Algemene Verordening Gegevensbescherming.

Protocol van Stichting Dorpshuis Austerlitz.

Voorwoord

In 2018 is de verouderde Nederlandse regelgeving omtrent de privacy vervangen door de nieuwe privacywet de AVG (Algemene Verordening Gegevensbescherming) . Binnen de EU bestonden nog verschillen in privacy wetgeving. Met de AVG is er één uniforme regelgeving voor de hele Europese Unie gekomen.

Deze nieuwe wet heeft gevolgen voor o.a. verenigingen en stichtingen zo ook voor de Stichting Dorpshuis Austerlitz (hierna te noemen SDA). Vanaf 25 mei 2018 moet op een vastgelegde manier omgegaan worden met privacygevoelige gegevens. Grote ondernemingen en overheidsinstanties moeten een Functionaris Gegevensbescherming (FG) aanstellen, dit is een toezichthouder die let op het naleven van de AVG. Voor kleine ondernemingen, verenigingen en stichtingen is dit vanwege hun geringe omvang niet nodig, in deze gevallen kan worden volstaan met aanstelling van een beheerder.

Er zijn veel veranderingen, vooral over hoe je met persoonsgegevens omgaat. Indien dit niet op de juiste wijze gebeurt kan dat leiden tot sancties van de landelijke toezichthouder. Bij mogelijke datalekken (gehackte systemen) kan het bestuur persoonlijk aansprakelijk worden gesteld voor de schade. Datalekken moeten direct worden gemeld bij de bevoegde autoriteiten.

De nieuwe wet regelt de bescherming en preventie van persoonlijke gegevens die een vereniging of stichting bewaart. Het gaat hierbij niet om wat mag, maar juist om wat je verplicht bent op orde te hebben. Hoe worden gegevens bewaard, hoe en waarvoor worden gegevens gebruikt, welke gegevens worden vastgelegd en beheerd. Allemaal zaken die in een protocol (register) moeten worden vastgelegd. De opzet van zo'n protocol (register) mag een vereniging zelf bepalen.

Het 'digitale bezit' van gegevens moet goed beschermd zijn (maar ook gegevens op papier moeten uiteraard aan dezelfde eisen voldoen). Iedereen die persoonlijke gegevens opslaat, moet kunnen aantonen dat hij of zij dit op een veilige en verantwoorde manier doet. Denk bij het soort opgeslagen gegevens bijvoorbeeld aan de ledenadministratie, het betalingsverkeer, administratie, websites, sociale media, adverteerders e.d.

De AVG geeft aan dat alleen relevante gegevens moeten worden opgeslagen. Persoonsgegevens welke niet worden gebruikt kunnen achterwege blijven om de fraudegevoeligheid zo klein mogelijk te houden. Bijzondere persoonsgegevens worden bij de SDA niet vastgelegd.

~~

Artikel 1.1; Doelstelling van de te beheren gegevens.

Persoonsgegevens worden beheerd i.v.m. het kunnen besturen van de SDA. wat inhoudt:

1. Het ontvangen en verstrekken van informatie per e- mail, per telefoon en/of post
2. Het regelen van betalingen voor verstrekte diensten zoals het verhuren van zaalruimte met de daarbij komende kosten
3. Het onderhouden van contacten met leveranciers van consumptieve producten.
4. Het onderhouden van contacten met vrijwilligers en overige relevante stakeholders

Voor andere doeleinden worden de gegevens niet benut.
Er worden geen overeenkomsten gesloten met externe partijen die de persoonsgegevens verwerken en/of gebruiken noch worden zij aan derden ter beschikking gesteld.

Artikel 1.2; Opgeslagen persoonsgegevens.

