J.SHOW

Data Processing Agreement (DPA)

pursuant to Art. 28(3) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR")

Translation for convenience. This is an English translation of the German "Auftragsverarbeitungsvertrag (AVV)". In the event of any discrepancy, the German version prevails (see Section 14(5)).

Preamble

This Data Processing Agreement ("DPA", "Agreement") sets out the data protection obligations of the parties in connection with the customer's use of the **j.show** platform. It forms part of the usage agreement concluded between the parties (the main contract, governed by the Terms of Use at https://j.show/terms/) and applies to all processing of personal data carried out by the processor on behalf of the controller in the course of providing the contractually agreed services.

To the extent that this DPA and the main contract diverge on data protection matters, the provisions of this DPA prevail.

---

1. Parties

Controller (hereinafter "Controller", "Customer" or "Client"):

> The customer who operates a j.show platform instance (artist or agency platform) and processes personal data on it. The specific details (name/company, address, authorized representative, subdomain of the platform instance) follow from the main contract or the registration data of the respective platform instance and are to be specified in **Annex 4**.

Processor (hereinafter "Processor", "Operator" or "we"):

> Jonas Stricker
> Im Geigersberg 8
> 74348 Lauffen am Neckar
> Germany
> VAT ID: DE288958387
> Email: hello@j.show

— hereinafter jointly the "Parties".

---

2. Subject matter, nature and purpose of the processing

(1) The subject matter of the engagement is the processing of personal data by the processor in the course of providing the cloud-based software-as-a-service platform j.show for professional tour and show management. The scope of services follows from the main contract and the Terms of Use.

(2) **Nature of the processing:** Storing, retrieving, organizing, modifying, querying, transmitting, linking, restricting and erasing personal data in the course of operating the platform instance, including hosting, database management, sending transactional emails, generating documents (e.g. invoices, contracts, day sheets), and — where activated or used by the controller — the optional functions described in **Annex 2** (AI assistant "Kira", AI advancing assistant, electronic signatures, geocoding/map display, accounting export, payment processing).

(3) **Purpose of the processing:** Exclusively the provision of the services agreed in the main contract. The processor does not process the data for its own purposes. In particular, the processor does **not** use the personal data processed on behalf of the controller for advertising, profiling or training purposes, and does not pass it on to third parties other than the sub-processors listed in **Annex 3**.

(4) **Place of processing:** Primary storage and processing take place on servers in **Germany**. When certain optional functions are used, sub-processors may process data to a limited extent outside Germany, including in third countries (see **Annex 3** and **Section 9**).

---

3. Duration of the processing

(1) This DPA applies for the term of the main contract. It begins when the main contract takes effect and ends upon its termination, but not before the obligations under **Section 11** (return and deletion) have been fully performed.

(2) The controller may terminate this DPA in whole or in part at any time without notice if there is a serious breach by the processor of data protection provisions or of this agreement, if the processor cannot or will not carry out an instruction, or if the processor unlawfully refuses access for an audit. Such termination of this DPA may make continuation of the main contract impossible.

---

4. Type of personal data and categories of data subjects

The specific data types and categories of data subjects follow from **Annex 1**, which forms part of this agreement. They typically include data of crew members, business partners (venues, hotels, promoters) and other persons recorded by the controller, including — depending on the controller's use — **special categories of personal data within the meaning of Art. 9 GDPR** (in particular health-related information such as allergies and dietary requirements).

The controller alone determines which personal data it enters into the platform instance. The controller is responsible for ensuring that there is a valid legal basis for every processing operation it initiates — including the entry of third-party data and special categories of data — and that any required consents of the data subjects have been obtained.

---

5. Rights and obligations of the controller

(1) Within the scope of this engagement, the controller is the controller responsible for the processing of the personal data within the meaning of Art. 4(7) GDPR. The controller is solely responsible for the lawfulness of the data processing and for safeguarding the rights of the data subjects.

