Nieuwe privacywet (AVG) voor webwinkels

Voorjaar 2018

ECOOKIE
De AVG compliant cookiebar

Hoe webwinkels zich kunnen voorbereiden op de komst van de nieuwe privacywet

Webwinkels verzamelen persoonsgegevens van klanten en websitebezoekers. Denk hierbij aan namen, e-mail adressen, IP adressen, maar ook orderdata en website gedrag. Hierbij krijgen zij per 25 mei 2018 te maken met de nieuwe privacywet, de Algemene Verordening Gegevensbescherming (AVG). In dit whitepaper lichten wij toe hoe webwinkels zich kunnen voorbereiden op de komst van de nieuwe privacywet.

Grondslag

Een webwinkel moet onder de AVG een grondslag hebben om persoonsgegevens te verwerken. Deze grondslag kan verkregen worden doordat de klant toestemming geeft voor de verwerking van persoonsgegevens. Echter, het verwerken van persoonsgegevens kan ook zonder toestemming, bijvoorbeeld als de persoonsgegevens noodzakelijk zijn voor het uitvoeren van een overeenkomst tussen de webwinkel en de gebruiker. Om een pakketje te kunnen verzenden heb je immers naam- en adresgegevens nodig.

In de checkout van een webshop worden persoonsgegevens verwerkt zonder toestemming. Het gebruiken van persoonsgegevens voor het versturen van direct marketing mag alleen op basis van toestemming, hiervoor komen andere grondslagen niet in aanmerking. U als webshop eigenaar moet zelf inschatten welke verwerkingsgrondslag benodigd is.

Omgaan met data onder de AVG

Webwinkels slaan (in de meeste gevallen) bij voorkeur zoveel mogelijk persoonsgegevens op, voor bijvoorbeeld marketingdoeleinden. Persoonsgegevens mogen alleen verzameld worden voor een specifiek doel en moeten voor dat doel noodzakelijk zijn. Onder de nieuwe privacywet moet een webwinkel beoordelen welke persoonsgegevens noodzakelijk zijn voor het bereiken van dat doel. Met andere woorden: de webwinkel moet ervoor zorgen dat alleen gegevens worden gebruikt die noodzakelijk zijn om het doel te bereiken.

Privacyregister

Het opstellen van een privacyregister is een goede eerste stap om aan de slag te gaan met de nieuwe privacywet. Webwinkels zijn, net als alle andere bedrijven in Nederland die structureel persoonsgegevens verwerken of meer dan 250 werknemers hebben, verplicht om een privacyregister bij te houden. In dit privacyregister moet worden bijgehouden welke (categorieën van) persoonsgegevens worden verwerkt, wie de ontvangers van deze persoonsgegevens zijn en voor welke doeleinden deze persoonsgegevens worden gebruikt.

Binnen dit privacyregister moeten ook de bewaartermijnen worden bijgehouden. Zo is gemakkelijk bij te houden welke data wanneer verwijderd moet worden. Het privacyregister moet op verzoek van de Autoriteit Persoonsgegevens overhandigd kunnen worden. Deze verplichting geldt overigens niet alleen voor eigenaren van webwinkels, maar ook voor dienstverleners die de webwinkels van hun klanten runnen.

Verwerkersovereenkomsten sluiten

Webwinkels die persoonsgegevens verwerken doen dit in de meeste gevallen als ‘verwerkingsverantwoordelijke’. Dit betekent dat de webwinkel bepaalt welke persoonsgegevens worden verwerkt, met welk doel en met welke middelen. Veel webwinkels huren voor het verwerken van persoonsgegevens andere partijen in. Denk hierbij aan een websitebouwer, hostingpartij, e-mail service provider, data management platform of een e-commerce bureau.

De partijen die door de webwinkel worden ingeschakeld zijn ‘verwerker’ onder de nieuwe privacywet. De verwerkers hebben toegang tot de persoonsgegevens nodig om hun werkzaamheden te kunnen uitvoeren. De webwinkel met de verwerker een verwerkersovereenkomst sluiten. In deze verwerkersovereenkomst ligt vastgelegd voor welke doeleinden de verwerker de gegevens mag gebruiken, welke beveiligingsmaatregelen de verwerker moet nemen, hoe met datalekken wordt omgegegaan en of de verwerker eventuele subverwerkers of derde partijen mag inschakelen. Uit uw privacyregister blijkt met wie u een verwerkersovereenkomst moet sluiten.

Privacyverklaring

De meeste webwinkels hebben een privacyverklaring. Een webwinkel is verplicht klanten en bezoekers te informeren over de persoonsgegevens die de winkel verzamelt en met welk doel. De nieuwe privacywet stelt strenge eisen aan de informatievoorziening. Als een webwinkel van een klant een profiel opbouwt om gedrag of interesses te voorspellen, dan moet dit worden vermeld in de privacyverklaring. De nieuwe privacywet verplicht webwinkels verder om de privacyverklaring begrijpelijk te maken voor de gemiddelde lezer, en niet alleen voor juristen. De privacyverklaring moet gemakkelijk te vinden zijn op de website en de verklaring moet duidelijk en gemakkelijk leesbaar zijn.

