Versie: 20180502

Doel van het gegevensbeschermingsbeleid

Het doel van het gegevensbeschermingsbeleid is om de juridische aspecten van gegevensbescherming in één samenvattend document weer te geven. Het kan ook worden gebruikt als basis voor wettelijk voorgeschreven controles op gegevensbescherming, bijvoorbeeld door de klant in het kader van de in opdracht gegeven verwerking. Dit is niet alleen bedoeld om de naleving van de Europese algemene verordening inzake gegevensbescherming te waarborgen, maar ook om aan te tonen dat de verordening wordt nageleefd.

Inleiding

Aangezien per 25 mei 2018 de AVG (Algemene Verordening Gegevensbescherming) in werking treedt maak ik van deze gelegenheid gebruik om mijn praktijk hierop aan te sluiten.

Vanzelfsprekend wordt er vertrouwelijk met de verstrekte gegevens omgegaan. Maar op zich positief dat hier één duidelijke lijn getrokken wordt.

Veiligheidsbeleid en verantwoordelijkheden binnen de onderneming

- Voor een bedrijf moeten naast de bestaande bedrijfsdoelstellingen ook de hoogste doelstellingen op het gebied van gegevensbescherming worden gedefinieerd en gedocumenteerd. De doelstellingen inzake gegevensbescherming zijn gebaseerd op de principes van gegevensbescherming en moeten voor elk bedrijf afzonderlijk worden aangepast.
- Bepaling van rollen en verantwoordelijkheden (bv. vertegenwoordigers van het bedrijf, operationele gegevensbeschermingsfunctionarissen, coördinatoren of gegevensbeschermingsteams en operationele managers).
- Verbintenis tot voortdurende verbetering van een systeem voor het beheer van gegevensbescherming.
- Opleiding, sensibilisering en verplichtingen van de werknemers.

Juridisch kader in de onderneming

- Sectorspecifieke wettelijke of gedragsregels voor de behandeling van persoonsgegevens.
- Eisen van interne en externe partijen.
- Toepasselijke wetten, eventueel met bijzondere lokale voorschriften.

Documentatie

- Uitgevoerde interne en externe controles.
- Gegevensbescherming: bepaling van de behoefte aan bescherming met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid. De categorie-indeling zal zijn: "normaal", "hoog" en "zeer hoog".

Bestaande technische en organisatorische maatregelen (TOM)

Passende technische en organisatorische maatregelen die moeten worden uitgevoerd en onderbouwd, rekening houdend met onder meer het doel van de verwerking, de stand van de technologie en de uitvoeringskosten.

De beschrijving van de uitgevoerde TOM kan bijvoorbeeld worden gebaseerd op de structuur van ISO/IEC 27002, rekening houdend met ISO/IEC 29151 (richtsnoeren voor de bescherming van persoonsgegevens). De respectieve hoofdstukken moeten worden onderbouwd door een verwijzing naar de bestaande richtsnoeren.

Voorbeelden van dergelijke richtsnoeren zijn onder meer:

- Richtsnoer voor de rechten van betrokkenen
- Toegangscontrole
- Indeling en verwerking van informatie
- Fysieke en omgevings-gerelateerde beveiliging voor eindgebruikers, zoals
    - Toelaatbaar gebruik van waarden
    - Richtsnoer voor informatieoverdracht op basis van werkomgeving en schermvergrendelingen
    - Mobiele apparaten en telewerken
    - Beperking van installatie en gebruik van software
- Back-up gegevens
    - Informatieoverdracht
- Bescherming tegen malware
- Behandeling van technische zwakke punten
- Cryptografische maatregelen
- Communicatiebeveiliging
- Privacy en bescherming van persoonsgegevens
- Relaties met leveranciers: Het verslagleggen van regelmatige inspectie en evaluatie van gegevensverwerking, in het bijzonder de effectiviteit van de geïmplementeerde technische en organisatorische maatregelen.