AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat FireChoir het AVG-programma geheel of gedeeltelijk heeft doorlopen. FireChoir verklaart hiermee dat de inspanningen zijn verricht zoals die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).

Indien niet alle programmaonderdelen zijn afgewerkt en de verklaring toch wordt aangevraagd, dan is geen volledige invulling gegeven aan de eisen van de wetgever. De Stichting AVG voor Verenigingen adviseert de openstaande punten alsnog zo snel mogelijk af te werken en in elk geval in het programma een aantekening te maken wanneer dit zal gebeuren.

In de hierna volgende verklaring staan alle onderdelen/stappen die FireChoir heeft doorlopen om te voldoen aan de AVG-wetgeving. Per onderdeel is duidelijk aangegeven welke gegevens en onderdelen van de wet van toepassing zijn en hoe daar aan voldaan is. Waar nodig is additionele informatie verstrekt ter verduidelijking van de situatie.

FireChoir begrijpt dat AVG-wetgeving continu van toepassing is en dat wij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft FireChoir kennis over de materie ontvangen die door de AVG wordt geraakt, en verklaart zelf naar eer en geweten aan de wet te voldoen. De onderdelen van de zelfverklaring door FireChoir zijn te vinden op de volgende pagina('s) van deze verklaring.

Aldus opgemaakt te Gorinchem,

d.d. 25-1-2019,

door Stichting AVG voor Verenigingen

gevestigd aan de Stephensonweg 14 te Gorinchem.

2.1 Inventarisatie persoonsgegevens.

Geef hieronder aan welke persoonsgegevens binnen jouw vereniging gebruikt worden.

Gewone persoonsgegevens

- [x] Naam/ voorletters/ tussenvoegsel
- [ ] Titels
- [x] Adres
- [x] Postcode
- [x] Plaats
- [ ] Provincie
- [x] Land
- [ ] Woonplaats
- [x] Telefoonnummer
- [ ] Faxnummer
- [x] E-mailadres
- [ ] Website
- [x] Geslacht
- [x] Geboortedatum
- [ ] Geboorteplaats
- [ ] Overlijdensdatum
- [ ] Burgerlijke staat
- [ ] LinkedIn
- [ ] Facebook
- [ ] Twitter
- [ ] Werkzaam bij organisatie
- [ ] Bankrekeningnummer
- [ ] Inloggegevens (gebruikersnaam/wachtwoord)
- [ ] Voertuig kentekenplaat
- [ ] Salarisgegevens Salarisgegevens worden niet gezien als bijzondere gegevens.

Andere gewone persoonsgegevens:

Bijzondere persoonsgegevens

- [ ] Etnische afkomst
- [ ] Politieke opvattingen of voorkeur
- [ ] Religieuze opvatting of overtuiging
- [ ] Lidmaatschap van een vakbond
- [ ] Genetische of biometrische gegevens met het oog op unieke identificatie
- [ ] Gegevens over gezondheid
- [ ] Gegevens over seksuele geaardheid
- [ ] Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen
- [ ] Paspoort kopie, waarop pasfoto zichtbaar is (zonder voorlegger gekopieerd)
- [ ] BSN-nummer Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Dit geldt bijvoorbeeld voor werkgevers, zorgverleners, zoals huisartsen, apotheken en zorgverzekeraars. Ook in het onderwijs en kinderopvang wordt het BSN gebruikt.

Toelichting bijzondere persoonsgegevens:

3.1 Inventarisatie doelbinding.

Welke persoonsgegevens verwerk je, met welk doel en heb je ze daar ook voor gekregen? Dat noemen we ‘doelbinding’. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen.
Voor de inventarisatie van de vormen van doelbinding binnen de verenigingen hebben wij onderstaand schema gemaakt. Voor doelbindingen die bij sommige verenigingen veel voorkomen, hebben wij het schema al ingevuld en die kun je dus zo aanvinken. (Voorbeeld: schoenmaat bij sportclubs). Komen er binnen je vereniging nog andere doelbindingen voor, dan kun je deze in de open vorm noteren bij 3.3.
LET OP: Het is verstandig om zo min mogelijk persoonsgegevens te hanteren. Vraag dus alleen de gegevens die je echt nodig hebt voor het goed functioneren van je vereniging.

