

Data Processing Agreement

within the meaning of Art. 28 (3) General Data Protection Regulation (GDPR)

Controller – hereinafter “Client”

Organiser as confirmed in the maintix dashboard

Processor – hereinafter “Contractor”

Maintix.World GbR

represented by its partners Maximilian Schunk and Nick Schwenderling
Brückstr. 35, 40882 Ratingen, Germany

Preamble

This Agreement specifies the data protection obligations of the parties arising from the Organiser Terms of maintix (hereinafter: main agreement). It applies to all activities in which the Contractor, its staff or persons engaged by it process personal data (hereinafter: data) on behalf of the Client.

Where the Contractor processes data for its own purposes as an independent controller – in particular for the operation and security of the platform, fraud and misuse prevention, the resale of tickets between purchasers via ReTix, billing with the Client, the fulfilment of statutory retention obligations and its own audience measurement – this Agreement does not apply; the Contractor's privacy notice applies instead.

§ 1 Subject matter, duration and specification of processing

The services to be provided by the Contractor for the Client under the main agreement comprise in particular:

- Provision of a technical platform (web and installable web app) for the online sale of admission tickets
- Processing of orders, payments and refunds via a payment service provider
- Issuing and sending personalised digital tickets, including binding to a device and live QR codes; physical tickets in future if applicable
- Admission control (scanner, guest lists, artist check-in)
- Support for purchasers and organisers, including live chat
- Evaluations and statistics in the organiser dashboard

Type of data:

- First and last names of purchasers and ticket holders, e-mail address, country
- Order, ticket and payment status data (no full card data)
- Technical device features for binding a ticket to a device
- Admission data (time and entry point of a scan)
- IP addresses and technical log data
- Content of support enquiries and chat messages

- Data of the Client's team members (name, e-mail address, role)

Categories of data subjects:

- Ticket purchasers and ticket holders (participants)
- Guests on guest lists and artists
- Team members of the Client with access to the dashboard

Nature and purpose of processing: collecting, storing, using, transmitting and deleting the data for the sale of tickets, admission and support as described above.

The term of this Agreement corresponds to the term of the main agreement, insofar as no further obligations arise from the provisions of this Agreement.

§ 2 Scope and responsibility, instructions

(1) The Contractor processes personal data on behalf of the Client. The Client is solely responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of the processing and of the disclosure of data to the Contractor ("controller" within the meaning of Art. 4 (7) GDPR).

(2) The instructions are defined by the main agreement and by the settings the Client makes in the dashboard. The Client may issue individual instructions in text form (e.g. by e-mail to hey@maintix.world). Instructions that go beyond the agreed scope of services are treated as a request for a change of service; the Contractor may charge appropriate remuneration for them. Verbal instructions must be confirmed promptly in text form.

(3) The Contractor uses the data for no purposes other than those stated in § 1. Copies are only made to the extent necessary for proper operation, in particular as backups.

§ 3 Obligations of the Contractor

(1) The Contractor processes data only on documented instructions of the Client, unless it is required to do so by Union or Member State law (Art. 28 (3) (a) GDPR); in such a case it informs the Client before processing, unless the law prohibits this. If the Contractor believes an instruction infringes data protection law, it informs the Client without delay and may suspend execution until the instruction is confirmed or changed.

(2) The Contractor takes the technical and organisational measures pursuant to Art. 32 GDPR described in Annex 1. They may be developed further as long as the agreed level of protection is not undercut.

(3) The Contractor supports the Client, taking into account the nature of the processing and with the means available to it, in responding to requests from data subjects (Chapter III GDPR) and in complying with the obligations under Art. 32 to 36 GDPR.

(4) The Contractor ensures that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This obligation continues after the end of the engagement.

(5) The Contractor informs the Client without undue delay, where possible within 24 hours of becoming aware, of any personal data breach, with the information required under Art. 33 (3) GDPR, takes the necessary measures to secure the data and mitigate possible adverse consequences, and coordinates with the Client.

(6) The contact persons for data protection at the Contractor are its partners Maximilian Schunk and Nick Schwenderling, reachable at hey@maintix.world. The Contractor is not obliged to appoint a data protection officer. It may name other contact persons in text form at any time.

(7) The Contractor regularly reviews the effectiveness of the technical and organisational measures (Art. 32 (1) (d) GDPR).

(8) The Contractor rectifies, erases or restricts the processing of data on the instruction of the Client. Where possible, the Client can do this itself in the dashboard.

