Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, „DSGVO")

Präambel

Dieser Auftragsverarbeitungsvertrag („AVV", „Vereinbarung") konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Nutzung der Plattform **j.show** durch den Kunden. Er ist Bestandteil der zwischen den Parteien geschlossenen Nutzungsvereinbarung (Hauptvertrag, geregelt durch die Nutzungsbedingungen unter https://j.show/terms/de.html) und gilt für alle Verarbeitungen personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Erbringung der vertraglich vereinbarten Leistungen durchführt.

Soweit dieser AVV und der Hauptvertrag in Datenschutzfragen voneinander abweichen, gehen die Regelungen dieses AVV vor.

---

1. Parteien

Verantwortlicher (im Folgenden „Verantwortlicher", „Kunde" oder „Auftraggeber"):

> Der Kunde, der eine j.show-Plattform-Instanz (Künstler- oder Agentur-Plattform) betreibt und auf dieser personenbezogene Daten verarbeitet. Die konkreten Angaben (Name/Firma, Anschrift, vertretungsberechtigte Person, Subdomain der Plattform-Instanz) ergeben sich aus dem Hauptvertrag bzw. den Registrierungsdaten der jeweiligen Plattform-Instanz und sind in **Anlage 4** zu konkretisieren.

Auftragsverarbeiter (im Folgenden „Auftragsverarbeiter", „Betreiber" oder „wir"):

> Jonas Stricker
> Im Geigersberg 8
> 74348 Lauffen am Neckar
> Deutschland
> USt-IdNr.: DE288958387
> E-Mail: hello@j.show

— nachfolgend gemeinsam die „Parteien".

---

2. Gegenstand, Art und Zweck der Verarbeitung

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung der cloudbasierten Software-as-a-Service-Plattform j.show für professionelles Tour- und Show-Management. Der Leistungsumfang ergibt sich aus dem Hauptvertrag und den Nutzungsbedingungen.

(2) **Art der Verarbeitung:** Das Speichern, Auslesen, Organisieren, Verändern, Abfragen, Übermitteln, Verknüpfen, Einschränken und Löschen personenbezogener Daten im Rahmen des Betriebs der Plattform-Instanz, einschließlich Hosting, Datenbankhaltung, Versand transaktionaler E-Mails, Erzeugung von Dokumenten (z. B. Rechnungen, Verträge, Daysheets) sowie — soweit vom Verantwortlichen aktiviert oder genutzt — der in **Anlage 2** beschriebenen optionalen Funktionen (KI-Assistent „Kira", KI-Advancing-Assistent, elektronische Signaturen, Geokodierung/Kartendarstellung, Buchhaltungs-Export, Zahlungsabwicklung).

(3) **Zweck der Verarbeitung:** Ausschließlich die Erbringung der im Hauptvertrag vereinbarten Leistungen. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt. Der Auftragsverarbeiter nutzt die im Auftrag verarbeiteten personenbezogenen Daten insbesondere **nicht** zu Werbe-, Profiling- oder Trainingszwecken und gibt sie nicht an Dritte außerhalb der in **Anlage 3** genannten Subunternehmer weiter.

(4) **Ort der Verarbeitung:** Die primäre Speicherung und Verarbeitung erfolgt auf Servern in **Deutschland**. Bei Nutzung bestimmter optionaler Funktionen können Subunternehmer Daten in begrenztem Umfang außerhalb Deutschlands, einschließlich Drittländern, verarbeiten (siehe **Anlage 3** und **Ziffer 9**).

---

3. Dauer der Verarbeitung

(1) Dieser AVV gilt für die Laufzeit des Hauptvertrags. Er beginnt mit dessen Wirksamwerden und endet mit dessen Beendigung, jedoch nicht vor vollständiger Erfüllung der Pflichten aus **Ziffer 11** (Rückgabe und Löschung).

(2) Der Verantwortliche kann diesen AVV jederzeit ganz oder teilweise ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften oder gegen diesen Vertrag vorliegt, der Auftragsverarbeiter eine Weisung nicht ausführen kann oder will, oder der Auftragsverarbeiter den Zutritt einer Kontrolle rechtswidrig verweigert. Eine solche Kündigung dieses AVV kann die Fortführung des Hauptvertrags unmöglich machen.

