Gegevensbeleid VU-Orkest

Dit document bevat een uitleg en verantwoording van het gegevensbeleid van het VU-Orkest geïnspireerd op het stappenplan van de Autoriteit Persoonsgegevens.

Informeren

Intern. De voorzitter van de vereniging ziet er op toe dat het gegevensbeleid wordt nageleefd. Er wordt precies bijgehouden (in het verwerkingsregister) wie er toegang heeft tot welke gegevens. In principe heeft alleen het bestuur toeging tot de persoonsgegevens. In enkele gevallen wordt hier vanaf geweken. De voorzitter ziet er ook dan op toe dat iedereen op de hoogte is van het gegevensbeleid en dat het wordt nageleefd. In het bijzonder wordt nieuwe bestuursleden gevraagd dit document zorgvuldig te bestuderen.

Extern. Een privacyverklaring wordt gepubliceerd op vu-orkest.l/privacy. Deze verklaring vat simpel samen welke gegevens er binnen het VU-Orkest verwerkt worden, welke rechten betrokkenen hebben en hoe betrokkenen een verzoek in kunnen dienen. Alle betrokkenen worden nadrukkelijk op deze verklaring gewezen. We onderscheiden verschillende groepen betrokkenen (zie hieronder) en zorgen dat het altijd voor iedereen duidelijk is bij welke groep betrokkenen horen.

Verwerking persoonsgegevens

Groepen. Het VU-Orkest verwerkt gewone persoonsgegevens van een aantal verschillende groepen. Namelijk van leden van het orkest, oud-leden, relaties (personen van wie we gegevens bewaren zoals projectleden, auditanten, invallers, dirigenten en repetitoren) en websitebezoekers. Alle details omtrent de verwerking (grondslag, duur, delen, etcetera) zijn gespecificeerd in ons verwerkingsregister. We streven ernaar geen gegevens van kinderen onder de 16 jaar te verwerken.

Verwerkingsregister. Het VU-Orkest heeft geen werknemers maar verzamelt wel structureel persoonsgegevens. De voorzitter van het VU-Orkest is verantwoordelijk voor het bijhouden van een verwerkingsregister[1] waarin alle details omtrent de verwerking van onze persoonsgegevens geregistreerd staan. Dit register wordt in elk geval bij elke overdracht van het voorzitterschap bijgewerkt.

[1] Het verwerkingsregister is opgesteld na zorgvuldig raadplegen van de richtlijnen van AP

‘privacy by design’ Het VU-orkest verzamelt niet meer gegevens dan strikt noodzakelijk. Verder houden we altijd rekening met ‘privacy by design’. Concreet betekent dit bijvoorbeeld dat geen persoonsgegevens verzamelen van bezoekers.

Interne audits

Minstens één keer per twee jaar, maar bij voorkeur jaarlijks, wordt er een interne audit uitgevoerd door een niet-bestuurslid (bij voorkeur een oud-voorzitter), bijgestaan door de huidige voorzitter op dat moment. Bij de audit wordt het volgende in elk geval gecontroleerd.

1. Bestandslocaties: zijn de locaties in het verwerkinsgerister actueel en volledig?
2. Wachtwoordbeleid: zijn alle wachtwoorden volgens het wachtwoordbeleid recent aangepast?
3. Actualiteit leden- en oud-ledenbestanden. Dit gebeurt d.m.v. een steekproef.
4. Website: is de software up-to-date; zijn er passende beveiligingsmaatregelen genomen?

Bij de eerste uitvoering van een interne audit wordt het gegevensbeleid helemaal nagelopen en wordt er een protocol voor de audit opgesteld. Dit protocol wordt opgenomen in dit document. Bevindingen en aanbevelingen die volgen uit de audit worden gerapporteerd en gearchiveerd.

Beveiligingsmaatregelen

Wachtwoorden Het VU-Orkest gebruikt lange gerandomiseerde wachtwoorden voor alle accounts. Deze wachtwoorden worden opgeslagen in één *passwordmanager* (LastPass). Het wachtwoordt waarmee ingelogd kan worden in LastPass is enkel bij de bestuursleden bekend en wordt minimaal een keer per jaar bijgewerkt. Het wachtwoord wordt nooit onversleuteld verzonden (bij digitaal overdragen wordt gebruik gemaakt van PrivNote). Het jaarlijks wijzigen van het wachtwoord wordt geregistreerd in het beveiligingslogboek.