De SDA slaat gegevens op in het administratiesysteem voor de volgende categorieën van contacten:

a. Bestuursraad
b. Bestuur en commissies
c. Personeel waaronder ook vrijwilligers
d. Zakelijke contacten
e. Overige stakeholders

Gegevens die door SDA worden opgeslagen zijn:

* naam van de betreffende vereniging,
* Van de bestuursraadleden de voorletters, de naam en tussenvoegsel alsmede de functie binnen de eigen vereniging..
* Voorletters,naam en tussenvoegsel van de bestuursleden en/of contactpersonen met de daarbij behorende functie,
* telefoonnummer
* e-mailadres

Artikel 1.3; Opslag gegevens SDA en beveiliging.

SDA beheert haar gegevens in een digitale Cloud omgeving (OneDrive). Het digitale systeem is beveiligd met een gebruikersnaam en wachtwoord. Binnen de stichting is de penningmeester de beheerder van het Cloud systeem, en verzorgt derhalve de autorisaties m.b.t. de toegang van het systeem. Deze autorisaties zijn binnen het bestuur afgesproken. Alleen bestuursleden van de SDA hebben toegang tot het systeem, echter met autorisaties voor bepaalde mappen. Elke gebruiker (bestuurder) heeft een persoonlijke inlogcode die bestaat uit een gebruikersnaam en een wachtwoord. Als een bestuurder stopt met zijn/haar werkzaamheden wordt deze inlogcode uit het systeem verwijderd.

Artikel 1.4; Opslag AVG gegevens en beveiliging.

De AVG gegevens staan in een separate map in de Cloud omgeving. Alleen de Secretaris heeft als AVG beheerder volledige toegang m.b.t. het invoeren en verwijderen van de gegevens van leden. De gegevens worden door de AVG beheerder ingevoerd op basis van de persoonlijk verstrekte gegevens door belanghebbenden. De map is beveiligd met een wachtwoord. De AVG beheerder bewaart een kopie van de dataset als periodieke back-up op een lokale externe harde schijf

Artikel 1.5: Vernietiging gegevens.

Na uitschrijving als lid van de bestuursraad/ bestuur of na overlijden worden alle gegevens van het betreffende lid geanonimiseerd en na twee jaar automatisch uit het systeem verwijderd. Gegevens blijven 2 jaar bewaard i.v.m. de statistieken. Eist een persoon dat gegevens direct bij opzegging worden verwijderd dan zal dat als zodanig worden uitgevoerd.
De SDA kent een aantal vrijwilligers waarvan de persoonsgegevens door de ledenadministrateur in het ledensysteem worden bijgehouden. Van leden die stoppen als vrijwilliger worden de persoonsgegevens door de secretaris verwijderd nadat ze zijn bedankt voor hun inzet.

2. Overige bepalingen

Artikel 2.1; Documentatieplicht

Om te voldoen aan de documentatieplicht heeft de SDA middels dit protocol de procedure vastgelegd m.b.t. het beheren van de privacygevoelige gegevens van de bij haar ingeschreven leden.

Artikel 2.2; Informeren leden

Leden dienen te worden geïnformeerd dat de SDA werkt volgens de AVG-regels. Dit dient te geschieden tijdens de ALV (Algemene Ledenvergadering).

Artikel 2.3; Training

Bestuursleden worden getraind in het verwerken van privacy gevoelige persoonsgegevens middels een korte training tijdens de bestuursvergadering. Tevens ontvangt elk bestuurslid een exemplaar van dit protocol.

Artikel 2.4; IT-zaken

Elk bestuurslid dient op zijn of haar computer te werken met de laatste update van het besturingssysteem. Tevens dient er op de computer een up-to-date viruskiller en firewall aanwezig te zijn. De gegevens zijn alleen online toegankelijk. Er mogen met uitzondering van de AVG-beheerder geen lokale kopieën worden aangemaakt.

Artikel 2.5; Website

Zonder toestemming van betrokkenen mag geen privacygevoelige informatie op de website van de SDA worden getoond, zoals persoonsgegevens, foto's of andere tot een persoon te herleiden informatie.