---

4. Art der personenbezogenen Daten und Kategorien betroffener Personen

Die konkreten Datenarten und Betroffenenkategorien ergeben sich aus **Anlage 1**, die Bestandteil dieses Vertrags ist. Sie umfassen typischerweise Daten von Crew-Mitgliedern, Geschäftspartnern (Venues, Hotels, Promotern) und sonstigen vom Verantwortlichen erfassten Personen, einschließlich — je nach Nutzung durch den Verantwortlichen — **besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO** (insbesondere gesundheitsbezogene Angaben wie Allergien und Ernährungsanforderungen).

Der Verantwortliche bestimmt allein, welche personenbezogenen Daten er in die Plattform-Instanz einstellt. Er ist dafür verantwortlich, dass für jede von ihm veranlasste Verarbeitung — einschließlich der Eingabe von Daten Dritter und besonderer Datenkategorien — eine gültige Rechtsgrundlage besteht und etwaige erforderliche Einwilligungen der betroffenen Personen vorliegen.

---

5. Rechte und Pflichten des Verantwortlichen

(1) Der Verantwortliche ist im Rahmen dieses Auftrags die für die Verarbeitung der personenbezogenen Daten Verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DSGVO. Er ist allein verantwortlich für die Rechtmäßigkeit der Datenverarbeitung und für die Wahrung der Rechte der betroffenen Personen.

(2) Der Verantwortliche ist allein für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

(3) Der Verantwortliche erteilt alle Weisungen grundsätzlich in dokumentierter Form (Textform genügt; auch über die Konfigurationsmöglichkeiten der Plattform). Mündliche Weisungen sind unverzüglich in dokumentierter Form zu bestätigen.

(4) Der Verantwortliche benennt dem Auftragsverarbeiter die für Weisungen empfangs- und entscheidungsberechtigten Personen. Standardmäßig gilt der Administrator der jeweiligen Plattform-Instanz als weisungsberechtigt.

(5) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.

---

6. Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen werden anfänglich durch diesen Vertrag und die im Rahmen der Plattform-Nutzung getroffenen Einstellungen festgelegt und können vom Verantwortlichen in dokumentierter Form geändert, ergänzt oder ersetzt werden.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wird.

---

7. Vertraulichkeit

(1) Der Auftragsverarbeiter verpflichtet sich, bei der Verarbeitung Vertraulichkeit zu wahren (Art. 28 Abs. 3 lit. b DSGVO).

(2) Der Auftragsverarbeiter setzt zur Verarbeitung der Daten nur Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(3) Der Auftragsverarbeiter ist ein Einzelunternehmen. Soweit der Inhaber die Verarbeitung selbst durchführt, gilt die Vertraulichkeitsverpflichtung unmittelbar für ihn. Werden weitere Beschäftigte eingesetzt, werden diese vor Aufnahme der Tätigkeit auf das Datengeheimnis verpflichtet.

---

8. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen (TOM), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 28 Abs. 3 lit. c i. V. m. Art. 32 DSGVO).

(2) Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter ist berechtigt, alternative angemessene Maßnahmen umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

(3) Die in **Anlage 2** beschriebenen Maßnahmen beschreiben den Stand zum Zeitpunkt des Vertragsschlusses (Stand: siehe Datum am Ende dieses Dokuments).

---

9. Inanspruchnahme weiterer Auftragsverarbeiter (Subunternehmer)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die **allgemeine schriftliche Genehmigung** zur Inanspruchnahme der in **Anlage 3** aufgeführten weiteren Auftragsverarbeiter (Subunternehmer) für die dort beschriebenen Zwecke (Art. 28 Abs. 2 Satz 1 DSGVO). Mit Abschluss dieses Vertrags gelten die zum Zeitpunkt des Vertragsschlusses in **Anlage 3** genannten Subunternehmer als genehmigt.

(2) Beabsichtigt der Auftragsverarbeiter, einen weiteren Subunternehmer hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Verantwortlichen hierüber **vorab** in Textform (z. B. per E-Mail oder über eine auf der Plattform bzw. unter https://j.show veröffentlichte, datierte Subunternehmerliste). Der Verantwortliche kann einer beabsichtigten Änderung innerhalb von **14 Tagen** nach Zugang der Information aus wichtigem, datenschutzbezogenem Grund widersprechen (Art. 28 Abs. 2 Satz 2 DSGVO). Erfolgt kein Widerspruch innerhalb dieser Frist, gilt der Subunternehmer als genehmigt.

