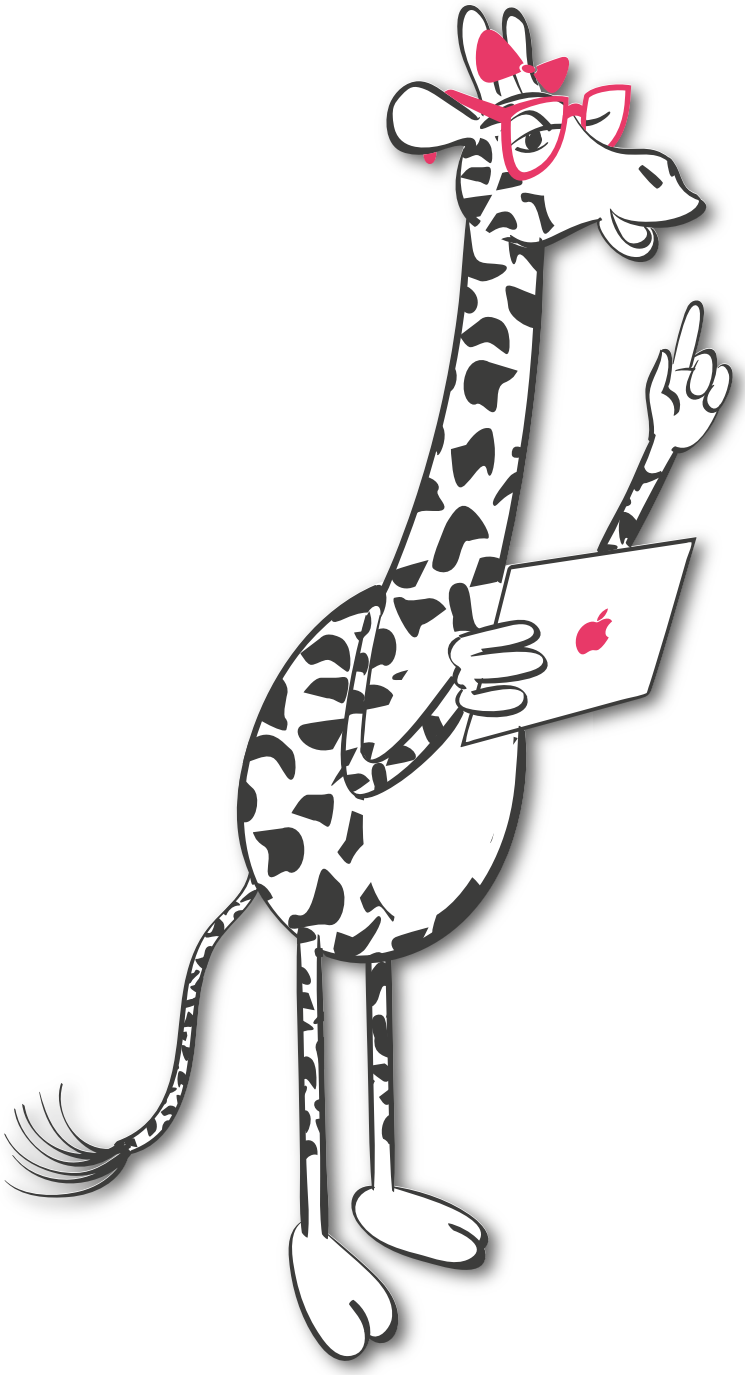

IN 11 STAPPEN JE WORDPRESS WEBSITE AVG-PROOF

BURO STAAL

[Checklist] In 11 stappen je WordPress website AVG-proof

Als je de afgelopen maanden niet onder een steen hebt gelegen, heb je ongetwijfeld gehoord over de AVG / GDPR. Dit een wet, die op 25 mei 2016 actief geworden is en waaraan iedereen zich vanaf 25 mei 2018 dient te houden.

Omdat we allemaal een beetje laat wakker geworden zijn wat betreft dit onderwerp, is er nu lichte paniek onder ondernemers.

En dat snappen we …

De hele wet AVG draait om het inzichtelijk maken van de persoonsgegevens die je verzamelt en om het vragen om toestemming voordat je specifieke persoonsgegevens verwerkt. Persoonsgegevens zijn namen, mailadressen, telefoonnummers en geboortedata, maar ook geloofsovertuiging, medische informatie etc. Zodra je een contactformulier op je website hebt, verwerk je dus al persoonsgegevens. Met de ingang van de AVG worden ook zakelijke mailadressen, telefoonnummers etc. als persoonsgegevens gezien.

Dus ja, die AVG is waarschijnlijk ook voor jou van toepassing.

En ja, je moet er iets mee.