(N = Naam, A = Adres, W = Woonplaats, T = Telefoon, E = e-mailadres)

☑ **Lidmaatschap**

Persoonsgegevens:	NAWTE + geboortedatum.
Grondslag:	Lidmaatschapsovereenkomst (papier of formulier op de website).
Verwerkingen:	Ledenadministratie, contributieheffing, informatieverstrekking en uitnodigingen voor bijeenkomsten.
Verwerkt door:	Afdeling ledenadministratie en afdeling communicatie.
Bewaartermijn:	Gedurende het lidmaatschap en daarna maximaal 7 jaar in de boekhouding.

Beschrijf hieronder kort uw situatie:

De enige informatie die leden moeten geven zijn hun naam en email adres, met als doel dat we met ze kunnen communiceren via een wekelijkse email en extra emails die nodig zijn voor belangrijke informatie en herinneringen. Een postadres en geboortedatum (dag en maand, niet het jaar) worden gevraagd, maar zijn niet verplicht, zodat we een kaartje via de post kunnen sturen (verjaardag, beterschap, medeleven) en om meerijden te helpen faciliteren als dat nodig is.

☑ **Digitale direct marketing (e-mail, facebook, LinkedIn, fax, SMS etc.)**

Persoonsgegevens:	NAWTE.
Grondslag:	Digitale toestemming vooraf, b.v. bij aanvragen van informatie of inschrijven voor een nieuwsbrief.
Verwerkingen:	Digitaal toesturen van (of benaderen over) informatie over de vereniging en/of producten/diensten.
Verwerkt door:	Afdeling marketing/communicatie.
Bewaartermijn:	Gedurende de periode dat men gezien wordt als prospect voor de vereniging of haar diensten/producten.

Beschrijf hieronder kort uw situatie:

Voor digitale marketing via email verzamelen we en slaan we alleen namen en email adressen op van diegenen die interesse hebben getoond om op de hoogte te worden gehouden over FireChoir concerten en toekomstige seizoenen. Zij kunnen zich ten allen tijde van deze lijst laten verwijderen. Er worden geen andere vormen van digitale marketing gebruikt.

4.1 Privacy policy vindbaar, verwijzing in documenten.

De privacy policy van de vereniging moet voor iedereen waarvan je persoonsgegevens verwerkt vindbaar zijn. Het eenvoudigste is om deze op de website van de vereniging te zetten en op elke pagina (onderaan) een link hier naar toe te leggen.

- [x] Wij als vereniging hebben onze privacy policy zichtbaar gemaakt op de website van de vereniging.
- [ ] Wij als vereniging hebben onze privacy policy niet vindbaar gemaakt op de website van de vereniging.

Beschrijf hieronder kort uw situatie:

In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy policy.

- [x] Wij als vereniging verwijzen in al onze documenten waarin persoonsgegevens staan (lidmaatschap overeenkomst, aanmeldingsformulier, etc.) naar onze privacy policy op de website van de vereniging.
- [ ] Wij als vereniging verwijzen in documenten waarin persoonsgegevens staan (lidmaatschap overeenkomst, aanmeldingsformulier, etc.) niet naar onze privacy policy op de website van de vereniging.

5.1 Werken met verwerkersovereenkomst.

Als vereniging mag je persoonsgegevens niet doorgeven aan een andere partij welke ten behoeve van jou persoonsgegevens verwerkt zonder een verwerkersovereenkomst. In een verwerkersovereenkomst spreek je af wat de ander met de gegevens mag doen én ook vooral wat niet.

- [x] Wij als vereniging verklaren dat wij nooit persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten als dit noodzakelijk is voor uitvoering van de doeleinden waarvoor we ze hebben gekregen.
- [ ] Wij als vereniging verklaren dat wij ook persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten.
- [ ] Wij als vereniging verklaren dat wij geen persoonsgegevens doorgeven aan andere partijen.

Beschrijf hieronder kort uw situatie:

We gebruiken Mailchimp.com om digitale nieuwsbrieven te sturen en zij voldoen aan onze privacy regels. Zij hebben alleen namen en email adressen ter beschikking.

