AVG / GDPR:

DEZE AANPASSINGEN AAN JOUW NIEUWSBRIEF EN WEBSITE ZIJN NODIG

Digital **Hosting**

WP **S**ite **C**are

Digital **Concepts**
van strategie tot realisatie

Je bent ongetwijfeld op de hoogte van de aankomende Privacywet, oftewel de GDPR of AVG (Algemene Verordening Gegevensbescherming). Deze wet gaat in op 25 mei 2018 en heeft ook voor jou consequenties. Deze Europese wet dwingt bedrijven ertoe maatregelen te nemen om aan de nieuwe verplichtingen te voldoen. Er zijn meer dan genoeg artikelen die dit volledig uitleggen. Dit artikel is bedoeld voor degenen die geen zin hebben om ze allemaal door te spitten. Niet voldoen aan deze wet kan boetes tot gevolg hebben. Aangezien elke (WordPress) website aan enige mate van persoonsgegevensverwerking doet, is het raadzaam om stappen te ondernemen.

1. Hoe om te gaan met de nieuwsbrief?

Vaak verzamelt je website e-mailadressen via een contact-, aanvraag- of inschrijfformulier, waarbij standaard de optie 'Schrijf me in voor de nieuwsbrief' staat aangevinkt. Vanaf 25 mei moet de bezoeker dit zelf aanvinken en wordt hij/zij dus niet meer automatisch ingeschreven voor een nieuwsbrief tenzij daar bewust voor gekozen is. Dit is dus een actieve handeling.

Je dient al je e-mail opt-ins 'registreren'. Achteraf moet je kunnen aantonen hoe je ze hebt verkregen en waarvoor deze personen precies toestemming hebben gegeven. Zo moet je dus onderscheid maken tussen opt-ins die worden verkregen als iemand een bestelling doet en bijvoorbeeld voor opt-ins die verkregen hebt via een pop-up of lead magnet (een gratis aanbod dat je doet aan je bezoeker in ruil voor het e-mailadres van deze bezoeker).

Let op! Kun je dit niet aantonen voor je huidige klantenbestand? Zorg dan nu eerst voor een e-mail met daarin een opt-in voor de daadwerkelijke e-maillijst, van waaruit je vervolgens gaat e-mailen. Alleen mensen die zich dan actief aanmelden zul je mogen blijven mailen. Overigens mag je klanten met wie je een betaalrelatie hebt, nog wel zonder actieve opt-in mailen over soortgelijke producten of diensten (yes!). Zelf zou ik altijd het zekere voor het onzekere nemen, heel transparant blijven communiceren én altijd een heel duidelijke opt-out bieden (mogelijkheid tot uitschrijving).

Tip! Stel een automatische mailing in om de nieuwe abonnees te verwelkomen. Zet hierin een aantrekkelijke (!) welkomsttekst met de informatie dat de ontvanger vanaf nu mail kan verwachten én die duidelijke opt-out. Vergeet daarin niet de links naar al je socialmedia-accounts te vermelden. Misschien wil de ontvanger geen nieuwsbrief van je, maar je wel volgen via social media.

Extra to-do's voor je nieuwsbrief

- Zorg dat alle opt-ins die je hebt binnen je website, shop, social media en landingspagina's voldoen aan de eisen die hierboven staan beschreven. Vergeet ook je lead-magnets niet!
- Als iemand nog geen 16 jaar is, moet iemand met ouderlijk gezag (mede)toestemming geven
- Overbodig om te vermelden eigenlijk, maar toch: je mag iemand natuurlijk niet meer mailen als iemand zich uitschrijft voor je nieuwsbrieven
- 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
- Alleen iemands naam en mailadres vallen onder 'gewone informatie' die je mag opvragen. Vraag je bijvoorbeeld om een geboortedatum, dan moet je laten weten waarom (een verrassing op je verjaardag). Zulke data niet verplicht moeten zijn om je te kunnen aanmelden.
- Ga na of de softwareleverancier van jouw nieuwsbrief AVG-proof is

2. Recht om vergeten te worden - Website

Accounts en profielen moeten (zo eenvoudig mogelijk) in te zien, aan te passen of te verwijderen zijn. Mensen met een account bij een website (vaak bij webshops of online cursus omgeving) kunnen wellicht al een aantal gegevens zelf inzien en wijzigen. Het is aan te raden om een plug-in te installeren waarbij de gebruiker haar/zijn eigen account kan opzeggen waarmee alle informatie verwijdert wordt. Houdt er wel rekening mee dat eventuele back-ups deze gegevens voor een bepaalde periode nog bevatten.

