SIERONLINE
thuis in websites, -shops en -techniek

Uw website en de nieuwe EU privacy wet AVG (Algemene verordening gegevensbescherming)

Vanaf 25 mei 2018 treedt de nieuwe EU privacy wet AVG omtrent persoonsgegevens in werking. Sieronline heeft uitgezocht wat dit voor u en uw website betekent en helpen met dit document je website te waarborgen voor deze nieuwe wetgeving.

Als eigenaar van uw website houdt het in dat u moet zorgen dat uw website moet voldoen aan deze regelgeving.

Elke organisatie in Europa moet voldoen aan de nieuwe wetgeving om persoonsgegevens te mogen verwerken en bewerken. Dit geldt dus ook voor de persoonsgegevens welke u op uw website opvraagt en/of laat vast leggen.

Het stappenplan

Onderstaande stappen hebben we opgezet waarmee u kunt nagaan welke acties u voor uw website moet uitvoeren. Het kan zijn dat er voor uw website specifiekere zaken gelden dan genoemd. Ga daarom zelf ook na welke zaken voor u en uw website gelden.

Stap 1 Inventariseren en documenteren.
Stap 2 Legitimeren
Stap 3 Beperking
Stap 4 Procedures opstellen
Stap 5 Informeren en toestemming vragen

In dit document wordt elke stap verder toegelicht en aangegeven welke acties u moet uitvoeren.

Uw inventarisatie document

We hebben voor u alvast de stappen in een inventarisatiedocument verwerkt, zodat u overzichtelijk alle stappen kunt doorlopen en documenteren. Download dit document op **https://www.sieronline.nl/wet-avg/**

Stap 1. Inventariseren en documenteren.

Beschrijf de doelgroepen die uw website bezoeken en noteer voor elke doelgroep welke persoonsgegevens uw website verzamelt. Denk hierbij bijvoorbeeld aan klanten en leads. Documenteer ook :

Hosting en beheer

Externe dienstverleners hebben ook toegang tot uw website. Ga na of de juiste afspraken zijn gemaakt en leg deze vast in een verwerkersovereenkomst. De verwerkersovereenkomst van ons is te downloaden op https://www.sieronline.nl/wet-avg/. Aandachtspunten zijn:

Hosting partij

- Uw hosting partij/webbouwer heeft toegang tot alle gegevens op uw website. Daarom dient u een verwerkersovereenkomst op te stellen met uw hosting partij en/of webbouwer. Veelal is Sieronline uw hostingpartij/webbouwer.

Externe ontwikkelaars en beheerders

- Welke beheerders hebben toegang tot uw website. Denk hierbij aan ontwerpbureaus, marketingbureaus etc.
- Huurt u bureaus of freelancers in? Zoja, dan dient u daar ook een verwerkersovereenkomst mee af te sluiten.

Backuplocaties

- Waar en hoe worden uw backups opgeslagen bij uw hosting partij? Sieronline zorgt ervoor dat alle dagelijkse backups van uw website op een veilige offline locatie staan, zodat anderen hier niet bij kunnen en geen misbruik van uw data kunnen maken.

Plugins

Ga na welke plugins er draaien op uw site en bepaal per plugin welke gegevens verzameld worden. Sieronline heeft in het document de meest gebruikte al opgenomen voor u.

Contactformulieren

- Welke formulieren gebruikt u en welke informatie vraagt u van uw gebruikers op?
- Waar wordt de informatie opgeslagen?

E-commerce (bv WooCommerce)

- Denk aan NAW en bankgegevens van uw klanten, maar ook aan de soort bestelde producten.

E-mailmarketing widgets (bv MailChimp)

- Welke informatie vraagt uw op? Wat doet uw met die informatie? Naar welke diensten stuurt u die informatie?

Koppeling met diensten en/of pakketten

- Heeft u bv een koppeling met een boekhoudpakket?

Ledennet plugins (bv BuddyPress)

- Welke informatie wordt er opgeslagen per lid?
- Wat zegt het lidmaatschap op uw site over uw leden?

Statistieken

- Denk aan Google Analytics of Google Tag Manager: weet u welke gegevens er opgeslagen worden van uw bezoekers en gebruikers?

