Klaar voor AVG? Doe de check!

☐ **De juiste personen zijn bewust van de wetgeving.**
De juiste mensen in je organisatie, zij die met persoonsgegevens werken, moeten zich bewust zijn van wat wel en niet mag onder de nieuwe wetgeving.

☐ **We hebben, indien nodig, een verwerkingsregister.**
Het is in veel gevallen verplicht om inzichtelijk te maken hoe je persoonsgegevens verwerkt (waarom noodzakelijk, bron, bewaartermijn, etc.).

☐ **We hebben, indien nodig, een functionaris gegevensbescherming aangewezen.**
Verwerkt jouw organisatie veel (bijzondere) persoonsgegevens? Dan kan deze verplichting voor de organisatie gelden. Deze functionaris ondersteunt een organisatie bij handelen conform de AVG-wet.

☐ **We voldoen aan privacy by design & privacy by default.**
Als organisatie dienen je producten en diensten in de basis privacy vriendelijk te zijn. Waar mogelijk moeten ze persoonsgegeven pseudonimiseren/anonimiseren. Bestaande producten en diensten zijn hierop worden aangepast.

☐ **Er zijn overeenkomsten met subverwerkers gesloten.**
Er zijn verwerkersovereenkomsten gesloten met dienstverleners, zoals je marketing- of webbureau, die namens jou persoonsgegevens verwerken.

☐ **We verkrijgen op de juiste manier toestemming.**
Om persoonsgegevens te verwerken is toestemming nodig. Die toestemming moet verleend worden middels een herleidbare opt-in.

☐ **Er zijn maatregelen getroffen voor rechten van betrokkenen.**
Individuen hebben met de nieuwe wet meer controle over hun gegevens. Ze hebben bijvoorbeeld het recht om vergeten te worden of op dataportabiliteit: Ze kunnen organisaties vragen om hun data en/of deze over te dragen aan andere organisaties. Om hieraan te kunnen voldoen moet je als organisatie procedures opstellen en eventueel technische maatregelen nemen.

☐ **Er is een databeveiligingsbeleid.**
Bij het maken van zo'n beleid moet je ook nadenken over de beveiliging van verbindingen, sterke wachtwoorden afdwingen en het beheer van kopieën en back-ups. Het gaat dus niet alleen om kwaadwillende van buitenaf, maar ook om risico's van binnenuit (rondslingerende USB-sticks, etc.).

☐ **We weten wat een DPIA is en hebben het wel/niet nodig.**
DPIA staat voor Data Protection Impact Assessment en is verplicht bij een hoog privacy risico. Het is een instrument om dat risico in kaart te brengen en een systeem voor de beschrijving van de beoogde maatregelen.

☐ **Er is een protocol voor de meldplicht datalekken.**
Als organisatie moet je binnen 72 uur melding doen bij de Autoriteit Persoonsgegevens als er sprake is van inbreuk persoonsgegevens. Hieronder valt de vernietiging, het verlies of de wijziging van gegevens of ongeoorloofde verstrekking daarvan of toegang tot die gegevens. Zorg dus dat iedereen in de organisatie weet wat er in zo'n geval moet gebeuren. Wanneer moet er gebeld worden en met wie?

Vragen over technische aspecten van het implementeren van AVG?

Bel 071 - 576 13 23, mail service@swis.nl of kijk op swis.nl