**Stappenplan AVG**

Naast dit document zijn beschikbaar:

* ***Inleiding AVG***
* ***De AVG, ook voor gilden***

Aan te passen en te gebruiken voorbeelden van

* ***Gegevens gildeleden***
* ***Privacy policy***
* ***Verwerkingsovereenkomst***

**Stap 1: Persoonsgegevens inventariseren**

Persoonsgegevens zijn alle gegevens die te herleiden zijn tot een persoon. Ga na waar in de vereniging welke gegevens worden verzameld of gebruikt. Om het overzichtelijk te maken kan het handig zijn om de personen te verdelen in groepen. Denk hierbij bijvoorbeeld aan bezoekers van de website, leden, bestuursleden en niet-leden (Beschermheer -vrouw, Gildeheer, Ere-Deken etc.). Van elke groep zullen andere persoonsgegevens worden bewaard.

**Checklist van persoonsgegevens**

– NAW-gegevens

– telefoonnummers

– e-mailadressen

– website

– geslacht

– geboortedatum en geboorteplaats

– nationaliteit

– overlijdensdatum

– lidmaatschapsnummer eigen gilde

– lidmaatschapsnummer andere vereniging/stichting (bijv. KNTS/KNSA)

– socialmedia-gegevens (facebook, twitter)

– bankrekeningnummer

– inloggegevens

– verklaring omtrent gedrag

– enz.

**Checklist bijzondere persoonsgegevens**

De hierna genoemde gegevens (bijzondere persoonsgegevens) mogen alleen worden verwerkt na toestemming van de betreffende persoon! Het gilde moet kunnen bewijzen dat deze toestemming is verkregen. De persoon kan de toestemming op ieder moment intrekken. De gegevens moeten dan worden verwijderd of vernietigd. Bijzondere persoonsgegevens zijn onder meer:

– Etnische afkomst

– kopie paspoort waar pasfoto op zichtbaar is

– geloofsovertuiging

– BSN

– lidmaatschap vakbond

– politieke voorkeur

– informatie over gezondheid

– seksuele geaardheid

– strafrechtelijke gegevens (bijvoorbeeld overtredingen van de wapenwet)

Let dus goed op als je bij bijvoorbeeld voor evenementen (bijv. gildedag -feest) aanmeldingsformulieren voor minder validen op je website hebt staan. Als iemand dit invult wil dit niet automatisch zeggen dat het gilde het recht heeft deze informatie op te slaan. Neem voor dit soort informatie een extra regel op op het aanmeldingsformulier als je naar dit soort specifieke gegevens vraagt en wilt opslaan.

Verwijs bij aanmeldingsformulieren ook altijd naar de algemene voorwaarden en de privacy policy van het gilde.

**Stap 2: Waar worden deze gegevens bewaard**

Beschrijf waar, welke gegevens worden bewaard en wie er toegang heeft tot deze bestanden

Bijvoorbeeld:

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam van het bestand** | **Welke gegevens bevat het** | **Waar is het bestand opgeslagen** | **Wie heeft toegang tot het bestand (zie stap 7)** |
| Ledenbestand | * NAW
* Lidmaatschapsnummer
* Telefoonnummer
* Mobielnummer
* E-mailadres
* Geboortedatum
* Datum aanvang lidmaatschap
* …
 | * Computer secretaris
* Cloudomgeving (Onedrive, Google drive, etc.) van secretaris
* …
 | * Deken-Schrijver / Secretaris
* Hoofdman / Voorzitter
* …
 |
| Incassobestand | * NAW
* Lidmaatschapsnummer
* Bankrekeningnummer
* …
 | * Computer penningmeester
* …
 | * Deken-Rentmeester / Penningmeester
* …
 |
| ….. | * …
 | * …
 | * …
 |

Beschrijf dit voor alle plaatsen waar persoonsgegevens zijn opgeslagen zoals in Excel- en Worddocumenten, papieren overzichten, derden (drukker van verenigingsblad).

**Stap 3: Doel van de informatie**

Je ontvangt en bewaart persoonsgegevens voor een bepaald doel. Dit doel moet worden omschreven. Bijvoorbeeld NAW voor de administratie en het verzenden van het clubblad; e-mail voor het gericht informatie zenden; telefoonnummer voor het benaderen i.v.m. vrijwilligerstaken.