3. Recht om vergeten te worden - Nieuwsbrief

Hetzelfde (zie punt 2) geldt voor e-mailvoorkeuren die gewijzigd kunnen worden binnen programma's zoals MailChimp. Men moet zich ook specifiek kunnen afmelden voor dataprofilering. Dit is – heel eenvoudig gesteld – het opdelen van de doelgroep in groepen, zodat je deze een nog beter toegespitste boodschap kunt voorleggen, die hoogstwaarschijnlijk eerder leidt tot conversie.

MailChimp doet dat al en geeft dat ook aan in de footer van een nieuwsbrief, er staat dan zoiets als 'klik hier om jouw profiel te wijzigen'. Dit geldt ook voor het verwijderen van gegevens (het recht om vergeten te worden). In de privacyverklaring moet daarom ook heel staan hoe mensen hun gegevens kunnen wijzigen of verwijderen.

4. Check je contactformulier

Schrijven mensen zich via je website in voor bijvoorbeeld een training? Kopen ze producten via je webshop? Of worden er gegevens verstuurd via een contact-formulier? Dan is de kans groot dat deze gegevens ook worden opgeslagen binnen WordPress. Wel zo handig, maar je moet je bezoekers hierover gaan informeren.

In een plug-in als Gravity of Ninja Forms worden gegevens automatisch opgeslagen binnen WordPress. Om aan de AVG/GDPR te voldoen, voeg je een checkbox toe aan het formulier waarbij de bezoeker aanvinkt akkoord te gaan met het versturen en opslaan van deze gegevens. Deze box is uiteraard een verplicht veld en zonder akkoord wordt het niet verstuurd. Je kunt onder andere met onderstaande plug-ins zo'n checkbox aan je contactformulier toevoegen.

AVG/GDPR Plugins voor formulieren

Onderstaande plug-ins voor WordPress kunnen je helpen met de instellingen:

- The GDPR Framework door Codelight
- WP GDPR door Appsaloon
- WP GDPR Compliance door Van Ons

We kunnen je hier natuurlijk ook mee helpen.

5. Gebruik je Google Analytics of Hotjar?

Bijna iedere site gebruikt Google Analytics om het gedrag van zijn of haar bezoekers te analyseren. Heeft jouw website dit nog niet? Start hier dan snel mee! Het is handig om te zien wat er wel of niet werkt op je site en waar bezoekers voor terugkomen.

Na de ingang van de AVG/GDPR kun je Google Analytics nog steeds gebruiken, maar dan zijn er wel een paar aanpassingen nodig.

- Sluit binnen jouw Google Analytics-account een Verwerkersovereenkomst af met Google
- Sla IP-adressen anoniem op; het laatste deel van het IP-adres is dan niet meer zichtbaar
- Deel geen gegevens meer met Google; in je account kun je instellen dat de Analytics gegevens niet meer gedeeld worden met Google, andere Google-producten en technische ondersteuning

Belangrijk

Informeer je websitebezoeker: vertel in je privacy statement hoe je de gegevens via Google Analytics verwerkt. Geef bijvoorbeeld aan dat de gegevens anoniem worden opgeslagen en niet worden gedeeld met anderen.

In deze Handleiding Privacy vriendelijk instellen van Google Analytics op de site van Autoriteit Persoonsgegevens worden deze aanpassingen verder uitgelegd. Gebruik je een tool als Hotjar, dan dien je soortgelijke stappen te zetten om bepaalde gegevens anoniem te maken.

