Vereinbarung über die Auftragsverarbeitung

gemäß Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

_____

_____

— nachstehend »Auftraggeber« oder »Verantwortlicher« —

und

Chorilo — Melanie Schneider
Tränkstraße 3, 65558 Holzheim
— nachstehend »Auftragsverarbeiter« — gemeinsam die »Parteien« —

§ 1 Gegenstand und Dauer des Auftrags

(1) Vertragsbestandteil ist die Nutzung der unter chorilo.com angebotenen Software als Software as a Service (im Folgenden »Software« genannt).

(2) Diese Auftragsverarbeitungsvereinbarung (»AVV«) ergänzt den zwischen den Parteien geschlossenen Leistungsvertrag auf Basis der aktuell geltenden AGB des Auftragsverarbeiters (nachstehend »Hauptvertrag« genannt). Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer sowie Art und Zweck der Verarbeitung.

(3) Die Laufzeit dieser AVV entspricht der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags beendet zugleich diese AVV. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen sind in **Anlage 1** beschrieben.

(2) Die Verarbeitung findet grundsätzlich in der Bundesrepublik Deutschland bzw. in einem Mitgliedstaat der Europäischen Union statt. Übermittlungen in Drittländer erfolgen nur unter den Voraussetzungen des § 8 dieser Vereinbarung.

§ 3 Rechte und Pflichten des Auftraggebers, Weisungsrecht

(1) Der Auftraggeber stellt die Daten dem Auftragsverarbeiter über die von diesem eingesetzte Software durch Eingabe über Formulare bzw. Uploads oder telefonisch oder per E-Mail zur Verfügung bzw. ermöglicht die Verarbeitung der Daten durch den Auftragsverarbeiter. Sämtliche Daten werden über eine transportverschlüsselte Verbindung (TLS) in die Software des Auftragsverarbeiters übertragen.

(2) Der Auftraggeber bleibt als »Verantwortlicher« i. S. d. Art. 4 Nr. 7 DSGVO Herr der Daten. Er ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er ist außerdem verantwortlich für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen.

(3) Die Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragsverarbeiters mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

(4) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag und diese AVV festgelegt und können vom Auftraggeber danach in Schriftform oder in Textform (E-Mail) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

(5) Weisungen sind an Chorilo — Melanie Schneider, Tränkstraße 3, 65558 Holzheim oder per E-Mail an datenschutz@chorilo.com zu richten. Mündlich erteilte Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt (Art. 28 Abs. 3 UAbs. 2 DSGVO). Er ist berechtigt, die Ausführung der betreffenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(4) Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses umgesetzten Maßnahmen sind in **Anlage 2** beschrieben. Der Auftragsverarbeiter darf diese Maßnahmen an den Stand der Technik anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

(5) Der Auftragsverarbeiter unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (Kapitel III DSGVO) nachzukommen (Art. 28 Abs. 3 lit. e DSGVO). Die Software stellt hierfür Selbstbedienungsfunktionen

bereit (u. a. Auskunft/Datenexport und Löschung durch die betroffene Person bzw. durch den Auftraggeber).

(6) Der Auftragsverarbeiter unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) (Art. 28 Abs. 3 lit. f DSGVO).

(7) Der Auftragsverarbeiter stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht und unterstützt Überprüfungen nach Maßgabe des § 9 (Art. 28 Abs. 3 lit. h DSGVO).

(8) Der Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gemäß Art. 30 Abs. 2 DSGVO.

(9) Ein Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzlichen Voraussetzungen für eine Bestellungspflicht (§ 38 BDSG, Art. 37 DSGVO) nicht vorliegen. Ansprechpartner in Datenschutzfragen ist die unter § 3 Abs. 5 genannte Stelle.

§ 5 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft, unverzüglich nach Bekanntwerden, damit der Auftraggeber seine Meldepflicht nach Art. 33 DSGVO (72-Stunden-Frist) erfüllen kann.

(2) Die Meldung enthält, soweit bereits bekannt, mindestens die in Art. 33 Abs. 3 DSGVO genannten Angaben. Noch nicht verfügbare Informationen werden unverzüglich nachgereicht.

(3) Der Auftragsverarbeiter dokumentiert Datenschutzvorfälle einschließlich der ergriffenen Abhilfemaßnahmen und stellt diese Dokumentation dem Auftraggeber auf Anforderung zur Verfügung.