Als je je echt in wilt lezen, kijk dan eens op de website van Charlotte's Law, daar vind je talloze goede blogs over de AVG. We gaan er hier verder niet te diep op in, want dan zijn we je aandacht al kwijt voor we bij het eerste punt van de checklist zijn.

We gaan dus direct de handen uit de mouwen steken en aan de slag. Het is even doorbijten, maar als je deze checklist doorlopen hebt, ben je aardig op de hoogte waar je website aan moet voldoen.

De checklist bestaat uit 11 onderdelen:

1. Een SSL-certificaat
2. Toegang tot je website
3. Beheerders van je website
4. Website up-to-date houden
5. Privacyverklaring toevoegen
6. Data minimaliseren
7. Formulieren controleren
8. Opt-in formulieren controleren
9. E-mailmarketing en site-tracking
10. Google Analytics
11. Cookies

Alle punten zijn belangrijk, maar punt 6 staat met stip bovenaan. Op de volgende pagina's worden alle onderdelen besproken en vind je de actiepunten die je moet ondernemen.

Ready? Daar gaan we!

By the way: deze checklist is gratis, ondanks dat er flink wat uren werk in zit. Je snapt dat we her en der wel een linkje naar onze website hebben toegevoegd. Met nog meer waardevolle informatie uiteraard hè, echt niet om reclame te maken of zo ;-) En we linken soms ook naar andere websites. Puur om jou de beste informatie te geven.

STAP #1

Een SSL-certificaat

Als er een SSL-certificaat op je website geïnstalleerd wordt, verandert je domeinnaam van http (in het grijs) naar https (in het groen) en komt er een groen slotje met de term “veilig” voor je domeinnaam te staan. Helemaal hip, maar wat doet zo’n SSL-certificaat nou precies?

Via je website worden er gegevens verzonden. Denk aan je gebruikersnaam en wachtwoord als je inlogt, je NAW- en bankgegevens als je iets besteld en je mailadres als je een contactformulier invult. Deze gegevens worden als het ware via een touwtje van jouw browser naar de browser van de ontvanger verzonden.

Stel, dat iemand bij het touwtje kan en er halverwege zijn eigen touwtje aan knoopt, dan komen de gegevens ook bij hem terecht. En dat is nou net niet de bedoeling.

Een SSL-certificaat zorgt ervoor dat de gegevens die via het touwtje verzonden worden versleuteld worden. De bedoelde ontvanger van de gegevens heeft de sleutel en kan de gegevens dus lezen. Degene die halverwege stiekem een touwtje aanknoopt, heeft de sleutel niet en kan dus niets met de gegevens.

Dit hele proces gaat overigens heel snel en volledig automatisch, dus je hoeft niet bang te zijn dat het je website vertraagt, of dat je de sleutel verliest ;-)

Een SSL-certificaat op zich is niet verplicht, maar omdat het een middel is om je website te beveiligen en je geacht wordt dit zo goed mogelijk te doen, is het dus wel zeker een dikke aanrader. Daarnaast zorgt het certificaat ervoor, dat je browser geen melding laat zien dat je website niet veilig is en krijgen https-websites voorrang in de zoekresultaten.

Je kunt een SSL-certificaat aanvragen bij je hostingpartij. Als je een beetje een fijne partij hebt, regelen die het verder voor je. Bij sommige type certificaten word je alleen nog gebeld door de partij die de certificaten uitgeeft om je identiteit te bevestigen.

☐ ***Voeg een SSL-certificaat toe aan je website***

STAP #2

Toegang tot je website

Het is belangrijk om ervoor te zorgen, dat niet zomaar iedereen in je website kan. Waarom? Omdat, als je persoonsgegevens binnen de website bewaart, je een datalek hebt als er onbevoegden inloggen en deze gegevens bekijken. En überhaupt wil je niet dat de gegevens die mensen in vertrouwen naar jou sturen bij vreemden terecht komen. Zorg daarom ten eerste altijd voor een sterk wachtwoord dat bestaat uit:

- minimaal 8 tekens;
- een combinatie van hoofdletters, kleine letters, speciale leestekens en cijfers;
- een volledige random reeks tekens die niet herleiden naar een adres, geboortedatum of iets dergelijks.

Het kan geen kwaad om het wachtwoord van je website regelmatig aan te passen. Hoe je dat kunt doen lees je in het blog *Wachtwoord en/of gebruikersnaam veranderen in WordPress*. Beveilig daarnaast de inlog van je website extra goed met behulp van two-factor authentication.

Two what?!