(3) Widerspricht der Verantwortliche aus wichtigem Grund und kann der Auftragsverarbeiter die Leistung ohne den betreffenden Subunternehmer nicht oder nur mit unzumutbarem Aufwand erbringen, sind beide Parteien berechtigt, den betroffenen Leistungsteil oder den Hauptvertrag mit angemessener Frist zu kündigen.

(4) Der Auftragsverarbeiter verpflichtet jeden Subunternehmer vertraglich auf datenschutzrechtliche Pflichten, die den in diesem AVV vereinbarten Pflichten im Wesentlichen entsprechen, insbesondere durch Abschluss einer Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Subunternehmers (Art. 28 Abs. 4 DSGVO).

(5) **Drittlandübermittlung:** Soweit Subunternehmer personenbezogene Daten in einem Drittland (insbesondere in den USA) verarbeiten, stellt der Auftragsverarbeiter sicher, dass eine zulässige Grundlage für die Übermittlung nach Kapitel V der DSGVO besteht, namentlich

- ein Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO), insbesondere die Zertifizierung des Empfängers unter dem **EU-US Data Privacy Framework**, soweit verfügbar, oder
- die von der Europäischen Kommission erlassenen **Standardvertragsklauseln** (Art. 46 Abs. 2 lit. c DSGVO) nebst gegebenenfalls erforderlicher ergänzender Maßnahmen.

(6) Subunternehmer, die ausschließlich der Wartung, Pflege oder vergleichbaren Nebenleistungen ohne wesentlichen Zugriff auf personenbezogene Daten dienen, gelten nicht als weitere Auftragsverarbeiter im Sinne dieser Ziffer; der Auftragsverarbeiter verpflichtet auch sie auf angemessene Vertraulichkeit.

---

10. Unterstützung des Verantwortlichen

(1) **Betroffenenrechte (Art. 28 Abs. 3 lit. e DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) nachzukommen. Soweit eine betroffene Person sich unmittelbar an den Auftragsverarbeiter wendet, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und erteilt selbst keine Auskunft, ohne vom Verantwortlichen dazu angewiesen worden zu sein. Der Verantwortliche kann betroffene Datenarten ganz überwiegend selbst über die Funktionen der Plattform einsehen, berichtigen, exportieren und löschen.

(2) **Sicherheit, Meldepflichten, Datenschutz-Folgenabschätzung (Art. 28 Abs. 3 lit. f i. V. m. Art. 32–36 DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten zur Sicherheit der Verarbeitung, zur Meldung von Verletzungen des Schutzes personenbezogener Daten, zur Benachrichtigung betroffener Personen sowie bei einer etwaigen Datenschutz-Folgenabschätzung und vorherigen Konsultation der Aufsichtsbehörde.

(3) **Meldung von Datenschutzverletzungen:** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, in der Regel **innerhalb von 48 Stunden**, nachdem ihm eine Verletzung des Schutzes der vom Verantwortlichen verarbeiteten personenbezogenen Daten bekannt geworden ist. Die Meldung enthält mindestens die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit dem Auftragsverarbeiter bekannt. Die Meldepflicht des Verantwortlichen gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) bleibt hiervon unberührt und liegt allein beim Verantwortlichen.

---

11. Rückgabe und Löschung nach Beendigung

(1) Nach Abschluss der Verarbeitungsleistungen löscht oder gibt der Auftragsverarbeiter — nach Wahl des Verantwortlichen — alle personenbezogenen Daten zurück (Art. 28 Abs. 3 lit. g DSGVO), sofern nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaats eine Verpflichtung zur Speicherung besteht.

(2) **Export vor Beendigung:** Der Verantwortliche hat die Möglichkeit, seine Daten vor Beendigung der Plattform-Instanz selbst über die Funktionen der Plattform zu exportieren. Es liegt in der Verantwortung des Verantwortlichen, einen solchen Export rechtzeitig vorzunehmen.