6. Pas je privacyverklaring aan

Bezoekers van je website moeten kunnen inzien wat je met hun persoonsgegevens doet. Dit is dus een goed moment om je privacyverklaring te controleren of aan te maken als je deze nog niet hebt. In dat statement vertel je welke gegevens je verzamelt en waarvoor je ze gebruikt. Niet met moeilijke woorden en vage zinnen, maar gewoon in begrijpelijke taal.

Je privacy verklaring moet deze onderwerpen bevatten:

- Bedrijfsgegevens
- Doeleinden (reden van de verwerking van de persoonsgegevens)
- Persoonsgegevens (welke persoonsgegevens verwerk je?)
- Recht van toestemming
- Recht op inzage, aanpassing en verwijdering
- Beveiligingsmaatregelen
- Cookies

Op de website van Frankwatching staat meer informatie over welke gegevens in je privacyverklaring moeten komen. Maak het jezelf makkelijk door je privacyverklaring op te stellen met de volgende tools:

- Privacyverklaring generator van Veiliginternetten.nl
- Privacy Policy Generator van WebwinkelKeur.
- Privacy Policy Generator van Thuiswinkel

De privacyverklaring moet heel eenvoudig te vinden zijn op je website. Geef deze dan ook een geheel eigen pagina, een link in de footer én op elke plek waar je persoonsgegevens verzamelt.

7. Cookiebeleid is aangepast

Cookies zijn tekstbestanden die jouw persoonlijke instellingen voor een bepaalde website opslaan op jouw apparaat. Dit zijn soms instellingen waar je zelf wat aan hebt, maar vaak ook instellingen waar de eigenaar van de website (en zijn marketingteam) wat aan heeft. Er is onderscheid te maken in drie soorten cookies:

- **Functionele cookies -** Dit zijn cookies die nodig zijn voor het goed functioneren van een website of zorgen ervoor dat je een website makkelijker kunt gebruiken.
- **Analytische cookies -** Deze cookies worden geplaatst om het gedrag van de bezoeker op de website te meten en zo te kunnen analyseren. Vaak wordt dit gedaan met Google Analytics
- **Tracking cookies -** Tracking cookies worden gebruikt om jouw surfgedrag binnen één of meerdere websites op te slaan.

De nieuwe AVG/GDPR wetgeving zorgt voor het verdwijnen van cookiemuren (schermvullende meldingen dat een website cookies wil plaatsen en dat je akkoord moet gaan). In het kader van transparantie moet de informatie op je website voor iedereen beschikbaar zijn en niet alleen als je analytische en tracking cookies accepteert. Met deze regel is een cookiemuur dus niet meer interessant en die zullen we dan ook snel uit het internetlandschap zien verdwijnen.

Laten we er even vanuit gaan dat jij helemaal marketing-minded bent. Je wilt zoveel mogelijk cookies plaatsen om maximaal rendement uit je online marketingbudget te halen. Technisch moet je dan waarschijnlijk de volgende aanpassingen gaan doorvoeren:

- Zorg dat er geen cookies waar toestemming voor nodig is, geplaatst worden bij het openen van de website.
- Keuzemogelijkheid maken voor het plaatsen van cookies. Je bezoeker moet de mogelijkheid hebben om een cookie of cookiecategorie aan- of uit te zetten.
- Opslaan van de keuze van de bezoeker. Je moet aan kunnen tonen dat iemand expliciet toestemming heeft gegeven.
- Gemakkelijke opt-out mogelijkheid maken. Als een bezoeker besluit geen toestemming meer te geven voor cookies moet hij dat gemakkelijk aan kunnen geven/aan kunnen passen.
- Je cookiepagina updaten met een duidelijke uitleg over welke zaken je meet met welke doeleinden.

8. Heb je al een SSL-certificaat?

Een website waar persoonsgegevens worden verwerkt, moet beveiligd zijn met een SSL-certificaat. Dit is te herkennen aan **https://** met een slotje in de adresbalk. Sites zonder certificaat zijn te herkennen aan http:// (zonder s). Bovendien heeft Google aangekondigd dat websites met een https-protocol voorrang hebben op websites met een http-protocol. Je komt met een certificaat dus hoger in Google.