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt die allgemeine Genehmigung zur Einschaltung der in **Anlage 3** aufgeführten Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).

(2) Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern in Textform (z. B. E-Mail an die hinterlegte Administrator-Adresse). Der Auftraggeber kann der Änderung innerhalb von 30 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Bei berechtigtem Widerspruch und fehlender zumutbarer Alternative steht beiden Parteien ein Sonderkündigungsrecht für den Hauptvertrag zu.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auf, die in dieser AVV festgelegt sind (Art. 28 Abs. 4 DSGVO). Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

(4) Nicht als Unterauftragsverhältnisse gelten Nebenleistungen Dritter ohne konkreten Bezug zu den Auftraggeber-Daten (z. B. Telekommunikationsleistungen, Wartung ohne Datenzugriff, Reinigung,

Prüfung durch Wirtschaftsprüfer).

§ 7 Betroffenenrechte

(1) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter, soweit sich das Ersuchen erkennbar auf Daten des Auftraggebers bezieht. Der Auftragsverarbeiter beantwortet solche Ersuchen nicht selbst, sofern der Auftraggeber ihn hierzu nicht angewiesen hat.

(2) Auskunft, Berichtigung, Löschung und Datenübertragbarkeit setzt der Auftraggeber vorrangig selbst über die Funktionen der Software um. Soweit dies nicht möglich ist, unterstützt der Auftragsverarbeiter gemäß § 4 Abs. 5.

§ 8 Verarbeitung in Drittländern

(1) Die Software wird ausschließlich in Deutschland gehostet (siehe Anlage 3). Eine Verarbeitung in Drittländern findet nur über die in Anlage 3 gekennzeichneten Unterauftragsverarbeiter statt.

(2) Soweit Unterauftragsverarbeiter personenbezogene Daten in einem Drittland verarbeiten, stellt der Auftragsverarbeiter sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (Angemessenheitsbeschluss — insbesondere EU-U.S. Data Privacy Framework — oder Standardvertragsklauseln der EU-Kommission nebst erforderlicher zusätzlicher Maßnahmen).

§ 9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung dieser AVV zu überprüfen. Der Auftragsverarbeiter erbringt den Nachweis vorrangig durch geeignete Unterlagen (Selbstauskünfte, Dokumentation der technischen und organisatorischen Maßnahmen, ggf. Zertifizierungen oder Prüfberichte).

(2) Genügen diese Nachweise im Einzelfall nicht, kann der Auftraggeber nach rechtzeitiger Anmeldung mit einer Frist von mindestens 14 Tagen zu den üblichen Geschäftszeiten eine Überprüfung durchführen oder durch einen zur Verschwiegenheit verpflichteten, nicht im Wettbewerb stehenden Dritten durchführen lassen. Die Überprüfung erfolgt ohne Störung des Betriebsablaufs.

§ 10 Löschung und Rückgabe nach Auftragsende

(1) Der Auftraggeber kann personenbezogene Daten jederzeit selbständig über die Funktionen der Software löschen oder exportieren (Selbstbedienung).

(2) Der Ablauf oder die Kündigung eines kostenpflichtigen Abonnements beendet den Hauptvertrag nicht. Das Nutzungskonto und die darin gespeicherten Daten bleiben bestehen, damit der Auftraggeber die Nutzung später fortsetzen kann. Der Hauptvertrag endet erst durch Löschung des Kontos bzw. des Ensembles durch den Auftraggeber oder durch Kündigung des Nutzungsverhältnisses.

(3) Nach Beendigung des Hauptvertrags im Sinne des Absatzes 2 bewahrt der Auftragsverarbeiter die personenbezogenen Daten des Auftraggebers entsprechend dem Hauptvertrag für 90 Tage auf, um eine Wiederherstellung bei versehentlicher Kündigung zu ermöglichen. Nach Ablauf dieser Frist werden alle personenbezogenen Daten unwiderruflich gelöscht, sofern der Auftraggeber nicht zuvor

deren Rückgabe (Datenexport über die Software) verlangt hat. Auf Weisung des Auftraggebers erfolgt die Löschung früher.

(4) Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters (z. B. handels- und steuerrechtliche Aufbewahrung von Rechnungsdaten) bleiben unberührt; betroffene Daten werden für die Dauer der Aufbewahrungspflicht gesperrt und anschließend gelöscht.

(5) Die Löschung wird dem Auftraggeber auf Verlangen bestätigt.

