Privacy in de reisbranche. Wat betekent de nieuwe Privacyverordening voor kleine reisorganisaties?

Auteur: Mr. P. Otto
Publicatiedatum: 8-5-2017

Vanaf 25 mei 2018 zijn de nieuwe regels op het gebied van privacy van toepassing. De Privacyverordening (Algemene Verordening Gegevensbescherming) geldt in de gehele Europese Unie en vervangt voor een groot deel de nationale privacywetgeving (in Nederland de Wet bescherming persoonsgegevens). De Privacyverordening is van toepassing op geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op verwerking in een geordende verzameling offline persoonsgegevens (bijvoorbeeld dossiers van klanten in de kast). Vanwege de digitale werkwijze in de reisbranche zullen reisorganisaties ook onder de Privacyverordening vallen.

Voor kleine reisorganisaties brengt de verordening veranderingen mee op het gebied van de informatieverstrekking, rechten van klanten, inrichting van processen, privacybeleid en documentatie.

Executive summary – to do

Het onderstaande overzicht geeft kort weer wat nodig is om de organisatie in lijn te brengen met de Privacyverordening en de rechten van klanten, personeel en andere betrokkenen te waarborgen:

- Stel een projectplan op voor de implementatie van de verordening (deadline 25 mei 2018).
- Inventariseer en categoriseer de gegevensverwerking, doeleinden, grondslagen en beveiligingsmaatregelen en bepaal bewaartermijnen;
- Richt processen goed in (privacy by design en default);
- Richt processen efficiënt in (in verband met het recht op inzage, correctie, verwijdering, beperking van de verwerking en dataoverdracht);
- Zorg voor passende organisatorische en technische beveiliging;
- Documenteer het bovenstaande;
- Zorg voor goede en juiste informatievoorziening richting betrokkenen (update de privacyverklaring);
- Controleer bestaande bewerkersovereenkomsten met verwerkers (zoals ICT dienstverleners) en pas deze aan;
- Stel een kort maar helder intern protocol datalekken op;
- Stel een privacybeleid op;
- Maak personeel en dienstverleners bewust;
- Evalueer geregeld het beleid;

Door het onderstaande artikel te lezen bent u op de hoogte van de relevante inhoud van de Privacyverordening.

Verwerking van persoonsgegevens

Persoonsgegevens zijn alle gegevens over een geïdentificeerd of identificeerbaar persoon (‘**de betrokkene**’).

Verwerking van persoonsgegevens is kort gezegd iedere handeling met die gegevens waaronder in ieder geval het opslaan, kopiëren, printen en het aan derden verstrekken van gegevens valt.

Bijzondere persoonsgegevens zijn gegevens waaruit ras, etnische afkomst, politieke opvattingen, religie, lidmaatschap van een vakbond, biometrie, gezondheid of seksuele geaardheid blijkt. Ook in de reisbranche worden deze gegevens vaak verwerkt. Denk daarbij aan dieetwensen uit religieuze gronden (koosjer of halal eten), allergieën (voedsel- of donsallergie) en andere medische informatie relevant voor geplande activiteiten. Voor verwerking van bijzondere persoonsgegevens van reizigers is uitdrukkelijke toestemming van de betrokkene nodig.

De belangrijkste beginselen van de gegevensverwerking

- **Transparantie:** Voor de betrokkenen dient het inzichtelijk te zijn welke persoonsgegevens worden verwerkt en voor welke doeleinden.
- **Rechtmatigheid:** De gegevensverwerking dient conform de normen van de Privacyverordening te geschieden.
- **Doelbinding:** De doeleinden van de gegevensverwerking dienen welbepaald, uitdrukkelijk omschreven en gerechtvaardigd te zijn. De gegevensverwerking mag enkel plaatsvinden voor het omschreven doel en doelen die hiermee verenigbaar zijn. Het is dus van belang dat er over het mogelijke gebruik van de gegevens wordt nagedacht voordat deze worden verzameld.
- **Minimale gegevensverwerking:** Elke verwerking, in het bijzonder het verzamelen van gegevens, dient geminimaliseerd te zijn in relatie tot het doel. Enkel de ‘noodzakelijke en ter zake dienende’ gegevens mogen worden gevraagd en verwerkt. Bepaal daarom bij het opstellen van bijvoorbeeld een boekingsformulier eerst wat de noodzakelijke gegevens zijn in relatie tot het beoogde doel.
- **Juistheid:** De verwerkte gegevens dienen juist te zijn. Onjuiste gegevens dienen te worden aangepast.
- **Beperkt bewaren:** De gegevens mogen niet langer worden bewaard dan noodzakelijk voor het doel waarvoor ze zijn verzameld. Indien men dus als doel enkel ‘de uitvoering van de reis’ vermeldt dan zijn de gegevens na afhandeling van de reis in beginsel niet meer noodzakelijk. Voor het houden van klantcontact na de reis is een andere doelomschrijving dus gewenst en zijn ook niet alle gegevens meer nodig. Gegevens die nodig zijn voor het voldoen aan een wettelijke plicht (zoals facturen) mogen bewaard worden gedurende de wettelijk verplicht gestelde bewaartermijn.
- **Passende technische of organisatorische maatregelen ter beveiliging:** De verwerking van gegevens dient zodanig te worden vorm gegeven dat de beveiliging van de persoonsgegevens passend is. Wat passende beveiliging is hangt af van de aard, de omvang, de context en het doel van de gegevensbewerking en het risico voor de betrokkenen.