(2) The controller is solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.

(3) The controller issues all instructions in documented form as a matter of principle (text form is sufficient; this includes the platform's configuration options). Verbal instructions are to be confirmed without undue delay in documented form.

(4) The controller designates to the processor the persons authorized to receive and decide on instructions. By default, the administrator of the respective platform instance is deemed authorized to issue instructions.

(5) The controller informs the processor without undue delay if it identifies errors or irregularities relating to data protection provisions when reviewing the results of the processing.

---

6. Bound by instructions

(1) The processor processes personal data exclusively within the scope of the agreements made and in accordance with the controller's documented instructions, unless it is required to process the data by Union law or the law of a Member State to which it is subject (Art. 28(3)(a) GDPR). In such a case, the processor informs the controller of those legal requirements before processing, unless that law prohibits such notification on important grounds of public interest.

(2) The instructions are initially defined by this agreement and by the settings made in the course of using the platform, and may be amended, supplemented or replaced by the controller in documented form.

(3) The processor informs the controller without undue delay if it is of the opinion that an instruction infringes the GDPR or other data protection provisions of the Union or the Member States (Art. 28(3) sentence 3 GDPR). The processor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the controller.

---

7. Confidentiality

(1) The processor undertakes to maintain confidentiality in the processing (Art. 28(3)(b) GDPR).

(2) The processor uses only persons to process the data who are bound to confidentiality and who have been familiarized beforehand with the data protection provisions relevant to them. The confidentiality obligation continues to apply after the activity has ended.

(3) The processor is a sole proprietorship. Insofar as the owner carries out the processing himself, the confidentiality obligation applies directly to him. Where further staff are engaged, they are bound to data secrecy before commencing their activity.

---

8. Technical and organizational measures (Art. 32 GDPR)

(1) The processor implements the technical and organizational measures (TOMs) described in **Annex 2** to ensure a level of protection appropriate to the risk (Art. 28(3)(c) in conjunction with Art. 32 GDPR).

(2) The TOMs are subject to technical progress and further development. The processor is entitled to implement alternative appropriate measures, provided that the security level of the defined measures is not undercut. Material changes are to be documented.

(3) The measures described in **Annex 2** reflect the state as at the time the agreement was concluded (status: see the date at the end of this document).

---

9. Engagement of further processors (sub-processors)

(1) The controller grants the processor **general written authorization** to engage the further processors (sub-processors) listed in **Annex 3** for the purposes described there (Art. 28(2) sentence 1 GDPR). Upon conclusion of this agreement, the sub-processors named in **Annex 3** as at the time of conclusion are deemed authorized.

(2) If the processor intends to engage a further sub-processor or to replace an existing one, it informs the controller of this **in advance** in text form (e.g. by email or via a dated sub-processor list published on the platform or at https://j.show). The controller may object to an intended change within **14 days** of receipt of the information on important data-protection-related grounds (Art. 28(2) sentence 2 GDPR). If no objection is raised within this period, the sub-processor is deemed authorized.

(3) If the controller objects on important grounds and the processor cannot provide the service without the relevant sub-processor, or can do so only with unreasonable effort, both parties are entitled to terminate the affected part of the service or the main contract with reasonable notice.

(4) The processor contractually binds each sub-processor to data protection obligations that substantially correspond to the obligations agreed in this DPA, in particular by concluding a data processing agreement pursuant to Art. 28 GDPR. If the sub-processor fails to fulfil its data protection

obligations, the processor remains liable to the controller for the performance of that sub-processor's obligations (Art. 28(4) GDPR).

(5) **Transfers to third countries:** Insofar as sub-processors process personal data in a third country (in particular in the USA), the processor ensures that there is a permissible basis for the transfer under Chapter V of the GDPR, namely

- an adequacy decision of the European Commission (Art. 45 GDPR), in particular certification of the recipient under the **EU-US Data Privacy Framework**, where available, or
- the **Standard Contractual Clauses** issued by the European Commission (Art. 46(2)(c) GDPR), together with any necessary supplementary measures.

