Algemene Verordening Gegevensbescherming (AVG)

De 8 voornaamste punten waar u als organisatie rekening mee moet houden:

- Er zijn nieuwe regels rondom het aanstellen van een Functionaris Gegevensbescherming.
  Dit betekent dat de AVG deze verplicht stelt wanneer u op grote schaal persoonsgegevens verwerkt of wanneer u bijzondere gegevens verwerkt (bijv. biometrisch, ras en etniciteit). Daarbij stelt de AVG eisen aan de aanstelling van de functionaris, bijvoorbeeld ten aanzien van opleiding en positie in de organisatie.
- De rechten van burgers worden beter beschermd.
  De belanghebbende moet makkelijker inzage krijgen in wat een organisatie registreert, maar moet ook onmiddellijk geïnformeerd worden wanneer haar gegevens zijn gehackt.
- De AVG stelt dat organisaties bij verwerkingen de principes "privacy-by-design" en "privacy-by-default" moeten hanteren.
  Technieken als "privacy enhancing technologies" en pseudonimisering moeten worden toegepast om de gegevens te beschermen.
- Bij de verwerking van Privacy gevoelige informatie bent u verplicht een impact analyse (Data Protection Impact Assessment) uit te voeren om de risico's van de verwerking te inventariseren en beoordelen.
- Hogere boetes worden opgelegd. Dit kan oplopen tot 4% van de wereldwijde omzet of 20 miljoen euro.
- Als organisatie moet u kunnen aantonen dat u voldoet aan de AVG.
  U moet hierbij denken aan de verwerkingsbeginselen, beveiliging van gegevens, bewerkersovereenkomsten, minimalisatie van verwerkingen, etc. Een omvangrijke compliance exercitie. Zorg ervoor dat u tijdig met verslaglegging en documentatie begint.
- De verplichting om een bewerkersovereenkomst af te sluiten met een bewerker kenden we al van de Wbp. De AVG gaat hierin een stap verder en noemt een aantal verplichte onderdelen in de overeenkomst, zoals doel van de verwerking, het soort persoonsgegevens en de beveiligingsmaatregelen die worden toegepast.
- De meldplicht datalekken kenden we ook al van de Wbp. Nieuw is echter dat een bewerker nu verplicht wordt datalekken te melden bij de verantwoordelijke (bijvoorbeeld de opdrachtgever). Mogelijk zult u uw protocol voor datalekken dus moeten herzien.