Rechtmatige verwerking / Grondslag

De verwerking van gegevens dient altijd gebaseerd te zijn op een grondslag. De voor de reisorganisaties relevante grondslagen worden hieronder besproken.

- **Uitvoering van de overeenkomst:** De reisovereenkomst vormt de grondslag van verwerking van gegevens die noodzakelijk zijn voor de uitvoer van de reis. De arbeidsovereenkomst en wettelijke plichten omtrent de personeelsadministratie vormen de grondslag voor de verwerking van persoonsgegevens van het personeel. Voor zover de gegevens noodzakelijk zijn, is voor de verwerking van deze gegevens geen aparte toestemming vereist.
- **Gerechtvaardigd belang:** Naast de overeenkomst als grondslag vormt het gerechtvaardigd belang van de onderneming of derden een belangrijke grondslag. Dit zijn bijvoorbeeld handelingen voor de normale bedrijfsvoering en het dagelijks beheer van de organisatie. Direct marketing doeleinden kunnen met deze grondslag worden onderbouwd. Ook het delen van deelnemersgegevens (naam en emailadressen) in het kader van het faciliteren van onderling vervoer of het afstemmen van mee te nemen reisattributen kan hieronder vallen. Wel geldt dat de verwerking noodzakelijk moet zijn en dus niet met minder gegevens of op een minder ingrijpende wijze hetzelfde doel kan worden bereikt. Ook dient er een belangenafweging plaats te vinden tussen de belangen van de betrokkene en het te dienen belang.
- **Wettelijke plicht:** Er gelden wettelijke plichten die de organisatie verplichten persoonsgegevens te bewaren zoals de financiële administratie en personeelsadministratie. Dit vormt ook een grondslag. Enkel de verplichte gegevens vallen hieronder.
- **Toestemming:** Indien men gegevens wenst te verwerken die niet onder een andere in de verordening genoemde grondslag vallen is toestemming nodig. Er worden veel eisen gesteld aan een rechtsgeldige toestemming:
    - De toestemming dient uit een actieve handeling te volgen. Het standaard aanvinken van een vakje bij de toestemmingsvraag op het boekingsformulier levert dus geen geldige toestemming op.
    - De toestemming dient vrij te worden verkregen.
    - De toestemming dient geïnformeerd te geschieden.
    - De toestemming dient specifiek te zijn. Dit wordt bereikt door de toestemmingsvraag goed te formuleren. Een vink plaatsen naast de opmerking “ik ga akkoord met de privacyverklaring” is geen specifieke toestemming.
    - De toestemmingsvraag dient in eenvoudige en duidelijke taal te worden gesteld. Juridische taal is dus niet wenselijk, maar nauwkeurige formulering wel.
    - Indien schriftelijk gesteld, dient de toestemmingsvraag gescheiden te zijn van andere informatie.
    - De betrokkene dient te zijn geïnformeerd dat de toestemming op ieder moment kan worden ingetrokken. Te verdedigen valt dat dit in de privacyverklaring kan worden opgenomen.

Informatieplichten

Men dient de boeker in ieder geval de volgende informatie te verstrekken bij de verkrijging van de persoonsgegevens:

- De identiteit en contactgegevens van de onderneming (de verwerkingsverantwoordelijke).
- De doeleinden van de verwerking.
- De rechtsgrond van de verwerking.
- De bewaartermijn.
- Het recht van de betrokkene op inzage, correctie, verwijdering, beperking van de verwerking, bezwaar en dataportabiliteit.
- Het recht om een gegeven toestemming te allen tijde te kunnen intrekken.
- Het klachtrecht bij de Autoriteit Persoonsgegevens.

