Auftragsverarbeitungsvertrag

gemäß Art. 28 Abs. 3 DSGVO · Stand: Oktober 2026 · Version 1.4

> Dieser AVV gilt automatisch mit Abschluss eines Nutzungsvertrags für DJCockpit und bedarf keiner gesonderten Unterzeichnung. Die elektronische Akzeptanz bei der Registrierung erfüllt die Schriftformpflicht gemäß Art. 28 Abs. 9 DSGVO.

Parteien

Auftragsverarbeiter (Anbieter)

Thomas Stroh – DJCockpit
Lankenstraße 3, 52428 Jülich
E-Mail: info@djcockpit.de

Auftraggeber (Nutzer)

Der im Rahmen der Registrierung auf djcockpit.de angegebene Nutzer. Die konkreten Daten ergeben sich aus dem Nutzerkonto.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung der SaaS-Plattform DJCockpit für den Auftraggeber. Der Auftraggeber nutzt DJCockpit zur Verwaltung seiner eigenen Kunden, Buchungen und Veranstaltungen und speichert dabei personenbezogene Daten Dritter in der Plattform.

(2) Dauer

Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Nutzungsvertrags gemäß den AGB von DJCockpit.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art der Verarbeitung

Erhebung, Speicherung, Übermittlung, Abruf, Verwendung, Abgleich, Löschung und Vernichtung personenbezogener Daten im Rahmen des Betriebs der Plattform.

(2) Zweck

Bereitstellung der vertragsgegenständlichen SaaS-Funktionen: Kundenverwaltung, Buchungsverwaltung, Rechnungserstellung, Musikwunsch-System, Buchhaltungsmodul und zugehörige Funktionen.

(3) Kategorien personenbezogener Daten

Stammdaten: Name, Anschrift, Geburtsdatum
Kontaktdaten: E-Mail-Adresse, Telefonnummer
Vertragsdaten: Buchungsdetails, Veranstaltungsinformationen, Rechnungsbeträge
Kommunikationsdaten: E-Mails mit den Kunden des Auftraggebers (Mailverlauf je Event), Nachrichten im Kundenbereich, Musikwünsche
Bilddaten: Fotos, die Gäste über die Fotowall hochladen
Technische Daten: IP-Adressen, Browser-Informationen (Zugriffslogs)

(4) Kategorien betroffener Personen

Kunden des Auftraggebers (Veranstaltungsauftraggeber, Hochzeitspaare, Firmen etc.)
Gäste von Veranstaltungen des Auftraggebers (Musikwünsche, Fotowall)
Sonstige Dritte, deren Daten der Auftraggeber in der Plattform erfasst

§ 3 Pflichten des Auftragsverarbeiters

(1) Weisungsbindung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die Nutzung der Plattform durch den Auftraggeber gilt als Weisung. Der Auftragsverarbeiter nutzt die Daten nicht für eigene Zwecke.

(2) Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle Personen mit Zugang zu den Daten zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen (TOM) zum Schutz der verarbeiteten Daten. Diese sind in Anhang 1 konkret beschrieben.

(4) Unterauftragsverarbeiter

Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter einzusetzen (Anhang 2). Der Auftraggeber erteilt die allgemeine Genehmigung hierfür. Über Änderungen wird der Auftraggeber mindestens 14 Tage im Voraus per E-Mail informiert und kann Einwände erheben.

(5) Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung von Betroffenenrechten gemäß Art. 15–22 DSGVO durch geeignete technische Maßnahmen.

(6) Meldung von Datenpannen

Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden, per E-Mail an die im Nutzerkonto hinterlegte Adresse.

(7) Löschung und Rückgabe

Der Auftraggeber kann die verarbeiteten Daten jederzeit während der Vertragslaufzeit über eine in der Anwendung bereitgestellte Exportfunktion selbst abrufen. Der Export erfolgt in einem gängigen, maschinenlesbaren Format und umfasst die Stamm-, Event- und Buchhaltungsdaten einschließlich des Schriftverkehrs je Event sowie die erzeugten Dokumente. Über diese Funktion erhält der Auftraggeber seine Daten zurück (Art. 28 Abs. 3 lit. g DSGVO); abweichend von

der dort geregelten Rückgabe nach Ende der Verarbeitung steht sie ihm jederzeit während der Vertragslaufzeit zur Verfügung. Fotos, die Kunden des Auftraggebers selbst in ihren Kundenbereich hochladen, sind Teil des Exports.

Musikwünsche und Fotos, die Gäste über die Plattform einreichen, sind nicht Gegenstand des Exports. Sie werden nur für die jeweilige Veranstaltung verarbeitet und gelöscht: Musikwünsche 30 Tage nach der Veranstaltung, Fotos 60 Tage nach der Veranstaltung; schaltet der Auftraggeber die Fotowall-Seite seines Kunden wieder frei, entsprechend später. Mit der Nutzung dieser Funktionen weist der Auftraggeber diese Löschung an.