(6) Sub-processors that serve solely for maintenance, support or comparable ancillary services without substantial access to personal data are not deemed further processors within the meaning of this section; the processor nevertheless binds them to appropriate confidentiality.

---

10. Support for the controller

(1) **Data subject rights (Art. 28(3)(e) GDPR):** The processor supports the controller, within its means and by appropriate technical and organizational measures, in fulfilling its obligation to respond to requests by data subjects exercising their rights (access, rectification, erasure, restriction, data portability, objection). Insofar as a data subject contacts the processor directly, the processor forwards the matter to the controller without undue delay and does not provide information itself without having been instructed to do so by the controller. The controller can, for the most part, view, rectify, export and delete the relevant data types itself via the platform's functions.

(2) **Security, notification obligations, data protection impact assessment (Art. 28(3)(f) in conjunction with Art. 32–36 GDPR):** Taking into account the nature of the processing and the information available to it, the processor supports the controller in complying with the obligations regarding the security of processing, the notification of personal data breaches, the communication to data subjects, and any data protection impact assessment and prior consultation of the supervisory authority.

(3) **Notification of personal data breaches:** The processor informs the controller without undue delay, as a rule **within 48 hours**, after becoming aware of a breach affecting the personal data processed for the controller. The notification contains at least the information required under Art. 33(3) GDPR, insofar as it is known to the processor. The controller's obligation to notify the supervisory authority (Art. 33 GDPR) remains unaffected and rests solely with the controller.

---

11. Return and deletion after termination

(1) After the processing services have ended, the processor — at the controller's choice — deletes or returns all personal data (Art. 28(3)(g) GDPR), unless there is an obligation to store the data under Union law or the law of a Member State.

(2) **Export before termination:** The controller has the option to export its data itself via the platform's functions before the platform instance is terminated. It is the controller's responsibility to carry out such an export in good time.

(3) **Deletion period after license expiry:** If the subscription (license) of a platform instance is terminated or cancelled, the associated personal data initially remains stored so that the platform instance can be reactivated at any time during this period. After one (1) year from license expiry, the data is deleted in the following weeks, unless a statutory retention obligation applies. From the moment the license expires, the controller may also request earlier archiving and/or complete deletion of the platform instance at any time; in that case deletion takes place correspondingly earlier.

(4) **Statutory retention obligations:** Invoicing and accounting-relevant documents are retained for the legally prescribed period (in particular up to 10 years pursuant to Section 147 of the German Fiscal Code (AO) and Section 257 of the German Commercial Code (HGB)) and deleted after these periods expire. For this period, processing is restricted to storage.

(5) **Log and function data:** Log data of the AI functions is deleted after a maximum of 90 days. Authentication logs (login attempts) are deleted automatically after 30 days. General access/activity logs are retained for backup and accountability purposes and pruned at reasonable intervals. Incoming raw emails of the AI advancing assistant are deleted promptly (as a rule within one hour after the processing has been completed).

(6) **Backups:** Personal data contained in backup copies is overwritten and deleted in the course of the regular backup cycle. Until then, processing is restricted to storage for the purposes of data backup and recovery.

(7) The processor demonstrates the deletion in a suitable manner upon the controller's request.

---

12. Audit and inspection rights

(1) The processor makes available to the controller, upon request, all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and agreed in this agreement (Art. 28(3)(h) GDPR).

(2) The processor allows for and contributes to reviews — including inspections — conducted by the controller or an auditor mandated by the controller. At the processor's choice, evidence may also be provided by submitting suitable, up-to-date certifications, attestations or reports (e.g. from independent bodies or of a current penetration test), provided these do not unreasonably restrict the controller's ability to audit.