(9) After the end of the main agreement the Contractor erases the data at the Client's choice or makes it available for export beforehand, unless there is a statutory obligation to store it (Art. 28 (3) (g) GDPR). Erasure takes place no later than 30 days after the end of the contract; backups are overwritten in rotation within a further 14 days.

(10) If a data subject asserts claims against the Client under Art. 82 GDPR, the Contractor supports the Client in defending them within its means.

(11) The Contractor keeps a record of processing activities pursuant to Art. 30 (2) GDPR.

§ 4 Obligations of the Client

(1) The Client informs the Contractor promptly and fully if it discovers errors or irregularities regarding data protection provisions.

(2) The Client is responsible for providing information to its participants (Art. 13, 14 GDPR) insofar as it collects data for its own purposes, and for assigning dashboard access to its team carefully.

(3) § 3 (10) applies accordingly if a data subject asserts claims against the Contractor.

§ 5 Requests from data subjects

If a data subject contacts the Contractor regarding rectification, erasure or access concerning data processed on behalf of the Client, the Contractor forwards the request to the Client without delay, insofar as an assignment to the Client is possible, and supports the Client on instruction. The Contractor is not liable if the Client does not answer the request, or does not answer it correctly or in time.

§ 6 Evidence and inspections

(1) On request, the Contractor provides the Client with suitable evidence of compliance with the obligations under this Agreement, in particular through this Agreement including Annex 1 and written information.

(2) If inspections by the Client or an auditor commissioned by it are necessary in individual cases, they take place during normal business hours, without disrupting operations, after notification at least 14 days in advance. The Contractor may make them dependent on a confidentiality undertaking. If the auditor is in competition with the Contractor, the Contractor has a right to object. The Contractor may claim reasonable remuneration for support with inspections that exceeds one working day per calendar year.

(3) Paragraph 2 applies accordingly to inspections by a supervisory authority; a confidentiality undertaking is not required in that case.

§ 7 Sub-processors

(1) The Client grants the Contractor general authorisation to engage further processors (Art. 28 (2) sentence

2 GDPR). The sub-processors listed in Annex 2 are deemed approved upon conclusion of this Agreement.

(2) The Contractor imposes on each sub-processor the same data protection obligations as set out in this Agreement (Art. 28 (4) GDPR) and selects them with due care, in particular with regard to their technical and organisational measures.

(3) The Contractor informs the Client at least four weeks in advance by e-mail or in the dashboard of any intended addition or replacement of a sub-processor. The Client may object within two weeks for an important data protection reason. If no agreement is reached, both parties have a special right of termination. In urgent cases (e.g. failure of a service provider) the period may be shorter; the Contractor then informs the Client without delay.

(4) Ancillary services such as telecommunications, postal and transport services or the maintenance of hardware are not sub-processing within the meaning of this provision.

§ 8 Place of processing

(1) The data is processed in a member state of the European Union or the European Economic Area. The application runs on servers in Germany, the database in a data centre in Ireland.

(2) Processing in a third country or by a body located in a third country only takes place if the requirements of Art. 44 et seq. GDPR are met, e.g. on the basis of an adequacy decision of the EU Commission or the EU Standard Contractual Clauses. The Client hereby approves the transfers to third countries described in Annex 2.

§ 9 Information duties, text form, applicable law

(1) If the Client's data is endangered at the Contractor by seizure, confiscation, insolvency proceedings or other events or measures of third parties, the Contractor informs the Client without delay and informs all parties involved that sovereignty over the data lies exclusively with the Client as controller.

(2) Amendments and supplements to this Agreement require text form and an express reference that they amend this Agreement. Amended versions are notified in the dashboard and require renewed consent.

(3) In the event of contradictions, the provisions of this Agreement on data protection take precedence over those of the main agreement. Should individual provisions be invalid, the validity of the remaining provisions is not affected.

(4) German law applies.

§ 10 Liability

The liability provisions of the main agreement also apply to the processing of data on behalf of the Client, unless otherwise expressly agreed; in the absence of such provisions, the statutory provisions apply. Art. 82 GDPR remains unaffected.

§ 11 Conclusion

The Agreement is concluded electronically by confirmation in the maintix dashboard. The time of confirmation, the confirming user and the version are logged in the Client's account and shown under "Legal".