Je mag de gegevens alleen voor de omschreven doel(en) gebruiken. Gegevens die bijvoorbeeld zijn verkregen voor het lidmaatschap, mogen niet zonder toestemming van de persoon worden gebruikt voor reclamedoeleinden of het verzenden van een clubblad.

Bijvoorbeeld:

|  |  |
| --- | --- |
| **Soort persoonsgegeven** | **Waarvoor wordt het persoonsgegeven verwerkt** |
| NAW-gegevens (Naam, Adres, Woonplaats) | * Ledenadministratie
* Versturen van ledenberichten (Memo)
 |
| E-mailadres | * Versturen van ledenberichten (Memo)
* …
 |
| Telefoonnummer (vast – mobiel) | * Benaderen i.v.m. vrijwilligerstaken
* …
 |
| Geboortedatum | * Ledenadministratie
* Versturen verjaardag felicitatie
 |
| Datum aanvang lidmaatschap | * Bepalen lengte lidmaatschap voor jubileum
 |
| … | * …
 |

**Stap 4: Privacy policy**

Mensen van wie je gegevens hebt opgeslagen moet je informeren over hun rechten. Dat doe je d.m.v. een privacy policy. Het opstellen hiervan is verplicht en dit moet je dus bekend maken. Een website is hier een goed platform voor. Hiernaar kun je naar verwijzen (bijvoorbeeld op ledenberichten of e-mailberichten).

De Noordbrabantse Federatie van Schuttersgilden (NBFS) heeft een privacy policy opgesteld die door de gilden gebruikt kan worden. Deze is op de website www.schuttersgilden.nl te downloaden en door het gilde aan te passen aan de eigen situatie.

***Let op:*** *Aangezien elk gilde zelf verantwoordelijk is om data lekken tegen te gaan, is het (zeker bij wisselingen in het bestuur of bij vrijwilligers) goed om het privacy policy-beleid en samenhangende regels, opnieuw onder de aandacht te brengen. Neem dit bijvoorbeeld op in de notulen als dit is gebeurd.*

**Stap 5: Verwerkersovereenkomst**

Voor contacten met andere partijen (bijvoorbeeld de drukker van het verenigingsblad) dat buiten de NBFS c.q. de zes Kringen behorende tot de NBFS om geregeld wordt dient het gilde zelf initiatief te nemen tot het vastleggen van verantwoordelijkheden d.m.v. een verwerkersovereenkomst met die partij.

De eigenaar van de gegevens is verantwoordelijk voor de verwerkersovereenkomst. Met betrekking tot de gegevensuitwisseling tussen het gilde en de Kring waarbij het gilde is aangesloten, blijft het gilde dus verantwoordelijk.

**Stap 6: (ICT) beveiligingsmaatregelen**

Het gilde is ook verantwoordelijk voor de ICT-beveiliging van de persoonsgegevens. Voor diensten en producten die het gilde afneemt van de NBFS heeft de NBFS dit zo goed mogelijk voor het gilde geregeld. Zo worden er back-ups gemaakt van de gegevens en wordt er gezorgd voor de beveiliging van de websites.

Heeft het gilde daarnaast nog andere diensten en producten dan dient het gilde zelf te controleren of deze zaken goed geregeld zijn en zo niet deze beveiligingen regelen.

***Let op:*** *Evenals gegevens die digitaal zijn opgeslagen moeten ook persoonsgegevens**op papier beschermd te zijn. Deze mogen dus niet voor iedereen zichtbaar op een tafel liggen.*

***Tip:*** *Voor het versturen van persoonsgegevens kun je beter geen gebruik van Dropbox of WeTransfer omdat je niet makkelijk kunt controleren of deze gegevens binnen de EU worden opgeslagen.*

**Stap 7: Wie hebben toegang/ geheimhouding**

Controleer welke personen toegang hebben tot persoonsgegevens. Wie hebben er bijvoorbeeld een account in de administratie van het gilde of de website. Het is veiliger om meerdere accounts te hebben en niet gebruikersnamen en wachtwoorden met elkaar te delen.