Administratie
Vrijwel alle administratie wordt online bijgehouden, in Google Drive, op zo’n manier dat alleen de bestuurs-accounts er toegang toe hebben. Hierbij is de login procedure de belangrijkste beveiliging. Er wordt door de bestuursleden gebruik gemaakt van lange gerandomiseerde wachtwoorden en op elk account staat de two-factor authenticatie aan.

Om de kans zo klein mogelijk te maken dat anderen dan de bestuursleden toegang hebben tot onze Google Drive omgeving worden alle bestuursleden aangespoord om toereikende anti-virus software op hun computer te installeren en niet ingelogd te blijven op google-accounts. Mocht er een incident voordoen kan op afstand uitgelogd worden.

Bestanden die persoonsgegevens bevatten worden nooit met anderen gedeeld. In het bijzonder hebben eventuele persoonlijke accounts van de bestuursleden geen toegang tot de administratie. Tenminste jaarlijks worden de deelinstellingen gecontroleerd, en wordt waar nodig toegang ingetrokken.

Website
De website draait op Wordpress, een van de best beveiligde content-management systemen en is beveiligd met een beveiligingscertificaat. De website wordt onderhouden door de PR-chef. De PR-chef is het enige bestuurslid dat toegang heeft tot het beheerdersaccount en ziet erop toe dat Wordpress *up to date* blijft.

Loggen
De meeste verwerkingen zijn niet geautomatiseerd. Om die reden zou het bijhouden van een logboek van alle verwerkingen een onredelijke druk op de administratie leggen. In plaats daarvan worden alle wijzigingen (1) in de toegang tot en (2) in de vorm van de verwerking gelogd in het verwerkingsregister. Dus als iemand toegang krijgt tot bepaalde gegevens, of als gegevens op een andere plek worden opgeslagen, wordt dit geregistreerd. Handelingen die specifiek over beveiliging gaan (bijvoorbeeld het aanpassen van het LastPass wachtwoord) worden in het beveiligingslogboek geregistreerd.

Protocollen

Protocol verzoeken inzage privacy-rechten
Omdat het VU-Orkest maar een beperkte hoeveelheid persoonsgegevens verwerkt, worden verzoeken handmatig afgehandeld door de secretaris. Het protocol is in grote lijnen hetzelfde voor alle aanvragen.

1. **Aanvraag.** De aanvrager dient een schriftelijk verzoek in bij de secretaris via secretaris@vu-orkest.nl
2. **Vaststellen identiteit.** De secretaris stelt de identiteit van de aanvrager vast (bij twijfel kan de secretaris vragen om een kopie van een idententiteitsbewijst).
3. **Ontvangstbevestiging.** De secretaris stuurt de aanvrager een ontvangstbevestiging.
4. **Controle richtlijnen.** De secretaris controleert de richtlijnen van de Autoriteit Persoonsgegevens voor het afhandelen van verzoeken aangaande de rechten van betrokkenen.
5. **Afhandeling.** De secretaris stelt een antwoord op, afhankelijk van het verzoek. Tenzij de richtlijnen van de AP anders suggereren, komt dat hierop neer;
    a. ***Dataportabiliteit.*** De secretaris verzamelt alle digitale gegevens in een geschikt formaat, eventueel in overleg met de aanvrager.
    b. ***Inzage.*** De secretaris stelt een antwoord op met daarin;
        i. **Overzicht van de gegevens.** Een overzicht van de door de aanvrager opgevraagde gegevens.
        ii. **Uittreksel van het verwerkingsregister** met daarin: (1) waarom bepaalde gegevens verwerkt zijn en worden; (2) welke

persoonsgegevens we verzamelen; (3) de bewaartermijnen; (4, indien van toepassing) aan welke organisaties de persoonsgegevens zijn doorgegeven; (5, indien van toepassing) van welke organisaties we persoonsgegevens hebben ontvangen als we die niet zelf hebben verzameld; (6, indien van toepassing) op basis van welke logica we een geautomatiseerd besluit over iemand nemen.