Afhankelijk van de verwerking en context kunnen er meer informatieplichten volgen uit de Privacyverordening. Voor de reizigers die niet zelf hebben geboekt, geldt dat de informatie bij het eerste contact en voordat de informatie wordt doorgespeeld naar derden wordt verstrekt en in ieder geval binnen een redelijke termijn (uiterlijk 1 maand). Dit zou kunnen worden ingevuld door na de boeking de betrokkene automatisch een email te sturen met daarin de genoemde informatie.

Rechten van de betrokkene

De betrokkene (boeker of reiziger) heeft meer rechten onder de nieuwe Privacyverordening. De belangrijkste rechten staan hierna vermeld:

- **Recht van inzage:** De betrokkene heeft het recht in te zien welke persoonsgegevens van hem of haar verwerkt worden.
- **Recht van correctie:** Een betrokkene heeft het recht op correctie van zijn persoonsgegevens indien deze onjuist zijn. De praktijk dat voor correcties in namen en geboortedata bij (vlieg)tickets een vergoeding in rekening wordt gebracht staat hiermee op gespannen voet.
- **Recht op verwijdering:** Een betrokkene heeft recht op verwijdering van gegevens. Een organisatie dient gegevens op eigen initiatief te verwijderen indien de gegevens niet meer nodig zijn voor de doeleinden waarvoor ze verkregen zijn. Daarnaast kan een betrokkene om verwijdering verzoeken (bezwaar maken tegen verwerking).
- **Recht op beperking van de verwerking:** Nieuw in de verordening is het recht op beperking van de verwerking wat inhoudt dat gegevens op verzoek van de betrokkene niet worden verwijderd, maar enkel nog verder worden verwerkt met toestemming van de betrokkene. Ik voorzie thans niet dat dit voor de reisbranche gevolgen heeft.
- **Recht van dataportabiliteit:** Eveneens nieuw is het recht van de betrokkene op overdraagbaarheid van gegevens. Op zijn verzoek moeten de gegevens op een gangbare voor een machine leesbare vorm worden beschikbaar gesteld. Ook dit recht heeft voor reisorganisaties naar verwachting geen grote implicaties. Dit recht dient het mogelijk te maken gebruikersdata van een dienstverlener bij de overstap naar een andere dienstverlener mee te nemen. Bij sommige diensten is de persoonlijke data over het gebruik van de dienst nuttig en waardevol. Bij reisorganisaties is dat vooralsnog niet goed voor te stellen.

Privacy door ontwerp (design) en privacy door standaardinstellingen (default)

Als invulling van passende maatregelen wordt privacy by design en privacy by default benadrukt. Dit houdt onder meer het volgende in:

- **Enkel de nodige gegevens verzamelen**: Door bijvoorbeeld niet onnodig open invoervelden te gebruiken, maar waar mogelijk slechts een beperkt aantal standaard antwoordopties te geven.
- **Gegevens niet verder verwerken dan nodig**: Door bijvoorbeeld geen onnodige kopieën te bewaren. Door de opkomst van het thuiswerken, het flexwerken en het werken op afstand is een goed privacybeleid en een goede ICT-inrichting noodzakelijk om de dataspreiding 'onder controle' te houden.
- **Pseudonimiseren**: Persoonsgegevens zo opslaan dat deze zonder dat er nadere gegevens worden gebruikt niet aan de betrokkene kunnen worden gekoppeld.
- **Enkel bewaren wat noodzakelijk is:** Persoonsgegevens niet langer dan noodzakelijk bewaren. Veel oudere ICT systemen zijn gebouwd om enkel automatische data-input mogelijk te maken. Verwijdering dient doorgaans handmatig te geschieden. Hierdoor blijven gegevens onnodig bewaard of is het verwijderen een tijdrovende bezigheid. Bij het ontwikkelen van nieuwe ICT systemen is de (semi)automatische verwijdering van gegevens naar gegevenscategorie mijns inziens een belangrijke factor.
- **Toegangsbeperking:** Persoonsgegevens offline en online enkel toegankelijk maken voor de medewerkers die deze gegevens nodig hebben. Het inrichten van een authorisatieschema is van belang. Ondanks dat een open office cultuur waar alle deuren open staan het vertrouwen binnen de organisatie uitspreekt, dienen gevoelige gegevens zoals de personeelsgegevens wel te worden afgeschermd.