Nach Beendigung des Nutzungsvertrags stellt der Auftragsverarbeiter dem Auftraggeber 30 Tage zur Verfügung, um Daten zu exportieren. Anschließend werden alle personenbezogenen Daten unwiderruflich gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(8) Nachweispflicht und Audit-Recht

Der Auftragsverarbeiter stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der DSGVO-Konformität zur Verfügung. Audits sind auf normale Geschäftszeiten mit angemessener Vorlaufzeit zu beschränken.

(9) Administrativer Zugriff

Im laufenden Betrieb findet kein Zugriff des Auftragsverarbeiters auf Inhaltsdaten des Auftraggebers statt. Die Anwendung selbst sieht keine Rolle vor, die mandantenübergreifend auf Kunden-, Event-, Angebots-, Vertrags-, Rechnungs- oder Umsatzdaten zugreifen kann: Die Zugriffsregeln der Datenbank binden jeden Lese- und Schreibvorgang an das Konto, dem die Daten gehören. Die Verwaltungsansicht des Auftragsverarbeiters zeigt ausschließlich Kontodaten (Name, E-Mail-Adresse, gebuchter Plan, Registrierungszeitpunkt).

Eine Ende-zu-Ende-Verschlüsselung besteht nicht, da Suche, Dokumentenerstellung und E-Mail-Versand eine serverseitige Verarbeitung im Klartext voraussetzen. Ein administrativer Zugriff über die Datenbankkonsole des Infrastrukturanbieters ist daher technisch möglich. Er erfolgt ausschließlich in den folgenden Fällen:

- zur Fehleranalyse auf ausdrückliche Anfrage oder mit Zustimmung des Auftraggebers
- zur Behebung einer konkreten Betriebsstörung, wenn eine Lösung ohne Zugriff nicht möglich ist
- zur Abwehr oder Aufklärung eines Sicherheitsvorfalls
- zur Erfüllung einer gesetzlichen Verpflichtung

Der Zugang zur Infrastruktur ist auf personengebundene Konten des Auftragsverarbeiters beschränkt und durch Zwei-Faktor-Authentifizierung gesichert. Administrative Vorgänge werden durch die Protokollierung des Infrastrukturanbieters erfasst. Auf Anfrage erteilt der Auftragsverarbeiter dem Auftraggeber nach Absatz 8 Auskunft darüber, ob und aus welchem Anlass ein Zugriff auf dessen Daten stattgefunden hat.

> **Klarstellung zur Branchenüberschneidung:** Der Auftragsverarbeiter ist selbst als DJ tätig. Er verpflichtet sich ausdrücklich, Daten des Auftraggebers weder unmittelbar noch mittelbar für diese eigene Tätigkeit zu verwenden — insbesondere nicht zur Ansprache oder Akquise von Kunden des Auftraggebers, nicht zur Auswertung von dessen Preisen, Gagen oder Umsätzen, nicht zur Erschließung von Veranstaltungsorten und nicht zur Markt- oder Wettbewerbsbeobachtung. Dies gilt auch für aggregierte oder anonymisierte Auswertungen, soweit sie Rückschlüsse auf einzelne Auftraggeber oder deren Kunden zulassen.

§ 4 Pflichten des Auftraggebers

Der Auftraggeber ist als Verantwortlicher für die Rechtmäßigkeit der Verarbeitung verantwortlich. Er ist insbesondere verpflichtet:

- Die Verarbeitung auf einer gültigen Rechtsgrundlage gemäß Art. 6 DSGVO zu stützen

Betroffene Personen gemäß Art. 13/14 DSGVO über die Verarbeitung zu informieren
Weisungen schriftlich oder elektronisch zu erteilen
Den Auftragsverarbeiter unverzüglich zu informieren, wenn er Fehler in der Verarbeitung feststellt

§ 5 Serverstandorte

Die in DJCockpit gespeicherten Inhaltsdaten — Kunden, Buchungen, Dokumente und Dateien — werden **ausschließlich auf Servern innerhalb der Europäischen Union** verarbeitet und gespeichert. Serverstandorte: Firebase (Google): Datenbank und Authentifizierung in Frankfurt am Main, Deutschland (europe-west3), Dateispeicher im Standort „EU“ (mehrere Rechenzentren innerhalb der Europäischen Union); Vercel: Frankfurt am Main, Deutschland (fra1).

