CHECKLIST AVG

VOOR JE WEBSITE

Checklist AVG voor je Website en Online Marketing

Vanaf 25 mei 2018 moet elke organisatie in Europa voldoen aan nieuwe wetgeving om persoonsgegevens te mogen verwerken en bewerken. Dat geldt dus ook persoonsgegevens op jouw website. Met deze checklist kun je bekijken of jouw website voldoet aan de eisen van de AVG.

Deze checklist wordt regelmatig bijgewerkt en uitgebreid. Deze versie is het laatst bijgewerkt op 28-04-2018.

1. Inventariseren en vastleggen

Sluit verwerkersovereenkomsten af met verwerkers van jouw website (bureau' s of andere partners) of pas deze aan. Verplichte onderdelen zijn:

- Verwerkingsduur;
- verwerkingsdoel van de privacy gevoelige gegevens;
- welke gegevens verwerkt worden;
- de manier waarop de waarborging geregeld is;
- én welke verplichtingen er gelden met betrekking tot veiligheid en controle.
- Omschrijf ook duidelijk in je overeenkomst welke taken en aan welke verantwoordelijkheden het bedrijf moet voldoen in verband met de echten en bevoegdheden van de betrokkenen.

Wat is een verwerkersovereenkomst?

Zodra een organisatie verwerking van persoonsgegevens uitbesteedt, moeten er volgens de AVG afspraken worden gemaakt over de verwerking. Die afspraken moeten 'schriftelijk' worden gemaakt. Dat mag ook zijn 'elektronisch', per e-mail bijvoorbeeld. Het document waarin deze afspraken worden vastgelegd noemen we vaak een verwerkersovereenkomst. Klik hier voor een model verwerkersovereenkomst.

Maak inzichtelijk wie (intern én extern) werkt met data die betrekking heef op jouw website. Breid je inventarisatie uit door onderstaande punten te doorlopen:

Webhosting partijen

Het hostingbedrijf waar jij jouw website op laat hosten heeft toegang tot alle gegevens op jouw website. Daarom dien je een verwerkersovereenkomst af te sluiten met je hosting partij.

Websitebeheerder en marketeers

Externe partijen hebben ook toegang tot jouw website. Ga na hoe zij hun zaken hebben geregeld en of je de juiste afspraken met ze hebt gemaakt. Ook hier zul je een verwerkersovereenkomst moeten opstellen.

Backup locaties

Waar en hoe worden backups opgeslagen van je website, database en mailboxen.

Plugins/modules

Log in als beheerder op je website en beantwoord de volgende vragen om de bovenstaande lijst verder uit te breiden. Bepaal per plugin/module welke gegevens er verzameld worden en of ze wel of niet opgeslagen worden.

Contactformulieren

Welke informatie vraag je van je gebruikers op? Is het toegestaan om deze gegevens te vragen? En waar worden ze opgeslagen?

E-commerce

Denk aan NAW- en bankgegevens van je klanten, maar ook aan het soort bestelde producten. Wanneer een consument producten koopt die een relatie hebben met bijvoorbeeld geloofsovertuigingen of politieke voorkeur dan mag je deze persoonsgegevens niet zomaar bewaren.

E-mailmarketing

Bekijk je huidige emaillijsten kritisch: voldoet jouw huidige database aan de nieuwe standaard? Kun je in jouw database achterhalen wanneer en hoe iemand een opt-in afgegeven heeft?

Als een consument uit jouw database verwijderd wil worden, heb je hier dan een procedure voor? Zet op papier hoe dit soort verzoeken verwerkt moeten worden.

Tip: Gebruik software zoals Mailchimp of Get Response voor je emailmarketing. Dan weet je er zeker van dat dit goed is geregeld. Mits je jezelf aan de regels houdt natuurlijk.