Overeenkomst met de verwerker

Bijna iedere reisorganisatie maakt gebruik van ICT platformen waarop persoonsgegevens worden opgeslagen zoals het boekingssysteem en het boekhoudsysteem. Doorgaans staan deze gegevens op de server bij de ICT dienstverlener.

De reisorganisatie mag enkel gebruik maken van verwerkers die passende technische en organisatorische maatregelen nemen. Een indicatie dat de verwerker haar beveiliging op orde heeft is het voldoen aan ISO-normen op het gebied van informatiebeveiliging (onder meer ISO 27001 en 27002). De reisorganisatie dient met deze verwerkers afspraken te maken in een verwerkersovereenkomst. Deze overeenkomst moet op basis van de Privacyverordening voldoen aan nieuwe eisen ten opzichte van de bewerkersovereenkomst die al verplicht was onder de huidige wetgeving. Onder de bestaande wetgeving moest dit verplicht een aparte overeenkomst zijn. Die eis is er niet op basis van de Privacyverordening.

Doorgifte aan derde landen

In de reisbranche worden persoonsgegevens naar derde landen gecommuniceerd voor de uitvoering van de reisovereenkomst. De lokale dienstverleners dienen immers op de hoogte te zijn van bepaalde gegevens. Dit is toegestaan voor zover de gegevens noodzakelijk zijn voor de uitvoering van de overeenkomst en ook in de voorbereiding van een overeenkomst zoals het aanvragen van een offerte of het nemen van een optie. Wel is het zo dat deze dienstverleners ook de privacy van de reizigers dienen te respecteren. Zo is een whatsappbericht van een Indonesisch hotel gericht aan de reiziger waarin aanvullende plaatselijke diensten worden aangeboden onrechtmatig indien hier geen toestemming voor is gegeven. Men dient in dit geval ook te overwegen of het uberhaupt wel noodzakelijk is om het telefoonnummer van de reiziger door te geven aan het hotel.

Daarnaast speelt doorgifte aan derde landen een rol bij de opslag van informatie en gebruik van bepaalde platforms en communicatiemiddelen. Dit is niet noodzakelijk voor de uitvoering van de overeenkomst en om die reden is dit slechts toegestaan indien er passende waarborgen zijn of de betrokkene geïnformeerd toestemming heeft gegeven. Het belangrijkste land van dataopslag en clouddiensten is de Verenigde Staten. Vanwege de actieve overheidsbemoeienis zijn er enkel passende waarborgen indien het bedrijf dat in de VS data verwerkt, beschikt over een Privacycertificaat. Dit is nader geregeld in het EU-US Privacyshield verdrag.

De praktische samenvatting van deze complexe materie is dat de reisorganisatie ervoor dient te zorgen dat er goede afspraken zijn met de eigen ICT-dienstverlener. Deze dienstverlener dient de opslag en communicatie van persoonsgegevens zo vorm te geven dat de data niet buiten de EU wordt verwerkt of indien dit wel nodig is dat wordt gewaarborgd door de ICT dienstverlener dat de reisorganisatie voldoet aan de privacywetgeving.

Gegevensbeschermingsbeleid

Een gegevensbeschermingsbeleid is nodig indien dit in verhouding staat tot de verwerkingsactiviteit. Mijns inziens doet een reisorganisatie er altijd goed aan om een gegevensbeschermingsbeleid te hebben, maar stemt zij de omvang en diepgang van het beleid af op het risico. De verordening stelt op verschillende plaatsen verplicht dat kan worden aangetoond dat de persoonsgegevens correct worden verwerkt. Het beleid helpt aan te tonen dat wordt gehandeld in overeenstemming met de privacyverordening.

Een periodieke evaluatie en afstemming op nieuwe ontwikkelingen is eveneens gewenst. Een dergelijk beleid met geregelde evaluatie en aanpassing leidt ertoe dat privacy de aandacht krijgt binnen de onderneming en de rechten van klanten en personeel worden gewaarborgd.

Documentatie/registerplicht

Organisaties hebben een registerplicht. Er geldt slechts een uitzondering voor organisaties met minder dan 250 werknemers indien de organisatie slechts incidenteel persoonsgegevens verwerkt en geen bijzondere persoonsgegevens verwerkt. Omdat zelfs kleinere reisorganisaties doorgaans meer dan incidenteel persoonsgegevens verwerken en enkele bijzondere persoonsgegevens verwerken zal de organisatie naar verwachting niet onder de registerplicht uit kunnen komen.