Two-factor authentication betekent dat je twee keer moet bewijzen dat jij bevoegd bent om in te loggen. De eerste keer doe je dit door je gebruikersnaam en wachtwoord in te voeren. Vervolgens wordt er bijvoorbeeld een code naar je e-mail of naar je telefoon gestuurd of moet je een veiligheidsvraag beantwoorden. Die code voer je in of je beantwoordt de vraag waarmee je voor de tweede keer bewijst dat jij het echt bent. Pas daarna ben je ingelogd.

Mocht iemand de inloggegevens van je website achterhalen, dan kunnen ze nog steeds niet inloggen omdat de code in jouw mail terecht komt of ze het antwoord op de vraag niet weten. Mits je die vraag natuurlijk niet te makkelijk maakt :-)

De plugin Google Authenticator (gratis) helpt je de two-factor authentication op je website toe te voegen.

- ☐ ***Pas je wachtwoord regelmatig aan in een sterk wachtwoord***
- ☐ ***Voeg two factor authentication toe aan je website***

STAP #3

Beheerders van je website

Log in in je website en controleer wie er allemaal een account hebben. Hebben deze personen ook echt toegang tot je website nodig? Staan er misschien nog stagiaires/collega's tussen die er niet meer werken, heb je een nieuwe webbouwer en heeft je oude webbouwer ook nog toegang, ben je van VA gewisseld etc. Doe dit regelmatig of wijs iemand aan die dit voor je kan doen.

Verwijder de personen die echt geen toegang meer nodig hebben. Dikke doei! Personen die wel toegang nodig hebben om bijvoorbeeld teksten aan te passen, hebben niet per se volledige toegang nodig. Je kunt hun rol inperken tot schrijver of redacteur.

Als er bureaus of freelancers aan je website werken en een eigen account hebben, dien je een verwerkersovereenkomst met hen af te sluiten. In een verwerkersovereenkomst maak je afspraken over de bescherming van persoonsgegevens en over de verantwoordelijkheden van beide partijen.

Zorg er ook voor, dat alle gebruikers een sterk wachtwoord gebruiken. In theorie heeft je hostingpartij ook toegang tot alle gegevens op je website. Sluit ook met hen een verwerkersovereenkomst af.

Alles over het vinden een aanpassen van gebruikers lees je in het blog *Extra gebruikers en hun rollen in WordPress*. Een verwerkersovereenkomst kun je ongetwijfeld ergens online genereren, maar wij vonden het zulke ingewikkelde materie, dat we het aan een jurist uitbesteed hebben.

- ☐ ***Controleer wie er toegang heeft tot je website, verwijder onnodige gebruikers en pas van nodige gebruikers eventueel hun rol aan.***
- ☐ ***Sluit met alle externe partijen een verwerkersovereenkomst af***

STAP #4

Website up to date houden

Het is belangrijk om je website veilig te houden en te voorkomen dat je wordt gehackt (en om te zorgen dat alles goed blijft werken). Dit is iets, wat niet letterlijk zo in de wet staat, maar wat weer terugvoert op het feit, dat je je uiterste best dient te doen de persoonsgegevens die via je website verwerkt worden te beveiligen.

Voer daarom consequent beschikbare updates uit van WordPress, het thema en de plugins. Maak, voordat je dat doet, altijd eerst een back-up en zorg dat die back-up op een veilige plek opgeslagen wordt. In de back-up van je website kunnen persoonsgegevens opgeslagen staan. Als iemand de back-up te pakken krijgt, kunnen ze dus alsnog bij de gegevens komen.

Vind je het spannend om te updaten? Lees *Zo kun je veilig updates uitvoeren*.

- ☐ ***Ga na of je hostingpartij back-ups voor je maakt en waar die opgeslagen worden. Maakt je hostingpartij geen back-ups, controleer dan of er een back-up plugin aanwezig is en ga na waar die de back-ups opslaat. Is dit een veilige locatie?***

- ☐ ***Maak een plan voorhet updaten van je website***

STAP #5

Privacyverklaring toevoegen

De AVG is er met name, om voor transparantie te zorgen. Om eerlijk te zijn over wat je van de bezoekers van je website verzamelt, zodat ze weten waar ze aan toe zijn en hun gegevens kunnen laten verwijderen als ze dat willen. Deze informatie zet je in je privacyverklaring.

In een privacyverklaring leg je o.a. aan je bezoekers uit:

- welke persoonsgegevens je bewaart;
- hoe lang je de persoonsgegevens bewaart;
- waarom je de persoonsgegevens bewaart;
- waar je de persoonsgegevens opslaat;
- met wie je de persoonsgegevens deelt.

Wat er precies in je privacyverklaring moet staan en aan welke voorwaarden deze moet voldoen, lees je in het blog *Zo is je privacyverklaring AVG/GDPR-proof*.

