Eenvoudig Stappenplan om AVG-proof te worden

Het originele artikel kun je hier vinden.

De afgelopen tijd kwamen we in onze community veel ondernemers tegen die zich de afvroegen wat er nu precies van ze wordt verwacht wat betreft de AVG. En, eerlijk is eerlijk, ik heb er ook best tegenop gezien om alles voor de Zakelijk Succes Academy te regelen. In de praktijk bleek dat overigens helemaal niet zo spannend als ik had gedacht.

In dit artikel geef ik je een eenvoudig stappenplan waar je op moet letten en hoe je AVG-proof kunt worden. Gedeeltelijk heb ik dit artikel zelf geschreven op een manier waarop ik er zelf wijs uit word, gedeeltelijk komt de informatie uit andere relevante artikelen. Deze bronnen vermeld ik onderaan het artikel. Let op: dit artikel is geschreven voor ZZP'ers en MKB'ers tot 10 personeelsleden. Het doel van dit artikel is je te informeren en de overstap naar de AVG makkelijker te maken. Je bent zelf verantwoordelijk om te achterhalen wat er specifiek in jullie organisatie gedaan moet worden.

Wat is de AVG precies?

Dit jaar komt er een nieuwe privacywetgeving. Op 25 mei 2018 vervangt de AVG (Algemene Verordening Gegevensbescherming) de huidige regelgeving. Binnen de EU bestaan nu nog verschillen, met de ingang van de AVG is er 1 privacywet voor de hele Europese Unie.

De AVG heeft zes basiselementen die iedere organisatie moet naleven:

1. transparantie over verwerking en gebruik van persoonsgegevens;
2. beperken van verwerking van persoonsgegevens tot specifieke, legitieme doeleinden;
3. beperken van verzameling en opslag van persoonsgegevens tot beoogd gebruik;
4. individuen in staat stellen om persoonsgegevens te corrigeren of om verwijdering te vragen;
5. de opslagduur van persoonsgegevens beperken tot zo lang als nodig is voor het beoogd gebruik;
6. persoonsgegevens beveiligen met geschikte beveiligingsmethoden.

Twee andere belangrijke punten: privacy by design en lekken melden

Het doel van de AVG is ervoor zorgen dat:
1. het internet veiliger wordt
Daarom mag je straks niet meer zonder toestemming van de bezoeker, cookies plaatsen op je website. Specifiek gaat het om cookies die activiteiten van de bezoeker in de gaten houden of zorgen dat ze tot in den treure worden achtervolgd door fijne advertenties van roze hondenmanden met diamantjes, omdat ze daar ooit op hebben gezocht. Mocht je dus in de hondenmanden-business zitten dan heb je vette pech. Je mag mensen alleen maar achtervolgen als ze achtervolgd willen worden.

2. organisaties zorgvuldiger omgaan met privacygevoelige informatie
In het verleden is het meerdere keren voorgekomen dat data van organisaties op straat

kwam te liggen met alle gevolgen van dien. Daarom zijn er een aantal regels ingesteld voor waar je data opslaat, hoe je data opslaat en hoe de data is beveiligd.

Ook wel uitgelegd in de tekst: “Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is”.

Gaat de autoriteit persoonsgegevens handhaven op de toepassing van de AVG?

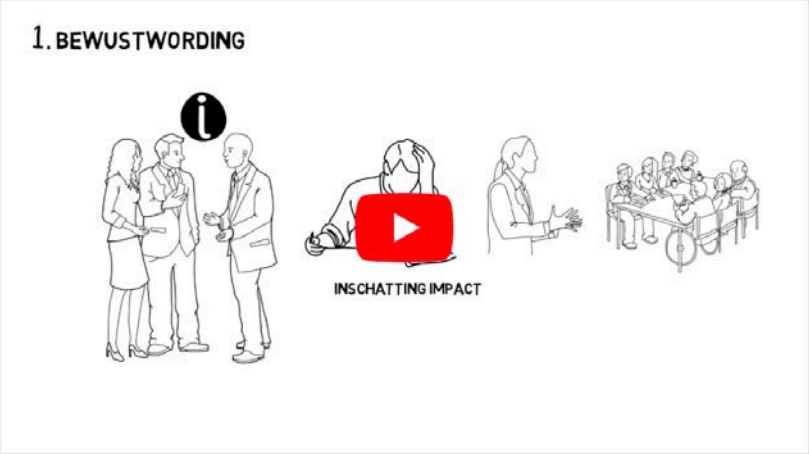
“De boetes kunnen oplopen tot wel 4% van onze omzet. HELP! Gaan ze ook echt handhaven?”