iii. **Samenvatting rechten.** De aanvrager wordt erop gewezen dat hij/zij het recht heeft om persoonsgegevens te laten wijzigen, aanvullen of wissen, om te vragen om minder persoonsgegevens te verwerken en om bezwaar te maken tegen de verwerking van persoonsgegevens. Ook kan de aanvrager een klacht indienen bij de Autoriteit Persoonsgegevens.

c. **Rectificatie.** De secretaris past de gegevens aan en geeft wijzigingen indien nodig aan derde partijen die de gegevens ook verwerken.

d. **Vergetelheid.** De secretaris controleert of er een wettelijke plicht is om bepaalde gegevens te bewaren. Als dat niet zo is, draagt de secretaris er zorg voor dat alle gegevens van de aanvrager binnen één maand verwijderd worden, ook eventuele back-ups.

e. **Bezwaar.** De secretaris zorgt ervoor dat persoonsgegevens niet meer verwerkt worden.

f. **Recht op menselijke blik.** Indien er een geautomatiseerd besluit is genomen, wordt het besluit opnieuw voorgelegd aan het bestuur.

6. **Antwoord.** De secretaris zorgt dat de aanvraag binnen één maand is afgehandeld. Mocht dat niet haalbaar zijn dan wordt tijdig onderzocht of het mogelijk is om een verlenging te vragen, en wordt de aanvrager direct op de hoogte gesteld.

In onze privacyverklaring is uitgelegd hoe verzoeken kunnen worden ingediend. In principe kan dit per e-mail naar secretaris@vu-orkest.nl. Dit is (excessen daargelaten) kostenloos, en de secretaris reageert bij eenvoudige verzoeken (conform de wet) binnen één maand. De secretaris is op de hoogte van de bovenstaande procedure voor de afhandeling van verzoeken.

Protocol beveiligingsincidenten en datalekken

Alle beveiligingsincidenten en datalekken worden direct geregistreerd in het “Logboek beveiligingsincidenten en datalekken”. De verdere afhandeling volgt de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens. Kort samengevat komt het er op neer dat we het volgende stroomdiagram volgen:

1. “heeft zich een beveiligingsincident voorgedaan?” Denk aan het “kwijtraken van een usb-stick, de diefstal van een laptop of aan een inbraak door een hacker.”

   → Vastleggen in het logboek.

2. “Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?”

   → Ja: er is sprake van een datalek

   → bekijk het beleidsplan ‘beleidsregels meldplicht datalekken’

3. “Gaat het om persoonsgegevens van gevoelige aard, of is er om andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?”

   → Melden aan Autoriteit Persoonsgegevens

4. “Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?”

   → Mogelijk melden aan de betrokkene. Het bestuur dient hier direct een zorgvuldige afweging over te maken, mogelijk na het raadplegen van de Autoriteit Persoonsgegevens. Bij besluit tot melding is het bestuur verantwoordelijk voor een snelle, zorgvuldige melding van alle betrokkenen.

Protocol deelinstellingen controleren
De Google Drive omgeving van het VU-Orkest is gedeeld met 8 bestuursaccounts. Jaarlijks wordt er gecontroleerd of dit daadwerkelijk nog zo is en wordt van eventuele extra accounts de toegang ontzegd.

→ bij de eerste controle wordt een protocol opgezet.

Protocol beveiliging bij bestuurswissel

1. Vraag vertrekkend bestuurslid om alle gegevens op de persoonlijke computer over te dragen aan het nieuwe bestuurslid en daarna te verwijderen.
2. Verander de wachtwoorden van alle google-accounts.
3. Verander het LastPass wachtwoord.
4. Verander alle overige belangrijke wachtwoorden (voorzitter).

→ bij de eerste bestuurswissel wordt dit protocol nagelopen en bijgewerkt.

