

AVG CHECKLIST

Lees mijn blog: <https://www.anitafaber.nl/avg-wat-moet-je-ermee/>

In deze checklist worden de volgende onderwerpen behandeld:

1. SSL-certificaat voor je website
2. Privacyverklaring
3. Optins aanpassen
4. Toestemming vragen aan je bestaande relatiebestand
5. Cookiemelding op je website
6. Verwerkersovereenkomsten

1. Je website moet een SSL-certificaat hebben

Een SSL-certificaat op je website zorgt voor een veilige verbinding. Sowieso was het al handig een veilige verbinding te hebben, aangezien Google sinds een poosje sites zonder SSL als onveilig markeerde. Maar als je contact- of aanmeldingsformulieren op je website hebt waarmee je dus gegevens van mensen verzamelt, dan is HTTPS vanaf 25 mei 2018 verplicht.

Een SSL certificaat kun je regelen door het bij de host van je website aan te vragen. Tot voor kort was dit gratis, maar met het zicht op de AVG en deze verplichting zijn hosts hier helaas geld voor gaan vragen. Wees dus wel op je hoede dat je waar krijgt voor je geld en geen torenhoge kosten die niet in verhouding staan tot wat ze ervoor moeten doen.

Let op: het is belangrijk dat bij het overzetten naar https alle linkjes van afbeeldingen e.d. die in je mediabibliotheek staan ook https krijgen. Of dat jouw site ergens nog vermeld staat met http en dat dat dus automatisch wordt geredirect naar https. Bij sommige hosts gaat dit allemaal automatisch, bij andere hosts niet. Vraag er dus naar of dit ook geregeld is en zo niet, hoe het wel geregeld kan worden!

- SSL certificaat aanvragen bij host
- Optioneel: Plugin installeren op website om alle linkjes ook over te zetten naar https

2. Privacyverklaring

Wat houdt een privacyverklaring in? Kort door de bocht: Hierin leg jij aan de lezers uit welke gegevens je van hen verzamelt, waar je die bewaart en wat er mee gedaan wordt. En ook hoe men de gegevens kan laten verwijderen indien gewenst. De privacyverklaring moet terug te vinden zijn op je website, maar ook bij alle aankopen of optins die je aanbiedt.

Hoe maak je zo'n privacyverklaring? Via [deze link](#) kom je bij een privacyverklaring generator. Stap voor stap beantwoord je vragen die benoemd moeten worden in deze verklaring. Vervolgens kun je deze aan het eind als Word-document downloaden en dan zelf nog aanpassen, als je dat wil (logo erin bijvoorbeeld).

Sla hem wel als pdf-bestand op voordat je deze uploadt op je website. Of maak er een pagina van op je website. Het slimst is om in de footer of op je contactpagina te verwijzen naar je privacyverklaring zodat als men erop klikt, het pdf-document of de pagina waar de tekst staat wordt geopend.

Het is niet nodig om iedereen over je privacyverklaring te informeren, hij is tenslotte verplicht per 25 mei 2018. Maar als je deze later aanpast, dan moet je de mensen van wie jij gegevens hebt wel informeren over de wijzigingen.

- Privacyverklaring maken.
Zie hoe ik het heb gedaan: <https://www.anitafaber.nl/privacyverklaring/>
Je kunt zelf een privacyverklaring maken met de Privacy Generator via deze link: <https://veiliginternetten.nl/privacyverklaring-generator/start/>
- Privacyverklaring op website zetten (dit kan als geupload pdf-bestand via de mediabibliotheek of als webpagina op je website) en dan in de footer en/of op de contactpagina van je website een link die naar je privacyverklaring leidt.
- De link naar je privacyverklaring moet ook in AR worden gezet als je met shoppingcart werkt. (Instellingen > Shoppingcart > Teksten)
- Werk je in AR met de shoppingcart en heb je producten die je online laat betalen, dan moet je vanaf nu ook akkoord laten geven op je privacyverklaring (en eventueel je algemene voorwaarden).
Bij een product is een button toegevoegd die standaard uit staat, en die moet dus aan worden gezet. Wanneer deze aan staat krijgt men in het betaalproces te zien dat ze akkoord moeten gaan met je privacyverklaring en die linkt dan naar de link die je in het vorige punt hebt ingesteld.