6.1 Toegangsbeveiliging.

Om zeker te weten dat alleen geautoriseerde personen de persoonsgegevens kunnen inzien en bewerken, moeten deze altijd beveiligd zijn met een wachtwoord en als het kan ook met een gebruikersnaam. Zo kun je een Excel-bestand beveiligen met een wachtwoord en een PC voorzien van een gebruikersnaam en een wachtwoord. Zorg er dus voor dat je altijd minimaal één keer een wachtwoord moet weten voordat je de persoonsgegevens van jouw vereniging kunt inzien of bewerken.

- [x] Wij als vereniging hebben persoonsgegevens altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- [ ] Wij als vereniging hebben persoonsgegevens niet altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- [ ] Wij als vereniging hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen toegangsbeveiliging.

7.1 Software en antivirussoftware up-to-date.

Om systemen zo veilig mogelijk te laten zijn, moet je ze up-to-date houden. Dit doe je door het aanzetten van het automatisch ophalen en installeren van updates van de software. Zorg ook voor goede antivirussoftware. Zorg ervoor dat alle software ingesteld is op het automatisch ophalen en uitvoeren van updates. Maak goede afspraken met al je softwareleveranciers.

- [x] Wij als vereniging hebben de persoonsgegevens alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.

- [ ] Wij als vereniging hebben de persoonsgegevens niet alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.

- [ ] Wij als vereniging hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen software updates.

8.1 Opslaan alleen binnen de EU.

Binnen de EU is het niveau van gegevensbescherming gelijk. Dat komt omdat alle EU-lidstaten moeten voldoen aan de AVG. Als je persoonsgegevens verwerkt buiten de EU, bijvoorbeeld door deze te laten verwerken door een partij buiten de EU of een internationale vereniging, moet je kijken of er een passend beschermingsniveau bestaat voor dat land , bijvoorbeeld door een adequaatheidbesluit van de Europese Commissie. Je moet ook weten en kunnen aantonen dat er passende of geschikte waarborgen zijn, en hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

De wetgever is dus extra streng als je persoonsgegevens wilt verwerken/opslaan buiten de EU. Als je dat toch zou willen, dan moet er heel veel geregeld worden bovenop de normale AVG-verplichtingen. Dus check of je dienstverlener (drukker, verspreider, enz.) de toevertrouwde persoonsgegevens binnen de EU opslaat.

Het is dus het makkelijkste om persoonsgegevens alleen te verwerken binnen de EU, dit raden wij daarom ook sterk aan.

- [ ] Wij als vereniging verklaren dat wij nooit persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.

- [x] Wij als vereniging verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.

Beschrijf hieronder kort uw situatie:

We bewaren persoonlijke gegevens in the cloud met gebruikmaking van OneDrive, dus dat kan zowel binnen als buiten de EU zijn. We hebben wel alle bestanden in de cloud voorzien van een gebruikersnaam en wachtwoord.

9.1 Data back-up.

Om de persoonsgegevens te beschermen tegen het verlies of diefstal moet je back-ups maken. Het is noodzakelijk om dat regelmatig te doen. Zorg ervoor dat deze back-up veilig wordt opgeborgen.

- [x] Wij als vereniging hebben de opgeslagen persoonsgegevens beveiligd met een back-up.

- [ ] Wij als vereniging hebben de persoonsgegevens niet beveiligd met een back-up.

- [ ] Wij als vereniging hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen back-up.

10.1 Geautoriseerde medewerkers.

Via autorisatie regel je wie binnen de vereniging welke persoonsgegevens mag verwerken.

- [x] In onze vereniging hebben alleen geautoriseerde personen toegang tot de persoonsgegevens van de vereniging.
- [ ] In onze vereniging hebben ook niet geautoriseerde personen toegang tot de persoonsgegevens van de vereniging.