(3) On-site inspections are to be carried out with reasonable advance notice (as a rule at least **two weeks** in advance), during normal business hours, without disrupting operations, and respecting confidentiality obligations towards third parties. They are to be limited to what is necessary and, as a rule, take place no more than once a year, unless there is a specific data-protection-related reason.

(4) The processor is obliged to inform the controller without undue delay if it is of the opinion that an instruction given in the context of an inspection infringes data protection provisions.

---

13. Liability

(1) Art. 82 GDPR applies to the liability of the parties. In their internal relationship, the parties bear responsibility according to their respective contribution to the cause.

(2) The controller indemnifies the processor against claims by third parties and data subjects that are based on the controller having entered or processed personal data in the platform without a sufficient legal basis or contrary to the provisions of the GDPR, or having instructed the processor to carry out unlawful processing, insofar as the processor is not itself at fault.

(3) The limitations of liability agreed in the main contract (Terms of Use) also apply to this DPA, insofar as they do not conflict with mandatory statutory provisions — in particular Art. 82 GDPR in the external relationship towards data subjects.

---

14. Final provisions

(1) Amendments and supplements to this agreement and its annexes require text form. This also applies to any waiver of this form requirement.

(2) Should individual provisions of this agreement be or become invalid or unenforceable, the validity of the remaining provisions remains unaffected. The parties shall replace the invalid provision with a valid one that comes closest to the economic purpose pursued by the invalid provision.

(3) In the event of contradictions between this DPA and the provisions of the main contract, the provisions of this DPA prevail on data protection matters.

(4) This agreement is governed by the law of the Federal Republic of Germany, excluding its conflict-of-laws rules. The place of jurisdiction is Stuttgart, Germany, insofar as this does not conflict with mandatory law.

(5) The German version of this agreement is authoritative. Translations are provided for information purposes only.

Annexes

The following annexes form part of this agreement:

- **Annex 1** — Subject matter of the processing: data types and categories of data subjects
- **Annex 2** — Technical and organizational measures (Art. 32 GDPR)
- **Annex 3** — List of authorized sub-processors

- **Annex 4** — Details of the controller and signing

Annex 1 — Subject matter of the processing

1.1 Categories of data subjects

Personal data of the following categories of data subjects is processed on behalf of the controller:

- **Crew members** of the platform instance (band members, technicians, touring staff and other invited users)
- **Business partners and contacts** (contact persons of venues, hotels, promoters, agencies, service providers, partners)
- **Guests** (e.g. persons on guest lists)
- **Administrators and other users** of the platform instance
- **Senders of instructions** to the AI advancing assistant (where activated)

1.2 Types of personal data

- **Master data / contact data:** first and last name, email address, telephone number, place of residence/address, language, function/role
- **Further profile data:** where applicable date of birth, gender/pronouns, profile picture (optional), device information
- **Special categories of personal data (Art. 9 GDPR):** health-related information such as allergies and dietary requirements/preferences — insofar as recorded by the controller
- **Business and contract data:** show and tour data, venues, hotel and travel data, contracts, deal and terms data
- **Financial and billing data:** invoicing data, amounts, bank details (IBAN), tax/client information
- **Travel-related data:** travel/routing data, where applicable frequent-flyer numbers, flight data (insofar as recorded)
- **Event addresses and geodata:** addresses and coordinates of venues (for map display and tour routing)
- **Usage and log data:** IP address at login, session identifiers, timestamps, device information, consent logs (timestamp, IP)
- **Contents of AI instructions (where activated):** texts and attachments (e.g. PDF contracts, images, text documents) received by the AI advancing assistant for processing, as well as the business data required for execution

1.3 Note on responsibility for the data types

The specific scope of the data processed is determined solely by the controller, who decides which information to enter into the platform instance. The processor has no influence on the nature and scope of the data entered by the controller.

Annex 2 — Technical and organizational measures (Art. 32 GDPR)

The processor takes the following technical and organizational measures to protect personal data. The state as at the date stated below is authoritative; measures are continuously adapted to the state of the art.