Zorg er voor, dat je privacyverklaring goed te vinden is op je website. Plaats deze bijvoorbeeld in je copyright regel helemaal onderaan je website of in je footer. Op deze manier staat de verklaring op elke pagina van je website en kunnen bezoekers niet zeggen dat je verklaring niet toegankelijk is.

- ☐ ***Stel een privacyverklaring op of laat deze opstellen***
- ☐ ***Voeg de privacyverklaring toe aan je website***

STAP #6

Data minimaliseren

Je mag niet meer gegevens vragen dan je nodig hebt. Controleer alle formulieren op je website en ga na welke informatie je vraagt.

Soms treedt het ***greedy marketeer*** effect op. Ken je dat? Van die marketeers/ondernemers die zoveel mogelijk van hun bezoekers willen weten en ze daarom een uitgebreid formulier voorschotelen terwijl de bezoeker alleen maar een simpel contactformulier verwacht.

Ten eerste is dit absoluut niet handig, omdat je je bezoeker ermee afschrikt en het killing is voor de conversie van je formulier. Maar daarnaast … heb je die informatie echt op dat moment nodig om het doel van het formulier te bereiken?

Een contactformulier is bedoeld om een bezoeker contact met je op te laten nemen. Om hem of haar te bereiken heb je een e-mailadres nodig of een telefoonnummer. Je kunt beide vragen, maar dat is eigenlijk niet nodig. Maak daarom slechts 1 van de velden verplicht. Overigens blijkt het achterlaten van een telefoonnummer voor veel bezoekers een drempel te zijn. Als dit een verplicht veld is, daalt de conversie van je formulier. Vraag dus alleen om een telefoonnummer als dat echt noodzakelijk is en houdt het anders bij een e-mailadres.

Verder is het natuurlijk handig om in ieder geval een voor- en/of achternaam te weten, zodat je de bezoeker op de juiste manier aan kan spreken als je reageert. En eigenlijk is dat genoeg. Je hoeft de geboortedatum of de NAW-gegevens niet te weten om contact op te nemen.

Echt niet.

Hoeft niet.

Greedy marketeer ;-)

☐ ***Controleer je formulieren en vraag alleen informatie die echt nodig is***

STAP #7

Formulieren controleren

Je hebt een grondslag nodig om persoonsgegevens te mogen verwerken. Je moet vooraf melden welke grondslag er van toepassing is. Dit kun je doen in je privacyverklaring. Je mag niet van grondslag wisselen en ook niet achteraf bedenken welke grondslag er zou passen.

De 6 grondslagen zijn:

1. Toestemming
2. Vitale belangen
3. Wettelijke verplichting
4. Overeenkomst
5. Algemeen belang
6. Gerechtvaardigd belang

Als grondslag 2-6 niet van toepassing zijn, kom je automatisch bij grondslag 1 terecht en moet je toestemming vragen. Het enige nadeel hiervan is dat die toestemming ook weer ingetrokken kan worden. De verschillende grondslagen worden uitgebreid besproken in *De 6 grondslagen van de AVG*.

Toestemming vragen om de persoonsgegevens te verwerken die in het formulier staan, kun je doen m.b.v. een checkbox in de buurt van de verzendknop. Je kunt daarbij verwijzen naar de privacyverklaring. Denk aan een zin als: Ik geef toestemming mijn gegevens te verwerken op de manier zoals omschreven in de privacyverklaring waarbij je het woord “privacyverklaring” kunt laten linken naar de privacyverklaring.

Als je een beetje bekend bent met de formulieren plugin op je website kun je aan elk formulier zelf zo’n checkbox toevoegen. Als je niet weet hoe het werkt, kun je de plugin WP GDPR Compliance gebruiken. Deze plugin is compatible met de populaire plugins Contact Form 7, Gravity Forms, WooCommerce en WordPress comments. De plugin helpt je om op de juiste plekken heel eenvoudig een checkbox toe te voegen waarin je om toestemming vraagt.

Reacties

Als je een blog op je website hebt, is er voor bezoekers vaak de mogelijkheid om een reactie achter te laten. Je raadt het al: ook daar moet een melding bij komen dat de bezoekers akkoord gaan met het verwerken van de persoonsgegevens. Hun naam wordt immers getoond op de website bij de reactie. Als je gewoon de standaard WordPress reacties gebruikt, kan de WP GDPR Compliance plugin je ook helpen de reactie AVG-proof te maken.

Handig!