(3) **Löschfrist nach Lizenzablauf:** Wird das Abonnement (die Lizenz) einer Plattform-Instanz beendet oder gekündigt, bleiben die zugehörigen personenbezogenen Daten zunächst erhalten, damit die Plattform-Instanz innerhalb dieses Zeitraums jederzeit reaktiviert werden kann. Nach Ablauf eines (1) Jahres ab Lizenzablauf werden die Daten in den darauffolgenden Wochen gelöscht, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Der Verantwortliche kann die Plattform-Instanz ab dem Lizenzablauf jederzeit auch eine frühere Archivierung und/oder vollständige Löschung verlangen; in diesem Fall erfolgt die Löschung entsprechend früher.

(4) **Gesetzliche Aufbewahrungspflichten:** Rechnungs- und buchhaltungsrelevante Unterlagen werden für die gesetzlich vorgeschriebene Dauer aufbewahrt (insbesondere bis zu 10 Jahre gemäß § 147 AO, § 257 HGB) und nach Ablauf dieser Fristen gelöscht. Für diesen Zeitraum wird die Verarbeitung auf die Speicherung beschränkt.

(5) **Protokoll- und Funktionsdaten:** Protokolldaten der KI-Funktionen werden nach maximal 90 Tagen gelöscht. Authentifizierungsprotokolle (Login-Versuche) werden nach 30 Tagen automatisch gelöscht. Allgemeine Zugriffs-/Aktivitätsprotokolle werden zu Sicherungs- und Nachvollziehbarkeitszwecken aufbewahrt und in angemessenen Abständen bereinigt. Eingegangene Roh-E-Mails des KI-Advancing-Assistenten werden kurzfristig (in der Regel innerhalb einer Stunde nach Abschluss der Verarbeitung) gelöscht.

(6) **Backups:** In Sicherungskopien (Backups) enthaltene personenbezogene Daten werden im Rahmen des regulären Backup-Zyklus überschrieben und gelöscht. Bis dahin wird die Verarbeitung auf die Speicherung zu Zwecken der Datensicherung und Wiederherstellung beschränkt.

(7) Der Auftragsverarbeiter weist die Löschung auf Verlangen des Verantwortlichen in geeigneter Weise nach.

---

12. Nachweis- und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten und in diesem Vertrag vereinbarten Pflichten zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Auftragsverarbeiter ermöglicht und unterstützt Überprüfungen — einschließlich Inspektionen —, die vom Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden. Der Nachweis kann nach Wahl des Auftragsverarbeiters auch durch die Vorlage geeigneter, aktueller Zertifizierungen, Testate oder Berichte (z. B. von unabhängigen Stellen oder eines aktuellen Penetrationstests) geführt werden, soweit diese die Prüfungsmöglichkeit des Verantwortlichen nicht unangemessen einschränken.

(3) Vor-Ort-Kontrollen sind mit angemessener Vorankündigung (in der Regel mindestens **zwei Wochen** im Voraus), während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und unter Wahrung der Geheimhaltungspflichten gegenüber Dritten durchzuführen. Sie sind auf das erforderliche Maß zu beschränken und finden im Regelfall höchstens einmal jährlich statt, es sei denn, es besteht ein konkreter, datenschutzbezogener Anlass.

(4) Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Anweisung im Rahmen einer Kontrolle gegen Datenschutzvorschriften verstößt.

---

13. Haftung

(1) Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Innenverhältnis tragen die Parteien die Verantwortung nach Maßgabe ihres jeweiligen Verursachungsbeitrags.

(2) Der Verantwortliche stellt den Auftragsverarbeiter von Ansprüchen Dritter und betroffener Personen frei, die darauf beruhen, dass der Verantwortliche personenbezogene Daten ohne hinreichende Rechtsgrundlage oder entgegen den Bestimmungen der DSGVO in die Plattform eingestellt, verarbeitet oder den Auftragsverarbeiter zu einer rechtswidrigen Verarbeitung angewiesen hat, soweit den Auftragsverarbeiter kein eigenes Verschulden trifft.

(3) Die im Hauptvertrag (Nutzungsbedingungen) vereinbarten Haftungsbeschränkungen gelten auch für diesen AVV, soweit sie nicht zwingenden gesetzlichen Vorschriften — insbesondere Art. 82 DSGVO im Außenverhältnis gegenüber betroffenen Personen — entgegenstehen.

