Activiteiten opstellen databeveiligingsbeleid:

Het opstellen van een beleid over privacy en informatiebeveiliging vereist een gestructureerde aanpak. Dit zijn de stappen die een goededoelenorganisatie kan volgen om een dergelijk beleid op te stellen, rekening houdend met relevante wetgeving:

1. **Onderzoek de relevante wet- en regelgeving**: Identificeer welke wetten en regelgeving van toepassing zijn op het goede doel met betrekking tot privacy en informatiebeveiliging. Voorbeelden zijn de Algemene Verordening Gegevensbescherming (AVG) en de relevante delen van de Telecommunicatiewet.
2. **Benoem verantwoordelijkheden**: Bepaal wie binnen de organisatie verantwoordelijk is voor het opstellen, implementeren en handhaven van het privacy- en informatiebeveiligingsbeleid. Dit kan bijvoorbeeld een Privacy Officer of informatiebeveiligingsmanager zijn.
3. **Voer een risicobeoordeling uit**: Bedenk en beoordeel welke risico's er zijn voor de persoonlijke gegevens en informatie binnen het goede doel. Kijk hierbij naar welke gegevens worden verzameld, hoe ze worden gebruikt en met wie ze worden gedeeld. Volgens de AVG is het verplicht om voor elke afzonderlijke verwerking die mogelijk een hoog risico inhoudt, een risicobeoordeling (Data Protection Impact Assessment) uit te voeren (artikel 35).
4. **Ontwikkel passende maatregelen**: Maak op basis van de risicobeoordeling passende organisatorische en technische maatregelen. Dit kan onder meer het implementeren van toegangscontroles, versleuteling van gegevens, bewustwordingstraining voor medewerkers en het opstellen van dataretentiebeleid omvatten.
5. **Stel het beleid op**: Formuleer een duidelijk en beknopt beleidsdocument waarin de doelstellingen, verantwoordelijkheden, maatregelen en procedures met betrekking tot privacy en informatiebeveiliging zijn vastgelegd. Het beleid moet in lijn zijn met de eerder geïdentificeerde wet- en regelgeving.
6. **Implementeer het beleid**: Zorg ervoor dat het opgestelde beleid wordt gebruikt in de (dagelijkse) werkwijze van het goede doel. Dit kan onder meer door het trainen van medewerkers, het uitvoeren van interne controles en het bijwerken van procedures.
7. **Monitor en evalueer**: Evalueer regelmatig het privacy- en informatiebeveiligingsbeleid. Hierdoor blijft het effectief in het beschermen van persoonsgegevens en informatie. Pas het beleid indien nodig aan in reactie op veranderende risico's of wetgeving.
8. **Documenteer en communiceer**: Zorg ervoor dat het privacy- en informatiebeveiligingsbeleid overzichtelijk en toegankelijk is voor alle betrokkenen, inclusief medewerkers, belanghebbenden en externe partijen zoals leveranciers en klanten.

Door deze stappen te volgen, kan een goed doel een adequaat en up-to-date beleid ontwikkelen en implementeren dat voldoet aan de normen voor privacy en informatiebeveiliging, inclusief de relevante wetgeving voor goede doelen.

Deze handreiking is ontwikkeld door het CBF en gecontroleerd door de Autoriteit Persoonsgegevens (AP).