- ☐ ***Voeg aan elk formulier op je website waar grond 2-6 niet op van toepassing is een checkbox toe waarin je om toestemming vraagt de persoonsgegevens te verwerken.***
- ☐ ***Heb je formulieren waar grondslag 2-6 wel op van toepassing is, vermeld dit dan in je privacyverklaring.***
- ☐ ***Zorg dat de reactie mogelijkheid op je website aangevuld wordt met een checkbox voor de acceptatie van de verwerking van persoonsgegevens.***

STAP #8

Opt-in formulieren controleren

Het verzenden van commerciële e-mails mag alleen naar contacten waar je óf expliciet toestemming van krijgt óf waar je een betaalrelatie mee hebt. Aan de bezoekers op je website moet je dus toestemming vragen om hen te mogen mailen.

Dit kun je doen door bij een contact- of opt-in formulier een checkbox toe te voegen met een zin in de trend van: *Ja, ik wil graag 1-2 keer per maand tips over online marketing per e-mail ontvangen*. Zorg er dan voor dat die checkbox niet automatisch aangevinkt is, want dan is de toestemming niet expliciet. De bezoeker moet de checkbox echt zelf aanvinken.

Het aanmelden voor een mailinglijst kan gezien worden als het aangaan van een overeenkomst (voor het toesturen van informatie), mits je duidelijk het doel erbij vermeldt (dus hoe vaak ga je iets sturen en waar over). Je hoeft dan geen toestemming te vragen om de persoonsgegevens te verwerken. Je moet wel in de privacyverklaring de grondslag vermelden.

Als je puur gegevens verzamelt die je later wilt gebruiken met een nu nog onbekend doel, heb je wel toestemming nodig om de persoonsgegevens te verwerken.

Je kunt de zin bij de checkbox natuurlijk ook nog iets aantrekkelijker maken door het resultaat te vermelden: *Ja, ik wil graag meer leads uit mijn website halen en meld me daarom aan om 1-2 per maand tips over online marketing per e-mail te ontvangen.*

Gratis weggevers

Dan nog even over gratis weggevers. Je weet wel, die “Download mijn gratis e-book/whitepaper/checklist/kalender/training etc.”-tactiek (die wij zelf ook toepassen hoor, niets mis mee).

Door de AVG mag je bezoekers die een gratis weggever downloaden niet meer zomaar op je nieuwsbrieflijst zetten. Je bezoekers downloaden een gratis weggever, maar geven niet expliciet toestemming voor het ontvangen van commerciële e-mails. En je hebt ook geen betaalrelatie met ze. Het downloaden van de gratis weggever is ook geen overeenkomst, dus de persoonsgegevens mag je ook niet zomaar verwerken. ***Oeps!***

De inschrijving voor je nieuwsbrieflijst mag trouwens ook geen voorwaarde zijn om de gratis weggever te downloaden. Je moet bezoekers dus de mogelijkheid bieden de gratis weggever te downloaden zonder op je lijst te komen. Duss …

Wil je je gratis weggever toch behouden, dan kun je dit op drie manieren aanvliegen:

1. Voeg een checkbox toe bij de gratis weggever waarmee de bezoeker kan aangeven dat ze ook op jouw maillijst willen komen. Hier moeten ze dus expliciet (dus met een vinkje) toestemming voor geven. Voeg ook een checkbox toe om toestemming te vragen voor het verwerken van hun persoonsgegevens zoals omschreven in de privacyverklaring.

2. Gebruik een dubbele opt-in waarbij je bij de tweede opt-in (een e-mail waarin mensen hun e-mailadres moeten bevestigen) alsnog vertelt dat ze op je e-maillijst terecht komen. Als ze hun e-mailadres bevestigen, geven ze expliciet toestemming. Leg vast sinds wanneer je de dubbele opt-in gebruikt, zodat je dit kunt verantwoorden. Je hoeft dan alleen maar een checkbox toe te voegen om toestemming te vragen voor de verwerking van de persoonsgegevens zoals omschreven in de privacyverklaring.

3. Schrijf heel duidelijk iets in de trend van *Schrijf je in voor onze nieuwsbrief/ mailing, ontvang 2 keer per maand een mail met tips en informatie over … en ontvang GRATIS …*, dan is het duidelijk dat ze zich voor je lijst inschrijven en wat het doel is. Aan een enkele opt-in (dus alleen de inschrijving op je site) heb je dan genoeg. Maak een screenshot van het inschrijfformulier en bewaar die met de datum erbij. Omdat er in dit geval een overeenkomst aangegeven wordt voor het ontvangen van informatie, is er ook geen checkbox nodig om toestemming te vragen voor de verwerking van de persoonsgegevens.