Het register dient te bestaan uit de volgende punten:

- De naam en contactgegevens van de verantwoordelijke van deze verwerkingen.
- De doeleinden van de verwerking.
- De categorieën betrokkenen (klanten, werknemers, etc.).
- De categorieën persoonsgegevens (NAW-gegevens, financiële gegevens, medische gegevens).
- De categorieën ontvangers van de persoonsgegevens en doorgifte naar derde landen.
- Bewaartermijnen per gegevenscategorie.
- Omschrijving van de technische en organisatorische beveiligingsmaatregelen.
    - Fysieke maatregelen (bijvoorbeeld afsluiten van ruimtes)
    - Technische maatregelen (bijvoorbeeld een ssl verbinding en wachtwoord voor de computer)
    - Organisatorische maatregelen (bijvoorbeeld het toegankelijk maken van informatie op een need-to-know basis).

Datalek

Indien er een inbreuk in verband met persoonsgegevens heeft plaats gevonden, dient dit onverwijld maar uiterlijk binnen 3 dagen te worden gemeld. Melding is niet nodig indien de onderneming kan aantonen dat het onwaarschijnlijk is dat de inbreuk risico's voor de betrokkenen met zich mee brengt.

Er is bijvoorbeeld sprake van een inbreuk indien persoonsgegevens per ongeluk of onrechtmatig zijn gewijzigd of verloren en ook indien een ongeoorloofd persoon digitaal of fysiek toegang had tot de persoonsgegevens.

Is de mailinglijst met enkele honderden emailadressen van klanten bij het versturen van de nieuwsbrief per ongeluk in de CC gezet in plaats van de BCC dan is er sprake van een inbreuk. Er kan verdedigd worden dat bij de gemiddelde reisorganisatie deze inbreuk geen risico's voor de betrokkenen meebrengt. Een melding is dan niet nodig. Is er een virus/Trojaans paard geplaatst op de server en kan niet worden uitgesloten dat bijvoorbeeld betalingsgegevens, medische gegevens of paspoortgegevens van het personeel zijn gekopieerd, bewerkt of verwijderd dan is er een inbreuk en zijn er wel risico's voor betrokkenen. Een melding is dan verplicht.

Er dienen na een inbreuk corrigerende maatregelen te worden genomen en iedere inbreuk en de corrigerende maatregelen dienen verplicht intern gedocumenteerd te worden. Indien de inbreuk een hoog risico voor de betrokkene vormt dient dit ook bij hem of haar te worden gemeld.

Gegevensbeschermingseffectbeoordeling

Indien het verwerken van gegevens een hoog risico meebrengt dient te worden beoordeeld of de gegevensbescherming effectief is. Dit geldt in het bijzonder bij grootschalige verwerking van bijzondere persoonsgegevens en profilering. Voor reisorganisaties is dit niet van toepassing omdat de verwerking doorgaans geen hoog risico voor de betrokkenen vormt.

Functionaris voor gegevensbescherming

Een functionaris voor de gegevensbescherming / data protection officer is nodig bij grootschalige verwerking van bijzondere persoonsgegevens. Kleine reisorganisaties zullen hier niet onder vallen. Uiteraard verdient het wel de aanbeveling om binnen de organisatie of extern een verantwoordelijke met kennis van het privacyrecht aan te wijzen die als taak heeft de naleving van de privacyregels binnen de organisatie te waarborgen.

Gedragscodes en certificering

De Privacyverordening stimuleert brancheverenigingen om een gedragscode op te stellen en deze te laten goedkeuren door de Autoriteit Persoonsgegevens. Door vervolgens aan de gedragscode te voldoen zal mogen worden verwacht dat de organisatie voldoet aan de normen van de Privacyverordening. Dit is een kostenefficiënte manier om concrete handvatten mee te geven op welke wijze reisorganisaties de privacy van klanten en personeel dienen te waarborgen. Praktische problemen bij de implementatie van nieuwe wetgeving zullen niet slechts bij één organisatie spelen. Een gezamenlijke aanpak werkt ook om die reden kostenbesparend.

Naast gedragscodes zullen er ook certificeringen voor privacy worden ontwikkeld door commerciële partijen die deze bevoegdheid hebben verkregen van de Autoriteit Persoonsgegevens. Afhankelijk van de prijsstelling van dergelijke certificeringstrajecten zal dit wel of geen reële mogelijkheid zijn voor reisorganisaties.

E-privacy (spam, cookies)

Er komt ook een E-privacy verordening die de bestaande richtlijn E-Privacy vervangt. In de verordening wordt het gebruik van cookies en ongevraagde communicatie gereguleerd en aangepast. Deze verordening is echter nog als Europees wetsvoorstel in behandeling.