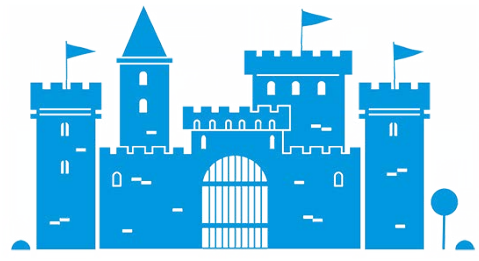
Stappenplan AVG



1

Bewustwording

Alle relevante personen binnen de organisatie moeten bewust zijn van de komst van de AVG. Denk aan beleidsmakers, security officers en andere personen die verantwoordelijk zijn voor datagevoelige bedrijfsprocessen. In deze fase moet worden bepaald wat de impact is van de wetgeving op de organisatie.

2

Rechten van betrokkenen

Mensen van wie de persoonsgegevens worden verwerkt krijgen onder de AVG meer en verbeterde privacyrechten. Hieronder vallen bestaande wetten zoals het recht op verwijdering. Nieuwe rechten zijn onder andere het recht op dataportabiliteit. Je moet er dan ook voor zorgen dat mensen deze rechten goed kunnen uitoefenen.

3

Overzicht verwerkingen

Onder de AVG heb je een verantwoordingsplicht. Dat houdt in dat je moet kunnen aantonen dat je je houdt aan de richtlijnen van de wet. Onderdeel hiervan is dat je moet bijhouden welke gegevens je verwerkt, met welk doel, waar deze gegevens vandaan komen en met wie ze worden gedeeld.

4

Data protection impact assesment (DPIA)

Als je gegevensverwerkingen een hoog privacyrisico met zich meebrengen ben je verplicht een data protection impact assesment uit te voeren. Hiermee breng je vooraf alle privacyrisico's in kaart, en benoem je maatregelen om de risico's te minimaliseren.

5

Privacy by design & privacy by default

Privacy by design betekent dat je bij het ontwerpen van producten en diensten zorgt dat persoonsgegevens goed beschermd zijn. Aanvullend moet je zorgen dat je alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel. Hiervoor moet je technische en organisatorische maatregelen treffen. Dit wordt ook wel privacy by default genoemd.

6

Functionaris voor de gegevensbescherming

In sommige gevallen kun je verplicht zijn een functionaris voor de gegevensbescherming aan te stellen. Deze persoon houdt toezicht op de naleving van de AVG. Dit is verplicht voor onder andere overheidsinstanties en publieke organisaties. Controleer vooraf of dit ook voor jouw organisatie geldt.

7

Meldplicht datalekken

De meldplicht datalekken blijft grotendeels hetzelfde. De eisen voor registratie van datalekken wordt wel strenger. Je moet al deze lekken registreren, zodat de Autoriteit Persoonsgegevens kan controleren of je aan de meldplicht voldoet.

8

Verwerkersovereenkomsten

Het kan natuurlijk zijn dat je je gegevensverwerking hebt uitbesteed. Controleer in dat geval of bestaande contracten met de verwerker voldoen aan de richtlijnen van de AVG. Zo niet, dan moeten daar aanpassingen in worden gedaan.

9

Leidende toezichthouder

Als je organisatie in meerdere EU-lidstaten is gevestigd hoef je maar met één toezichthouder (de 'leidende toezichthouder') zaken te doen, in plaats van meerdere zoals voorheen. Dat geldt ook als je gegevensverwerkingen impact hebben in meerdere lidstaten. Vooraf moet worden bepaald onder welke toezichthouder de organisatie valt.

10

Toestemming

Onder de AVG worden de regels rondom toestemming voor dataverwerking strenger. Je moet onder andere kunnen aantonen dat je geldige toestemming hebt gekregen om gegevens van klanten en andere betrokkenen te verwerken. Ook moet het makkelijk worden gemaakt voor personen om hun toestemming in te trekken.