Beim **Versand von E-Mails** und bei der **Zahlungsabwicklung** werden Daten an Dienstleister mit Sitz in den USA übermittelt (Anhang 2). Betroffen sind dabei die Empfängeradresse und der Inhalt der jeweiligen Nachricht beziehungsweise die zur Abrechnung erforderlichen Angaben — nicht der Datenbestand der Plattform. Grundlage sind die EU-Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO sowie, soweit der jeweilige Anbieter zertifiziert ist, das EU-US Data Privacy Framework. Diese Absicherung gilt auch gegenüber möglichen behördlichen Zugriffen nach US-Recht (CLOUD Act).

§ 6 Haftung

Im Außenverhältnis haften Verantwortlicher und Auftragsverarbeiter gemäß Art. 82 DSGVO gesamtschuldnerisch gegenüber betroffenen Personen. Im Innenverhältnis trägt jede Partei die Haftung entsprechend ihrem Verschuldensanteil. Der Auftragsverarbeiter haftet dem Auftraggeber nur, soweit er nachweislich gegen diesen Vertrag verstoßen hat.

§ 7 Schlussbestimmungen

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Aachen. Salvatorische Klausel: Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anhang 1: Technische und organisatorische Maßnahmen (TOM)

Gemäß Art. 32 DSGVO eingesetzte Maßnahmen (Stand: Oktober 2026):

Maßnahmenkategorie	Konkrete Maßnahmen
Zutrittskontrolle	Keine physischen Serverräume beim Anbieter. Infrastruktur liegt bei Google Firebase und Vercel (ISO 27001-zertifizierte Rechenzentren in Frankfurt und innerhalb der EU). Physischer Zugang Dritter ausgeschlossen.
Zugangskontrolle	Passwortgeschützte Nutzerkonten, Firebase Authentication mit sicheren Token, Passwort-Hashing durch Firebase, Brute-Force-Schutz integriert.
Zugriffskontrolle	Multi-Tenant-Architektur: Jeder DJ-Nutzer hat ausschließlich Zugriff auf seine eigenen Daten. Firestore Security Rules verhindern Cross-Tenant-Zugriff technisch.

Maßnahmenkategorie	Konkrete Maßnahmen
Weitergabekontrolle	Datenübertragung ausschließlich über HTTPS/TLS-Verschlüsselung (TLS 1.2 oder höher). Keine unverschlüsselte Übertragung personenbezogener Daten.
Eingabekontrolle	Alle Datenbankoperationen über validierte API-Endpunkte. Firebase-Logs ermöglichen Nachvollziehbarkeit von Datenänderungen.
Verfügbarkeitskontrolle	Regelmäßige automatische Backups durch Firebase. Redundante Cloud-Infrastruktur. Monitoring über Vercel und Firebase Console.
Trennungsgebot	Strikte Datentrennung zwischen verschiedenen DJ-Nutzern durch Firestore-Datenbankstruktur (users/{uid}/...). Technisch erzwungene Isolation.
Verschlüsselung	Datenverschlüsselung at rest durch Firebase/Google. Verschlüsselung in transit über HTTPS/TLS. Passwort-Hashing mit sicheren Algorithmen.

Anhang 2: Liste der Unterauftragsverarbeiter

Eingesetzte Unterauftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO (Stand: Oktober 2026):

Anbieter	Zweck	Serverstandort	Rechtsgrundlage
Google LLC (Firebase)	Datenbank, Authentifizierung, Dateispeicherung, Cloud Functions	Datenbank Frankfurt (europe-west3), Dateien EU-weit	EU-Server; SCC + DPF
Vercel Inc.	Hosting, CDN, Serverless-Deployment	Frankfurt (fra1)	EU-Server; SCC + DPF
Resend Inc.	Transaktionaler E-Mail-Versand	USA	SCC 2021/914
Stripe Payments Europe Ltd.	Zahlungsabwicklung der Abonnements (Name, E-Mail, Rechnungsdaten des Auftraggebers)	Irland, Verarbeitung teilweise USA	SCC 2021/914; DPF
Spotify AB	Songsuche für Musikwünsche. Übermittelt werden Suchbegriffe, keine personenbezogenen Daten der Gäste	EU / USA	SCC 2021/914

Nicht als Unterauftragsverarbeiter aufgeführt sind Dienste, an die keine personenbezogenen Daten der vom Auftraggeber erfassten Personen übermittelt werden — etwa Abfragen von Ortsnamen zur Adressvervollständigung oder von

Musikmetadaten. Funktionen, die sich noch in Entwicklung befinden und ausschließlich vom Anbieter selbst genutzt werden, verarbeiten keine Daten von Auftraggebern und sind daher nicht Gegenstand dieses Vertrags. Werden sie allgemein freigeschaltet, wird diese Liste vorher entsprechend ergänzt und der Auftraggeber nach § 3 Abs. 4 informiert.
