Privacyreglement Koor Feelin'Good te Huissen

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing voor alle organisaties die gegevens van personen (persoonsgegevens) in een bestand bewaren. Deze organisaties moeten zich aan de regels in deze nieuwe verordening houden. Dat geldt zowel voor het bewaren in digitale bestanden als in mappen op een plank. Ook deze laatste moeten voortaan veilig worden opgeborgen zonder dat vreemden daar bij kunnen.

Het volgende wordt bewaard:

1. De ledenadministratie ligt bij het bestuurslid met PR in portefeuille. Dit bestuurslid heeft de beschikking over de volgende gegevens: de naam, voornaam, adresgegevens, emailadres en telefoonnummer; de vermelding van de stemgroep. Deze gegevens worden door het nieuwe lid via het inschrijfformulier aangeleverd.
Doel: De mailadressen zijn van belang om leden direct te kunnen benaderen en de adresgegevens zijn van belang voor het sturen van een kaartje of bloemetje bij een festiviteit en/of ziekte; regelen van carpoolen t.b.v. optredens.
2. De voorzitter beschikt over een actuele namenlijst en NAW - gegevens van de leden en het emailadres. Ook beschikt de voorzitter over de NAW en emailgegevens van de dirigent.
Doel: Maandelijks toesturen van de Nieuwsbrief en het jaarlijks versturen van de agenda, vergaderstukken en verslagen van de Algemene Vergadering. De mails aan leden worden als BCC verstuurd. Het onderhouden van contact met de dirigent.
3. De penningmeester beschikt over een actuele namenlijst, NAW- gegevens, emailadres en Ibannummer. De penningmeester beschikt ook over de naam, emailadres en Ibannummer van de dirigent.
Doel: maandelijks innen van de contributie/incasso en de maandelijkse betaling te doen aan de dirigent.
4. De secretaris beschikt over de emailadressen van de bestuursleden.
Doel: om de agenda, de stukken en verslagen voor de Bestuursvergadering te mailen.
5. Het bestuurslid repertoire-/concertcommissie beschikt over de emailadressen van de bestuursleden en van de leden repertoire-/concertcommissie.
Doel: contact te onderhouden met de overige leden van bestuur en de leden van de commissie.
6. De coördinator barcommissie beschikt over een namenlijst met voor- en achternaam en telefoonnummer.
Doel: planning bardienst en bij wisseling van bardienst moet de coördinator contact kunnen opnemen met de leden.
7. De website moet een beveiligde website zijn. Er zal een SSL certificaat nodig zijn en/of moeten beschikken over een https://browser. De functioneel beheerder beschikt over een actuele namenlijst en emailadressen voor vermelding op de ledenlijst op de website.
Doel: Op de website staat op de ledenpagina vermeld wie er lid zijn met emailadres; dit is alleen toegankelijk met wachtwoord voor de leden. In het informatieve gedeelte staat het inschrijfformulier vermeld.

Voorwaarden:

- De leden moeten schriftelijk toestemming geven voor het opnemen en het gebruik van hun persoonsgegevens. Van belang is dat de leden moeten weten dat hun persoonsgegevens worden verwerkt en met welk doel. Ze hebben het recht hun gegevens in te zien en aan te laten passen.
- De leden moeten schriftelijk akkoord verklaren dat dat zij geen probleem hebben met het maken en het publiceren van foto's.
- De nieuwe leden moeten het inschrijfformulier ondertekenen, waarin is opgenomen dat zij geen probleem hebben met het maken en het publiceren van foto's. Daarnaast zullen zij moeten aangeven dat ze er geen probleem mee hebben dat zij vermeld staan op een ledenlijst met NAW-gegevens en emailadres en tevens Ibannummer. Deze gegevens zijn alleen beschikbaar voor de penningmeester, de PR-functionaris en de voorzitter; het Ibannummer alleen bij de penningmeester.
- De website moet beveiligd zijn.

Procedure melden van datalekken

Elke organisatie die persoonsgegevens opslaat, is verplicht datalekken te melden binnen 72 uur na ontdekking. Om dit zorgvuldig te doen is het handig hiervoor vooraf procedures af te spreken en vast te leggen. We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, een gestolen geprinte ledenlijst of cliëntgegevens. Andere voorbeelden zijn cyberaanvallen, verkeerd verzonden e-mail, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

• Een datalek wordt gemeld bij de voorzitter; bij afwezigheid bij de penningmeester;

• Binnen de vereniging moeten tevens de overige bestuursleden geïnformeerd worden;

• Het dagelijks bestuur checkt wat er gelekt is;

• Vervolgens wordt in kaart gebracht wat de gevolgen zijn voor de personen van wie de persoonsgegevens gelekt zijn; Welke gegevens nodig zijn voor de melding. De melding moet in ieder geval bestaan uit:

- de aard van de inbreuk;
- de instanties of persoon waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

• De voorzitter doet de melding bij de Autoriteit Persoonsgegevens.