Logging

- Maakt u gebruik van activiteitsmonitors die gebruikersactiviteit registreren?

Diensten buiten de EU

Controleer of u gebruik maakt van diensten buiten de EU. Zoja, ga na of ze voldoen aan de AVG.

Duur

Ga na hoelang persoonsgegevens worden bewaard en of dit niet langer is dan noodzakelijk. U zult namelijk moeten overwegen of deze duur te rechtvaardigen is.

Overige zaken

Welke gebruikers hebben toegang tot uw website en hoe gaat u met de wachtwoorden om?

Maakt u gebruik van marketing automation of A/B testing? Zoja, zijn de bezoekers hiervan op de hoogte?

Stap 2. Legitimeren

Van alle gegevens die u op je website verzameld moet u kunnen uitleggen waarom u deze verzamelt. Als u op uw WordPress website gegevens verzamelt en bewaart mag dat alleen als een van de volgende redenen van toepassing is:

- Dit is afgesproken in een overeenkomst. Denk bijvoorbeeld aan betaalde abonnementen op uw website waarvoor je bankgegevens van personen nodig hebt.

- Omdat u dit wettelijk verplicht bent vast te leggen. Denk aan facturen in WooCommerce die u ook nodig heeft voor uw boekhouding.

- Omdat u expliciet toestemming hiervoor heeft gekregen. Denk aan een cookiemelding of een akkoord bij een invulformulier. Let op:
  - Toestemming moet vrijwillig gegeven zijn
  - Toestemming moet expliciet gegeven te zijn (dus geen vooraf aangevinkte checkbox)
  - Toestemming moet per onderdeel gegeven zijn
  - Organisaties welke gegevens gaan verwerken moeten genoemd zijn
  - Toestemming moet ingetrokken kunnen worden.

- Verzamelen van gegevens is te rechtvaardigen. Denk bijvoorbeeld aan het afvangen van locatie zodat er een extra veiligheidscontrole uitgeoefend kan worden. Let op, dit is een grijs gebied, schrijf uit wat u van mening bent dat te rechtvaardigen is en win advies in bij twijfel.

Indien bovengenoemde zaken nog niet op uw website van toepassing zijn, dan zult u aanpassingen op uw website moeten doen. Neem contact op met Sieronline om na te gaan welke aanpassingen nodig zijn en welke eventuele kosten dit met zich mee brengt. U bent uiteindelijk zelf verantwoordelijk dat dit op orde is.

Stap 3: Beperking

Verwijder persoonsgegevens waarvan u niet kan legitimeren dat uw website ze verzamelt en opslaat. Dit kan via de beheeromgeving van je website.

Stap 4: Procedures opstellen

Zorg dat u helder heeft welke gegevens u op welke plaatsen verzamelt en opgeslagen worden. Leg protocollen vast voor situaties waar u mee te maken heeft of mee te maken kunt krijgen. Leg de volgende procedures vast:

Verzoeken van personen voor toegang via de website.
Personen kunnen om toegang vragen tot hun persoonsgegevens in uw website maar ook om te bewerken of verwijderen hiervan.

Veiligheid
Leg vast hoe u er voor zorgt dat gegevens veilig zijn en blijven.

Veilige opslag backups.
Sieronline zorgt dagelijks voor een veilige offline opslag van uw backups.

Complex wachtwoordbeleid.
Update uw account regelmatig

Datalekken
In geval van een datalek moet u binnen 72 uur de autoriteit persoonsgegevens en de betrokken personen informeren.

Stap 5: Informeren en toestemming vragen

Informeer bezoekers helder en transparant, bv in privacyverklaring waar u naar verwijst. Een privacyverklaring kan u ook online genereren en op u website (laten) plaatsen. Een hulpmiddel hiervoor vindt u op https://veiliginternetten.nl/privacyverklaring/.

Vraag expliciet om toestemming op de activiteiten die u in de privacyverklaring hebt vastgelegd. Sieronline kan u bijstaan om deze verklaring op uw site te plaatsen.

Het kan zijn dat uw website nog niet aan alle bovengenoemde punten voldoet. Sieronline kan u helpen om uw website hiervoor aan te passen. Neem in dat geval contact met ons op, zodat we kunnen kijken welke aanpassingen dit met zich mee gaan brengen.