

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Verantwortlicher – nachstehend „Auftraggeber“

Veranstalter gemäß Bestätigung im maintix-Dashboard

Auftragsverarbeiter – nachstehend „Auftragnehmer“

Maintix.World GbR

vertreten durch die Gesellschafter Maximilian Schunk und Nick Schwenderling

Brückstr. 35, 40882 Ratingen, Deutschland

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den Veranstalterbedingungen von maintix (nachfolgend: Hauptvertrag) ergeben. Sie gilt für alle Tätigkeiten, bei denen der Auftragnehmer, seine Beschäftigten oder von ihm Beauftragte personenbezogene Daten (nachfolgend: Daten) im Auftrag des Auftraggebers verarbeiten.

Soweit der Auftragnehmer Daten für eigene Zwecke als eigener Verantwortlicher verarbeitet – insbesondere für Betrieb und Sicherheit der Plattform, die Verhinderung von Betrug und Missbrauch, den Weiterverkauf von Tickets zwischen Käufern über ReTix, die Abrechnung mit dem Auftraggeber, die Erfüllung gesetzlicher Aufbewahrungspflichten und die eigene Reichweitenmessung –, gilt diese Vereinbarung nicht; insoweit gelten die Datenschutzhinweise des Auftragnehmers.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Gegenstand der vom Auftragnehmer für den Auftraggeber nach dem Hauptvertrag zu erbringenden Leistungen sind insbesondere:

- Bereitstellung einer technischen Plattform (Web und installierbare Web-App) zum Online-Vertrieb von Eintrittskarten
- Abwicklung von Bestellungen, Zahlungen und Erstattungen über einen Zahlungsdienstleister
- Ausstellung und Versand personalisierter digitaler Tickets einschließlich Gerätebindung und Live-QR-Code; künftig gegebenenfalls physische Tickets
- Einlasskontrolle (Scanner, Gästelisten, Artist-Check-in)
- Support für Käufer und Veranstalter einschließlich Live-Chat
- Auswertungen und Statistiken im Veranstalter-Dashboard

Art der Daten:

- Vor- und Nachnamen von Käufern und Ticketinhabern, E-Mail-Adresse, Land
- Bestell-, Ticket- und Zahlungsstatusdaten (keine vollständigen Kartendaten)
- Technische Gerätemerkmale zur Bindung eines Tickets an ein Endgerät

- Einlassdaten (Zeitpunkt und Einlassstelle eines Scans)
- IP-Adressen und technische Protokolldaten
- Inhalte von Supportanfragen und Chatnachrichten
- Daten der Teammitglieder des Auftraggebers (Name, E-Mail-Adresse, Rolle)

Kategorien betroffener Personen:

- Ticketkäufer und Ticketinhaber (Teilnehmer)
- Gäste auf Gästelisten sowie Artists
- Teammitglieder des Auftraggebers mit Zugang zum Dashboard

Art und Zweck der Verarbeitung: Erheben, Speichern, Verwenden, Übermitteln und Löschen der Daten für Ticketverkauf, Einlass und Support wie oben beschrieben.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus ihren Bestimmungen nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit, Weisungen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Verarbeitung und der Datenweitergabe an den Auftragnehmer, allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen ergeben sich aus dem Hauptvertrag und den Einstellungen, die der Auftraggeber im Dashboard vornimmt. Einzelweisungen kann der Auftraggeber in Textform erteilen (z. B. per E-Mail an hey@maintix.world). Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, werden als Antrag auf Leistungsänderung behandelt; der Auftragnehmer kann dafür eine angemessene Vergütung verlangen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer verwendet die Daten für keine anderen als die in § 1 genannten Zwecke. Kopien werden nur erstellt, soweit sie für den ordnungsgemäßen Betrieb erforderlich sind, insbesondere als Sicherungen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder eines Mitgliedstaats dazu verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO); in einem solchen Fall teilt er dem Auftraggeber dies vor der Verarbeitung mit, sofern das Recht dies nicht verbietet. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen Datenschutzrecht verstößt, informiert er den Auftraggeber unverzüglich und darf die Umsetzung aussetzen, bis die Weisung bestätigt oder geändert wurde.