§ 11 Haftung

Für die Haftung der Parteien gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser AVV bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Bestimmungen dieser AVV unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag gehen die Regelungen dieser AVV in datenschutzrechtlicher Hinsicht vor.

Holzheim, 07.07.2026

Ort, Datum, Unterschrift — Auftraggeber	Ort, Datum, Unterschrift — Auftragsverarbeiter Chorilo — Melanie Schneider

Anlage 1 — Gegenstand der Verarbeitung, Datenkategorien, betroffene Personen

Gegenstand und Zweck: Bereitstellung einer Software zur Verwaltung von Chören und Ensembles (Mitgliederverwaltung, Terminplanung mit Zu-/Absagen, Kommunikation und Mitteilungen, Notenverwaltung, Kassenbuch/Beitragsverwaltung, Dateiablage).

Kategorien personenbezogener Daten (insbesondere):

- Stammdaten der Mitglieder (Name, Anschrift, Geburtsdatum, Stimmgruppe)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer)
- Mitgliedschafts- und Funktionsdaten (Rollen, Berechtigungen, Ein-/Austritt)
- Termin- und Anwesenheitsdaten (Zu-/Absagen, Teilnahme)
- Kommunikationsdaten (Mitteilungen, Kommentare, Chat-Nachrichten)
- Dateien und Fotos, soweit vom Auftraggeber oder den Mitgliedern hochgeladen
- Finanzdaten im Rahmen von Kassenbuch und Beitragsverwaltung (Beiträge, Zahlungsstatus, bei Nutzung der Bankanbindung: Kontoumsätze)
- Nutzungs- und Protokolldaten (Login-Daten, technische Protokolle)

Kategorien betroffener Personen:

- Mitglieder der Ensembles des Auftraggebers
- Chorleitung, Verwaltungs- und Funktionspersonen des Auftraggebers
- Kontaktpersonen (z. B. externe Ansprechpartner im Adressbuch)
- Erziehungsberechtigte minderjähriger Mitglieder

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- **Vertraulichkeit:** Transportverschlüsselung TLS 1.3 für alle Verbindungen; Verschlüsselung gespeicherter Daten (AES-256); rollenbasiertes Berechtigungskonzept; Mehr-Faktor-Authentifizierung für administrative Zugriffe; zeitlich begrenzte, signierte Zugriffs-Links für Datei-Abrufe.
- **Integrität:** Tägliche Datenbank-Backups; Versionierung kritischer Datenbestände; manipulationssicheres, nur anfügbares Sicherheits-Protokoll für sicherheitsrelevante Ereignisse (Logins, Berechtigungsänderungen, Kontolöschungen).
- **Verfügbarkeit und Belastbarkeit:** Hosting in deutschem Rechenzentrum (Hetzner) mit Monitoring und Ausfall-Alarmierung; jährliche Wiederherstellungstests; Lasttests vor größeren Releases.
- **Datenminimierung:** Entfernung von Metadaten (EXIF) aus hochgeladenen Bildern; keine Drittanbieter-Tracker; erste-Partei-Telemetrie ohne IP-Speicherung.
- **Verfahren zur regelmäßigen Überprüfung:** Automatisierte Datenschutz-Tests in der Entwicklungs-Pipeline; dokumentierter Prozess für Datenschutzvorfälle mit 72-Stunden-Überwachung.
- **Betroffenenrechte:** Datenexport und Kontolöschung als Selbstbedienungsfunktion.

Anlage 3 — Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Sitz	Leistung	Drittland-Garantie
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Deutschland	Hosting, Datenbank, Dateispeicher	— (Verarbeitung in DE)
Google LLC	USA	Push-Benachrichtigungen (Android und iOS, Firebase Cloud Messaging)	EU-U.S. Data Privacy Framework
Stripe Payments Europe, Ltd.	Irland	Zahlungsabwicklung	Standardvertragsklauseln (konzernintern USA)
BANKSapi Technology GmbH, Pettenkoferstr. 35, 80336 München	Deutschland	Bankanbindung Kassenbuch (nur bei Nutzung)	—
STRATO AG, Otto-Ostrowski-Straße 7, 10249 Berlin	Deutschland	Betrieb des Support-E-Mail-Postfachs	—

System-E-Mails werden über einen eigenen, in Deutschland betriebenen Mailserver des Auftragsverarbeiters versendet (kein externer E-Mail-Dienstleister).