2.1 Confidentiality

Physical access control:

- Hosting with Hetzner Online GmbH in a data center in Germany with access protection, access control and secured infrastructure provided by the hosting service provider.

System access control:

- Authentication of users via individual credentials; passwords are stored exclusively as cryptographic hashes (no plaintext storage).
- Session management via secure cookies (HttpOnly, Secure, SameSite=Lax).
- Protective measures against automated attacks (e.g. rate limiting on certain functions).

Data access control (authorizations):

- Role- and permission-based authorization concept (e.g. admin, agency, tour manager, artist, crew, guest) restricting data access to what is necessary for the respective role.
- Strict tenant separation: each artist platform has its own separate database.

Separation control:

- Logical and partly physical separation of the data of different tenants/platform instances.

2.2 Integrity

Transfer/transport control:

- Encrypted data transmission between end device and server (TLS/HTTPS).
- Encrypted transmission to sub-processors (TLS); particularly sensitive keys and credentials are protected separately.

Input control:

- Logging of security-relevant operations (e.g. logins, security-relevant actions) for traceability.
- Measures against typical web attacks (protection against SQL injection through parameterized queries, protection against cross-site scripting, CSRF protection).

2.3 Availability and resilience

- Regular data backups for recoverability in the event of damage.
- Ability to restore platform instances from backups/archives.
- The software and systems used are maintained and updated.

2.4 Procedures for regular review, assessment and evaluation

- Data protection by design and by default (Art. 25 GDPR): the **email advancing assistant** (processing of instructions sent by email to the platform address) is **disabled by default** and must be explicitly enabled by the Admin; in addition, only instructions from senders on an authorization list are processed. The **AI assistant in the chat widget** and the **AI-supported file analysis on upload** are available to administrators by default; the Admin can restrict access via an authorization list. **Electronic signatures** are disabled by default and are only enabled once the Admin connects a provider account via OAuth.
- No advertising trackers, analytics pixels or behavioral analyses (no Google Analytics, no Meta Pixel, no Matomo); only technically necessary cookies are used.
- Regular review of the security measures, including external security reviews (penetration tests).
- Sub-processor management: contractual obligation of sub-processors to comply with data protection pursuant to Art. 28 GDPR.

> **Note:** This overview describes the measures taken at a level of abstraction appropriate for a legal document. A more detailed description can be made available to the controller upon reasoned request within the framework of Section 12, insofar as this does not disclose security information that would jeopardize the level of protection.

Annex 3 — List of authorized sub-processors

Status: see the date at the end of this document. A current, dated version of this list is available on request. Unless stated otherwise, every transmission is encrypted (TLS).

Sub-processor	Location / place of processing	Purpose of processing	Data transmitted	Active
Hetzner Online GmbH	Germany (data center in Germany)	Operation of the server and database infrastructure (hosting)	All platform data (stored in Germany)	Always
Mailgun (Sinch Email)	EU region	Sending transactional emails (verification, notifications, invoices)	Recipient addresses, message contents, where applicable attachments	Always
Anthropic PBC	USA	AI assistant "Kira" and AI advancing assistant (Claude model)	For Kira: chat text, role, language, subdomain, platform type, email, IP, page URL. For the advancing assistant, additionally the required business data and attachments	Only when used / activated
OpenAI, L.L.C.	USA	AI assistant "Kira" and AI advancing assistant (GPT/ChatGPT model)	As for Anthropic; API content is not used for model training	Only when used / activated
Stripe	EU (Stripe Payments Europe)	Payment processing for subscriptions and AI credit purchases	Payment and invoicing data	Only when paying via Stripe
DocuSign, Inc.	EU (eu.docusign.net)	Electronic signatures for contracts	Documents to be signed, signer data	Only when connected by the admin via OAuth
Box, Inc.	USA	Electronic signatures (Box Sign), alternative to DocuSign	Documents to be signed, signer data	Only when connected by the admin via OAuth
OneSignal, Inc.	USA	Sending push notifications to mobile app users	Device push tokens, notification content (title, text)	Only when using the mobile app with push notifications enabled
Google LLC (Google Maps Platform)	USA	Server-side address verification/normalization (geocoding), place search (Places), calculation of travel distances/times (Distance Matrix) and time zone determination for venue, hotel and travel data as well as tour routing	Event/venue/hotel addresses (street, postal code, city, country), search texts (place/venue names), coordinates	When using address, map, travel or routing functions