(2) Der Auftragnehmer trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Sie dürfen weiterentwickelt werden, solange das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und mit den ihm zur Verfügung stehenden Mitteln bei der Beantwortung von Anträgen betroffener Personen (Kapitel III DSGVO) und bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO.

(4) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Pflicht

besteht auch nach Beendigung des Auftrags fort.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich, nach Möglichkeit innerhalb von 24 Stunden nach Kenntnis, über Verletzungen des Schutzes personenbezogener Daten mit den nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sich hierzu mit dem Auftraggeber ab.

(6) Ansprechpartner für Datenschutz beim Auftragnehmer sind die Gesellschafter Maximilian Schunk und Nick Schwenderling, erreichbar unter hey@maintix.world. Zur Benennung eines Datenschutzbeauftragten ist der Auftragnehmer nicht verpflichtet. Er kann jederzeit in Textform andere Ansprechpartner benennen.

(7) Der Auftragnehmer überprüft regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO).

(8) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung von Daten auf Weisung des Auftraggebers ein. Soweit möglich, kann der Auftraggeber dies selbst im Dashboard vornehmen.

(9) Nach Ende des Hauptvertrages löscht der Auftragnehmer die Daten nach Wahl des Auftraggebers oder stellt sie ihm zuvor zum Export bereit, sofern keine gesetzliche Pflicht zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO). Die Löschung erfolgt spätestens 30 Tage nach Vertragsende; Sicherungen werden innerhalb weiterer 14 Tage turnusmäßig überschrieben.

(10) Macht eine betroffene Person Ansprüche nach Art. 82 DSGVO gegenüber dem Auftraggeber geltend, unterstützt der Auftragnehmer den Auftraggeber im Rahmen seiner Möglichkeiten bei der Abwehr.

(11) Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

(2) Der Auftraggeber ist für die Information seiner Teilnehmer (Art. 13, 14 DSGVO) verantwortlich, soweit er Daten für eigene Zwecke erhebt, und vergibt Dashboard-Zugänge an sein Team mit der gebotenen Sorgfalt.

(3) Macht eine betroffene Person Ansprüche gegenüber dem Auftragnehmer geltend, gilt § 3 Abs. 10 entsprechend.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person wegen Berichtigung, Löschung oder Auskunft zu Daten, die im Auftrag des Auftraggebers verarbeitet werden, an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung möglich ist, und unterstützt ihn auf Weisung. Der Auftragnehmer haftet nicht, wenn der Auftraggeber die Anfrage nicht, nicht richtig oder nicht fristgerecht beantwortet.

§ 6 Nachweise und Kontrollen

(1) Der Auftragnehmer weist dem Auftraggeber auf Anfrage die Einhaltung der Pflichten aus dieser Vereinbarung mit geeigneten Mitteln nach, insbesondere durch diese Vereinbarung samt Anlage 1 und schriftliche Auskünfte.

(2) Sind im Einzelfall Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer erforderlich, finden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach

Anmeldung mit einer Frist von mindestens 14 Tagen statt. Der Auftragnehmer kann sie von einer Verschwiegenheitserklärung abhängig machen. Steht der Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer, hat dieser ein Einspruchsrecht. Für die Unterstützung bei Inspektionen, die über einen Arbeitstag pro Kalenderjahr hinausgeht, kann der Auftragnehmer eine angemessene Vergütung verlangen.

(3) Für Inspektionen durch eine Aufsichtsbehörde gilt Absatz 2 entsprechend; eine Verschwiegenheitserklärung ist dann nicht erforderlich.

§ 7 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen (Art. 28 Abs. 2 Satz 2 DSGVO). Die in Anlage 2 genannten Unterauftragsverarbeiter gelten mit Abschluss dieser Vereinbarung als genehmigt.