Let op

Heb je geen contactformulieren, maar gebruik je wel Google Analytics om het gedrag van je websitebezoeker te analyseren? Ook dan ben je verplicht om https in te stellen, aangezien je daarmee IP-adressen registreert.

9. Zorg voor een up-to-date website

Zorg voor een goede en veilige hostingpartij en het adequaat updaten van WordPress, het thema en de plug-ins om beveiligingslekken te minimaliseren. De gemiddelde WordPress website moet tussen de 150 en de 250 keer per jaar ge-update worden. Dat is bijna elke werkdag een update. En eigenlijk mag je er niet een missen... Wij hebben een onderhoudscontract waarbij we deze werkzaamheden voor je uitvoeren.

10. Veilig versturen van informatie

Wanneer e-mail of bestanden met persoonsgegevens worden verstuurd, zorg dan voor een veilige methode en/of het versleutelen van bestanden. Dit kan bijvoorbeeld al door de website geen mails meer te laten versturen maar d.m.v. een beveiligde verbinding met de mailserver te laten versturen. Dit zorgt er vaak ook voor dat mail minder vaak als spam gezien wordt.

11. Meld het wanneer er een datalek is

De meldplicht voor datalekken kennen we al in Nederland. Deze is ook in de AVG-wet opgenomen. Concreet betekent het dat je in actie moet komen wanneer er per ongeluk (of opzettelijk) data op straat terecht komt. Dit moet je melden bij het meldloket datalekken Autoriteit Persoonsgegevens. Houdt het lek waarschijnlijk een hoog risico in voor de personen waar de gegevens betrekking op hebben? Dan moeten zij ook van het lek op de hoogte worden gesteld.

12. Bewerkersovereenkomsten

Je hebt een bewerkersovereenkomst (ook wel DPA – *data processing agreement* genoemd) nodig met alle partijen die toegang hebben tot de persoonsgegevens die jij verzamelt. Dit is het vervelendste punt van die hele AVG/GDPR, hoewel het niet nieuw is. De verwachting is dat er veel strenger gecontroleerd gaat worden en ook zijn er een aantal verplichte zaken bijgekomen.

Het betreft dus een overeenkomst die je afsluit met partijen als Google Analytics, MailChimp, hostingbedrijf, webbouwer, programmeur, et cetera. De overeenkomst biedt garanties dat de bescherming van de rechten van personen wordt gewaarborgd. Als er problemen ontstaan, kan de verwerker hier verantwoordelijk en aansprakelijk voor zijn.

Maak een lijstje van de partijen waarmee jij samenwerkt inzake de verwerking van persoonsgegevens. Ga na hoe dit eventueel nu is geregeld. Er bestaat een grote kans dat de betreffende partij al zo'n overeenkomst heeft klaarliggen. Is er geen overeenkomst, zorg dan dat dit in orde komt. Er zijn diverse modelovereenkomsten in omloop, zoals deze van Juridox. Veel meer over bewerkingsovereenkomsten lees je bij Justitia.

Tot slot, waar gaat het nu echt over?

Het belangrijkste doel van de Privacywetgeving is dat je als organisatie bewust wordt van het omgaan met persoonsgegevens en jouw bezoekers hierover informeert. Je bezoekers moeten actiever goedkeuring geven voor het opslaan van deze gegevens. Daar is niets mis mee en helemaal niet zo ingewikkeld! Het is zo geregeld en een fijn idee dat je goed omgaat met de gegevens van jouw bezoekers.

Op het moment dat gebruikers persoonsgegevens achterlaten op je website, bijvoorbeeld met een e-mail opt-in, moet voor deze gegevens helder zijn waarom je ze nodig hebt en hoe je ze gaat gebruiken. Je moet bij het verzamelen van gegevens altijd verwijzen naar de privacyverklaring van jouw website of onderneming.

Voor de duidelijkheid: een opt-in is waar de eigenaar van een e-mailadres expliciet en aantoonbaar toestemming geeft voor het ontvangen van e-mail van een bepaalde mailinglist. Een opt-out daarentegen is exact het tegenovergestelde: waar je je kunt afmelden.

Heb je onze hulp nodig?

Neem dan contact met ons op via info@digitalconcepts.nl.