11.1 Vernietigen persoonsgegevens.

Geef hieronder aan dat je vereniging alle persoonsgegevens vernietigt door bijvoorbeeld een regel te wissen in Excel en/of het versnipperen van een aanmeldingsformulier als er geen overeenkomst meer is. Persoonsgegevens mogen niet langer worden bewaard dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt. Dus: na beëindiging van een overeenkomst worden de persoonsgegevens van die persoon vernietigd.
Wijs aan wie verantwoordelijk is voor het vernietigen van persoonsgegevens of de controle op de vernietiging.

NB: Verscheuren en weggooien is onvoldoende. Schaf daarom een versnipperaar aan.

Let op: In de financiële administratie mogen (of eigenlijk: moeten!) deze persoonsgegevens nog wel blijven staan, want daar geldt een (wettelijke) bewaarplicht van 7 jaar.

- [x] Wij als vereniging verklaren dat wij alle persoonsgegevens vernietigen als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.
- [ ] Wij als vereniging verklaren dat wij geen persoonsgegevens vernietigen als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.

12.1 Toestemming voor direct marketing en bij minderjarigheid.

Bij direct marketing.

De wetgever maakt onderscheid tussen gewone direct marketing (bellen en post sturen) of digitale marketing (via e-mail, fax, Facebook, LinkedIn of sms). Doordat gewone direct marketing een organisatie geld kost zal dat altijd beperkt blijven. Juist digitale marketing is nagenoeg gratis en kan daardoor heel veel toegepast worden met alle gevolgen van dien.

- [x] Wij als vereniging vragen vooraf altijd toestemming voordat we iemand benaderen via digitale direct marketing.
- [ ] Wij als vereniging vragen vooraf geen toestemming voordat we iemand benaderen via digitale direct marketing.
- [ ] Wij als vereniging maken geen gebruik van digitale direct marketing.

Bij minderjarigheid (jonger dan 16 jaar).

Als je persoonsgegevens online verwerkt van personen jonger dan 16 jaar via bijvoorbeeld een app, online game, webwinkel of via sociale media, dan moet je daarvoor altijd schriftelijk een toestemming hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hieronder aan dat je vereniging dat ook altijd zo doet.

- [ ] Wij als vereniging verklaren dat wij alleen online persoonsgegevens van minderjarigen verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media als daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- [ ] Wij als vereniging verklaren dat wij persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media zonder dat daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- [x] Wij als vereniging verklaren dat wij geen persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media.

13.1 Papieren documenten en beveiliging.

Als persoonsgegevens ook vastliggen op papier (denk aan aanmeldingsformulieren), dan moeten die papieren met persoonsgegevens achter slot en grendel zijn opgeslagen. Praktisch: bewaar dus alle papieren met persoonsgegevens in een kast die je steeds op slot doet. Alleen personen die voor hun werk voor de vereniging daarvoor toestemming hebben, mogen in die kast komen.

- ○ Wij als vereniging hebben papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- ○ Wij als vereniging hebben niet alle papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- ⊘ Wij als vereniging hebben geen papieren documenten waarop de persoonsgegevens staan.

14.1 Datalekken.

Iedereen in de vereniging moet op de hoogte zijn wat een een datalek is en wat je eraan moet doen. Geef aan wat voor jullie van toepassing is:

- ⊘ Binnen onze vereniging is iedereen op de hoogte van wat een datalek is. Ook is bekend waar dit intern gemeld moet worden zodat wij als vereniging adequaat het datalek kunnen afhandelen en documenteren.
- ○ Binnen onze vereniging is niet iedereen op de hoogte van wat een datalek is. Ook is niet bekend waar dit intern gemeld moet worden zodat wij als vereniging adequaat het datalek kunnen afhandelen en documenteren.

15.1 Medewerkers geïnstrueerd

Wij hebben onze medewerkers als volgt geïnstrueerd:

- ☐ Alle medewerkers hebben de video van de Stichting AVG bekeken.
- ☑ We hebben het onderwerp privacy bescherming in alle afdelingsoverleggen besproken.
- ☐ We hebben uitlegposters opgehangen.
- ☐ We hebben alle medewerkers een brief gestuurd met uitleg en instructie.
- ☐ We hebben met alle medewerkers een workshop over privacy bescherming gevolgd.
- ☐ We hebben een nieuwsbrief voor alle medewerkers waarin we regelmatig aandacht besteden aan privacy bescherming.
- ☐ Onze directeur/voorzitter heeft alle medewerkers opgeroepen extra aandacht te besteden aan privacy bescherming.

