AVG-GDPR check uitvoeren bij MKB klanten

Alleen een beveiligingsbeleid opstellen is niet voldoende voor de compliance.

Het hebben van een beleid is overigens niet verplicht, maar is een zogenaamde 'aanvullende' maatregel op de standaard verantwoordingsplicht.
Volgens de AVG is een gegevensbeschermingsbeleid wél verplicht als dit in verhouding staat tot de verwerkingsactiviteiten van de organisatie.
Bijvoorbeeld Ziekenhuizen, gemeenten, social mediabedrijven en marketing-informatiebureaus.
Een gegevensbeschermingsbeleid wordt ook wel privacy beleid genoemd binnen de AVG. Binnen de AVG is helder beschreven waaraan het beleid moet voldoen.
Geen rocket science.

Overigens; een gegevensbeschermingsbeleid is niet hetzelfde dan de privacyverklaring.
Alle organisaties die persoonsgegevens verwerken, moeten mensen op een heldere manier informatie geven over de persoonsgegevens die zij verwerken en
voor welk doel zij deze gegevens verwerken.
De meest aangewezen manier hiervoor is het beschikbaar stellen van een privacyverklaring op de website van de organisatie.

Wat een organisatie moet doen mbt hun verantwoordingsplicht komt uit de inventarisatie – compliance check. Dit kan dan weer input zijn voor het 'beveiligingsbeleid'
Wat een organisatie moet doen is sterk afhankelijk of en welke persoonsgegevens ze hebben, toegang hebben of verwerken.
En dan ook nog eens welt type persoonsgegevens. Standaard of hoog-gevoelig. Dit alles heeft invloed op de te nemen maatregelen en het beleid

Volgens de AVG is een gegevensbeschermingsbeleid overigens wél verplicht als dit in verhouding staat tot de verwerkingsactiviteiten van de organisatie.
Bijvoorbeeld Ziekenhuizen, gemeenten, social mediabedrijven en marketing-informatiebureaus.
Een gegevensbeschermingsbeleid wordt ook wel privacy beleid genoemd binnen de AVG. Binnen de AVG is helder beschreven waaraan het beleid moet voldoen.
Of een organisatie een gegevensbeschermingsbeleid moet maken, volgt dus ook uit de inventarisatie.

Overigens; een gegevensbeschermingsbeleid is niet hetzelfde dan de privacyverklaring.
Alle organisaties die persoonsgegevens verwerken, moeten mensen op een heldere manier informatie geven over de persoonsgegevens die zij verwerken en
voor welk doel zij deze gegevens verwerken. De meest aangewezen manier hiervoor is het beschikbaar stellen van een privacyverklaring op de website van de organisatie.

Als uit de inventarisatie komt, dat de organisatie een register van verwerkingsactiviteiten, DPIA (Data Privacy Impact Analyse) = soort risicoanalyse moet maken,
kunnen wij daar ook op een heldere manier invulling aan geven. Hoeveel werk dit is, is per klant verschillend.
Ik schat in dat de meeste IT en MKB industrie bedrijven er geen spannende dingen gaan gebeuren mbt persoonsgegevens en de AVG.
Anders is het bijvoorbeeld: een klein marketingbureau of IT bedrijf, ook al is het klein, die heel veel persoonlijke data analyseert voor zijn klant, moet zeker een register opstellen van die bewerking én daar een DPIA over doen. Maar dat lijkt me logisch, immers, als er iets fout gaat in die verwerking, liggen de persoonsgegevens op straat. Het is hun 'core business'
Zo praktisch moet je het zien en begrijpen.

Voorstel:

AVG-GDPR inventarisatie / compliance check
1 dagdeel, met begeleiding van een adviseur informatiebeveiliging
Aanleveren inventarisatie rapport
Aanleveren templates tbv verwerkingsregister en DPIA (de klant kan hier zelf mee aan de slag)
Voorbeeld basis gegevensbeschermingsbeleid
€595,-

Indien klanten hulp willen bij het realiseren van verschillende beheersmaatregelen, kunnen wij dat verzorgen.

Coachende variant of uitvoerende variant.

Opstellen register + toestemming van de verwerking
Uitvoeren DPIA
Opstellen procedure en register datalekken
Aanstellen / eisen FG
Opzetten interne informatiebeveiliging – ISO 27001/NEN 7510
Opstellen van het gegevensbeschermingsbeleid (indien noodzakelijk)

Voor bovenstaande werkzaamheden, kunnen wij ondersteunende software inzetten om de maatregelen beheersbaar & overzichtelijk te houden.
Deze software is specifiek bedoeld om organisaties te ondersteunen bij het managen van hun informatie en privacy risico's.