



Zicht krijgen op persoonlijke gegevens die je verzamelt

Op 25 mei 2018 gaat een nieuwe Europese privacyregeling van kracht, General Data Protection Regulation (GDPR) ook wel Algemene Verordening Gegevensbescherming (AVG) genoemd.

Voor bedrijven die niet aan de nieuwe verordening voldoen, kunnen de boetes oplopen tot € 20 miljoen of 4% van de omzet, als die hoger uitvalt.

Om aan de AVG te kunnen voldoen, is het belangrijk om de herkomst van alle persoonlijke gegevens binnen je bedrijf in kaart te brengen, evenals waar en hoe deze informatie wordt opgeslagen. Het is ook belangrijk om vast te leggen wat je specifiek met de gegevens doet.

Onder persoonlijke gegevens vallen onder andere IP-adres, geografische locatie, geslacht, inkomen, interesses en bezochte websites.

Checklist persoonlijke gegevens

Gebruik deze vragenlijst als hulpmiddel voor het analyseren van de persoonlijke gegevens die in systemen zijn opgeslagen.

Een goede manier om deze gegevens te verzamelen is met een Excel spreadsheet, maar er zijn natuurlijk nog diverse andere manieren waarop je de gegevens kunt verzamelen.

Het belangrijkste is dat je voor elke vorm van persoonlijke gegevens die je verzamelt, antwoord geeft op de volgende 13 vragen.

1 Welke persoonlijke gegevens worden er verzameld?

Beschrijf welke persoonlijke gegevens worden verzameld, zoals naam, (e-mail) adres, telefoonnummer. Vergeet niet om ook de overige persoonlijke informatie te vermelden, zoals geboortedatum, burgerservicenummer en alle andere aanvullende gegevens die iemand identificeren.

2 Waarvoor worden persoonlijke gegevens verzameld?

Geef specifiek aan waarvoor je de gegevens verzameld, zodat er geen twijfel over kan bestaan. Als je de geboortedatum van iemand nodig hebt, moet je specifiek kunnen aantonen waarvoor je dit gegeven nodig hebt.

3 Wat is de juridische basis?

Geef per gegeven aan, op basis van welke rechtsgrondslag jouw bedrijf deze informatie verzamelt. Verwijs hierbij naar GDPR Artikel 6.1 lid A t/m F.

4 Wat is de herkomst van de persoonlijke gegevens?

Geef informatie over de wijze waarop je persoonlijke gegevens verzamelt. Komen de gegevens binnen via webformulieren, visitekaartjes die worden verzameld, integraties met andere systemen en dergelijke?

5 Hoe zijn de gegevens geclassificeerd?

Persoonlijke gegevens kunnen geclassificeerd worden als vertrouwelijk, anoniem, gevoelig, enzovoort. Zo kan informatie over salaris of vergoedingen onder de gevoelige gegevens vallen. Houd er rekening mee dat alle gevoelige en vertrouwelijke persoonlijke gegevens extra beveiliging vereisen.



6 Hoelang worden persoonlijke gegevens bewaard?

Geef aan hoelang je de persoonlijke gegevens gaat bewaren. De duur kan afhankelijk zijn van het doel en de juridische basis. Zo kunnen salarisgegevens zo lang bewaard worden als de archiefwet en de wet- en regelgeving voor boekhouding vereisen.

7 Wie hebben er toegang tot persoonlijke gegevens?

Geef aan wie er toegang hebben tot persoonlijke gegevens. Medewerkers van de salarisadministratie hebben bijvoorbeeld toegang tot de loonadministratie, medewerkers van personeelszaken hebben toegang tot personeelsinformatie, verkoopmedewerkers hebben toegang tot klanteninformatie.

8 Worden de persoonlijke gegevens doorgegeven aan andere landen?

Persoonlijke gegevens dienen bij voorkeur binnen de EU te blijven. Als dat niet zo is, geef dan aan dat persoonlijke gegevens worden doorgegeven en waarom.

9 Op welk systeem wordt de informatie opgeslagen?

Je hebt waarschijnlijk afzonderlijke systemen voor loonadministratie en klanteninformatie. Je dient aan te geven welk systeem je voor persoonlijke gegevens gebruikt. Je dient tevens aan te geven of het systeem dat je gebruikt een systeem 'in de cloud' is.

10 Is er uitdrukkelijk toestemming gegeven voor gebruik van de gegevens?

Leg uit of de persoon in kwestie je vrijwillig zijn persoonlijke gegevens heeft verstrekt voor marketingcommunicatie. Het is met name van belang of er uitdrukkelijk toestemming is verleend als je persoonlijke gegevens bewaart en verwerkt van mensen waar je geen actieve klantrelatie mee hebt.

11 Is betrokkene ingelicht over het verzamelen van de gegevens?

Deze informatie wordt meestal vermeld in het klantencontract, bij een eerste bijeenkomst en/of in de privacyverklaring op de website. Ook hierbij mag geen ondubbelzinnigheid bestaan, over het doel van het verwerken van de informatie.

12 Worden deze persoonlijke gegevens doorgegeven aan derden en zo ja, waarom?

Als er informatie aan derden wordt doorgegeven, geef dan aan welke informatie wordt doorgegeven en aan wie.

Als je persoonlijke gegevens voor marketingdoeleinden gebruikt, zul je in de privacyverklaring en contractuele documenten specifiek moeten aangeven of deze gegevens al dan niet worden doorgegeven aan derden.

13 Hoe wordt de informatie beveiligd?

Beschrijf de beveiligingsmaatregelen die je toepast voor het beschermen van persoonlijke gegevens. Dit is met name van belang als je gevoelige informatie bewaart (Controller). Als verwerkingsverantwoordelijke (Processor) ben je verantwoordelijk voor de veiligheid van deze gegevens.

Volgende stappen

De ingevulde vragenlijst kan je helpen bij het selecteren van de gegevens die je wilt bewaren. Bewaar niet meer informatie dan nodig is en verwijder gegevens die je niet gebruikt.

Als jouw bedrijf veel gegevens verzamelt zonder aanwijsbare reden of noodzaak, mag je daar niet meer mee doorgaan na invoering van de AVG wetgeving.

Het in kaart brengen van de persoonlijke gegevens in jouw bedrijf en nagaan welke gegevens je moet bewaren, zijn al belangrijke eerste stappen om te voldoen aan de nieuwe regelgeving.

Je zult ook beveiligingsmaatregelen moeten treffen om gegevens te beschermen en procedures moeten ontwikkelen voor het openen, verwijderen en archiveren van persoonlijke gegevens.

Als je vragen hebt over hoe SuperOffice CRM je kan helpen in het ondersteunen van het GDPR proces, kun je ons bereiken op info@superoffice.nl

Disclaimer: de inhoud van dit artikel dient enkel ter informatie en niet als juridisch advies.