Algemene informatie Algemene Verordening Gegevensbescherming

De huidige privacywetgeving is stamt uit 1995 en is door de snelle technologische ontwikkelingen niet meer up-to-date. De nieuwe verordening biedt een hoger beschermingsniveau en zorgt voor harmonisatie van privacywetgeving in Europa. Alle webshops in Europa moeten op 25 mei 2018 aan de regels van de nieuwe verordening voor informatiebeveiliging en de bescherming van persoonsgegevens voldoen. Deze nieuwe verordening bepaalt dat persoonsgegevens alleen 'rechtmatig, behoorlijk en transparant' mogen worden verwerkt en dat daar een 'wettelijk omschreven grondslag' voor nodig is. Uw webshop moet onder andere voldoen aan de eisen van beschikbaarheid (= de gegevens zijn beschikbaar om te kunnen handelen), integriteit (= de gegevens zijn correct en actueel) en vertrouwelijkheid (= de gegevens zijn afgeschermd).

Persoonsgegevens

Persoonsgegevens bestaat uit de informatie waarmee je iemand hebt geïdentificeerd of waarmee je een persoon kunt identificeren. Als webwinkel heb je al gauw met persoonsgegevens van klanten en niet-klanten te maken. Denk aan naam, telefoonnummer, e-mailadres, IP-adres of locatiegegevens. Van het moment van verzameling tot en met het moment van vernietiging van persoonsgegevens moet je voldoen aan de verordening.

Informatieverplichting

Bedrijven die persoonsgegevens van consumenten verzamelen moeten hierover transparant communiceren. Hierbij zijn enkele aspecten verplicht te vermelden. Tevens dient deze informatie op een duidelijke vindplaats te worden medegedeeld. Vooralsnog wordt ervanuit gegaan dat een privacyverklaring hierin voldoet. Controleer daarom of uw privacyverklaring voldoet aan de eisen en of deze makkelijk te raadplegen is door bijvoorbeeld een hyperlink onder elke pagina. In dit kader van transparantie is het gebruik van bijvoorbeeld een noreply-mailadres ook niet langer gewenst. Zorg daarom voor een mailadres waarop de consument kan reageren en waarbij het direct duidelijk is van welke organisatie de mail afkomt.

Cookiebeleid

In 2019 komt naar verwachting de e-Privacy Verordening. Deze zal specifieker ingaan op onder andere cookies, direct marketing en metadata. Tot die tijd dient er een goed cookiebeleid te zijn dat makkelijk te raadplegen is door de klant.

Privacy by design

Privacy dient al een rol te spelen vanaf het moment dat (nieuwe) producten of diensten worden ontwikkelen. Privacy by design betekent het treffen van de nodige beschermingsmaatregelen. Volgens de verordening dienen daarom passende technische en organisatorische maatregelen te worden genomen. Zorg dat u als webshop zo min mogelijk gegevens verzamelt voor de verwerking. Maak daarom onderscheid tussen gegevens die noodzakelijk zijn en gegevens die door de webshop gewild zijn. Geef bij elke opt-in vervolgens aan waarvoor de gegevens zullen worden gebruikt (bijvoorbeeld de geboortedatum wordt gebruikt om de klant een verrassing op zijn/haar verjaardag te geven – overweeg dan ook om enkel de geboortedag of zowel de geboortedag als het -jaar te verwerken). De werkelijkheid dient overeen te komen met de privacyverklaring.

Grondslag

Er moet sprake zijn van een wettelijke basis die de verwerking van persoonsgegevens rechtvaardigt, dit is nu ook het geval. De grondslag toestemming wordt echter aangescherpt. Wanneer u om toestemming vraagt, is het belangrijk dat u altijd kunt aantonen dat de bewuste toestemming daadwerkelijk gegeven is. Deze toestemming dient een duidelijke, actieve handeling te zijn waarbij de toestemming vrijelijk, ondubbelzinnig en geïnformeerd wordt gegeven voor een specifieke verwerking en een specifiek doel. Standaard een vinkje aanzetten of toestemming opnemen in de algemene voorwaarden is niet meer toegestaan. De consument mag bovendien niet worden benadeeld als hij/zij geen toestemming geeft. Bedrijven dienen er

verder voor te zorgen dat consumenten hun toestemming te allen tijde kunnen intrekken. Let hierbij op dat kinderen onder de 16 jaar geen toestemming mogen geven, maar dat toestemming van de ouders nodig is. Bedrijven moeten op zijn minst kunnen aantonen dat een redelijke inspanning is verricht om te controleren of een ouder deze toestemming heeft gegeven.

Bewaartermijnen

Persoonsgegevens mogen onder de verordening niet langer bewaard worden dan noodzakelijk is voor het doel waarvoor ze verzameld zijn. Een bedrijf moet goed kunnen beargumenteren hoelang gegevens van een consument bewaard worden voor het oorspronkelijke doel. Zorg dan ook dat u als webshop per verwerking weet hoelang u bepaalde gegevens mag verwerken. Deze termijn dient dan ook te worden nageleefd, bijvoorbeeld door juiste technische en organisatorische maatregelen te treffen. Aan te raden is verschillende databases/opslaglocaties te gebruiken voor veel verschillende soorten persoonsgegevens van één persoon en/of zoveel mogelijk diensten op het device van de consument te laten plaatsvinden.