Een 'noreply@'-e-mailadres mag onder de nieuwe wetgeving niet meer. Als je dat nu gebruikt als afzender voor je (nieuwsbrief)mailverkeer, dan moet je dat aanpassen naar een adres waar de ontvanger wel naar kan mailen

---

Statistieken

Denk aan Google Analytics of Google Tag Manager: heb je in kaart welke gegevens er opgeslagen worden van je gebruikers en bezoekers?

2. Verantwoorden

Voor alle gegevens die je verzamelt op je website, moet je kunnen verantwoorden waarom je die verzameld. Zorg er dus voor dat je binnen de kaders van de wet blijft met de gegevens die je verzamelt. Als je op je website gegevens verzamelt en bewaart, mag dat alleen als één van onderstaande redenen van toepassing is:

A. Omdat dit is afgesproken in een overeenkomst
Denk bijvoorbeeld aan betaalde abonnementen op je website waarvoor je bankgegevens van personen nodig hebt.

B. Omdat de wet van je vereist om dit vast te leggen
Denk aan facturen met klantgegevens in je webshop die je ook voor je boekhouding nodig hebt volgens de regels van de belastingdienst.

C. Omdat je expliciet toestemming hebt gekregen om dit te doen
Denk aan een cookie melding op je website of een inschrijfformulier op je nieuwsbrief. Let erop dat:

- De toestemming vrijwillig is gegeven (men kan niet misleid of gedwongen worden)
- De toestemming expliciet is (geen vooraf aangevinkte checkbox dus!)

- De toestemming per onderdeel gegeven moet worden (bijv. als men zich aanmeldt voor een evenement, én men zich tegelijk kan inschrijven op de nieuwsbrief)
- De organisaties genoemd worden die de gegevens zullen verwerken
- De toestemming weer ingetrokken moet kunnen worden

Ga na hoelang de persoonsgegevens worden bewaard en of dit niet langer dan noodzakelijk is. Je zult namelijk moeten kunnen aantonen dat deze duur te rechtvaardigen is.

3. Procedures opstellen

Leg protocollen vast voor de verschillende situaties waar je mee te maken kunt krijgen in de toekomst. Zorg dat je helder hebt welke informatie zich op welke plekken bevindt, zodat je dat niet later hoeft uit te zoeken. Leg in elk geval de volgende procedures vast:

Verzoeken van personen

Alle data die je verzamelt, moet eenvoudig in te zien, aan te passen of te verwijderen zijn. Zorg ervoor dat je hier een systeem voor hebt dat jou de mogelijkheid geeft alle data te sorteren. Er zijn een aantal aanvullende rechten op basis van wat we hierboven hebben beschreven:

- Het recht om eigen gegevens in te zien, te corrigeren of te verwijderen
- Het recht om de gegevens op te vragen
- Het recht om bij de Autoriteit Persoonsgegevens een klacht in te dienen

Datalekken

In het geval van datalekken moet je volgens de wet binnen 72 uur de autoriteit persoonsgegevens én de betrokken personen informeren. Zorg er dus voor dat je vast hebt gelegd welke stappen je moet nemen, omdat tijd op zo'n moment kostbaar is.

Beveiligingsbeleid

Stel een beveiligingsbeleid t.b.v. het beschermen van data op en blijf dit beleid toetsen en verbeteren. Denk bij het opstellen van een beveiligingsbeleid de volgende onderdelen:

- Toegangscontrole, met gebruik van sterke wachtwoorden.
- Logging van handelingen rondom de persoonsgegevens
- Fysieke maatregelen voor toegangsbeveiliging
- Encryptie van bestanden met persoonsgegevens

- Steekproefsgewijze controle op naleving van het beleid
- Beheer van kopieën en back-ups
- Beveiliging van netwerkverbindingen

4. Informeren en toestemming vragen

Informeer de bezoekers van je website helder en transparant. Zorg dat je een privacyverklaring heb waar alle benodigde informatie in staat.

