

AVG een goed idee

De Algemene Verordening Gegevensbescherming vraagt van organisaties om te verantwoorden wat er met de gegevens van mensen gebeurt. Daarbij gaat het om:

- mag je het verzamelen en verwerken?
- open zijn wat je verzamelt en verwerkt
- er moet een doel zijn voor alles wat je structureel verzamelt
- je moet je best doen de gegevens correct te bewaren

Maar het belangrijkste is het beginsel dat de gegevens in beginsel van de persoon zijn en niet van het bedrijf. De EU wil dat mensen invloed hebben op wat, waar en door wie wordt opgeslagen. En zelfs dat gegevens verwijderd worden als de persoon dit vraagt.

Nog een belangrijk punt is dat je je niet zo makkelijk kan verschuilen als je de verwerking of opslag uitbesteedt aan een ander: dan moet je een verwerkersovereenkomst opstellen.

Wat wil je in ieder geval doen? 5 tips

1. **beveilig je website met SSL.** Voorkom dat anderen internetgedrag van je bezoekers kunnen volgen door je website te beveiligen met SSL (encryptie, zodat ook via open wifi netwerken de informatie niet zo te volgen is).
2. **beperk de vragen in de formulieren op je website.** Veel formulieren vragen te veel en websites slaan dit meestal ook nog op de achtergrond op. Verzamel alleen wat je expliciet nodig hebt.
3. **vraag leveranciers van software om een verwerkersovereenkomst** als je de verwerking van persoonsgegevens doet door een tool van een ander (bijvoorbeeld een online ledensysteem).
4. **zorg voor goede beveiliging van je basisinformatie.** Meestal is 'de cloud' veiliger dan een eigen server op kantoor. Kies voor een Nederlandse partij (die je ook kunt bellen).
5. **Check of er oude back-ups en accounts 'zwerven'** bij Google, mailchimp, Microsoft, dropbox etc

Is de AVG van toepassing?

Er is veel bangmakerij. Het is zo dat de AVG geldt voor álle organisaties, zelfs ZZP'ers. Daar komt vast niet het zwaartepunt te liggen, maar het is wel belangrijk om ook als klein bedrijf even te controleren of je wat moet veranderen om niet draconische boetes te riskeren. De Autoriteit Persoonsgegevens zegt daarover dat de AVG geldt voor alle organisaties die persoonsgegevens verwerken. Het moet daarbij gaan om persoonsgegevens: dat betekent informatie die iets zegt over mensen.

Verwerken moet je trouwens ruim zien: gewoon gestructureerd bewaren valt ook al onder verwerken. Voor persoonsgegevens geldt dat de zekerheden die je moet bieden enorm toenemen als je 'gevoelige persoonlijke informatie' bewaart. En hetzelfde geldt voor verwerken.

De verplichtingen nemen toe als je bijvoorbeeld met persoonsgegevens:

- mensen indeelt in categorieën (profiling)
- gevoelige gegevens verzamelt en bewaard over gezondheid, voorkeuren, financiën etc.
- de schaal waarop je dit doet, is van belang omdat hiermee samenhangt of extra maatregelen (FG en DPIA) verplicht zijn.
- bepaalt of iemand bepaalde rechten heeft of van diensten wel of niet gebruik mag maken (een vorm van profiling), zeker als dit geautomatiseerd plaatsvindt.

De AVG richt zich niet op informatie waar je toevallig over beschikt. Bedenk maar eens wat er allemaal in e-mails staat. Dit is geen gestructureerde opslag van informatie van personen. Dat is anders op het moment dat je een systeem gebruikt om informatie uit e-mails te halen en deze op te slaan en zo een database aan te leggen met persoonlijke gegevens die je uit email haalt.

Een eenvoudige versie hiervan is als je een webformulier gebruikt om van personen informatie te verzamelen. Dat kan gestructureerde informatie zijn, die ook nog verwerkt wordt (tot profielen?) en dat is iets

anders dan informatie waar je toevallig over beschikt.

Als je alleen zaken met bedrijven doet, sla je bij bedrijven vaak een contactpersoon op. Een factuuradres of doorkiesnummer zijn geen persoonsgegevens. Hobby's of muziekvoorkeuren wel.

wat moet ik doen?

Als je nou twijfelt, kijk dan eerst eens op de site van de autoriteit persoonsgegevens (AP). Het is de officiële informatie over de AVG en heel goed leesbaar opgesteld. Het advies van de AP is eens goed nagaan wat je van wie opslaat, waarvoor dit gebruikt wordt en hoe dit beveiligd is.

De meest voor de hand liggende plekken waar je kunt kijken zijn bijvoorbeeld:

- het CRM systeem
- eigen site of mailinglist
- systeem voor facturatie, ledenbeheer, klantinformatie etc..
- oude kopieën en back-ups van systemen die je niet meer gebruikt

Tot slot

De AVG richt zich met name op organisaties die leven van persoonsgegevens, zoals zorginstellingen, scholen, overheid, verzekeraars, banken, datingsites, social media en online retailers. Toch is het voor iedereen spannend, omdat de rechter in de komende periode moet gaan uitspreken wat nou echt de grenzen zijn. Voorkom dat je risico loopt dat gegevens gestolen worden of dat je ruzie krijgt met mensen over wat je van ze weet.

In het algemeen is het een goede zaak dat mensen het recht hebben om te weten (en beïnvloeden) wat andere organisaties van je opslaan. En aan de andere kant is het ook helemaal niet gek om nog eens te checken welke persoonsgegevens organisaties bewaren, welk doel dat dient en of dat wel veilig is.

WHITEPAPER ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG GDPR) - mei 2018