Persoonsgegevens mogen nooit zonder toestemming van de betrokken persoon aan derden worden verstrekt. Wijs (nieuwe) leden er op dat zij een geheimhoudingsplicht hebben wat betreft persoonsgegevens van derden.

**Stap 8: Bewaartermijn**

Je mag persoonsgegevens niet oneindig lang bewaren. Beschrijf hoe lang de verschillende gegevens worden bewaard. Het kan gaan om papieren lijsten met telefoonnummers maar ook bijvoorbeeld om e-mails en digitale ledenbestanden.

Voor financiële gegevens is de wettelijke bewaartermijn 7 jaar na het afsluiten van het boekjaar.

Voor persoonsgegevens in het Vademecum zorgt de NBFS er voor dat deze gegevens t.z.t. worden verwijderd.

Bijvoorbeeld:

|  |  |
| --- | --- |
| **Soort persoonsgegeven in** | **Bewaartermijn** |
| Ledenlijst NAW – telefoonnummer (fysiek en digitaal) | Onbeperkt (archivering) |
| E-mails (digitaal) | Directe verwijdering na verwerking in overzicht poststukken |
| E-mails (in overzicht poststukken) | Onbeperkt (archivering) |
| Ledenadministratie | Onbeperkt (archivering) |
| Financiële gegevens | 7 (zeven) jaar na afsluiting boekjaar |
| … | … |

***Tip:*** *Organisaties mogen persoonsgegevens in een archief bewaren als dit bestemd is voor historische, statistische of wetenschappelijke doeleinden.*

*Zorg dus dat in de doelstelling in de Statuten of in het Huishoudelijke Reglement dit staat opgenomen, bijvoorbeeld via de vermelding: “het aanleggen en bijhouden van een documentair gilde-archief”.*

**Stap 9: Direct marketing**

Bij direct marketing heb je vooraf toestemming nodig om iemand te mogen benaderen.

Daarom dien je aan te kunnen tonen

– waarom er contact wordt opgenomen

– met welke organisaties het gilde deze gegevens zal delen

– wat de rechten van de persoon zijn om bezwaar te maken tegen deze direct marketing

**Foto’s van evenementen**

In principe is het maken van foto’s in de openbare ruimte en het publiceren van die foto’s in de krant, het clubblad of op de website van het gilde toegestaan. Dit ligt anders als de afgebeelde persoon een 'redelijk belang' heeft om zich tegen publicatie van zijn portret te verzetten. Vaak gaat het dan om een privacybelang. Een foto van iemand bij een nieuwsbericht kan gerechtvaardigd zijn door de nieuwswaarde ervan, ook al is die persoon er zelf niet blij mee dat zijn foto wordt gepubliceerd. Het algemene belang van de vrije nieuwsgaring gaat in dat geval vaak voor een persoonlijk belang.

Het is dus meestal wel toegestaan foto's te maken in de openbare ruimte en die te publiceren, zonder dat de personen die in beeld komen toestemming hoeft te worden gevraagd. De fotograaf moet zich wel rekenschap geven van de belangen die de gefotografeerde mensen zouden kunnen hebben. Denk bijvoorbeeld aan het fotograferen van kinderen. Bij twijfel is het beter vooraf om toestemming te regelen, bijvoorbeeld door op een aanmeldingsformulier aan te geven dat door deel te nemen aan het evenement, de kans bestaat dat er foto’s worden gemaakt die op de website of ander medium kunnen worden gepubliceerd.

**Stap 10: Controle en evaluatie**

Voer bovenstaande stappen uit en documenteer alles wat is gedaan. Leg ook vast wanneer er wijzigingen hebben plaatsgevonden. Denk hierbij aan informatievoorziening aan (nieuwe) leden en bestuursleden, wanneer er een update heeft plaatsgevonden in het beveiligingssysteem of wanneer er bijvoorbeeld niet eerder vastgelegde persoonsgegevens worden opgeslagen.

Bekijk jaarlijks of alles wat betreft het beveiligen van de persoonsgegevens nog up-to-date is en of er verdere maatregelen nodig zijn. Documenteer dit, ook als er geen nieuwe maatregelen nodig zijn.