Artikel 2.6; Beeldmateriaal

Beeldmateriaal (foto's en video's) mogen alleen worden gemaakt met uitdrukkelijke toestemming van de betrokkenen. Voor het plaatsen van foto's en video's op de website moet eveneens uitdrukkelijk toestemming van de betrokkenen zijn.

Artikel 2.7; Datalekken

Datalekken (gehackte systemen) worden direct gemeld aan de bevoegde autoriteit(en). Op dit moment is dat het meldloket van de Autoriteit Persoonsgegevens.

Met betrekking tot datalekken zal er, zo als vastgelegd in de AVG-regels, mails worden geadresseerd volgens onderstaande methode, te weten:

Methode 1; Mail aan een persoon met kopie aan een derde persoon
In vakje **Aan** staat mailadres van geadresseerde, in vakje **BCC** het adres van hen die een kopie ontvangt. CC wordt niet meer gebruikt.

Methode 2; Mail aan meerdere personen.
In vakje **Aan** staat mailadres van verzender, in vakje **BCC** het adres van alle ontvangers. CC wordt niet meer gebruikt.

Methode 3; Mail aan een groep personen.
In vakje **Aan** staat mailadres van verzender, in vakje **BCC** het adres van alle ontvangers. CC wordt niet meer gebruikt.

Indien men van alle personen een antwoord verwacht, dan werkt dat niet met **BCC**. Men beantwoordt dan naar de verzender terwijl de verzender, indien noodzakelijk, de antwoorden mailt naar de andere personen.
Het is raadzaam om in het mailbericht te vermelden bij gebruik van **BCC** aan welke personen het bericht is verzonden. Bijvoorbeeld "dit mailbericht is verzonden aan alle voorzitters"
Indien er sprake is van een besloten groep c.q. kring kan gewoon **Aan** en **CC** worden gebruikt, mits de geadresseerden vooraf hiervoor toestemming hebben gegeven.

3. Rechten.

De AVG zorgt er tevens voor dat u verschillende rechten verkrijgt.

Artikel 3.1; het recht op informatie.
U heeft het recht om te weten wat er met uw persoonsgegevens gebeurt en waarom de gegevens worden opgeslagen.

Artikel 3.2; het recht op inzage.
U heeft het recht om de persoonsgegevens die van u zijn verzameld in te zien.

Artikel 3.3; het recht op rectificatie.
Mocht het voorkomen dat uw persoonsgegevens niet of niet meer kloppen dan kunt u opdracht geven de gegevens te corrigeren of aan te vullen wanneer deze incompleet zijn.

Artikel 3.4; het recht op verwijdering en het recht om vergeten te worden.
In bepaalde gevallen heeft u het recht om uw gegevens te laten verwijderen. Bijvoorbeeld als de gegevens niet langer nodig zijn of wanneer deze onrechtmatig zijn verkregen.

Artikel 3.5; het recht om vergeten te worden.
Wanneer uw gegevens openbaar zijn gemaakt heeft u het recht om de gegevens te laten wissen.

Artikel 3.6; het recht op beperking van de gegevensverwerking.
Wanneer de gegevens niet correct zijn weergegeven of op onrechtmatige wijze zijn verkregen kun u de geselecteerde gegevens voor gebruikers tijdelijk onbeschikbaar laten maken.

Artikel 3.6; het recht op verzet tegen de gegevensverwerking.
U kunt onder bepaalde omstandigheden bezwaar maken tegen de verdere verwerking van uw gegevens en het recht van verzet oproepen. De verwerking van de gegevens moet dan gestaakt worden.

Artikel 3.7; het recht op overdraagbaarheid.
Het recht op overdraagbaarheid van persoonsgegevens geeft u het recht om een kopie te krijgen van de persoonsgegevens die u heeft verstrekt.

Artikel 3.8; Het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.
Betrokkenen hebben het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking gebaseerd besluit.

Bestuursraadvergadering, 2 oktober 2019.