Annex 1 – Technical and organisational measures

1. Confidentiality (Art. 32 (1) (b) GDPR)

Physical access control

- maintix does not operate its own server rooms. Servers are located in data centres of IONOS SE in Germany and of the database operator in Ireland, both certified to ISO/IEC 27001, with access control, video surveillance and security staff provided by the operators

System access control

- Personal user accounts, passwords stored only as salted hash values (bcrypt) with minimum requirements
- Two-factor authentication (TOTP) available for all accounts, mandatory for the maintix team
- Automatic blocking after repeated failed logins
- Server access only via SSH key; password login and root login disabled
- Sessions in secure, HttpOnly cookies; deleting an account ends all sessions immediately

Data access control

- Role and permission concept for organisers (e.g. owner, back office, ticket help, crew, admission) and for the maintix team according to the need-to-know principle
- Software-based client separation: every query is bound to the respective organisation
- Database not accessible via public interfaces (row level security, public rights revoked)
- Card data is entered directly with the payment service provider and is never stored by maintix

Separation control

- Separate test and production systems; tests are technically prevented from running against the production database
- Demonstration accounts are separated and only use a simulated payment provider

Pseudonymisation and encryption

- All connections encrypted via TLS (HTTPS with HSTS); database connection encrypted
- Database stored encrypted at rest by the operator
- Access links to tickets and orders are cryptographically signed; session and login tokens are stored only as hash values
- Access links are masked before transmission to audience measurement

2. Integrity (Art. 32 (1) (b) GDPR)

Transfer control

- Transmission exclusively via encrypted connections
- Messages from the payment service provider are checked via signature
- Ticket QR codes are cryptographically signed and change continuously (forgery protection)

Input control

- Logging of security-relevant actions (login, changes to conditions, refunds, payouts, team changes) with user, time and IP address
- Clear responsibilities through roles

3. Availability and resilience (Art. 32 (1) (b), (c) GDPR)**Availability control**

- Backups of the database every 6 hours, checked for readability and kept for 14 days; restoration has been tested
- Several application processes run in parallel; failed processes restart automatically
- Monitoring of the system every minute
- Protection of the infrastructure (power supply, fire protection, redundancy) by the certified data centre operators

Rapid recoverability

- Documented restore procedure from the backups

4. Procedures for regular review (Art. 32 (1) (d), Art. 25 GDPR)**Data protection management**

- Named contact person for data protection
- Persons with access to data are committed to confidentiality
- Automated tests before every release
- Review of the measures in the event of relevant changes, at least annually

Data protection by default

- Data minimisation: only data required for sale and admission is collected
- Audience measurement only with the visitor's consent

Order control

- Sub-processors only with a data processing agreement or EU Standard Contractual Clauses
- No processing on behalf without an instruction from the Client

Annex 2 – Sub-processors**IONOS SE**

Elgendorfer Str. 57, 56410 Montabaur, Germany · Data: all data categories ·
Location / safeguards: Germany

**Hosting of the application (servers
in Germany), backups**

Supabase, Inc.

USA – data stored in the Ireland data centre (EU) · Data: all data categories ·
Location / safeguards: Ireland (EU); access from the USA only on the basis of
the EU Standard Contractual Clauses

Operation of the database

Stripe Payments Europe, Limited

1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland ·
Data: purchaser and payment data, data of the Client · Location / safeguards:
EU; transfer to the USA on the basis of the EU-US Data Privacy Framework or
the EU Standard Contractual Clauses

**Payment processing, refunds,
payouts to organisers**

STRATO GmbH

Otto-Ostrowski-Straße 7, 10249 Berlin, Germany · Data: names, e-mail
addresses, e-mail content · Location / safeguards: Germany

**Sending and receiving e-mails
(tickets, confirmations, support)**

OpenAI Ireland Ltd

1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01
YC43, Ireland · Data: content of chat messages; no order or payment data ·
Location / safeguards: EU; processing in the USA possible on the basis of the
EU Standard Contractual Clauses; no use for training

**Automated first response in the live
chat (support)**

Google Ireland Limited

Gordon House, Barrow Street, Dublin 4, Ireland · Data: usage data without
names or e-mail addresses, truncated IP addresses · Location / safeguards:
EU; transfer to the USA on the basis of the EU-US Data Privacy Framework

**Audience measurement (Google
Analytics 4) – only with the visitor's
consent**

Physical tickets (hard tickets) are not currently offered. Should a printing or shipping service provider be engaged for this in future, the Contractor will announce it in advance in accordance with § 7 (3).

Conclusion

Concluded by confirmation in the maintix dashboard; time and user are logged.
For the Contractor: Maximilian Schunk and Nick Schwenderling, partners of Maintix.World GbR.