---

14. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags und seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem mit der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt.

(3) Im Falle von Widersprüchen zwischen diesem AVV und den Regelungen des Hauptvertrags gehen die Bestimmungen dieses AVV in datenschutzrechtlichen Fragen vor.

(4) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. Gerichtsstand ist Stuttgart, Deutschland, soweit dies nicht zwingendem Recht entgegensteht.

(5) Maßgeblich ist die deutsche Fassung dieses Vertrags. Übersetzungen dienen ausschließlich der Information.

Anlagen

Die folgenden Anlagen sind Bestandteil dieses Vertrags:

- **Anlage 1** — Gegenstand der Verarbeitung: Datenarten und Kategorien betroffener Personen
- **Anlage 2** — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)
- **Anlage 3** — Liste der genehmigten Subunternehmer (Subprozessoren)
- **Anlage 4** — Angaben zum Verantwortlichen und Unterzeichnung

---

Anlage 1 — Gegenstand der Verarbeitung

1.1 Kategorien betroffener Personen

Im Auftrag des Verantwortlichen werden personenbezogene Daten folgender Kategorien betroffener Personen verarbeitet:

- **Crew-Mitglieder** der Plattform-Instanz (Bandmitglieder, Techniker, Tourpersonal und sonstige eingeladene Nutzer)
- **Geschäftspartner und Ansprechpartner** (Kontaktpersonen von Venues, Hotels, Promotern, Agenturen, Dienstleistern, Partnern)
- **Gäste** (z. B. Personen auf Gästelisten)
- **Administratoren und sonstige Nutzer** der Plattform-Instanz
- **Absender von Anweisungen** an den KI-Advancing-Assistenten (soweit aktiviert)

1.2 Arten personenbezogener Daten

- **Stammdaten / Kontaktdaten:** Vor- und Nachname, E-Mail-Adresse, Telefonnummer, Wohnort/Anschrift, Sprache, Funktion/Rolle
- **Weitere Profildaten:** ggf. Geburtsdatum, Geschlecht/Pronomen, Profilbild (optional), Geräteinformationen
- **Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO):** gesundheitsbezogene Angaben wie Allergien und Ernährungsanforderungen/-präferenzen — soweit vom Verantwortlichen erfasst
- **Geschäfts- und Vertragsdaten:** Show- und Tourdaten, Veranstaltungsorte, Hotel- und Reisedaten, Verträge, Deal- und Konditionsdaten
- **Finanz- und Abrechnungsdaten:** Rechnungsdaten, Beträge, Bankverbindungen (IBAN), Steuer-/Mandantenangaben
- **Reisebezogene Daten:** Reise-/Routingdaten, ggf. Vielfliegernummern, Flugdaten (soweit erfasst)
- **Veranstaltungsadressen und Geodaten:** Adressen und Koordinaten von Veranstaltungsorten (für Kartendarstellung und Tour-Routing)
- **Nutzungs- und Protokolldaten:** IP-Adresse beim Login, Session-Kennungen, Zeitstempel, Geräteinformationen, Einwilligungs-Protokolle (Zeitstempel, IP)
- **Inhalte von KI-Anweisungen (soweit aktiviert):** Texte und Anhänge (z. B. PDF-Verträge, Bilder, Textdokumente), die der KI-Advancing-Assistent zur Bearbeitung erhält, sowie die zur Ausführung erforderlichen Geschäftsdaten

1.3 Hinweis zur Verantwortlichkeit für die Datenarten

Der konkrete Umfang der verarbeiteten Daten wird allein durch den Verantwortlichen bestimmt, der entscheidet, welche Informationen er in die Plattform-Instanz einstellt. Der Auftragsverarbeiter hat keinen Einfluss auf Art und Umfang der vom Verantwortlichen eingestellten Daten.

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

Der Auftragsverarbeiter ergreift folgende technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten. Maßgeblich ist der Stand zum unten genannten Datum; Maßnahmen werden dem Stand der Technik fortlaufend angepasst.