☐ ***Zorg dat de opt-in formulieren duidelijk zijn of dat bezoekers die zich inschrijven expliciet toestemming geven om op je mailing lijst te komen.***

STAP #9

E-mailmarketing en site-tracking

Als je een gratis weggever op je site hebt staan, heb je hoogstwaarschijnlijk ook een e-mailmarketingsysteem waar de opt-in voor je gratis weggever aan gekoppeld is. Met deze partij moet je ook een verwerkersovereenkomst afsluiten omdat je persoonsgegevens met hen uitwisselt.

Gebruik je Active Campaign? Dan kun je hier een verwerkersovereenkomst opvragen. Gebruik je Mailchimp? Klik dan hier voor een verwerkersovereenkomst.

Daarnaast is het van belang om te controleren of het e-mailmarketingsysteem gebruik maakt van site-tracking. Dat betekent, dat het systeem kan zien wie van de mensen op jouw mailinglijst welke pagina's op je website bezocht hebben.

Active Campaign is zo'n systeem dat beschikt over site-tracking. Active Campaign legt zelf in een blog uit hoe je site-tracking AVG-proof kunt maken. Eerlijk is eerlijk: dit is misschien wat te technisch. Als je het niet aandurft besteedt het uit of stop (voorlopig) met site-tracking. Het zal vast niet lang duren voordat iemand hier een slimme plugin voor bedenkt.

- ☐ ***Verwerkersovereenkomst afsluiten met e-mailmarketingsysteem***
- ☐ ***Controleren of e-mailmarketingsysteem site-tracking gebruikt. Zo ja, aanpassen of uitschakelen***

STAP #10

Google Analytics

Google Analytics is een gratis tool die je kunt gebruiken om de statistieken van je website te monitoren. Je kunt zien waar de bezoekers van je website vandaan komen, hoe ze op je website terecht gekomen zien, welke pagina's ze bezoeken, hoe lang ze op je website blijven etc.

Deze informatie is enorm waardevol om te begrijpen wie je website bezoekt en waar hun interesse naar uitgaat. Iets dat je dus zeker wilt blijven gebruiken.

Maak je nog geen gebruik van Google Analytics? Zie dit dan als wake-up call en regel het. Maar dan wel gelijk op onderstaande manier zodat je aan de AVG-eisen voldoet ;-)

Je kunt in Google Analytics niet zien in welke straat een van je bezoekers woont of hoe je bezoeker heet, maar toch worden er een aantal zaken met Google gedeeld waar je toestemming van de gebruiker voor nodig hebt.

Je kunt twee dingen doen:

1. Google Analytics volledig gebruiken en toestemming vragen aan de bezoeker (zie punt 11). Je hoeft dan alleen stap 1 en 6 uit te voeren. Het risico is alleen dat bezoekers geen toestemming geven en dan heb je helemaal geen data. Dus wat je ook kunt doen is;
2. Google Analytics anonimiseren. Er wordt dan alleen een functionele cookie geplaatst in de browser van de gebruiker, waar je geen toestemming voor hoeft te vragen. Je moet wel nog altijd in je privacyverklaring melden dat je Google Analytics gebruikt. Deze optie is niet aan te raden als je een webshop hebt of AdWords gebruikt.

Je kunt in zes eenvoudige stappen jouw Google Analytics account AVG-proof maken:

1. Sluit een verwerkersovereenkomst af met Google
2. Anonimiseer de IP-adressen
3. Zet het delen van gegevens uit
4. Zet het delen van gegevens voor advertentiedoelen uit
5. Controleer of de tracking info optie uit staat
6. Informeer je bezoekers

Als je meer uitleg wilt over deze zes stappen, lees dan het blog *Privacyvriendelijk instellen van Google Analytics*. Gebruik je Google Tag Manager? Lees dan ook *GDPR, GA en GTM: 4 concrete tips*.

☐ ***Doorloop de zes stappen om je Google Analytics te anonimiseren***

STAP #11

Cookies

Hoe zit dat nou met dit cookies?! Lastig uit te leggen, dus laten we eens zien wat Wikipedia zegt:

"Een cookie of magic cookie is een hoeveelheid data die een server naar de browser stuurt met de bedoeling dat deze opgeslagen wordt en bij een volgend bezoek weer naar de server teruggestuurd wordt. Zo kan de server de browser opnieuw herkennen en bijhouden wat de gebruiker, c.q. de webbrowser, in het verleden heeft gedaan. Een dergelijk historie is bijvoorbeeld voor marketingdoeleinden interessant."

Oké, dat dus. Hotjar, Facebook, Google Analytics en Disqus software zijn bijvoorbeeld bekende voorbeelden van tools die gebruik maken van cookies. Maar als je bijvoorbeeld YouTube video's op je website hebt staan, plaatst YouTube ook een cookie.

