BURO BLANCHARD START CHECK PROTECT SELL
CREATIVE INDUSTRY BUSINESS SERVICES

EU Privacy & ePrivacy Wet

Je kunt het nauwelijks gemist hebben.

De EU Privacywet, Algemene Verordening Gegevensbescherming, (AVG) komt eraan. Tot nu toe kon ieder land binnen de EU-kaders zijn eigen Privacywet hebben. Met ingang van 25 mei 2018 is dat voorbij en geldt de EU Privacywet of AVG.

Uniformering
De essentie van de EU Privacywet is dus uniformering en een verdere versterking van de bescherming van persoonsgegevens en een grotere aantoonbare verantwoordelijkheid van organisaties om privacy rechten te waarborgen.

Persoonsgegevens
Persoonsgegevens zijn onder te verdelen in gewone en bijzondere.

Gewone persoonsgegevens zijn alle gegevens die direct of indirect een natuurlijk persoon identificeerbaar maken.
Daarbij gaat niet alleen om naam, adres, telefoonnummer, emailadres, etc. Zelfs als een persoon binnen een groep geselecteerd wordt zonder koppeling aan een naam (behavioural targeting) is sprake van persoonsgegevens.

Bijzondere persoonsgegevens zijn gegevens waaruit 'ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en (…) genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Kortom het gaat hier om bijv. medische, persoonsfraudegevoelige en inkomen gegevens.
Verwerking van dit soort gegevens is verboden, tenzij er een wettelijke uitzondering geldt dan wel uitdrukkelijk toestemming van betrokkene is verkregen.

Partijen en Verantwoordelijkheid
Bij persoonsgegevens zijn bijna altijd 3 partijen betrokken, te weten:

- De persoon die het betreft (betrokkene).
- Degene, die bepaalt voor welk doel en op welke wijze de gegevens worden verzameld (verwerkingsverantwoordelijke).
- En vaak is er ook nog sprake van een derde partij die in opdracht van de verantwoordelijke de gegevens verwerkt (verwerker).

De verwerkingsverantwoordelijke is altijd verantwoordelijk voor het nakomen van alle verplichtingen uit de wet. Ook als de verwerking is uitbesteed aan een verwerker. Dat betekent dat een deugdelijke verwerkersovereenkomst in dat geval een must is.

Met het oog op de komende wet dien je als mogelijk verantwoordelijke na te gaan of je bedrijf aan de regels voldoet. Daarnaast is van belang als je klanten adviseert of data voor hen verwerkt, dat dit gebeurt in overeenstemming met de AVG. Denk bijvoorbeeld aan promotionele kansspelen.

Er wordt met de nieuwe wet een nog grotere verantwoordelijkheid bij organisaties gelegd. Zo zal er aan de betrokkene toestemming gevraagd moeten worden om gegevens te mogen verwerken.

Tien stappenplan ter voorbereiding
Mede om die reden heeft de Autoriteit Persoonsgegevens een 10 stappenplan ter voorbereiding gepubliceerd.

1. Het begint er mee dat je ervoor zorgt dat iedereen in je bedrijf op de hoogte is met de nieuwe regels.

2. De betrokkene krijgt meer en verbeterde rechten. Aan het recht op inzage, inzicht in gebruik, correctie, bezwaar en verwijdering wordt het recht op data portabiliteit toegevoegd.

3. De verantwoordelijke krijgt een documentatieplicht en moet dus kunnen aantonen welke gegevens waarvoor verwerkt zijn, hoe ze verkregen zijn (toestemming) en met wie ze zijn gedeeld.

4. Soms is de verantwoordelijke verplicht een zogenaamd Privacy Impact Assessment uit te voeren. Hiermee worden de privacy risico's in kaart gebracht om maatregelen te kunnen nemen om die te beperken. PIA is in ieder geval vereist als systematisch en uitvoerig persoonsgegevens worden geëvalueerd of op grote schaal systematisch mensen worden gevolgd (winkelklantvolgsystemen).

5. Als verantwoordelijke organisatie moet je bij het ontwerp van nieuwe producten en diensten direct rekening houden met een goede bescherming van persoonsgegevens. Dat betekent tevens dat als default alleen gegevens mogen worden verzameld en verwerkt die nodig zijn voor het specifiek te bereiken doel. En ook dat geen vinkjes vooraf op 'ja' gezet mogen worden.

6. De verantwoordelijke organisatie moet een Functionaris Gegevensbescherming (FG) aanstellen als gegevensverwerking een kernactiviteit is en dat grootschalig gebeurt. Grootschaligheid hangt af van het aantal personen, aantal gegevens, de duur van de verwerking en het geografisch gebied. Een marktonderzoeker zal dus al snel een FG in house of extern moeten aanstellen.

7. Het verplicht melden van datalekken verandert niet wezenlijk, maar er worden wel strengere eisen aan registratie ervan gesteld.

8. Bewerkersovereenkomsten zullen in overeenstemming moeten worden gebracht met de nieuwe EU-wettelijke eisen.

9. Als de verantwoordelijke organisatie vestigingen in meer EU-lidstaten heeft of de gegevensverwerking in meerdere lidstaten effect heeft, dan doe je als verantwoordelijke nog maar zaken met een toezichthouder.