Rechten van betrokkene(n)

Consumenten hebben momenteel verschillende rechten en daar komen nog twee nieuwe rechten bij. Zorg dat alle rechten van betrokkenen begrijpelijk en toegankelijk worden weergegeven op de site.

Dataportabiliteit

Webshops en andere organisaties moeten de persoonsgegevens die zij hebben verzameld kunnen overdragen als de betrokkene daar om vraagt. Als de consument de gegevens zelf wil ontvangen, dient dit in een eenvoudig te downloaden vorm te worden verstrekt. Als de consument verzoekt de gegevens over te dragen aan een derde partij, dan moet dat in een gangbaar elektronisch formaat naar een ander informatiesysteem worden verstuurd. Voor de toepassing van het recht op dataportabiliteit moet de grondslag toestemming zijn of moeten de gegevens voortkomen uit een overeenkomst tussen onder andere de webshop en de consument. Het gaat hierbij ook om gegevens zoals titels van bijvoorbeeld boeken of films die de betrokkene bij de aankoop in de webshop heeft gedaan.

Recht op vergetelheid

In een aantal gevallen dienen webshops persoonsgegevens te verwijderen als de consument hierom verzoekt. Hierbij kan het zijn dat een derde, zoals een verwerker, op de hoogte moet worden gebracht van het verzoek. Dit geldt ook voor kopieën en/of reproducties van de persoonsgegevens. Alleen als de webshop een gerechtvaardigd belang heeft of er een wettelijke plicht bestaat om de gegevens te bewaren, hoeven de persoonsgegevens niet te worden verwijderd. Bij verwerking voor direct-marketingdoeleinden moeten overigens de gegevens altijd worden verwijderd als de consument hier bezwaar tegen maakt.

Profilering

Er is sprake van profilering als een organisatie op basis van verkregen persoonsgegevens automatisch een profiel van de consument opstelt door de gegevens te verzamelen, te analyseren en te koppelen. Hierbij worden de gegevens gecombineerd om de consument in te kunnen delen in een bepaalde groep of categorie voor bijvoorbeeld direct marketing of het gebruik van gerichte advertenties. Onder de verordening is elke vorm van geautomatiseerde verwerking van persoonsgegevens (waaronder profilering) niet toegestaan als daar voor de consument rechtsgevolgen aan zijn verbonden of als het besluit hem/haar in aanzienlijke mate treft. Op dit verbod gelden uitzonderingen zoals de noodzakelijkheid van verwerken voor de totstandkoming of uitvoering van de overeenkomst of verwerking met uitdrukkelijke toestemming van de betrokkene. U dient de consument dan wel van specifieke informatie te voorzien. Daarnaast heeft de consument recht op menselijke tussenkomst om zijn/haar standpunt kenbaar te maken, uitleg te krijgen over het genomen besluit en het recht om dit besluit aan te kunnen vechten. Het is aan te raden om hiervoor een contactpersoon aan te stellen binnen uw organisatie.

Data Protection Officer (DPO)

Een DPO kan zowel binnen als buiten de organisatie door u worden aangesteld. Een DPO ziet onder andere toe op de naleving van de AVG. De plicht om een DPO aan te stellen is afhankelijk gemaakt van hoeveel impact de gegevensverwerking op de persoonlijke levenssfeer van betrokkenen heeft. Voor webshops kan het instellen van een DPO verplicht zijn als de webshop:

- Hoofdzakelijk belast is met gegevensverwerking waarvoor op grote schaal regelmatige en stelselmatige observatie van betrokkenen nodig is.
- Hoofdzakelijk belast is met de verwerking van bijzondere persoonsgegevens op grote schaal.

Als de aanstelling niet verplicht is, wordt deze door onder andere de Autoriteit Persoonsgegevens toch aangeraden.

Data Protection Impact Assessment (DPIA)

Een DPIA geeft bedrijven inzicht in hoe groot de kans is dat de privacy van de betrokkenen wordt geschaad, waar deze risico's zich bevinden en welke gevolgen daaraan verbonden zijn. Dit inzicht kan noodzakelijk zijn om passende technische en organisatorische maatregelen te kunnen nemen. Organisaties moeten een DPIA opstellen als een verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. De Autoriteit Persoonsgegevens verwijst naar een handreiking voor meer informatie.

Meldplicht datalekken

De Wet Meldplicht Datalekken is al van kracht in Nederland. Deze blijft met de komst van de AVG grotendeels hetzelfde.

Toezicht en boetes

Er zijn twee categorieën overtredingen en bijbehorende maximale boetes:

1. Niet nakomen van een wettelijke verplichting met een maximale boete van €10 miljoen of 2% van de wereldwijde jaaromzet.
   Denk aan de verantwoordingsplicht, informatieplicht of de eventuele verplichting om een DPO aan te stellen en een DPIA uit te voeren.

2. Overtreden van beginselen of grondslagen van de verordening met een maximale boete van €20 miljoen of 4% van de wereldwijde jaaromzet.
   Denk aan het respecteren van de privacyrechten van betrokkenen en het hebben van een juiste grondslag voor de verwerking.