Handreiking voor Goededoelenorganisaties:

Tips en aanbevelingen voor data- en informatiebeveiliging

Als goed doel ben je belangrijk voor de samenleving, en waarschijnlijk verzamel, gebruik en bewaar je persoonlijke gegevens van mensen. Het is cruciaal om te weten welke regels je moet volgen om ervoor te zorgen dat je dit op een juiste en eerlijke manier doet.

Deze handreiking geeft je een overzicht van de belangrijkste regels waar je als goed doel aan moet voldoen. We bespreken onder andere de privacywetgeving (AVG), regels over financiële transacties (Wwft), en wetten met betrekking tot communicatie (Telecommunicatiewet).

Elk deel van deze handreiking behandelt een ander onderwerp, met eenvoudige tips en voorbeelden die nuttig zijn voor goede doelen. Door deze informatie te begrijpen en toe te passen, kun je ervoor zorgen dat je de privacy van mensen beschermt en risico's vermijdt.

Het is niet alleen belangrijk om aan de regels te voldoen omdat het moet, maar ook omdat het helpt om het vertrouwen van donateurs en de samenleving te winnen. We moedigen je dus aan om deze handreiking goed door te lezen, eventueel hulp te vragen als iets niet duidelijk is, en actie te ondernemen om aan de regels te voldoen.

Deze handreiking is ontwikkeld door het CBF in samenwerking met de Autoriteit Persoonsgegevens (AP).

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.

Wettelijke bepalingen

1. **Algemene Verordening Gegevensbescherming (AVG):** De AVG is de Europese privacywetgeving die in 2018 van kracht is gegaan. De wet regelt de verwerking van persoonsgegevens en geeft betrokkenen meer controle over hun persoonlijke informatie. Goededoelenorganisaties moeten voldoen aan de bepalingen van de AVG bij het verwerken van persoonsgegevens.
2. **Uitvoeringswet AVG (UAVG):** De UAVG is een Nederlandse wet die geen zelfstandige regels bevat, maar onderdelen van de AVG nader uitwerkt waar de Europese verordening ruimte laat voor nationale invulling.
3. **Telecommunicatiewet:** Deze wet regelt onder meer het gebruik van elektronische communicatiemiddelen en de verwerking van verkeers- en locatiegegevens; ook het gebruik van cookies valt onder deze wet.
4. **Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft):** Als het goede doel betrokken is bij financiële transacties, kan de Wwft van toepassing zijn. Deze wet stelt eisen aan het identificeren van cliënten en het melden van ongebruikelijke transacties.

De Algemene Verordening Gegevensbescherming (AVG) heeft betrekking op de bescherming van persoonsgegevens en is van toepassing op alle organisaties, inclusief goede doelen. Dit zijn enkele belangrijke aspecten van de AVG en wat ze betekenen voor goede doelen in de uitvoering:

1. **Toestemming, transparantie en andere grondslagen:** Goededoelenorganisaties moeten ervoor zorgen dat ze een grondslag hebben als zij persoonsgegevens verwerken. Ze moeten transparant zijn over hoe ze gegevens verzamelen, gebruiken en delen. Dit kan bijvoorbeeld van toepassing zijn op het verzamelen van gegevens van donateurs of deelnemers aan evenementen. Voor bijzondere persoonsgegevens zoals medische gegevens worden gelden extra eisen (artikel 9).
2. **Doelbinding:** Goededoelenorganisaties mogen persoonsgegevens alleen verzamelen en verwerken voor specifieke, expliciete en rechtmatige doeleinden. Ze moeten ervoor zorgen dat de verzamelde gegevens niet worden gebruikt voor doeleinden die niet verenigbaar zijn met het oorspronkelijke doel. Een goed doel mag bijvoorbeeld geen gegevens verkopen die zij hebben ontvangen van donateurs zonder hun expliciete toestemming.
3. **Dataminimalisatie:** Goededoelenorganisaties moeten streven naar het verzamelen van alleen de strikt noodzakelijke persoonsgegevens voor het beoogde doel. Ze moeten ervoor zorgen dat de gegevens die ze verzamelen relevant zijn en beperkt tot wat nodig is voor het doel.
4. **Rechten van betrokkenen:** Individuen waarvan de gegevens worden verwerkt (betrokkenen) hebben verschillende rechten onder de AVG. Goededoelenorganisaties moeten bijvoorbeeld de mogelijkheid bieden voor betrokkenen om toegang te krijgen tot hun gegevens, deze te corrigeren en in sommige gevallen te laten verwijderen.
5. **Datalekken:** Goededoelenorganisaties zijn verplicht om datalekken te melden aan de toezichthoudende autoriteit (autoriteit persoonsgegevens) en, in bepaalde gevallen, ook aan de betrokkenen. Ze moeten passende maatregelen nemen om de veiligheid van persoonsgegevens te waarborgen en moeten in staat zijn om eventuele inbreuken te identificeren en te melden.
6. **Functionaris voor Gegevensbescherming (FG):** In sommige gevallen kan het verplicht zijn om een Functionaris voor Gegevensbescherming aan te stellen, vooral als de verwerking van gegevens complex is of op grote schaal plaatsvindt.

