Joost Maassen

Met een webshop verzamel je meestal persoonsgegevens

Hoe voldoe je aan alle privacy-wetgeving?

E-commerce rukt op, ook bij zakendoen over de grenzen. In deze laatste aflevering van een serie over grensoverschrijdende e-commerce beantwoordt Joost Maassen vragen over de privacyaspecten van jouw website. Zoals de regels voor het verzamelen van klantinformatie, cookies en marketing.

Joost Maassen is zowel Nederlands advocaat als solicitor of Engeland & Wales. Hij adviseert over Nederlands en Engels recht bij grensoverschrijdende zaken op het gebied van het vennootschaps-, handels-, contracten- en overnamerecht.

Is een privacyverklaring voor mijn webshop verplicht?

Wie een webshop heeft, verzamelt meestal persoonsgegevens. Op grond van de Algemene Verordening Gegevensbescherming (2016/679) (AVG) van de Europese Unie (EU) ben je in dit geval als verwerkingsverantwoordelijke verplicht de persoon van wie je persoonsgegevens verzamelt (verder 'data subject' genoemd), in een privacyverklaring te informeren over hoe je met deze gegevens omgaat. Wanneer een datasubject in de Europese Economische Ruimte (EER; de EU plus Noorwegen, IJsland en Liechtenstein) woont, dan geldt de AVG. Deze regelt wanneer en hoe lang je persoonsgegevens mag verwerken, hoe je daar verantwoording over aflegt, wat de rechten van datasubjecten zijn, hoe persoonsgegevens moeten worden beschermd en dat je een eventueel datalek moet melden. Wanneer je gegevens verzamelt over een persoon die buiten de EER woont, is meestal de privacywetgeving van zijn land van toepassing.

> "De datasubject moet bij toestemming voor het gebruik van zijn persoonsgegevens altijd een geïnformeerde beslissing kunnen maken"

Wat zijn persoonsgegevens?

Dit is alle informatie die direct over een persoon gaat, ofwel naar hem te herleiden is. Bijvoorbeeld naam, adres, geboortedatum, financiële gegevens of IP-adres. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens, maar wel die van een eenmanszaak of personen die bij een organisatie werkzaam zijn. Behoudens enkele uitzonderlijke gevallen is het verboden bijzondere persoonsgegevens te verwerken (zie artikel 9 AVG), tenzij de betrokkene hiervoor vóóraf uitdrukkelijk toestemming heeft gegeven.

Hoe zit het met bijzondere persoonsgegevens?

Bijzondere persoonsgegevens zijn gegevens over iemands ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie (denk aan foto's, films en identiteitsbewijzen), gezondheid, seksuele leven en strafrechtelijk verleden.

Wanneer ben ik een verwerkingsverantwoordelijke en wat is een verwerker?

Je bent een verwerkingsverantwoordelijke wanneer je het doel van en de middelen voor de werking van persoonsgegevens vaststelt. Een verwerker is iemand die voor een verwerkingsverantwoordelijke persoonsgegevens verwerkt. Bijvoorbeeld degene die jouw website onderhoudt of host, of een reclamebureau. Als verwerkingsverantwoordelijke blijf jij verantwoordelijk en moet je met de verwerker in een verwerkersovereenkomst afspraken maken over de verwerking, bijvoorbeeld of en zo ja onder welke voorwaarden persoonsgegevens de EER mogen verlaten.

Wat moet ik in mijn privacyverklaring opnemen?

De naam en contactgegevens van je bedrijf, de wettelijke grondslag voor de verwerking, wie de persoonsgegevens krijgt en hoe jij daaraan gekomen bent, de bewaartermijn, of de gegevens de EER verlaten, de rechten van de datasubject en hoe deze een klacht kan indienen. Een datasubject heeft het recht op inzage, vergetelheid, rectificatie en aanvulling, overdracht van de gegevens aan een andere partij, beperking van de verwerking, bezwaar en op een menselijke blik bij geautomatiseerde besluitvorming of profilering.

Wanneer en hoe lang mag ik persoonsgegevens verwerken?

Je mag persoonsgegevens verwerken wanneer en zo lang dat nodig is om de overeenkomst te kunnen uitvoeren (bijvoorbeeld naam, adres, bankgegevens), om aan een wettelijke verplichting te voldoen (bijvoorbeeld een fiscale bewaarplicht) of omdat je een gerechtvaardigd belang hebt. Dit laatste moet wel een *noodzakelijk* gerechtvaardigd belang zijn en het moet worden afgewogen tegen het belang van de datasubject. Daarnaast zijn er nog twee gronden die bij e-commerce minder zullen voorkomen: de acute bescherming van vitale belangen van een ander of het uitvoeren van een taak van algemene belang of openbaar gezag.
Tot slot mag je persoonsgegevens bewerken met toestemming van de datasubject. Het is meestal beter de verwerking zo veel mogelijk op een van de andere gronden te baseren. De toestemming kan namelijk altijd worden ingetrokken. Let op, bij kinderen weegt jouw gerechtvaardigd belang minder snel op tegen hun rechten en vrijheden. Bovendien heb je niet de toestemming van het kind maar van zijn ouders nodig.

Wat zijn de eisen die aan toestemming worden gesteld?

