Checklist

Heeft u de juiste maatregelen getroffen voor de AVG-wetgeving?

Juridische maatregelen

- ☐ Zorg voor een privacyverklaring en toon deze op uw website
- ☐ Zorg voor verwerkersovereenkomsten met zowel klanten leveranciers als onderaannemers
- ☐ Stel een register met verwerkingsactiviteiten op
- ☐ Zorg indien nodig voor geheimhoudingsplicht richting uw personeel
- ☐ Zorg voor een register met beveiligingsincidenten
- ☐ Richt een proces op om verzoeken van betrokkenen te borgen
- ☐ Stel een ICT-beveiligingsbeleid op

Algemene maatregelen

- ☐ Vraag toestemming aan de klant voor het verwerken van zijn/haar gegevens
- ☐ Verwerkt u gevoelige persoonsgegevens? Stel iemand aan als functionaris van gegevensbescherming. (Toezichthouder op het naleven van de AVG)
- ☐ Noteer welke maatregelen er worden genomen om persoonsgegevens veilig te verwerken
- ☐ Voer een gegevensbeschermingsbeoordeling uit (DPIA)
- ☐ Stel een camerabeleid op en leef deze na
- ☐ Stel een continuïteitsplan op en leef deze na
- ☐ Maak een protocol: Wat te doen bij een data lek?
- ☐ Richt een bewaarbeleid in voor de persoonsgegevens

Veiligheidsmaatregelen voor het personeel

- ☐ Sla zo minmogelijk persoonsgegevens op de lokale harde schijf, USB-stick of externe schijf
- ☐ Vernietig alle data zodat alles onleesbaar is bij verkoop/ verwijdering van oude apparatuur
- ☐ Maak gebruik van het bedrijfsnetwerk als u werkt met persoonsgegevens
- ☐ Bij extern werken: Maak gebruik van een beveiligde (VPN)verbinding
- ☐ Creëer bewustwording aangaande het veilig omgaan met persoonsgegevens
- ☐ Houdt zakelijk en privé gescheiden als het gaat om e-mail gebruik

Technische maatregelen

- ☐ Pas encryptie toe waar mogelijk
- ☐ Pas een wachtwoord beleid toe
- ☐ Pas twee factor authenticatie toe waar mogelijk
- ☐ Zorg voor een complete documentatie
- ☐ Zorg voor een goede back-up (3-2-1 regel)
- ☐ Zorg voor een recovery plan wanneer u toch wordt getroffen
- ☐ Zorg voor een slimme firewall met licenties om datalekken te voorkomen
- ☐ Zorg voor gescheiden en veilige IT-netwerken om inbreuk te voorkomen
- ☐ Centraliseer de toegang en het beheer van de gebruikersaccounts
- ☐ Maak gebruik van frequent werkplek en update beheer
- ☐ Maak gebruik van monitoring en registreer incidenten
- ☐ Controleer regelmatig of je bovenstaande maatregelen juist functioneren