Op veel websites zie je een melding dat de website cookies gebruikt en dat er van uit gegaan wordt dat je daar oké mee bent als je de website blijft gebruiken.

Leuk geprobeerd, maar het voldoet niet aan de AVG :-(

Bezoekers moeten namelijk expliciet toestemming aan je website geven om analytische en tracking cookies te mogen plaatsen. En pas nadat die toestemming gegevens is, mogen de cookies geplaatst worden.

Als je alleen zo'n balk hebt, worden de cookies direct al geplaatst op het moment dat de website geopend wordt en heeft een bezoeker geen mogelijkheid om deze te weigeren. Dat mag dus niet. De cookies mogen pas geplaatst worden na de toestemming.

Sommige websites gebruiken een cookiewall. Je krijgt pas toegang tot de website als je akkoord gaat met de cookies. Dat mag met ingang van de ePrivacy verordening die er volgend jaar aankomt ook niet meer. Of je nou wel of geen cookies accepteert, je moet de website gewoon kunnen bezoeken zonder dat deze er anders uit ziet.

Hoe vlieg je die hele cookiemelding nou goed aan?

Door eerst om toestemming te vragen.

Krijg je geen toestemming, dan mogen de analytische en tracking cookies niet geplaatst worden. En je YouTube video's mogen dan dus ook niet getoond worden. Das een pijnlijke, vind je niet?!

Krijg je wel toestemming, dan mogen de cookies daarna geplaatst worden.

Ben je benieuwd of en welke cookies jouw website gebruikt? Vraag een gratis scan aan op de website van Cookiebot. Binnen 10 – 20 minuten ontvang je een mail met daarin een exact overzicht van de cookies die jouw website gebruikt.

Cookiebot levert ook een dienst die je kan helpen met de cookies. We hebben flink wat tools vergeleken. Cookiebot voldoet tot nu toe het meest aan alle eisen die er gesteld worden. De tool zorgt ervoor dat de cookies pas geplaatst worden als je daadwerkelijk toestemming hebt gehad. De tool op zich is op zich vrij snel en eenvoudig te installeren, maar je moet wel nog e.e.a. in je website aanpassen.

Het hele cookieverhaal vinden we een lastige omdat we niet weten wat er volgend jaar gaat gebeuren als de ePrivacy verordening ingaat. Het zou kunnen zijn dat je dan heel eenvoudig in je browser aan kunt geven of je cookies wel of niet wilt toestaan. Dan is het niet meer nodig om daar zelf actie op te ondernemen op je website. Maar tot die tijd ... tja ... het is aan jou of je het helemaal goed geregeld wilt hebben of dat je het risico neemt niet aan de AVG te voldoen en afwacht wat er volgend jaar gebeurt.

☐ ***Zorg dat analytische en tracking cookies pas geplaatst worden nadat je toestemming hebt gehad***

YOU DIT IT

Tot slot

Je hebt de checklist overleefd! Als het goed is, ben je een stukje wijzer geworden. Ja, het is veel werk. Niet alleen voor jou, voor iedereen. Maar ga er wel mee aan de slag.

- Wees transparant.
- Laat zien welke gegevens je verzamelt.
- Vraag toestemming als dat nodig is.
- Zet je greedy marketeer complex aan de kant en houd je aan de regels.

En misschien is niet direct alles helemaal dik in orde. Maar zo lang je kunt zien dat je je ingespannen hebt om aan de AVG te voldoen, verwachten we dat je bij een eventuele controle eerst een waarschuwing zult krijgen en niet direct een boete.

Gaat er een keer iets mis en heb je een (serieus) datalek? Meld dit dan binnen 72 uur bij de Autoriteit Persoonsgegevens en bij de betrokken personen. Je bent dit wettelijk verplicht, dus denk er niet te makkelijk over. Leg vooraf vast hoe je dit aan gaat pakken en documenteer je melding, mocht dat ooit nodig zijn.

Houd er verder rekening mee, dat bezoekers van je website het recht hebben om te vragen welke persoonsgegevens je van hem/haar hebt verzameld. Zorg dus, dat je hier een overzicht van hebt. Je mag hier geen kosten voor rekenen. In je privacyverklaring kun je aangeven hoe iemand een verzoek tot recht van inzage kan doen. Spreek ook intern en met de partijen waar je een verwerkersovereenkomst mee hebt afgesloten hoe je dit soort verzoeken gaat afhandelen.