2.1 Vertraulichkeit

Zutrittskontrolle (physisch):

- Hosting bei der Hetzner Online GmbH in einem Rechenzentrum in Deutschland mit Zutrittsschutz, Zugangskontrolle und gesicherter Infrastruktur durch den Hosting-Dienstleister.

Zugangskontrolle (Systeme):

- Authentifizierung der Nutzer über individuelle Zugangsdaten; Passwörter werden ausschließlich als kryptografische Hashes gespeichert (keine Klartextspeicherung).
- Session-Verwaltung über sichere Cookies (HttpOnly, Secure, SameSite=Lax).
- Schutzmaßnahmen gegen automatisierte Angriffe (z. B. Ratenbegrenzung bei bestimmten Funktionen).

Zugriffskontrolle (Berechtigungen):

- Rollen- und rechtebasiertes Berechtigungskonzept (z. B. Admin, Agentur, Tourmanager, Künstler, Crew, Gast) mit Beschränkung des Datenzugriffs auf das für die jeweilige Rolle Erforderliche.
- Strikte Mandantentrennung: Jede Künstler-Plattform verfügt über eine eigene, getrennte Datenbank.

Trennungskontrolle:

- Logische und teils physische Trennung der Daten verschiedener Mandanten/Plattform-Instanzen.

2.2 Integrität

Weitergabe-/Transportkontrolle:

- Verschlüsselte Datenübertragung zwischen Endgerät und Server (TLS/HTTPS).
- Verschlüsselte Übertragung an Subunternehmer (TLS); besonders schützenswerte Schlüssel und Zugangsdaten werden gesondert abgesichert.

Eingabekontrolle:

- Protokollierung sicherheitsrelevanter Vorgänge (z. B. Anmeldungen, sicherheitsrelevante Aktionen) zur Nachvollziehbarkeit.
- Maßnahmen gegen typische Web-Angriffe (Schutz vor SQL-Injection durch parametrisierte Abfragen, Schutz vor Cross-Site-Scripting, CSRF-Schutz).

2.3 Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherungen (Backups) zur Wiederherstellbarkeit im Schadensfall.
- Wiederherstellungsmöglichkeit von Plattform-Instanzen aus Sicherungen/Archiven.
- Eingesetzte Software und Systeme werden gewartet und aktualisiert.

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO): Der **E-Mail-Advancing-Assistent** (Verarbeitung von Anweisungen per E-Mail an die Plattform-Adresse) ist **standardmäßig deaktiviert** und muss vom Admin ausdrücklich aktiviert werden; zusätzlich werden nur Anweisungen von Absendern auf einer Freigabeliste verarbeitet. Der **KI-Assistent im Chat-Widget** sowie die **KI-gestützte Datei-Analyse beim Upload** stehen Administratoren standardmäßig zur Verfügung; der Admin kann den Zugang über eine Freigabeliste einschränken. **Elektronische Signaturen** sind standardmäßig deaktiviert und werden erst durch die OAuth-Verbindung eines Anbieter-Kontos durch den Admin freigeschaltet.
- Verzicht auf Werbe-Tracker, Analyse-Pixel und Verhaltensanalysen (kein Google Analytics, kein Meta Pixel, kein Matomo); Einsatz ausschließlich technisch notwendiger Cookies.
- Regelmäßige Überprüfung der Sicherheitsmaßnahmen, u. a. durch externe Sicherheitsüberprüfungen (Penetrationstests).
- Auftragsverarbeiter-Management: vertragliche Verpflichtung der Subunternehmer auf Datenschutz nach Art. 28 DSGVO.

> **Hinweis:** Diese Übersicht beschreibt die getroffenen Maßnahmen auf einem für ein Rechtsdokument angemessenen Abstraktionsniveau. Eine detailliertere Darstellung kann dem Verantwortlichen auf begründete Anfrage im Rahmen von Ziffer 12 zur Verfügung gestellt werden, soweit dadurch keine Sicherheitsinformationen offengelegt werden, die das Schutzniveau gefährden.

Anlage 3 — Liste der genehmigten Subunternehmer (Subprozessoren)

Stand: siehe Datum am Ende dieses Dokuments. Eine aktuelle, datierte Fassung dieser Liste ist auf Anfrage erhältlich. Sofern nicht anders angegeben, erfolgt jede Übermittlung verschlüsselt (TLS).

