Privacy in de recreatiebranche. Wat betekent de nieuwe Privacyverordening voor mkb-recreatiebedrijven?

Auteur: mr. P. Otto
Publicatiedatum: 31-8-2017

Vanaf 25 mei 2018 gelden er nieuwe regels op het gebied van privacy. De Algemene Verordening Gegevensbescherming (hierna: Privacyverordening) geldt in de gehele Europese Unie en vervangt voor een groot deel de nationale privacywetgeving (in Nederland de Wet bescherming persoonsgegevens). Ieder recreatiebedrijf zal in de regel onder deze Privacyverordening vallen.

Kenmerkend aan de nieuwe Privacyverordening is dat de ondernemer moet kunnen aantonen dat zij voldoet aan de regelgeving en dat de privacy effectief wordt gewaarborgd. Dit kan men aantonen door onder meer een goed privacybeleid, een privacycultuur, het goed inrichten van processen, adequate documentatie, informatie aan de betrokkenen en passende organisatorische en technische beveiligingsmaatregelen.

Achtergrond van de regelgeving

De nieuwe regelgeving speelt in op de ontwikkelingen op het gebied van datavergaring, dataverwerking en het inzetten van deze data voor allerlei doeleinden. Zo zijn door de digitalisering persoonsgegevens die uit allerlei bronnen worden verkregen op slimme wijze te combineren waardoor er profielen van personen worden gemaakt en op die profielen worden aanbiedingen, tarieven en ook andere keuzes afgestemd. Dat is soms prettig, maar vaak ook zeer onwenselijk. Daarnaast is bijvoorbeeld de misbruik van identiteit explosief toegenomen doordat gegevens worden verkregen via hacking en virussen. Ook steeds vaker is er sprake van ransomware (soort van virus) die data vernietigt of ontoegankelijk maakt. De correcte omgang met persoonsgegevens en de beveiliging daarvan dient om die reden te worden gewaarborgd binnen ondernemingen.

Een tweede doelstelling van de Privacyverordening is het samenwerken met andere bedrijven binnen de Europese Unie en het grensoverschrijdend verlenen van diensten makkelijker te maken. Voorheen waren er in ieder land aparte regels voor de privacy. Door de nieuwe privacyverordening geldt er – in hoofdlijnen – één set regels binnen de gehele Europese Unie.

Wat valt onder de verwerking van persoonsgegevens

Persoonsgegevens zijn alle gegevens over een geïdentificeerd of identificeerbaar persoon (‘de betrokkene’). Het betreft niet alleen gegevens van consumenten. Het betreft alle gegevens van personen die worden verwerkt in de onderneming waaronder bijvoorbeeld ook de gegevens van personeel. Verwerking van persoonsgegevens is kort gezegd iedere handeling met die gegevens waaronder in ieder geval het opslaan, bewerken, kopiëren, printen, het aan derden verstrekken van gegevens en het verwijderen. De Privacyverordening is van toepassing op geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens (kort gezegd alle digitale verwerking) en op verwerking in een geordende verzameling offline persoonsgegevens (bijvoorbeeld dossiers van klanten in de kast).

Accountability

Een belangrijk onderdeel van de Privacyverordening voor ondernemers is het kunnen aantonen dat er wordt voldaan aan de regelgeving en dat de privacy van betrokkenen is gewaarborgd door effectief beleid en maatregelen. Dat vergt een actievere houding dan voorheen en het vergt dat het waarborgen van privacy een continu proces is dat meegroeit met de ontwikkelingen van het bedrijf. Om die reden is het belangrijk binnen het bedrijf iemand aan te wijzen die hiervoor verantwoordelijk is en die dit waarborgt.

Wat dient er te gebeuren

Voor mkb-recreatiebedrijven brengt de verordening onder meer veranderingen mee op het gebied van privacybeleid, de inrichting van processen en ICT, documentatie, informatieverstrekking, de rechten van betrokkenen en de verwerkersovereenkomsten.

Privacybeleid

Een goed privacybeleid beschrijft hoe de waarborging van privacy binnen de onderneming is vormgegeven, van aandacht op bestuursniveau en uitgangspunten bij de inrichting van processen tot de wijze waarop op operationeel niveau met gegevens en ontwikkelingen wordt omgegaan. Het beleid verbindt alle verschillende instrumenten die de onderneming heeft om de privacy te waarborgen.

Processen

Processen dienen zo te zijn ingericht dat het ontwerp reeds een waarborging van privacy in de hand werkt. Voorbeelden zijn dat enkel de noodzakelijke data wordt gevraagd en dat enkel medewerkers die met de

persoonsgegevens werken hiertoe toegang hebben. ICT-aanpassingen zullen in de regel nodig zijn.