3. OPTINS MOETEN WORDEN Aangepast

Heb je optin formulieren op je website, waar mensen dus hun gegevens invullen, dan moeten die aangepast worden met een tekst die aangeeft wat er gebeurt met de gegevens die de website bezoeker daar invult. Liefst moet men dit ook voor akkoord aanvinken.

Ook mag je alleen maar relevante gegevens vragen die je écht nodig hebt om de diensten of producten te kunnen leveren waar om gevraagd is.

Als iemand zich dus voor je nieuwsbrief aanmeldt, of voor een webinar, dan mag je geen telefoonnummer vragen. Die heb je namelijk niet nodig om de nieuwsbrief toe te sturen of om je webinar te kunnen tonen. Eigenlijk mag je niet eens om het geslacht vragen als dat niet echt nodig is. Ook hier: het gaat best ver wat allemaal niet meer mag.

Werk je met Autorespond, dan kun je de formulieren daar aanpassen en moet je de codes op je website daarna vervangen door de nieuwe embedcode, zodat de 'vinkjes' getoond worden. Dit doe je overigens niet alleen bij je optin-formulieren, maar ook bij de producten die je in Autorespond kunt aanmaken en die men dus online kan aanschaffen. Ook daar kun je vanaf nu een optie aanzetten dat men bij betaling akkoord moet gaan met de privacyverklaring. Hier kun je lezen wat Autorespond er zelf over zegt.

- Optins moeten worden aangepast. Dit doe je bij de lijstmanager > Formulier > AVG Toestemming.

Let op: als je dit in AR aanpast wordt dit NIET automatisch ook aangepast op je website. De link/code op je website moet dan dus worden vernieuwd om de nieuwe versie te tonen.

- Optins aanpassen op je website.

4. TOESTEMMING VRAGEN AAN JE BESTAANDE RELATIEBESTAND

In het registratie-/mailsysteem waar jij de gegevens bewaart moet te herleiden zijn sinds wanneer iemand in jouw systeem staat en hoe jij aan hun gegevens bent gekomen. Als jij bijvoorbeeld met Autorespond werkt, en je hebt je bestand opgebouwd doordat mensen zich inschreven voor een nieuwsbrief of een weggever hebben aangevraagd, of zich aanmeldden voor een webinar, en je hebt dat telkens netjes in een eigen groep gezet (bijv groep 'aanvraag weggever X', 'webinar titel d.d. datum'), dan kun je dus herleiden hoe iemand zijn gegevens in jouw bestand zijn gekomen. En als dit nou voor al je relaties zo is, dan hoeft je dus helemaal niemand opnieuw toestemming te vragen.

Is dat niet het geval, dan moet je dus je opnieuw toestemming vragen of ze ermee akkoord gaan dat je hun gegevens bewaart (en dus vertellen over welke gegevens je nu beschikt) en als ze dat niet willen dat ze zich kunnen uitschrijven of hun gegevens kunnen wijzigen.

Onthoud ook dat als men zich uitschrijft voor je nieuwsbrief en aangeeft dat zij in het geheel geen mails meer wil ontvangen, je vanaf nu verplicht bent om die gegevens ook echt helemaal uit je bestand te verwijderen. (Tenzij het om een klant of oud-klant gaat, want die gegevens moet je bewaren t.b.v. de Belastingdienst)

- Ben je mijn klant? Als het goed is dan heb ik er dan in AR in het verleden al voor gezorgd dat van alle optins en andere manieren waarmee men in jouw bestand kwam (aankopen e.d.) men in een eigen groep kwam (en ook op je hoofdlijst).
Check dit voor de zekerheid. Is dit inderdaad het geval, dan hoeft je je relaties dus niet opnieuw aan te schrijven voor toestemming.
- Is dit niet het geval, dan moeten we je relaties gaan mailen met de vraag of ze willen blijven of willen vertrekken.