De toestemming moet vrij, ondubbelzinnig en voor een specifiek doel worden gegeven. Wanneer het doel verandert, moet je daarvoor apart toestemming vragen. De datasubject moet altijd een geïnformeerde beslissing kunnen maken. Dit houdt in dat je hem moet informeren over je organisatie, het doel van de verwerking en dat de toestemming altijd weer even gemakkelijk kan worden ingetrokken. Je moet bovendien kunnen aantonen dat je hieraan hebt voldaan.

Hoe zit het met cookies?

Cookies zijn bestanden die op het apparaat van de bezoeker van je website worden geplaatst.

Cookies zijn zowel aan de AVG als artikel 11.7a van de Telecommunicatiewet (TW) onderworpen. Dit artikel is een implementatie van de EU e-privacy richtlijn (2009/136). Je moet bezoekers van je website informeren over het gebruik en de werking van cookies en in bepaalde gevallen om toestemming vragen. Je hebt in beginsel geen toestemming nodig voor functionele cookies (cookies om je website goed te laten functioneren) en analytische cookies (cookies om inzicht in het functioneren van de site te krijgen), mits je die cookies alleen gebruikt om bezoekers te tellen en personen niet op grond van die cookies anders behandelt.

Bij het gebruik van trackingcookies verzamel je persoonlijke informatie, bijvoorbeeld het IP-adres. In dat geval moet je de bezoeker nader informeren over de verwerking van zijn persoonsgegevens en hem vooraf om toestemming vragen. De EU werkt momenteel aan een e-privacy verordening. Deze moderniseert en komt in de plaats van de e-privacy richtlijn en is bijvoorbeeld gericht op het gebruik van trackingmethoden en de beveiliging van communicatie.

Mag ik klantgegevens gebruiken voor digitale direct marketing?

Digitale marketing mag alleen nadat daarvoor toestemming is verkregen. Tenzij je iemand die eerder bij je heeft gekocht, benadert met aanbiedingen voor eigen soortgelijke producten en hij tegen dit gebruik van zijn gegevens geen verzet heeft aangetekend (artikel 11.7 TW). Dit verzet moet hij gemakkelijk en gratis kunnen doen, allereerst wanneer de persoonsgegevens worden verkregen en daarna iedere keer wanneer digitale marketing wordt verzonden. Het verstrekken van persoonsgegevens aan derden voor marketingdoeleinden is altijd aan toestemming onderhevig. Wanneer jij gegevens die door derden zijn verkregen gebruikt, moet je kunnen aantonen dat daarvoor toestemming is verkregen.

Wat is een verwerkingsregister en is dat verplicht?

Het verwerkingsregister bevat informatie over de doeleinden van de verwerking, de categorieën van datasubjecten, de soorten van persoonsgegevens die worden verwerkt, bewaartermijnen, ontvangers van de gegevens, buiten de EU gevestigde ontvangers en beveiliging. Je bent verplicht een verwerkingsregister bij te houden wanneer je organisatie meer dan 250 medewerkers heeft, je bijzondere persoonsgegevens verwerkt of gegevens die een hoog risico inhouden voor de rechten en vrijheden van de datasubjecten, en wanneer je niet incidenteel gegevens verwerkt. Dat laatste is bij een webshop al snel het geval.

Wanneer moet ik een functionaris gegevensbescherming aanstellen?

Dit moet als je een overheidsinstantie of bedrijf bent, die op grote schaal personen observeert of bijzondere of strafrechtelijke persoonsgegevens verzamelt. De functionaris gegevensbescherming moet je aanmelden bij de Autoriteit Persoonsgegevens.

Gelden binnen de EU dezelfde privacyregels?

Nee, dit komt omdat landen bij de uitvoering en implementatie van de AVG enige vrijheid hebben. Zo moeten in Nederland en Duitsland ouders toestemming geven voor de verwerking van persoonsgegevens van een kind tot zestien jaar oud. In Frankrijk is dit vijftien jaar en in België zelfs dertien jaar (de laagste grens volgens de AVG). Andere voorbeelden zijn de sancties op overtredingen en de invulling van het begrip bijzondere persoonsgegevens. Het is dus altijd zaak lokaal na te gaan hoe de AVG geïmplementeerd is en wordt uitgevoerd.

Hoe zit het met de verwerking van persoonsgegevens uit EER-landen buiten dit gebied?

Je mag, behoudens enkele uitzonderlijke gevallen, alleen persoonsgegevens doorgeven naar een land met een zogenaamd passend beschermingsniveau. Op de website van de Autoriteit Persoonsgegevens kun je zien welke landen dit zijn. Daarnaast heeft de EU een drietal modelcontracten gemaakt, die je kunt gebruiken voor een land zonder passend beschermingsniveau. Voor een grote multinational loont het wellicht om de EU toestemming te vragen voor zogenaamde Binding Corporate Rules voor interne grensoverschrijdende datastromen.

Vaak realiseren ondernemers zich niet dat hun website plug-ins of analysetools van derden gebruikt, waardoor persoonsgegevens toch de EU verlaten. Het onbedoeld verstrekken van die gegevens aan een derde brengt tevens met zich mee dat je de betrokkene daarover onterecht niet in je privacyverklaring hebt geïnformeerd of om toestemming gevraagd.

Wat houdt het ‘onestopshop-beginsel’ in?

Sinds de invoering van de AVG heb je in beginsel te maken met één toezichthouder, namelijk die van het land van je hoofdvestiging. Deze werkt vervolgens samen met de andere nationale toezichthouders, bijvoorbeeld bij een datalek.