Oei, het is moeilijk om hier een uitspraak over te doen. Er zijn miljoenen websites en tienduizenden bedrijven in Nederland. Het is makkelijk om websites te crawlen (met een algoritme automatisch zoeken) op cookie-gebruik, het is alleen onmogelijk om iedere organisatie in Nederland volledig door te lichten.

Vermoedelijk zal de autoriteit persoonsgegevens een selectie maken van bedrijven waar er een ‘rode vlag’ naar boven komt. Organisaties die een voorbeeld zijn, organisaties waarbij op grote schaal melding wordt gemaakt van misbruik van persoonsgegevens of organisaties waar eerder datalekken zijn voorgekomen.

“In essentie is de AVG een fatsoenlijke gedragscode die is vastgelegd in regelgeving.”
Dit is wat je moet onthouden: als je *de gegevens* van je klanten op dezelfde manier behandeld als *je klanten* zelf is er waarschijnlijk niet zoveel aan de hand. Het gaat erom dat je als bedrijf alleen waardevolle informatie stuurt aan mensen die daar expliciet om hebben gevraagd. Verwerk niet meer gegevens dan strikt noodzakelijk en beveilig die goed.

Ah, een video. Handig.



Met dank aan de maker van deze video: Karel Roos.

Wat betekent dit nu voor mij als ZZP'er of kleine MKB'er?

Dit betekent dat er een gedragscode is voor hoe je met gegevens van prospects of klanten omgaat.
√ je alleen gegevens mag verwerken van personen als zij ervan op de hoogte zijn
√ je alleen data mag verwerken als je een specifiek doel hebt met die data, dat kunt verwoorden en in het belang is van de persoon waar het om draait
√ je de gegevens alleen mag gebruiken voor dat doel waarover je de persoon in kwestie hebt geïnformeerd
√ de mensen in je database hun gegevens mogen laten aanpassen of geheel verwijderen
√ je niet langer dan nodig informatie opslaat
√ je zorgvuldig omgaat met de gegevens

Wacht even… ik las ergens iets over een DPIA?
Jep, zou kunnen. Het Data Protection Impact Assessment (DPIA).

Een DPIA moet je in ieder geval uitvoeren als je:

- bijzondere persoonsgegevens als ras, godsdienst, gezondheid, politieke opvattingen, genetische – of biometrische gegevens op grote schaal verwerkt, of
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied, bijvoorbeeld met cameratoezicht, of
- gegevens zo combineert, dat iemand in een bepaalde categorie of groep is in te delen en daardoor zo kan worden benaderd of beoordeeld (profilering)

En hoe zit dat met die DPO?
In bepaalde gevallen is het verplicht om voor uw organisatie een functionaris gegevensbescherming (FG) aan te stellen, ook wel data protection officer (DPO), genoemd. De funtionaris gegevenbescherming is een onafhankelijk persoon die binnen uw organisatie adviseert en rapporteert over naleving van de AVG.

Aanstelling van een functionaris gegevensbescherming is verplicht wanneer:

- het de kernactiviteit van uw bedrijf is om op grote schaal gevoelige persoonsgegevens (zoals gezondheidsgegevens) te verwerken;
- uw organisatie structureel mensen observeert (fysiek of digitaal, bijvoorbeeld via cameraobservatie).

Een DPIA en PDO is minder relevant* als je:

- geen grote hoeveelheden persoonsgegevens verwerkt
- geen gebruik maakt van gezichtsherkenning of speciale software met biometrische identificatie
- er geen grote individuele belangen worden geschaad wanneer er een datalek is
- je geen grote organisatie bent met veel medewerkers die toegang hebben tot de data

** Ik schrijf hier bewust relevant, omdat dit artikel wordt gelezen door veel ondernemers. Zoals ik het zelf lees is een DPIA niet nodig als ZZP'er of kleine MKB'er, maar het is verstandig dit even te laten checken door een jurist.*

Tip: lees dit artikel waarin 9 criteria worden beschreven of je een DPIA moet uitvoeren.

Stappenplan om je bedrijf AVG-proof te maken

"Okay, schitterend verhaal. Wat moet ik nu doen?"
Ah, prima vraag. We hebben hier blijkbaar te maken met een doener. Officieel goed bezig.