Cookies

Iedere webwinkel gebruikt cookies of vergelijkbare technieken. De regels over cookies staan niet in de nieuwe privacywet, maar in de e-Privacywet. Deze wordt ook vernieuwd, maar dat zal waarschijnlijk niet meer in 2018 gebeuren.

Bij het gebruik van cookies onderscheiden we noodzakelijke cookies, analytische cookies en marketing cookies. Onder de huidige e-Privacywet mogen de noodzakelijke cookies zonder toestemming van de bezoeker geplaatst worden. De noodzakelijke cookies zijn bijvoorbeeld cookies die worden geplaatst tijdens het betalingsproces, als de betaling niet mogelijk is zonder deze cookies.

Voor analytische cookies hoeft onder voorwaarden geen expliciete toestemming verkregen te worden. Een goed voorbeeld van analytische cookies is de cookie voor Google Analytics. Voor de cookie van Google Analytics hoeft geen expliciete toestemming verkregen te worden, als Google Analytics privacy vriendelijk wordt ingesteld. De Autoriteit Persoonsgegevens heeft hier een handleiding over geschreven.

Voor marketing cookies moet toestemming worden gegeven door de bezoeker. Dit kan via een cookie banner. De scheidslijn tussen analytische cookies waar geen expliciete toestemming voor nodig is en marketing cookies waar wel expliciete toestemming voor nodig is, is soms dun. Kijk altijd kritisch of de desbetreffende cookie alleen wordt gebruikt om informatie te verkrijgen over de kwaliteit of effectiviteit van de website, en niet ook voor marketing doeleinden. Bij twijfel adviseert Yellowgrape om een gespecialiseerde privacy advocaat te raadplegen.

E-mail marketing en de nieuwe privacy wet

De meeste webwinkels versturen regelmatig een nieuwsbrief. De hoofdregel is al jaren dat dat vooraf aan de ontvanger toestemming moet worden gevraagd. Dit is jaren geleden onder de Telecommunicatiewet verplicht geworden. Het verkrijgen van toestemming kan door het actief laten aanvinken van een vakje waarin de klant toestemming geeft om zijn e-mailadres te gebruiken voor de nieuwsbrief.

De toestemmingsvraag moet onder de nieuwe privacywet voldoen aan een aantal vereisten. Zo moet duidelijk zijn waar de toestemming voor wordt gegeven, hoe vaak de ontvanger de nieuwsbrief mag verwachten en waar de nieuwsbrief uit zal bestaan. De webwinkel moet kunnen aantonen waar, wanneer en hoe de toestemming is verkregen, en onder welke voorwaarden (bijvoorbeeld welke privacyverklaring werd getoond).

Indien de webwinkel bij het versturen van nieuwsbrieven gebruikt maakt van ‘profiling’, dan moet de ontvanger hier apart toestemming voor geven. Wat is profiling precies? De Autoriteit Persoonsgegevens schrijft op zijn website het volgende: ‘Met big data kunnen organisaties mensen in groepen indelen. Ook kunnen zij big data gebruiken om het gedrag van mensen te voorspellen. Zowel groepsindelingen als voorspellingen worden ‘profiling’ genoemd.’

Met de komst van de nieuwe privacywet is de webwinkel verplicht om voor nieuwsbrieven waarbij gebruik wordt gemaakt van profiling een aparte toestemming te verkrijgen. Wanneer een bepaalde geautomatiseerde campagne onder ‘profiling’ valt, is een behoorlijk grijs gebied. De Autoriteit Persoonsgegevens zegt zelf het volgende: ‘Bedrijven kunnen dit doen voor verschillende commerciële doelen. Bijvoorbeeld om een specifieke winstgevende klantengroep te behouden of om gerichte advertenties te tonen op basis van voorspelde interesses. Of juist om ongewenste klanten te weren, zoals bij een aanvraag voor een lening.’ De eigenaar van de webwinkel zal dit van geval tot geval moeten bepalen.

Uitzondering voor bestaande klanten

In de Telecommunicatiewet staat een uitzondering voor het versturen van nieuwsbrieven aan bestaande klanten. Dit mag zonder toestemming als aan de volgende voorwaarden is voldaan: Het e-mailadres is verkregen bij de verkoop van een product of dienst (let op: dit betekent dat deze uitzondering niet geldt voor gratis producten of diensten);

1. Op het moment dat het e-mailadres werd verkregen, kon de ontvanger aangeven géén nieuwsbrieven te willen ontvangen (een 'opt-out');
2. De nieuwsbrieven gaan over dezelfde of vergelijkbare producten of diensten (de webshophouder mag bijvoorbeeld geen aanbiedingen voor auto's sturen, naar aanleiding van de aankoop van een telefoon);
3. De nieuwsbrieven zijn van hetzelfde bedrijf (dus niet van een moeder- of dochtermaatschappij); en
4. In iedere nieuwsbrief wordt de mogelijkheid geboden voor de ontvanger om zich uit te schrijven (een 'opt-out').