5. COOKIEMELDING OP JE WEBSITE

Je bent verplicht om mensen toestemming te vragen voor het verzamelen van gegevens, en daar vallen cookies ook onder. Als je dus via je website gegevens van bezoekers verzamelt, bijvoorbeeld doordat je gebruik maakt van Google Analytics, of de FB pixel omdat je adverteert op Facebook, dan verzamel je dus gegevens en moet je dus de cookiemelding tonen. Toen je deze blog ging lezen zag je het ook in beeld. En als je klikte op 'lees hier mijn cookies en privacy policy', dan kwam je op [deze pagina](#).

Dit is hoe ik het heb ingericht, maar er zijn meerdere manieren mogelijk. Waar het om gaat is dat je aangeeft wat voor soort cookies er worden verzameld en met welk doel.

Als je Google analytics gebruikt, dan kun je ervoor kiezen om [de instellingen bij Google te veranderen](#), zodat de cookies anoniem blijven. Op deze manier hoeft je in principe ook geen ingewikkelde instellingen in te (laten) voeren in je cookiemelding en volstaat het om bijv te schrijven: Op deze site gebruiken we cookies om het verkeer te analyseren, je voorkeuren te onthouden en je optimaal gebruiksgemak te bieden.

- Check of er cookies op je site worden verzameld via <http://www.cookiechecker.nl>
- Is dit het geval, dan moet er (door mij of je websitebouwer) een cookie plugin worden geïnstalleerd die de cookiemelding geeft.
NB: er zijn nog maar weinig AVG proof cookie plugins, maar 1 daarvan is deze: <https://www.cookiebot.com/en/pricing/>
- Er moet een pagina worden gemaakt waarin staat uitgelegd wat cookies zijn en welke cookies je verzamelt. Ik heb dit op [deze pagina](#) uitgelegd aan mijn websitebezoekers.

6. VERWERKERSOVEREENKOMSTEN

Derde partijen kunnen mogelijk bij de persoonsgegevens van jouw klanten en relaties. Met die partijen moet dan ook duidelijk afgesproken worden, hoe zij omgaan met die persoonsgegevens. En wie er aansprakelijk is. Denk bijvoorbeeld aan mij (virtueel assistent), je boekhouder, je host, je websitebouwer, je webinarsoftware (bijv WebinarGeek) de leverancier van het mailprogramma waar je mee werkt (Autorespond, Activecampaign, Mailchimp, etc), de leverancier van je online boekhoudprogramma waar je mee werkt... Het gaat heel ver helaas. Maar deze mensen hebben direct of indirect ook toegang tot de systemen waar jij de gegevens van anderen verzamelt of bewaart. En dus moet dit worden vastgelegd. Jij dient iedereen die toegang heeft tot de gegevens die jij van derden verzamelt een verwerkersovereenkomst te sturen.

Autorespond heeft dit afgedicht door een verwerkersovereenkomst in je account aan te bieden. Kijk in je account bij Instellingen > tabje Administratie > Abonnementsgegevens > tabje AVG Verwerkersovereenkomst.

WebinarGeek heeft het als volgt opgelost: <https://app.webinargeek.com/changelog/> en wanneer je nu weer voor het eerst inlogt verschijnt er een pop up hierover.

Mijn online boekhoudprogramma Acumulus heeft ook een verwerkersovereenkomst aangeboden tussen hen en mij om dit af te dichten. Sommige partijen zijn daar pro-actief in dus.

- Alle derde partijen een verwerkersovereenkomst toesturen.
Een voorbeeld template daarvan kun je [hier](#) downloaden.