Sub-processor	Location / place of processing	Purpose of processing	Data transmitted	Active
Mapbox, Inc.	USA	Client-side map display of venues and tour routes	Venue coordinates, venue name, show date; client-side additionally the IP address and map section of the user's device	When opening the map view
FlightAware (AeroAPI)	USA	Retrieval of flight schedule/flight status data for crew travel planning	Flight number, airline code, flight date	When using the flight data function
Open-Meteo GmbH	Germany	Retrieval of weather forecasts for venues	Geocoordinates (latitude/longitude) of the venue and date	When using the weather function
DATEV eG	Germany	Accounting export / transmission of accounting data (where connected by the admin)	Invoicing/accounting data, client information	Only when connected by the admin
Pdfcrowd s.r.o.	Czech Republic	Server-side rendering of PDF documents (e.g. invoices, contracts)	Document contents; no permanent storage at the provider	When generating PDFs
Frankfurter / Exchange Rate API	EU/USA	Retrieval of daily currency exchange rates	Currency codes and date only — no personal data	When converting currencies
ip-api.com	USA	One-off country detection of the website visitor for regional price display (public website only, not within the platform)	IP address	Public website only

Notes:

1. **Optional sub-processors:** The services marked "Only when used / activated" are used exclusively when the controller activates or uses the respective optional function. If the controller does not activate a function, no data is transmitted to the relevant sub-processor in that respect.

2. **AI providers (Anthropic, OpenAI):** The AI help assistant "Kira" runs via a gateway operated by the processor and hosted in Germany. The AI advancing assistant and the AI-supported receipt/document analysis transmit the required data directly to the respective AI provider. The providers process the contents in accordance with their respective enterprise or API data policy; use for training purposes is excluded thereunder. This assurance is based on the providers' contractual terms. For the AI advancing assistant, only instructions from authorized senders are processed; instructions from non-authorized senders are discarded before any AI processing.

3. **Third-country transfers:** Transfers to sub-processors in third countries (in particular the USA) are based on the grounds set out in Section 9(5) of this agreement (Standard Contractual Clauses and/or the EU-US Data Privacy Framework, where available).

4. **Map/geo services (Google Maps, Mapbox):** The address, travel and routing functions use the Google Maps Platform server-side (addresses/coordinates/travel routes) and Mapbox for client-side map display. With client-side map display, the user's browser loads content directly from the respective provider; this may transmit the IP address and map section. In this respect, the map provider may act partly as an independent controller. The controller is responsible for informing its users and obtaining any required consents, insofar as the use falls within its area of responsibility.

Annex 4 — Details of the controller and signing

4.1 Controller (to be completed by the customer)

Field	Entry
Name / company	_____
Address	_____
Authorized representative	_____
Platform instance (subdomain)	_____
Email (data protection contact)	_____
Data protection officer (if any)	_____

4.2 Processor

Field	Entry
Name	Jonas Stricker
Address	Im Geigersberg 8, 74348 Lauffen am Neckar, Germany
VAT ID	DE288958387
Email	hello@j.show

4.3 Signing

This Data Processing Agreement takes effect with the consent of both parties. Consent may be given by signing (including electronically) or by express confirmation within the framework of the main contract or the platform.

Place, date	Place, date
Name / signature For the controller	Jonas Stricker For the processor

Document status: 25 June 2026

Note: The German version (AVV) is the authoritative version; this English translation is provided for convenience.