- Je bedrijfsgegevens
- Doeleinden (reden van de verwerking van de persoonsgegevens)
- Persoonsgegevens (en welke verwerk je)
- Recht van toestemming
- Recht op inzage, aanpassen en verwijderen
- Beveiligingsmaatregelen
- Cookies

Tip: Wanneer je een keurmerk hebt zoals een keurmerk van thuiswinkel.org of lid bent van een brancheverenigingkan je navragen wat zij voor je kunnen betekenen.

Privacyverklaring-pagina

Maak een pagina aan voor je privacyverklaring en zet hier een link van in de footer van je website zodat deze op ieder moment te benaderen is.

Cookiemelding

Vraag de bezoekers op je website bovendien ook expliciet om toestemming op de activiteiten die je hebt vastgelegd in je privacyverklaring of apparte cookie notice.

Functionele cookies

Functionele cookies zijn momenteel nodig om een website te laten werken. Een voorbeeld van een functionele cookie is het opslaan van de producten die de bezoeker in het winkelmandje plaatst. Ook als je ‘ingelogd blijven’ aanvinkt bij het inloggen, worden cookies geplaatst. Bij een later bezoek word je dan automatisch ingelogd, wat voor veel gebruikers erg prettig werkt. Deze voorbeelden vallen in de categorie functionele cookies.

Voor het plaatsen van functionele cookies hoef je volgens de wet geen toestemming aan de bezoeker te vragen.

Analytische cookies

Diensten zoals Google Analytics maken gebruik van analytische cookies. Door middel van deze cookies krijgen eigenaren van websites inzicht in het gebruik van hun website. De privacy van de bezoeker blijft met deze analytische cookies gewaarborgd. Met deze data kunnen websites geoptimaliseerd worden, waardoor je de gebruikerservaring voor bezoekers kunt verbeteren.

Voor analytische cookies die worden gebruikt om het verkeer op een website te analyseren, hoef je geen toestemming aan de bezoeker te vragen.

Hierover moeten bezoekers wel geïnformeerd worden in een cookie- of privacyverklaring.

Tracking-cookies

Tracking-cookies, ook wel marketingcookies, zijn cookies die binnen een domein of over verschillende domeinen gebruikt worden om surfgedrag van de bezoekers vast te leggen. Hiermee kunnen uiteindelijk gerichte aanbiedingen gedaan worden. Een bekend voorbeeld hiervan zijn de remarketingcampagnes van Google AdWords. Niet alleen Google AdWords maakt gebruik van tracking-cookies, ook socialmedia-accounts, nieuwsbrieven en partnersites maken gebruik van deze cookies.

Voor het bijhouden van persoonsgerichte gegevens is toestemming vereist. Nadat een gebruiker geaccepteerd heeft dat cookies worden bijgehouden, mogen deze cookies worden geplaatst.

Het informeren of toestemming vragen aan de bezoekers van je website doe je d.m.v. een cookie melding.

Maak je gebruik van een cookiewall? Dan voldoe je vanaf de invoering van de Europese cookiewet niet meer aan de privacyvoorwaarden van de EU. De volledige toegang tot een website is volgens de EU essentieel voor internetgebruikers om (digitaal) te communiceren.

Gebruik van Google Analytics

Om Google Analytics te mogen blijven gebruiken, is het van belang om aan bepaalde voorwaarden te voldoen, zoals onder andere een bewerkingsovereenkomst met Google Analytics af te sluiten. Ook is het van belang om het IP-adres anoniem te maken en het delen van statistieken met Google uit te zetten. Analytische cookies werken ook met een unieke code waaraan een bezoeker te herkennen is.

Gebruik van tracking en re-marketing

Voor online marketeers heeft de wetswijziging veel invloed. De eindgebruiker gaat in de toekomst beslissen of jij gebruik kunt maken van tracking-cookies. Als een eindgebruiker beslist om de tracking-cookies te accepteren, mogen de cookies worden geplaatst. Als een bezoeker beslist om de tracking-cookies niet te accepteren, dan mogen deze tracking-cookies dus niet geplaatst worden op het apparaat van de gebruiker.

Dit is geen juridisch artikel en hieraan kunnen geen rechten worden ontleend.