10. Als de gegevensverwerking is gebaseerd op toestemming van betrokkene, dan gelden daarvoor straks strengere eisen. Deze moet niet alleen uitdrukkelijk gevraagd worden. Ook moet je kunnen aantonen dat je geldige toestemming voor de verwerking hebt verkregen. En het moet even makkelijk zijn die weer in te trekken. Bovendien moet van elke verwerking worden vastgesteld of deze rechtmatig is, een gerechtvaardigd belang dient en proportioneel is gelet op het doel. En of niet met minder gegevens volstaan kan of had kunnen worden.

Grondslagen voor gegevensverwerking
Er zijn limitatief 6 grondslagen voor gegevensverwerking. De eerste is hiervoor onder 10 al genoemd, te weten de toestemming van betrokkene. Daarbij zijn dus additionele eisen en voorwaarden van toepassing zijn.
De overige grondslagen tot gegevensverwerking zijn gebaseerd op het feit dat deze noodzakelijk is:

- voor precontractuele maatregelen of uitvoering van een overeenkomst
- voor nakoming wettelijke verplichting
- voor uitvoering publieke taak
- voor behartiging van een gerechtvaardigd belang
- voor vrijwaring van een vitaal belang van betrokkene

In het bedrijfsleven zullen de meeste verwerkingen plaatsvinden vanwege de uitvoering van een overeenkomst. Dan hoeft er ook geen toestemming te worden gevraagd en gelden dus ook niet die extra zware eisen

Let wel op dat je ook dan niet meer gegevens vraagt/verwerkt dan noodzakelijk is. En dat je tot personen herleidbare gegevens niet langer bewaart, dan noodzakelijk is voor het te bereiken doel of wettelijk is vereist.

ePrivacy
Het belangrijkste dat op het gebied van ePrivacy wetgeving verandert is dat deze gelijk getrokken wordt met die op het gebied van de Privacy. En dat deze wetgeving straks geldt voor alle electronische (marketing)communicatiekanalen. Daarmee heeft deze wetgeving betekenis voor alle online reclame en marketing. Of dit nu gebeurt via email, Skype, Facebook of Whatsapp

Verder worden de boetes voor geval van overtreding geweldig opgehoogd. Tot zelfs een bedrag van € 20 miljoen of 4% van de wereldwijde omzet. En de regels worden van toepassing op ieder die zaken doet met afnemers/consumenten in de EU.

Cookies
Een grote verandering komt er op het gebied van cookies. De consument hoeft straks voor minder cookies om toestemming te worden gevraagd. Dit geldt met name de functionele cookies. Daarnaast is het de bedoeling dat de toestemming voor cookies straks via de browser geregeld kunnen worden. Die toestemming vereist wel een ondubbelzinnige actieve handeling van de consument. Deze moet aantoonbaar vrijwillig, specifiek met kennis van zaken en ondubbelzinnig instemmen met die cookies.
Uiteraard moet je die toestemming als consument-eindgebruiker altijd weer kunnen intrekken. Nieuw is dat de consument ieder half jaar aan dit recht herinnerd moet worden!

eMarketingcommunicatie & Opt-in
Grote impact zal het voornemen hebben voor contact met niet-klanten. Net als nu al geldt voor email marketing, geldt straks ook voor de andere eMarketingcommunicatiekanalen het opt-in systeem. Slechts voor telemarketing geldt een uitzondering. Daar is en blijft het bel-me-niet-register een alternatief.
Maar er mag straks niet meer anoniem (onbekend nummer) gebeld worden.

Met bestaande klanten mag over producten, die vergelijkbaar zijn met eerder afgenomen producten of diensten zonder toestemming contact worden opgenomen. Deze regel geldt voor alle kanalen. Voor andere communicatie moet vooraf specifiek toestemming worden gevraagd en verkregen.

Een sub onderwerp is hier de vraag van de dubbele opt-in, zoals deze in Duitsland verplicht is. Deze verplichting geldt niet in Nederland. Het zenden van een email naar aanleiding van de aanmelding/aanvraag met bevestigingslink is derhalve (nog) niet verplicht. Dit neemt niet weg dat voor het verhogen van de kwaliteit van je bestand een tweede opt-in zeer nuttig is. En dat voorkomt last met spam-filters. Bovendien maak je het zo onmogelijk dat de aanmelder het email adres van een ander gebruikt.

Metadata
Wezenlijk is verder dat de ePrivacy niet alleen eist dat de privacy van de inhoud van de communicatie gegarandeerd wordt maar in principe ook de bijbehorende metadata zoals bijvoorbeeld identiteit, datum, tijdstip en locatie.
Voor het gebruik van zowel inhoud als metadata moet uitdrukkelijk vooraf steeds toestemming worden gevraagd. Er is slechts een uitzondering voor klantgegevens die noodzakelijk zijn voor facturatie. En de eis leidt ook uitzondering als de metagegevens geanonimiseerd worden.

Advies
Voor vragen of advies bel (0650205672) of mail (frans@blanchard.nl) met Buro Blanchard