Procedures

Nieuw lid

1. Lidmaatschapsformulier in laten vullen
2. Opnemen in ledenbestand: voornaam, achternaam, e-mailadres, telefoonnummer, studeert wel/niet aan de VU, instrumentgroep, soort lidmaatschap (vast/proef/project)
3. Lidmaatschapsformulier archiveren (incl. ondertekende privacy statement)

Van lid naar oud-lid

1. Kopiëren naar oud-ledenbestand: Voor- en achternaam, e-mailadres, telefoonnummer, instrumentgroep, datum in- en uitschrijving
2. Verwijderen uit ledenbestand
3. Communiceren naar betrokkene

Van bestuurslid naar lid

1. Actualiseren KvK
2. protocol bestuurswissel uitvoeren

Van bestuurslid naar oud-lid
Zie achtereenvolgens “van bestuurslid naar lid” en “van lid naar oud-lid”

Beëindiging relatie
1. relatie verwijderen uit relatiebestand

Aanmelding auditant via de website
1. binnenkomst ingevuld formulier via www.vu-orkest.nl/speelmee
2. auditant opnemen in relatiebestand: voor- en achternaam, e-mailadres, instrumentengroep en evt. het bericht
3. notificatie e-mail verwijderen
4. contact opnemen met de auditant

Binnenkomst inzage persoonsgegevens
1. Per e-mail: zie protocol ‘verzoeken inzage privacy-rechten’
2. Per telefoon, post of anders: antwoorden dat dit enkel via de mail kan en verwijzen naar secretaris@vu-orkest.nl

Kaart Reserveringen op naam via PR-chef
1. Reservering registreren in het kaartenbestand (drive)
2. Mail met reservering verwijderen
3. Kaartenbestand na afloop van het concert verwijderen

Verzameling adresgegevens Maten voor ansichtkaarten (donateurs)
1. Opnemen in adresbestand Maten
2. Mail met gegevens verwijderen
3. Adresbestand verwijderen na afloop tournee

Overige verantwoording

Functionaris voor de gegevensbescherming (FG)
Het VU-Orkest heeft geen FG aangezien we daartoe niet verplicht zijn: (1) we zijn geen publieke organisatie of overheidsinstantie; (2) we verwerken geen persoonsgegevens op grote schaal en (3) we verwerken geen bijzondere persoonsgegevens.

Het VU-Orkest heeft ook geen vrijwillige FG, aangezien van een FG bovengemiddelde vakkennis van privacywetgeving en gegevensbescherming wordt verwacht. We kunnen er niet van op aan dat er altijd een dergelijk persoon lid is van de vereniging en beschikken niet over de financiële middelen om een externe FG aan te stellen.

De voorzitter van het VU-orkest functioneert als informele FG, dat wil zeggen, is belast met het toezien op het naleven van ons beleid (conform de AVG) voor gegevensbescherming, maar is niet geregistreerd als FG bij de AP.

Data protection impact assessment (DPIA)
Het VU-Orkest heeft geen DPIA uitgevoerd, aangezien dit onredelijk zwaar op de begroting zou drukken en, belangrijker, omdat er geen gegevens met hoog privacyrisico verwerkt worden. In het bijzonder vindt er geen systematisch en uitvoerige evaluatie van persoonlijke aspecten plaats; worden er geen geautomatiseerde beslissingen genomen; worden er geen bijzondere persoonsgegevens verwerkt (laat staan op grote schaal); volgen we geen mensen in publiek toegankelijk gebied; verwerken we geen gegevens van kwetsbare personen en gebruiken we alleen standaard technologieën.

Pseudonimiseren of anonimiseren
Het VU-Orkest pseudonimiseert of anonimiseert persoonsgegevens niet, omdat dit onwerkbaar zou worden. Vrijwel alle gegevens die binnen het orkest verzameld worden zijn ten slotte contactgegevens. Als het echter wel mogelijk is om gegevens geanonimiseerd te verwerken (zoals bij aantallen concertbezoekers), heeft dat vanzelfsprekend de voorkeur.

Tot slot: ***wijzigingen in het gegevensbeleid.*** *We staan vrij ons gegevensbeleid te wijzigen mochten wij dat nodig achten. We stellen u alleen op de hoogte van wijzigingen indien deze direct op u van toepassing zijn. Als wij bijvoorbeeld onze ledenadministratie wijzigen stellen wij daar een solist niet van op de hoogte.*
Versie 1.0, vastgelegd 21 oktober 2018