16.3 Ondertekening.

Met het inzenden van dit stappenplan verklaar ik hierbij dat ik naar eer en geweten dit stappenplan heb ingevuld namens de vereniging.
Aldus verklaard door:

Naam vereniging:	Allegro Foundation Arts Network
Naam persoon:	Jackee Raught
Plaats:	Nieuw-Vennep
Datum:	25/1/2019

English Summary
Hereby, the AVG Foundation for Associations declares that FireChoir has completed the AVG program in whole or in part. FireChoir hereby declares that the efforts have been made as regards the General Data Protection Regulation (AVG). In the following statement are all components / steps that FireChoir has gone through to comply with the AVG legislation. It is clearly indicated for each component which data and parts of the law are applicable and how this has been fulfilled. Where necessary, additional information has been provided to clarify the situation. FireChoir understands that AVG legislation is continuously applicable and that we regularly have to check and update the data. With the complete AVG program from the AVG Foundation for Associations, FireChoir declares itself in compliance with the law in good conscience. The parts of the self-declaration by FireChoir can be found on the next page (s) of this declaration.

3.1 Inventory of Personal Data.
- **Membership personal data**: Name, address, telephone, email address, birthday.
- Basis: Membership agreement (paper or form on the website).
- Processed by: Department of member administration and communication department.
- Retention period: During the membership and after that a maximum of 7 years in the accounting.
- Comments: The only information our members are required to give is their name and email address for the purpose of communicating by way of a weekly email and additional emails as needed to share important information and reminders. Mailing address and birthday (day and month, not year) are requested but not required so we can send cards by mail (birthday, get well, sympathy) and to help facilitate ride sharing as needed.

- **Digital direct marketing personal data**: Name, email address.
- Basis: Digital permission beforehand, e.g. when requesting information or registering for a newsletter.
- Actions: Digital sending of (or contact about) information about the association.
- Processed by: Department of marketing/communication.
- Retention period: During the period that one is seen as a prospect for the association.
- For digital marketing via email we only collect and store names and email addresses from those who expressed an interest in being kept informed about FireChoir concerts and upcoming seasons. They can unsubscribe from this mailing list at any time. No other forms of direct digital marketing are used.

4.1 Privacy policy availability.
As an association we have made our privacy policy available on the website of the association. In all association documents which contain personal data (membership agreement, application form, etc.) we refer to our privacy policy on the website.

5.1 Working with outside data processors.
As an association that we never pass on personal data to other parties with whom we have not entered into a processing agreement if this is necessary for the execution of the purposes for which we received them. We use Mailchimp.com to send digital newsletters and they comply with privacy regulations. They only have names and email addresses.

6.1 Access security.
As an association, we always store personal data behind the security of at least one username and a password.

7.1 Software and antivirus software.
As an association we have stored the personal data only on computers / servers with security software where both the security software and the operating system are set up to automatically retrieve and install updates.

8.1 EU data storage.
As an association we may also transfer or store personal data with parties that are based outside the EU, namely OneDrive cloud. All files on the cloud are username and password protected.

9.1 Data backup.
As an association, we have secured the stored personal data with a backup.

10.1 Authorized employees.
Only authorized persons have access to the personal data of the association.

11.1 Destruction of personal data.
As an association we destroy all personal data if the agreement on the basis of which it is obtained has expired or the consent has been withdrawn.

12.1 Permission for direct marketing and minors.
Direct marketing: As an association, we always ask for permission before we contact someone via digital direct marketing.
In the case of minors (younger than 16 years): As an association, we do not have any personal data of minors.

13.1 Paper documents and security.
As an association we do not have paper documents on which personal data are stored.

14.1 Data breach.
In our association, everyone is aware of what a data breach is. It is also known where this needs to be internally reported so that we can adequately handle and document the data breach.

15.1 Employee training.
We have trained our employees as follows: We have discussed the subject of privacy protection in departmental meetings.