Vijf stappen om AVG-proof te worden:

1. **Vul hier de privacy statement generator in**
2. **Plaats het privacy statement op je website**
3. **Neem een link naar je privacy statement op in alle communicatie richting je klant waar je ook je algemene voorwaarden hebt opgenomen**
4. **Maak je website AVG-klaar met deze plugin**
5. **Maak je emailmarketing AVG-proof met onderstaand mini-stappenplan**

Mini-stappenplan om je emailmarketing AVG-proof te maken:

De meeste vragen van ondernemers gaan over emailmarketing. Belangrijk, want emailmarketing is een krachtig onderdeel van je online marketing machine. Mag je nog steeds emails versturen naar je mailinglijst? Laat ik je gerust stellen; ja, dat mag!

Ik heb inmiddels veel gelezen over de AVG en dit zijn, zover ik het begrijp, de voorwaarden voor het gebruik blijven maken van emailmarketing. Dit overzicht met voorwaarden zijn geschreven met 'de geest der wet' in het achterhoofd. De 'letter der wet' is immers nog niet voldoende uitgekristalliseerd.

Allereerst:
1. Je schrijft een duidelijke privacystatement waarin je het doel van de mailings vastlegt;
2. Bij je opt-in formulier (voorbeeld) verwijs je naar het privacystatement;
3. Bij je opt-in formulier vertel je exact wat men toegestuurd krijgt;
4. Je hebt waarschijnlijk één of meerdere soorten contacten op je mailinglijst staan:

Contacten met een dubbele opt-in
Deze groep stuur je een mailtje met daarin een link naar je privacy statement. Je vertelt ze over de wijzigingen in de privacywet en wat ze in de toekomst kunnen verwachten van je zodat ze exact weten waarom ze emails krijgen.

Contacten met een enkele opt-in, waar je wel een audit-trail (historie met herkomst) van hebt
Deze groep stuur je een mailtje met daarin een link naar je privacy statement. Je vertelt ze over de wijzigingen in de privacywet en wat ze in de toekomst kunnen verwachten van je zodat ze exact weten waarom ze emails krijgen. Daarnaast zend je een double-opt-in link mee waarmee ze bevestigen emails te willen ontvangen. Wat als deze mensen hier niet op klikken? Geen probleem, zolang je je maar houdt aan de 'geest der

AVG': "Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is".

Contacten waar je geen audit-trail van hebt en die geen dubbele optin hebben:
die moet je officieel verwijderen van je mailinglijst per 25 mei 2018.

Daarnaast:
– Je stuurt per definitie alleen mensen een email die daar expliciet om hebben gevraagd;
– Je verwijdert regelmatig opt-out klanten uit je database en legt dat vast.

Alle grote emailmarketing pakketten (ActiveCampaign, Mailchimp, Infusionsoft, Ontraport) zijn hiermee AVG proof. Sowieso zijn de meeste Amerikaanse emailmarketing en inbound-marketing pakketten waarschijnlijk AVG-proof, omdat ze allemaal veel klanten in Europa hebben. Ze zijn dus per definitie al voorbereid op de GDPR.

Persoonlijk woordje… Gewoon, omdat het kan.

Ik kan me goed voorstellen dat je als ondernemer er tegenop ziet om dit te regelen. Misschien denk je wel: "Wat hangt me boven het hoofd?". Bedenk dan dit: de AVG is primair bedoeld om jouw klanten verder te helpen en de markt transparanter te maken. Als jij het beste voor ogen hebt voor je klanten dan is er niets aan de hand.

Ik hoop dat dit artikel je op weg heeft geholpen. Voel je vrij om de PDF (in ongewijzigde vorm) te sturen naar wie jij denkt dat er baat bij heeft.

Succes met de uitvoering en wellicht ontmoeten we elkaar eens.

Met een glimlach,
Bart van den Belt

Kleine lettertjes

Gebruikte bronnen:

KVK – Voorbereiden op de AVG
Autoriteit persoonsgegevens – Voorbereiding op de AVG
Autoriteit persoonsgegevens – Algemene informatie AVG
Autoriteit persoonsgegevens – Mag je persoonsgegevens bewerken?
Autoriteit persoonsgegevens – In 10 stappen voorbereid op de AVG (PDF)
ICT recht over de AVG
VeiligInternetten.nl