Goededoelenorganisaties moeten hun gegevensverwerkingsactiviteiten evalueren, zorgen voor naleving van de AVG en passende maatregelen nemen om de privacy van betrokkenen te beschermen. Het is belangrijk dat goede doelen zich bewust zijn van hun verantwoordelijkheden en mogelijk juridisch advies inwinnen om ervoor te zorgen dat ze aan de AVG voldoen.

De **Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)** is een Nederlandse wet die onderdelen van de **Europese Algemene verordening gegevensbescherming (AVG)** nader uitwerkt. De UAVG bevat geen zelfstandige regels, maar vult de AVG aan waar op Europees niveau ruimte is gelaten voor nationale keuzes of verduidelijkingen. Het doel is om de uitvoering van de AVG in Nederland in goede banen te leiden.

Voor goede doelen betekent dit dat de UAVG in specifieke gevallen aanvullende bepalingen biedt, die altijd binnen het kader van de AVG blijven. Enkele relevante onderwerpen waarin de UAVG nadere invulling geeft:

1. **Verwerking van bijzondere categorieën van persoonsgegevens**
   De AVG stelt strikte voorwaarden aan het verwerken van gevoelige gegevens (zoals gezondheidsgegevens of gegevens over religie). De UAVG werkt deze voorwaarden soms nader uit, bijvoorbeeld voor specifieke sectoren of doeleinden. Goede doelen moeten dan beschikken over een geldige grondslag en passende waarborgen.
2. **Verwerking van persoonsgegevens van kinderen**
   De UAVG bevat extra bescherming bij verwerking van gegevens van kinderen, bijvoorbeeld door regels over toestemming van ouders. Goede doelen die met kinderen werken of hun gegevens verzamelen, moeten hier extra alert op zijn.
3. **Functionaris voor Gegevensbescherming (FG)**
   De AVG verplicht in bepaalde gevallen een FG. De UAVG biedt aanvullingen, bijvoorbeeld voor organisaties in de publieke sector of andere nationaal gevoelige situaties. Goede doelen moeten beoordelen of aanstelling van een FG verplicht of wenselijk is.
4. **Verwerking voor journalistieke, academische, artistieke of literaire doeleinden**
   De UAVG bevat uitzonderingen op grond van de vrijheid van meningsuiting en informatie. Verwerken goede doelen persoonsgegevens in deze context, dan kunnen specifieke regels gelden.
5. **Verwerking voor archiveringsdoeleinden in het algemeen belang**
   De UAVG biedt ook hier aanvullingen, bijvoorbeeld over bewaartermijnen of toegang tot gegevens. Dit is van belang voor goede doelen die bijvoorbeeld historische data of donateursarchieven langdurig bewaren.

Het is belangrijk voor goede doelen om zowel de AVG als de UAVG zorgvuldig te bestuderen en ervoor te zorgen dat ze voldoen aan alle relevante bepalingen. Het naleven van zowel de Europese AVG als de nationale UAVG is essentieel om te zorgen voor een volledige en adequate bescherming van persoonsgegevens. Het raadplegen van juridisch advies kan nuttig zijn om volledig op de hoogte te zijn van de specifieke verplichtingen die van toepassing zijn op het goede doel.

De Telecommunicatiewet in Nederland is van toepassing op alle organisaties, waaronder goededoelenorganisaties, en reguleert het gebruik van elektronische communicatiemiddelen en de verwerking van verkeers- en locatiegegevens. Hier volgen enkele belangrijke aspecten van de Telecommunicatiewet en wat ze kunnen betekenen voor goede doelen in de uitvoering:

