Belangrijke informatie over je website: AVG/GDPR wetgeving

Vanaf 25 mei 2018 moet elke organisatie in Europa voldoen aan nieuwe wetgeving om persoonsgegevens te mogen verwerken en bewerken. Dat geldt dus ook voor de verwerking van persoonsgegevens op jouw website.

Waarschijnlijk heb je al van de AVG / GDPR gehoord (Algemene verordening gegevensbescherming / General Data Protection Regulation).

Wat is het doel van AVG?

Doel van de Algemene verordening gegevensbescherming is het versterken en uitbreiden van privacyrechten, het scheppen van meer verantwoordelijkheden voor organisaties en het creëren van dezelfde bevoegdheden voor alle Europese privacytoezichthouders (zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen).

Wat betekent dit voor je website?

De Algemene verordening gegevensbescherming heeft betrekking op de gegevensverwerking binnen je gehele bedrijf. Lees hier meer over op de website van Autoriteit Persoonsgegevens. Wij willen je in dit document informeren over een de voorwaarden waaraan je website na 25 mei moet voldoen:

- Privacyverklaring
- Cookiegebruik
- SSL Certificaat
- Contactformulieren
- Dataverwerkers (Google Analytics, MailChimp, Hostingpartij)
- Security/Updates

Privacyverklaring

Een privacyverklaring is vanaf 25 mei verplicht. In begrijpbare taal en zo beknopt en duidelijk mogelijk. Hierin leg je uit welke (persoons)gegevens je waar verzamelt, waarom en wat ermee gebeurt. Daarnaast geef je mogelijkheden om persoonsgegevens op te vragen, te verwijderen of te verplaatsen naar een concurrent. Je noemt ook de verantwoordelijke binnen het bedrijf die gaat over privacy.

Cookies

Voor iedere cookie die een bezoeker apart kan identificeren, moet toestemming worden gegeven. Hierdoor kun je bezoekers niet meer ongevraagd over verschillende websites volgen. We onderscheiden drie verschillende soorten cookies, ieder met zijn eigen regels:

- *Functionele cookies*: functionele cookies zijn soms 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. ***Geen toestemming nodig, geen meldingsplicht***

- *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. ***Geen toestemming nodig, wel melding van cookiegebruik in 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. ***Expliciet toestemming nodig, wel melding van cookiegebruik in privacyverklaring***

SSL-certificaat (https)

Met een SSL-certificaat versleutel je het dataverkeer van en naar je website. Er komt dan HTTPS voor je URL (een groen slotje), waaraan bezoekers kunnen zien dat hun gegevens versleuteld worden verzonden. Verstuur je formulieren of nieuwsbriefaanmeldingen via je website? Dan is HTTPS verplicht. Ook als je geen persoonsgegevens verstuurd is SSL (bijna) verplicht want vanaf juli 2018 gaat Google websites zonder SSL als onveilig markeren.

Contactformulieren

Hiervoor geldt: vraag alleen gegevens die je echt nodig hebt om je doel te bereiken. Vaak genoeg worden al je contactgegevens uitgevraagd, terwijl de follow-up van een aanvraag bijvoorbeeld digitaal verloopt (complete adresgegevens zijn dan niet nodig). Kunnen er velden weggelaten worden? Bijkomend voordeel: kortere formulieren converteren doorgaans beter.

Vraag je gevoelige informatie uit op je website? Vraag je dan af of dit ook via een alternatieve route kan, die beter te beveiligen is. Een bijlage met bijvoorbeeld medische informatie kun je ook achteraf laten versturen via secured e-mail. Benoem het doel van deze gegevens in je privacy policy, zodat duidelijk is voor welk doel de gegevens wel (en ook vooral waarvoor ze niet) worden gebruikt.

Ingevulde formulieren krijg je meestal via de mail binnen. Vaak worden de berichten ook in de database en/of het CMS opgeslagen. Vraag jezelf af of dit echt nodig is. En als dit nodig is (bijvoorbeeld als backup wanneer een mail niet aankomt of per ongeluk wordt verwijderd), hoe lang je ze dan wilt bewaren. Je kunt deze bijvoorbeeld na x dagen automatisch laten verwijderen.

Dataverwerkers

Externe partijen die toegang hebben tot gegevens van jouw website zijn databewerkers. Met deze partijen moet een verwerkersovereenkomst afgesloten worden.

- *Google Analytics*: Als je Google Analytics in je website (tracking cookie) gebruikt, dan moet je een overeenkomst sluiten met Google. Google is namelijk een dataverwerker die je toestemming geeft om de persoonsgegevens van jouw bedrijf te verwerken. Daarnaast moet het IP-adres van de bezoeker, dat is namelijk ook een persoonsgegeven, geanonimiseerd worden.
- *MailChimp*: Ook de externe partij waarmee je je nieuwsbrief verstuurt, is een dataverwerker waarmee je een overeenkomst afgesloten moet worden. Een e-mailadres en klikgedrag zijn persoonsgegevens.
- *Hosting partij*: Ook met de partij die de website beheert moet een verwerkersovereenkomst afgesloten worden. Van de persoonsgegevens die op je website worden gebruikt, wordt een backup opgeslagen op de server van de hostingpartij en/of zij hebben vaak toegang tot de gegevens voor beheerdoeleinden.