(2) Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter dieselben Datenschutzpflichten auf, wie sie in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO), und wählt ihn sorgfältig, insbesondere unter Berücksichtigung seiner technischen und organisatorischen Maßnahmen, aus.

(3) Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen im Voraus per E-Mail oder im Dashboard über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann innerhalb von zwei Wochen aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, steht beiden Parteien ein Sonderkündigungsrecht zu. In Eilfällen (z. B. Ausfall eines Dienstleisters) kann die Frist kürzer sein; der Auftragnehmer informiert dann unverzüglich.

(4) Nebenleistungen wie Telekommunikations-, Post- und Transportdienstleistungen oder die Wartung von Hardware sind keine Unterauftragsverarbeitung im Sinne dieser Regelung.

§ 8 Ort der Datenverarbeitung

(1) Die Daten werden in einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeitet. Die Anwendung läuft auf Servern in Deutschland, die Datenbank in einem Rechenzentrum in Irland.

(2) Eine Verarbeitung in einem Drittland oder durch eine Stelle mit Sitz in einem Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, etwa auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission oder der EU-Standardvertragsklauseln. Die in Anlage 2 beschriebenen Drittlandbezüge genehmigt der Auftraggeber hiermit.

§ 9 Informationspflichten, Textform, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich und weist alle Beteiligten darauf hin, dass die Hoheit über die Daten ausschließlich beim Auftraggeber als Verantwortlichem liegt.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform und des ausdrücklichen Hinweises, dass es sich um eine Änderung dieser Vereinbarung handelt. Geänderte Fassungen werden im Dashboard angekündigt und bedürfen der erneuten Zustimmung.

(3) Bei Widersprüchen gehen die Regelungen dieser Vereinbarung zum Datenschutz denen des Hauptvertrages vor. Sollten einzelne Teile unwirksam sein, berührt dies die Wirksamkeit der übrigen

Regelungen nicht.

(4) Es gilt deutsches Recht.

§ 10 Haftung

Die im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, soweit nicht ausdrücklich etwas anderes vereinbart ist; fehlt eine solche Regelung, gelten die gesetzlichen Bestimmungen. Art. 82 DSGVO bleibt unberührt.

§ 11 Abschluss

Die Vereinbarung wird elektronisch durch Bestätigung im maintix-Dashboard geschlossen. Zeitpunkt der Bestätigung, bestätigender Benutzer und Fassung werden im Konto des Auftraggebers protokolliert und unter „Rechtliches“ angezeigt.

Anlage 1 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- maintix betreibt keine eigenen Serverräume. Die Server stehen in Rechenzentren der IONOS SE in Deutschland und des Datenbankbetreibers in Irland, beide nach ISO/IEC 27001 zertifiziert, mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal durch die Betreiber

Zugangskontrolle

- Persönliche Benutzerkonten, Passwörter nur als gesalzene Hashwerte (bcrypt) mit Mindestanforderungen
- Zwei-Faktor-Anmeldung (TOTP) für alle Konten verfügbar, für das maintix-Team verpflichtend
- Automatische Sperre nach wiederholten Fehlversuchen
- Serverzugang nur per SSH-Schlüssel; Passwort- und Root-Anmeldung deaktiviert
- Sitzungen in sicheren HttpOnly-Cookies; das Löschen eines Kontos beendet alle Sitzungen sofort

Zugriffskontrolle

- Rollen- und Rechtekonzept für Veranstalter (z. B. Veranstalter, Backoffice, Ticket-Hilfe, Crew, Einlass) und für das maintix-Team nach dem Need-to-know-Prinzip
- Softwareseitige Mandantentrennung: jede Abfrage ist an die jeweilige Organisation gebunden
- Datenbank nicht über öffentliche Schnittstellen erreichbar (Row Level Security, entzogene öffentliche Rechte)
- Kartendaten werden direkt beim Zahlungsdienstleister eingegeben und bei maintix nie gespeichert