Subunternehmer	Sitz / Verarbeitungsort	Zweck der Verarbeitung	Übermittelte Daten	Aktiv
Hetzner Online GmbH	Deutschland (Rechenzentrum in Deutschland)	Betrieb der Server- und Datenbankinfrastruktur (Hosting)	Sämtliche Plattformdaten (gespeichert in Deutschland)	Immer
Mailgun (Sinch Email)	EU-Region	Versand transaktionaler E-Mails (Verifikation, Benachrichtigungen, Rechnungen)	Empfänger-Adressen, Nachrichteninhalte, ggf. Anhänge	Immer
Anthropic PBC	USA	KI-Assistent „Kira" und KI-Advancing-Assistent (Claude-Modell)	Bei Kira: Chat-Text, Rolle, Sprache, Subdomain, Plattformtyp, E-Mail, IP, Seiten-URL. Beim Advancing-Assistenten zusätzlich erforderliche Geschäftsdaten und Anhänge	Nur bei Nutzung / Aktivierung
OpenAI, L.L.C.	USA	KI-Assistent „Kira" und KI-Advancing-Assistent (GPT-/ChatGPT-Modell)	wie Anthropic; keine Nutzung der API-Inhalte zum Modell-Training	Nur bei Nutzung / Aktivierung
Stripe	EU (Stripe Payments Europe)	Zahlungsabwicklung für Abonnements und KI-Credit-Käufe	Zahlungs- und Rechnungsdaten	Nur bei Zahlung über Stripe
DocuSign, Inc.	EU (eu.docusign.net)	Elektronische Signaturen für Verträge	Zu signierende Dokumente, Unterzeichner-Daten	Nur wenn vom Admin per OAuth verbunden
Box, Inc.	USA	Elektronische Signaturen (Box Sign), Alternative zu DocuSign	Zu signierende Dokumente, Unterzeichner-Daten	Nur wenn vom Admin per OAuth verbunden
OneSignal, Inc.	USA	Versand von Push-Benachrichtigungen an Nutzer der mobilen App	Geräte-Push-Kennungen, Benachrichtigungsinhalt (Titel, Text)	Nur bei Nutzung der mobilen App mit aktivierten Push-Benachrichtigungen

Subunternehmer	Sitz / Verarbeitungsort	Zweck der Verarbeitung	Übermittelte Daten	Aktiv
Google LLC (Google Maps Platform)	USA	Serverseitige Adressverifizierung/-normalisierung (Geocoding), Ortssuche (Places), Berechnung von Fahrtdistanzen/-zeiten (Distance Matrix) und Zeitzonenermittlung für Venue-, Hotel- und Reisedaten sowie Tour-Routing	Veranstaltungs-/Venue-/Hotel-Adressen (Straße, PLZ, Ort, Land), Suchtexte (Orts-/Venue-Namen), Koordinaten	Bei Nutzung von Adress-, Karten-, Reise- oder Routing-Funktionen
Mapbox, Inc.	USA	Clientseitige Kartendarstellung von Veranstaltungsorten und Tour-Routen	Venue-Koordinaten, Venue-Name, Showdatum; clientseitig zusätzlich IP-Adresse und Kartenausschnitt des Nutzergeräts	Bei Aufruf der Kartenansicht
FlightAware (AeroAPI)	USA	Abruf von Flugplan-/Flugstatusdaten zur Reiseplanung der Crew	Flugnummer, Airline-Code, Flugdatum	Bei Nutzung der Flugdaten-Funktion
Open-Meteo GmbH	Deutschland	Abruf von Wettervorhersagen für Veranstaltungsorte	Geokoordinaten (Breiten-/Längengrad) des Veranstaltungsorts und Datum	Bei Nutzung der Wetter-Funktion
DATEV eG	Deutschland	Buchhaltungs-Export / Übertragung von Buchungsdaten (sofern vom Admin verbunden)	Rechnungs-/Buchungsdaten, Mandanteninformationen	Nur wenn vom Admin verbunden
Pdfcrowd s.r.o.	Tschechien	Serverseitiges Rendern von PDF-Dokumenten (z. B. Rechnungen, Verträge)	Dokumenteninhalte; keine dauerhafte Speicherung beim Dienstleister	Bei PDF-Erzeugung
Frankfurter / Exchange Rate API	EU/USA	Abruf tagesaktueller Währungs-Wechselkurse	Nur Währungscodes und Datum — keine personenbezogenen Daten	Bei Währungsumrechnung
ip-api.com	USA	Einmalige Länder-Erkennung des Website-Besuchers zur regionalen Preisanzeige (nur öffentliche Website, nicht innerhalb der Plattform)	IP-Adresse	Nur öffentliche Website