Security/Updates

Na oplevering van de website is de site eigenaar verantwoordelijkheid voor de veiligheid ervan. Denk hierbij aan het pro-actief beveiligen van je website, het op de juiste manier updaten van scripts / plugins en het maken van back-ups. Ben je hier niet goed in thuis of ontbreekt het je aan de tijd om dit te doen? Dan kun je deze taken d.m.v. een beheer- en onderhoudsovereenkomst aan ons overdragen.

Je site AVG-proof maken

Wil je meer weten over de te nemen maatregelen m.b.t. je website? Wij kunnen je helpen. Tegen eenmalige kosten passen we de site aan zodat hij voldoet aan de nieuwe regelgeving.

1. *Privacyverklaring*
   - Opstellen/aanpassen
   - Toevoegen aan de site
2. *Cookiegebruik:*
   - in geval van gebruik trackingcookie: AVG compliant cookiemelding op de site plaatsen
   - een alternatief is het verwijderen van de code die trackingcookies plaatst, in dat geval is een AVG compliant cookiemelding niet noodzakelijk
3. *SSL Certificaat:*
   - SSL certificaat activeren
   - Site strict over https laten lopen (groen slotje in de browser).
   - De eventuele kosten voor aanschaf van een SSL certificaat zijn voor rekening van de site eigenaar
4. *Contactformulieren*:
   - Check op overbodige velden in de gebruikte formulieren in de site.
   - Check op de noodzaak om formuliergegevens in de database van de site op te slaan.
5. *Dataverwerkers (Google Analytics, MailChimp, Hostingpartij):*
   - Aanvragen van verwerkersovereenkomst bij Google en Mailchimp (indien van toepassing) en hostingpartij.
   - Aanpassing van de Google Analytics tracking code met geanonimiseerde IP-adressen.
6. *Security/Updates:*
   - Voor het up to date houden van de scripts en plugins bieden wij een jaarlijks onderhoud- en beheerovereenkomst, zie details in de bijlage.

Wij kunnen je assisteren bij het "AVG-proof" maken van je website. Op basis van een scan op bovenstaande punten passen we de site aan waar dat nodig is. De kosten hiervan zijn afhankelijk van wat er gedaan moet worden en variëren tussen de €150,- en €350,-. Neem contact met ons op voor het maken van een afspraak en/of meer informatie.

Sancties en boetes

Indien na 25 mei de website niet aangepast is conform bovenstaande punten dan kan de Autoriteit Persoonsgegevens een boete opleggen van maximaal € 20.000.000,- of 4 % van de wereldwijde jaaromzet (welke van de twee hoger is). In de praktijk worden dit soort boetes feitelijk niet opgelegd.

De Autoriteit Persoonsgegevens is dus spaarzaam met het uitdelen van boetes. Dat valt te verklaren omdat boetes een bestraffend instrument zijn, terwijl de Autoriteit Persoonsgegevens nu juist als taak heeft corrigerend op te treden. Omdat de privacywetgeving zeer complex is lijkt de Autoriteit Persoonsgegevens ervan uit te gaan dat een overtreding bijna altijd per ongeluk plaats vindt. Daarom kiest de Autoriteit er bijna altijd voor om overtreders eerst te waarschuwen en te gebieden de

verwerking te staken. Mocht zo'n waarschuwing niet worden opgevolgd dan legt de Autoriteit een last onder dwangsom op. Wanneer de overtreder dan zijn processen niet aanpast binnen een bepaalde periode is hij de dwangsom verschuldigd. Sinds 2011 is de dwangsom in 87 gevallen opgelegd, dat is in ongeveer 15 % van de onderzoeken.

Het is niet waarschijnlijk dat de Autoriteit Persoonsgegevens haar boetebeleid drastisch gaat veranderen met de GDPR. Immers, onder de Wet bescherming persoonsgegevens kon zij ook al boetes uitdelen.

De kans op een boete is redelijk klein. Toch zijn er veel goede redenen om de privacy van klanten serieus te nemen. Overtreding kan tot imagoschade leiden, de media is happig op berichten over privacyschendingen. De belangrijkste reden om aan de GDPR te voldoen is dat privacy tegenwoordig nu eenmaal onderdeel is van een goede bedrijfsvoering. Klanten accepteren privacy-inbreuken niet meer. Ook B2B-klanten, want zij weten dat een privacyinbreuk bij hun toeleveranciers ook op hen afstraalt.

Meer informatie / bronnen

- autoriteitpersoonsgegevens.nl: AVG nieuwe Europese privacywetgeving
- thuiswinkel.org: AVG: De rechten van betrokkenen
- security.nl: Juridische vraag: is webshop verplicht accounts op te heffen?
- ictrecht.nl: functionele cookies
- econsultancy.com: GDPR: 10 examples of best practice UX for obtaining marketing consent
- veiliginternetten.nl (initiatief van de overheid): privacyverklaring
- Frankwatching: Zo is je privacyverklaring AVG/GDPR-proof
- ictrecht.nl: privacyverklaring
- Lexxit.nl: GDPR-boetes, laat je niet bangmaken