Documentatie

Onder de nieuwe privacyverordening geldt -kort gezegd- een registerplicht voor alle bedrijven die niet-incidenteel persoonsgegevens verwerken. In dit register dient onder meer te worden opgenomen welke gegevens worden verzameld, voor welke doeleinden, op basis van welke wettelijke grondslag, de bewaartermijnen en hoe de beveiliging in hoofdlijnen is geregeld. Voor zover het niet verplicht is, is dit overzicht voor iedere onderneming toch te adviseren omdat het zorgt voor een systematische en volledige aanpak van het 'privacyproof' maken van de onderneming. In de regel blijkt pas hoeveel (onnodige) persoonsgegevens worden verzameld en waar de risico's zitten na een gedegen inventarisatie. Welke data verzamelt de onderneming? Is die data noodzakelijk? Wat zijn de bewaartermijnen? Hoe is deze data beveiligd? Met wie wordt de data gedeeld? Wordt niet meer dan nodig gedeeld? Dit zijn vragen waar de onderneming onderbouwd antwoord op moet kunnen geven.

Informatieverschaffing

De informatie die aan betrokkenen dient te worden verschaft wordt veel uitgebreider waarbij de doelen van de verwerking en de grondslag nauwkeuriger moet worden aangegeven. Onder andere de privacyverklaring zal dus moeten worden aangepast. Opgelet moet worden dat bij de formulering van het doel een goede balans bestaat tussen de privacy van de betrokkene en het mogelijk beoogde gebruik van de onderneming. Persoonsgegevens mogen alleen gebruikt worden overeenkomstig het doel en hetgeen daarmee verenigbaar is. Een te nauwe doelomschrijving leidt er toe dat de data in de toekomst niet gebruikt kan worden zonder nadere toestemming van de betrokkene.

Rechten van betrokkene

De rechten van de betrokkene zijn nog duidelijker dan voorheen vastgelegd en zullen veel bekender worden bij het grote publiek. Het recht op inzage, correctie en verwijdering van gegevens zal dan ook een grotere impact gaan krijgen en een organisatie dient na te denken over hoe ze aan dergelijke verzoeken kunnen voldoen. Weet u bijvoorbeeld waar alle data van de betrokkene inmiddels staat in de onderneming? Denk daarbij naast het centrale datasysteem en de boekhouding aan kopieën op veelal onbeveiligde usb-sticks, mailaccounts, (onbeveiligde) privé-laptops, telefoons, iPads, Dropbox, WeTransfer, Google Docs, Faxonline, etc. Als u de datastromen niet op voorhand beheerst, wordt het naleven van een simpel recht op verwijdering een organisatorische nachtmerrie.

Afspraken met verwerkers

Met externe partijen die persoonsgegevens voor uw onderneming verwerken dient de onderneming verplicht een verwerkersovereenkomst overeen te komen die voldoet aan de gestelde eisen.

Kennis & implementatie

Om de onderneming 'privacyproof' te maken en te houden is het noodzakelijk om kennis van de Privacyverordening in huis te halen. Doorgaans is een samenwerking van een extern deskundige en een intern verantwoordelijke medewerker het meest ideaal voor het eerste traject van het 'privacyproof' maken. Als het raamwerk eenmaal staat en is ingevuld heeft de interne medewerker inmiddels voldoende ervaring en kennis opgedaan om het te onderhouden.

Balans tussen risico en inspanning

De nieuwe Privacyverordening zorgt ervoor dat bedrijven meer tijd en middelen dienen te investeren in het waarborgen van de privacy. De inspanningen die moeten worden geleverd om de privacy te waarborgen mogen wel in verhouding te staan tot de risico's die met de verwerkte persoonsgegevens en de context gepaard gaan. Ook kleine recreatiebedrijven dienen zich dus in te spannen, zij het dat de omvang van deze inspanning beperkter zal zijn dan een grote onderneming of een bedrijf dat systematisch zeer gevoelige data verwerkt. Indien men als mkb-bedrijf een gedegen inspanning heeft geleverd om de privacy te waarborgen dan zal de Autoriteit Persoonsgegevens die belast is met het toezicht in de regel bij een melding van een overtreding door een betrokkene volstaan met een verzoek om een en ander toe te lichten en een opmerking het proces in lijn met de wetgeving te brengen. Indien een onderneming in het geheel niet kan aantonen aandacht te hebben besteed aan de privacy dan ligt een boete uiteraard wel veel eerder voor de hand. Zorg daarom dat er tijdig wordt begonnen aan het privacyproof maken. Een kleine onderneming dient rekening te houden met meerdere maanden doorlooptijd van aanvang tot afronding. Bij een middelgrote onderneming kan dit oplopen tot een jaar.