Zolang aan deze voorwaarden wordt voldaan, mag de webwinkel nieuwsbrieven versturen zonder daarvoor eerst toestemming te vragen.

Rechten van gebruikers

Elke gebruiker van wie persoonsgegevens worden verwerkt door een webwinkel heeft bepaalde rechten. De gebruiker heeft bijvoorbeeld recht op inzage. Dit betekent concreet dat de webwinkel inzage moet geven in de persoonsgegevens die worden gebruikt en waar die persoonsgegevens voor worden gebruikt. Daarnaast moet de webwinkel de gebruiker een kopie van zijn of haar persoonsgegevens verstrekken.

De gebruiker mag vervolgens verzoeken om rectificatie of verwijdering van de gegevens of de beperking van verwerking. Daarnaast moet de gebruiker in iedere nieuwsbrief de mogelijkheid worden geboden om zich uit te schrijven.

Yellowgrape adviseert webwinkels om tenminste de rechten van gebruikers duidelijk te omschrijven op de klantenservice-pagina en de procedure duidelijk uit te leggen. Een pragmatische aanpak kan het plaatsen van een contactformulier zijn, indien een klant gebruik wil maken van zijn rechten. De gegevens kunnen vervolgens per e-mail worden verzonden aan de klant. De webwinkel moet wel oppassen dat geen persoonsgegevens aan de verkeerde gebruiker worden verstrekt, dat zou immers een datalek zijn. Daarom moet de webwinkel eerst de identiteit van de gebruiker controleren, bijvoorbeeld doordat het ingevoerde e-mailadres overeenkomt met het emailadres waarmee het gebruikersaccount werd aangemaakt.

Een webwinkel maakt het zichzelf het makkelijkst als deze mogelijkheden worden ingebouwd in het klantaccount. De grootste uitdaging hierbij is dat de persoonsgegevens in de meeste gevallen in meerdere systemen worden bijgehouden.

Datalekprocedure

Als persoonsgegevens ongepland en/of ongewenst worden vernietigd of gewijzigd, of als er ongeoorloofde toegang tot de gegevens is geweest, dan kan sprake zijn van een datalek. In het geval van een datalek moet in sommige gevallen melding worden gedaan bij de Autoriteit Persoonsgegevens. Is de inbreuk zeer nadelig voor de gebruiker op wie de persoonsgegevens betrekking hebben, dan moeten ook de betreffende personen worden geïnformeerd.

Een voorbeeld van een datalek is wanneer een hacker toegang krijgt tot de webserver waarop de webwinkel draait. Een interne datalekprocedure is onmisbaar voor iedere webwinkel. Hierin is beschreven aan wie een datalek (intern) moet worden gemeld en hoe het datalek verder moet worden afgehandeld.

Beveiligingsmaatregelen

Een webwinkel is verplicht om passende technische en organisatorische beveiligingsmaatregelen te nemen om misbruik en ongeautoriseerde toegang tot persoonsgegevens tegen te gaan. Een webwinkel moet in ieder geval zorgen dat wachtwoorden gehasht worden opgeslagen en moet toegang tot persoonsgegevens logisch en fysiek beperken. Verder is een beveiligde verbinding in de checkout verplicht.

Yellowgrape en Hipex lanceren Ecookie, de kosteloze AVG-compliant cookiebar voor webshops

E-commerce bureau Yellowgrape en Magento-hosting specialist voor webshops Hipex hebben samen Ecookie ontwikkeld, een cookiebar die voldoet aan de Algemene Verordening Gegevensbescherming (AVG) die vanaf 25 mei a.s. van kracht is. Met Ecookie kunnen webshops noodzakelijke, analytische en marketingcookies met één klik onder controle houden. De cookiebar wordt gratis ter beschikking gesteld door Yellowgrape en Hipex, en kan eenvoudig worden aangepast aan de huisstijl van de webshop.

Over Yellowgrape

Yellowgrape helpt e-commerce organisaties bij het creëren van een krachtige mix van relevantie, unieke kansen en urgentie, met behulp van goede data en slimme software. Met totaal-strategieën helpt Yellowgrape bedrijven bij de transitie van snelle groei naar de volgende fase: duurzame groei.

Yellowgrape.nl
Johan Smits
johan@yellowgrape.nl
Bel +31 (0)20 244 0313

yellowgrape
de e-commerce marketeers

Over Hipex

Hipex is meervoudig recordbreker op het gebied van hosting performance. Ontwikkelaars prijzen de gebruiksvriendelijke en vooruitstrevende aanpak; het resultaat van het snel kunnen schakelen in kansrijke technieken. Andere kenmerken van Hipex zijn snelheid, stabiliteit en scherpe tarieven.

Hipex.io
Milan Bosman
milan@hipex.io
Bel +31 85 888 77 54

HIPEX