

1. CONTACTFORMULIEREN

- Verklaar bij contactformulieren waarom informatie nodig is en waarom die betrekking heeft op de specifieke offerte- / contactaanvraag.
- Plaats een toestemmings-vinkboxje, om bezoekers akkoord te laten gaan met data opslag.
- Bewaar daarnaast ingevulde contactformulieren NIET online, om datalekken bij een hack te voorkomen.



2. PRIVACYVERKLARING

- Het is van belang dat op de website een **privacyverklaring** wordt geplaatst. Hierin staat onder andere: bedrijfsgegevens, reden van de verwerking van persoonsgegevens, waar personen toestemming voor geven, rechten van personen (zoals recht op inzage, aanpassing en verwijdering), welke beveiligingsmaatregelen genomen worden om de privacy van personen te waarborgen.
- Google naar voorbeelden van Privacy verklaringen in uw branche en pas deze aan naar uw eigen situatie.
- Meer info? -> [Bekijk video op VeiligInternetten.nl](https://www.veiliginternetten.nl) <-



3. SSL-CERTIFICAAT (HTTPS)

- Onder de AVG is het verplicht om te zorgen voor een optimale beveiliging van persoonsgegevens. Heb je formulieren of nieuwsbrief-aanmeldingen via de website? Dan is een SSL-certificaat (HTTPS) verplicht. Dit zorgt ervoor dat de gegevens die je bezoeker invult versleuteld worden verstuurd.
- Een SSL-certificaat is te herkennen aan een slotje en <https://> in de URL.
- Wij helpen je om te zorgen dat je website voorzien wordt van een certificaat.
- Een voorbeeld:



4. MOBIELVRIENDELIJKHEID EN GOOGLE

Houdt uw website al rekening met de smartphone? Doe hier de gratis test:

<https://search.google.com/test/mobile-friendly>

Komt uw website niet goed door de test? Geen zorgen, wij hebben een handige tool waarmee we uw website relatief snel mobielvriendelijk kunnen maken, zodat u in elk geval niet zakt in de zoekresultaten van Google en bezoekers een aangename website ervaring zullen hebben op hun mobiele apparaten, zoals de tablet en de smartphone.

Zie ook: <https://www.geniusapps.nl/niet-mobiele-website-en-de-smartphone/>

5. GEBRUIKERS IN CMS

- Wanneer iemand een account heeft in het CMS (Content Management Systeem) van de website, moet die persoon daar een geldige reden voor hebben. Dit moet apart vastgelegd worden, zodat duidelijk is wie waarom toegang heeft tot persoonsgegevens. Onnodige accounts moeten worden verwijderd.
- Stel een verklaring op waarin per gebruiker staat verklaard waarom diegene toegang heeft tot het CMS.

6. ACTIEVE BEHEER EN BEVEILIGING

- Een bedrijf is zelf verantwoordelijk voor de veiligheid van de website. Denk hierbij aan het pro-actief beveiligen van de website, het op de juiste manier updaten van thema's + plugins en het maken van dagelijkse back-ups.
- Ben je hier niet in thuis? Vraag dan Ellis om snelle hulp en advies hierbij.
- Gebruikt u Wordpress? Wij weten exact welke toepassingen u in gebruik kunt nemen (gratis) die ervoor zorgen dat u aan een groot aantal criteria voldoet. Ook hiervoor geldt dat we u graag helpen bij het instellen van deze add-ons.



7. RECHT OP VERWIJDEREN VAN GEGEVENS GEBRUIKER

Mensen kunnen reageren op artikelen op uw website, zoals blogs of nieuwsberichten. Men moet in de gelegenheid worden gesteld om eigen reacties te kunnen verwijderen. Hiervoor is een gratis tool beschikbaar dat u op uw website kunt installeren en zorgt dat de bezoeker een 'Verwijder mij' optie krijgt. Dit is geen harde eisen vanuit de AVG, maar wel prettig voor uw bezoekers.

EN WAT ALS IK DIT ALLEMAAL NIET DOE?

- De nieuwe wetgeving is erg uitgebreid, aangezien het zowel over online middelen als interne processen gaat.
- De autoriteit Persoonsgegevens, die verantwoordelijk is voor handhaving, heeft aangegeven dat er boetes tot 20 miljoen of 4% van een jaaromzet kunnen worden opgelegd. De hoogte van de boete gaat afhankelijk zijn van het type overtreding en de intentie.