1. **Toestemming voor elektronische communicatie:** De Telecommunicatiewet stelt regels voor het versturen van elektronische communicatie, zoals e-mails en nieuwsbrieven. Goede doelen moeten in veel gevallen toestemming verkrijgen van de ontvanger voordat ze elektronische berichten mogen sturen. Dit geldt bijvoorbeeld voor nieuwsbrieven die aan donateurs worden verzonden.
2. **Cookiewetgeving:** De Telecommunicatiewet bevat regels met betrekking tot het gebruik van cookies en vergelijkbare technologieën. Goede doelen moeten bezoekers van hun websites informeren over het gebruik van cookies en in bijna alle gevallen toestemming verkrijgen voordat ze cookies plaatsen of uitlezen.
3. **Vertrouwelijkheid van communicatie:** De wet beschermt de vertrouwelijkheid van communicatie, waaronder telefoongesprekken en elektronische berichten. Goededoelenorganisaties moeten ervoor zorgen dat ze deze vertrouwelijkheid respecteren en geen ongeoorloofde toegang tot of onderschepping van communicatie mogelijk maken.
4. **Melden van datalekken:** Net als onder de Algemene Verordening Gegevensbescherming (AVG) zijn goede doelen onder de Telecommunicatiewet verplicht om datalekken te melden aan de Autoriteit Persoonsgegevens en in sommige gevallen ook aan de betrokkenen. Dit geldt met name als het lek de persoonsgegevens van gebruikers van elektronische communicatiediensten betreft.
5. **Geheimhoudingsplicht voor aanbieders van communicatiediensten:** Aanbieders van communicatiediensten, zoals internetproviders, hebben een geheimhoudingsplicht met betrekking tot communicatie. Dit houdt in dat zij in principe geen kennis mogen nemen van de inhoud van communicatie, behalve onder strikte voorwaarden.

Het is van belang dat goede doelen zich bewust zijn van de Telecommunicatiewet en de specifieke verplichtingen die daaruit voortvloeien. Goededoelenorganisaties moeten er bijvoorbeeld goed op letten dat zij niet zonder toestemming cookies van derden plaatsen. Zorgvuldige naleving van deze wet is essentieel om de privacy van gebruikers te waarborgen en om mogelijke juridische consequenties te voorkomen. Het raadplegen van juridisch advies kan nuttig zijn om ervoor te zorgen dat goede doelen voldoen aan de vereisten van de Telecommunicatiewet.

De Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) is een Nederlandse wet die tot doel heeft het witwassen van geld en de financiering van terrorisme tegen te gaan. De Wwft stelt verplichtingen voor verschillende soorten instellingen, waaronder goede doelen, om maatregelen te nemen ter voorkoming van deze strafbare feiten. Hier zijn enkele aspecten van de Wwft en de mogelijke impact op goede doelen:

1. **Identificatie en verificatie:** De Wwft verplicht goede doelen om de identiteit van hun cliënten vast te stellen en te verifiëren voordat zij een zakelijke relatie aangaan of een transactie uitvoeren. Dit betekent dat goede doelen moeten weten met wie zij zaken doen, bijvoorbeeld bij het ontvangen van donaties of het verstrekken van subsidies.
2. **Meldingsplicht ongebruikelijke transacties:** Goededoelenorganisaties hebben een meldingsplicht bij de Financial Intelligence Unit Nederland (FIU-NL) als zij een ongebruikelijke transactie signaleren. Dit betreft transacties waarbij het vermoeden bestaat dat ze verband kunnen houden met witwassen of financieren van terrorisme.
3. **Bewaarplicht:** Goededoelenorganisaties moeten bepaalde gegevens, waaronder identificatiegegevens van cliënten en informatie over uitgevoerde transacties, bewaren voor een bepaalde periode. De bewaarplicht is bedoeld om toezichthoudende instanties in staat te stellen hun controle uit te oefenen.
4. **Interne procedures en beleid:** Goede doelen moeten interne procedures en beleid ontwikkelen en implementeren ter voorkoming van witwassen en financieren van terrorisme. Dit kan onder meer het trainen van medewerkers en het uitvoeren van risicobeoordelingen omvatten.
5. **Melding aan toezichthouder:** In sommige gevallen kan het goede doel verplicht zijn om bepaalde transacties vooraf te melden aan de toezichthoudende autoriteit, zoals De Nederlandsche Bank (DNB) of de Autoriteit Financiële Markten (AFM), afhankelijk van de aard van de activiteiten van het goede doel.

Het is van belang dat goede doelen zich bewust zijn van de verplichtingen onder de Wwft en stappen ondernemen om hieraan te voldoen. Het niet naleven van de Wwft kan leiden tot juridische consequenties en boetes. Het kan daarom verstandig zijn om juridisch advies in te winnen om ervoor te zorgen dat het goede doel voldoet aan de wettelijke vereisten van de Wwft.