Hinweise:

1. **Optionale Subunternehmer:** Die mit „Nur bei Nutzung / Aktivierung" gekennzeichneten Dienste werden ausschließlich dann eingesetzt, wenn der Verantwortliche die jeweilige optionale Funktion aktiviert oder nutzt. Aktiviert der Verantwortliche eine Funktion nicht, werden insoweit keine Daten an den betreffenden Subunternehmer übermittelt.

2. **KI-Anbieter (Anthropic, OpenAI):** Der KI-Hilfe-Assistent „Kira" läuft über ein vom Auftragsverarbeiter betriebenes, in Deutschland gehostetes Gateway. Der KI-Advancing-Assistent sowie die KI-gestützte Beleg-/Dokumentenauswertung übermitteln die erforderlichen Daten unmittelbar an den jeweiligen KI-Anbieter. Die Anbieter verarbeiten die Inhalte gemäß ihrer jeweiligen Enterprise- bzw. API-Datenrichtlinie; eine Nutzung zu Trainingszwecken ist danach ausgeschlossen. Diese Zusicherung beruht auf den vertraglichen Bedingungen der Anbieter. Beim KI-Advancing-Assistenten werden nur Anweisungen freigegebener Absender verarbeitet; Anweisungen nicht freigegebener Absender werden vor jeder KI-Verarbeitung verworfen.

3. **Drittlandübermittlung:** Die Übermittlung an Subunternehmer in Drittländern (insbesondere USA) wird auf die in Ziffer 9 Abs. 5 dieses Vertrags genannten Grundlagen gestützt (Standardvertragsklauseln und/oder EU-US Data Privacy Framework, soweit verfügbar).

4. **Karten-/Geodienste (Google Maps, Mapbox):** Die Adress-, Reise- und Routing-Funktionen nutzen serverseitig die Google Maps Platform (Adressen/Koordinaten/Fahrtstrecken) sowie zur clientseitigen Kartendarstellung Mapbox. Bei der clientseitigen Kartendarstellung lädt der Browser des Nutzers Inhalte direkt vom jeweiligen Anbieter; dabei können IP-Adresse und Kartenausschnitt übermittelt werden. Insoweit kann der Kartenanbieter teilweise als eigenständig Verantwortlicher auftreten. Der Verantwortliche ist für die Information seiner Nutzer und etwaige erforderliche Einwilligungen verantwortlich, soweit die Nutzung in seinem Verantwortungsbereich liegt.

Anlage 4 — Angaben zum Verantwortlichen und Unterzeichnung

4.1 Verantwortlicher (vom Kunden auszufüllen)

Feld	Angabe
Name / Firma	_____
Anschrift	_____
Vertretungsberechtigte Person	_____
Plattform-Instanz (Subdomain)	_____
E-Mail (Datenschutz-Kontakt)	_____
Ggf. Datenschutzbeauftragter	_____

4.2 Auftragsverarbeiter

Feld	Angabe
Name	Jonas Stricker
Anschrift	Im Geigersberg 8, 74348 Lauffen am Neckar, Deutschland
USt-IdNr.	DE288958387
E-Mail	hello@j.show

4.3 Unterzeichnung

Dieser Auftragsverarbeitungsvertrag wird mit Zustimmung beider Parteien wirksam. Die Zustimmung kann durch Unterzeichnung (auch elektronisch) oder durch ausdrückliche Bestätigung im Rahmen des Hauptvertrags bzw. der Plattform erfolgen.

Ort, Datum	Ort, Datum
Name / Unterschrift Für den Verantwortlichen	Jonas Stricker Für den Auftragsverarbeiter

Stand dieses Dokuments: 25. Juni 2026