Als de gegevens aangevuld, verbeterd of verwijderd (recht op vergetelheid) moeten worden, heb je aan die vraag opvolging te geven. Dat kan nog wel eens een lastige zijn, omdat sommige plugins bijvoorbeeld een IP-adres bewaren en je niet 1 IP-adres kunt verwijderen. Als het echt niet mogelijk is om alle gegevens te verwijderen (omdat je bijvoorbeeld van elke dag een back-up hebt), dan mag worden volstaan met een technische oplossing.

Google is er al wel mee bezig om de gegevens van 1 IP-adres te kunnen verwijderen uit de statistieken. Maar Google is een grote partij. Of de kleinere plugin-bouwers hun voorbeeld gaan volgen zal de toekomst uitwijzen.

ECHT WAAR!

Echt het allerlaatste

Als we jurist hadden wilden worden, zouden we Rechten zijn gaan studeren, maar dat hebben we niet gedaan. We hebben deze checklist puur en alleen gemaakt om die hele AVG-toestand voor onze klanten iets overzichtelijker te maken. Dit is geen juridisch document en er kunnen geen garanties aan deze checklist ontleend worden. We hebben de checklist overigens wel door een jurist laten controleren om te kijken of wat we roepen wel echt klopt.

Zelfs juristen zijn het niet allemaal met elkaar eens wanneer je website, formulieren en opt-ins nou wel of niet voldoen aan de AVG. Als zij het al niet eens zijn ...

We pretenderen op geen enkele manier dat deze checklist compleet is. We kunnen je wel vertellen dat je na het uitvoeren van deze checklist je in ieder geval ingespannen hebt om aan de wet te voldoen. Vink netjes in de checklist af wat je gedaan hebt, maak screenshots van wanneer je iets gedaan hebt en bewaar dit bij elkaar in een map. Als je alle handelingen vastlegt, heb je gelijk een soort verwerkingsregister. Niet verplicht voor kleine bedrijven, maar wel handig om te hebben. Mocht je een controle krijgen, dan kun je aantonen dat je er actief mee aan de slag gegaan bent.

De AVG is niet alleen van toepassing op je website, maar op alles waar je persoonsgegevens bewaart. Je bent dus niet helemaal klaar als je deze checklist hebt doorlopen. Wat er verder nog bij komt kijken, ligt buiten de scope van onze kennis. Sorry, het houdt ergens een keer op. Als we jurist hadden willen worden ... juist ;-)

VOOR KLANTEN

Voor klanten

Als je klant bij ons bent, heb je misschien meer informatie nodig of wil je misschien een bepaalde dienst afsluiten na het lezen van dit hele verhaal. We hebben hieronder bij een aantal punten opmerkingen geplaatst die van toepassing kunnen zijn.

Mocht je een mail sturen over de AVG of een product aanvragen dat eraan gerelateerd is, dan kan het iets langer duren voor je een reactie krijgt. We krijgen op dit moment namelijk enorm veel (aan)vragen die we allemaal moeten verwerken.

Opmerking bij punt 1:
Host je je website bij ons en wil je een SSL-certificaat aanvragen? Bestel deze dan online: https://www.burostaal.nl/domeinnamen-hosting/bestellen/?keuze=ssl

Het certificaat van € 30 is voldoende als je puur een informatieve website hebt met een contactformulier. Heb je bestelformulieren of een webshop op je site staan, kies dan voor het certificaat van € 60.

Opmerking bij punt 2:
Host je je website bij ons? Dan zit er standaard two factor authentication op. Mochten we dit op jouw verzoek uitgeschakeld hebben, dan is dat je eigen verantwoordelijkheid.

Opmerking bij punt 3:
Host je je website bij ons? Sluit dan een verwerkersovereenkomst af. Stuur een mail naar support@burostaal.nl om de verwerkersovereenkomst aan te vragen.

Opmerking bij punt 4:
Wil je het updaten van je website uitbesteden? Sluit dan een backUPdate abonnement af: https://www.burostaal.nl/onderhoud-support/onderhoud-website/ Wij maken dan back-ups en verzorgen de updates. De back-ups die gemaakt worden, worden opgeslagen op een beveiligde cloud locatie in Amerika die gebruik maakt van de Amazon S3 infrastructuur.

Opmerking bij punt 10:
Hebben wij jouw Google Analytics account ingesteld en wil je je account anonimiseren? Stuur een mail naar support@burostaal.nl, dan regelen we dit gratis voor je.

Opmerking bij punt 11:
Je kunt Cookiebot via ons aanvragen. Wij helpen je dan ook met de implementatie. De kosten hiervoor zijn afhankelijk van het aantal cookies dat je website gebruikt. Mocht je onze hulp hierbij nodig hebben, stuur dan een mail naar support@burostaal.nl.

AANTEKENINGEN

AANTEKENINGEN