake is van een datalek, en welke handelingen u dient te verrichten wanneer een datalek heeft plaatsgevonden.

Er is sprake van een datalek indien een inbreuk plaatsvindt op de beveiliging van persoonsgegevens. Dat is bijvoorbeeld het geval wanneer onbedoeld toegang wordt geboden tot persoonsgegevens of als sprake is van vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Niet alleen het vrijkomen of lekken van gegevens resulteert in een datalek, ook wanneer onrechtmatig gegevens worden verwerkt is hiervan sprake. Om een voorval te kunnen kwalificeren als een datalek, moet sprake zijn van een daadwerkelijk beveiligingsincident.

Er kan al snel sprake zijn van een datalek; zo zijn het verlies van een usb-stick of laptop, het versturen van een e-mail naar het verkeerde e-mailadres of een brand in een datacentrum al aan te merken als datalek. Indien een datalek resulteert in een aanzienlijke kans op, of ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, dient dit datalek binnen 72 uur te worden gemeld aan de Autoriteit Persoonsgegevens. Is het waarschijnlijk dat het datalek ook resulteert in ongunstige gevolgen voor de privacy van de betrokkene, dan dient ook deze betrokkene van het datalek op de hoogte te worden gesteld.

b. Documenteren datalekken

De AVG vereist dat ondernemingen alle datalekken registreren. Om die reden ontvangt u van ons ook een model voor de registratie van datalekken. Per datalek dient onder meer een beschrijving te worden gegeven van het datalek, de betrokkenen, hoe het datalek is ontstaan en hoe in de toekomst getracht zal worden een soortgelijk datalek te voorkomen.

c. Datalekplan

U kunt uw onderneming het beste voorbereiden op een dergelijk datalek en het documenteren ervan, door reeds nu een datalekplan te hanteren. In een dergelijk plan wordt vastgesteld op welke manier

datalekken zullen worden behandeld en welke gegevens er precies zullen worden gedocumenteerd indien sprake is van een datalek.

Het opstellen van een dergelijk datalekplan is ook voor uw onderneming van groot belang, omdat u daarmee zorgt dat u op de best mogelijke manier bent voorbereid op datalekken in de toekomst. Op dit moment heeft u nog geen dergelijk datalekplan, en worden datalekken niet door u gedocumenteerd. Omdat in de AVG grote waarde wordt gehecht aan een dergelijke documentatie, is het belangrijk voor uw onderneming om dit wel op te pakken.

4. Arbeidsrechtelijk

a. Algemeen

In het algemeen is het van groot belang te realiseren dat de AVG niet alleen van toepassing is op persoonsgegevens van klanten, cliënten of contacten van uw bedrijf, maar bovendien op persoonsgegevens van uw werknemers. Dat betekent dat, wanneer uw organisatie gegevens verwerkt van werknemers –en aan dat vereiste zal door praktisch elke organisatie met werknemers worden voldaan-, de AVG hiervoor ook bepaalde vereisten met zich meebrengt. Dit wordt hieronder nader toegelicht.

b. Informatieplicht werknemers

Als werkgever heeft u op grond van de AVG de plicht om uw werknemers informatie te verstrekken zodra u persoonsgegevens van het personeel verwerkt. De eisen hieromtrent zijn grotendeels gelijk aan die van de klanten als behandeld onder punt 2 van dit advies (privacyverklaring website). Voor personeel verdient het echter de voorkeur om dergelijke informatie op te nemen in een personeelshandboek. Indien u een dergelijk handboek niet hanteert, kunt u de privacyverklaring echter ook van toepassing verklaren op uw werknemers.

c. Geheimhoudingsverklaring werknemers

De AVG schrijft voor dat uw onderneming alle werknemers die met persoonsgegevens werken, moet verplichten tot het alleen in opdracht van uw onderneming verwerken van de persoonsgegevens. Om aan dit vereiste te voldoen, dient u de betreffende werknemers een geheimhoudingsclausule te laten ondertekenen. Deze clausule kan worden opgenomen in de arbeidsovereenkomst, maar ook afzonderlijk daarvan worden opgesteld en ondertekend.

5. Overig

Tot slot is nog van belang dat de AVG nog meer onderwerpen behelst dan in onderhavig handboek behandeld, maar door ons worden deze onderwerpen voor uw onderneming niet van belang geacht, waardoor deze buiten beschouwing zijn gelaten. Het gaat dan met name om regelgeving gericht op bedrijven met meer dan 250 werknemers, of bedrijven die zeer privacygevoelige persoonsgegevens op grote schaal verwerken.