Trennungskontrolle

- Getrennte Test- und Produktivsysteme; Tests gegen die Produktivdatenbank sind technisch gesperrt
- Demonstrationskonten sind getrennt und nutzen ausschließlich einen simulierten Zahlungsanbieter

Pseudonymisierung und Verschlüsselung

- Alle Verbindungen per TLS verschlüsselt (HTTPS mit HSTS); Datenbankverbindung verschlüsselt
- Datenbank beim Betreiber verschlüsselt gespeichert
- Zugangslinks zu Tickets und Bestellungen sind kryptografisch signiert; Sitzungs- und Anmeldetoken werden nur als Hashwert gespeichert
- Zugangslinks werden vor der Übermittlung an die Reichweitenmessung unkenntlich gemacht

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Übertragung ausschließlich über verschlüsselte Verbindungen
- Nachrichten des Zahlungsdienstleisters werden per Signatur geprüft
- Ticket-QR-Codes sind kryptografisch signiert und wechseln laufend (Fälschungsschutz)

Eingabekontrolle

- Protokollierung sicherheitsrelevanter Aktionen (Anmeldung, Änderungen an Konditionen, Erstattungen, Auszahlungen, Teamänderungen) mit Benutzer, Zeitpunkt und IP-Adresse
- Klare Zuständigkeiten über Rollen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)**Verfügbarkeitskontrolle**

- Sicherung der Datenbank alle 6 Stunden, auf Lesbarkeit geprüft und 14 Tage aufbewahrt; Wiederherstellung getestet
- Mehrere Anwendungsprozesse laufen parallel; ausgefallene Prozesse starten automatisch neu
- Überwachung des Systems im Minutentakt
- Schutz der Infrastruktur (Stromversorgung, Brandschutz, Redundanz) durch die zertifizierten Rechenzentrumsbetreiber

Rasche Wiederherstellbarkeit

- Dokumentiertes Wiederherstellungsverfahren aus den Sicherungen

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d, Art. 25 DSGVO)**Datenschutz-Management**

- Benannter Ansprechpartner für Datenschutz
- Personen mit Datenzugriff sind auf Vertraulichkeit verpflichtet
- Automatisierte Tests vor jeder Veröffentlichung
- Überprüfung der Maßnahmen bei relevanten Änderungen, mindestens jährlich

Datenschutzfreundliche Voreinstellungen

- Datenminimierung: es werden nur Daten erhoben, die für Verkauf und Einlass erforderlich sind
- Reichweitenmessung nur mit Einwilligung des Besuchers

Auftragskontrolle

- Unterauftragsverarbeiter nur mit Auftragsverarbeitungsvertrag bzw. EU-Standardvertragsklauseln
- Keine Auftragsverarbeitung ohne Weisung des Auftraggebers

Anlage 2 – Unterauftragsverarbeiter**IONOS SE**

Elgendorfer Str. 57, 56410 Montabaur, Deutschland · Daten: alle
Datenkategorien · Ort / Garantien: Deutschland

**Hosting der Anwendung (Server in
Deutschland), Sicherungen**

Supabase, Inc.

USA – Datenhaltung im Rechenzentrum Irland (EU) · Daten: alle
Datenkategorien · Ort / Garantien: Irland (EU); Zugriff aus den USA nur auf
Grundlage der EU-Standardvertragsklauseln

Betrieb der Datenbank

Stripe Payments Europe, Limited

1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland ·
Daten: Käufer- und Zahlungsdaten, Daten des Auftraggebers · Ort / Garantien:
EU; Übermittlung in die USA auf Grundlage des EU-US Data Privacy Framework
bzw. der EU-Standardvertragsklauseln

**Zahlungsabwicklung, Erstattungen,
Auszahlungen an Veranstalter****STRATO GmbH**

Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland · Daten: Namen,
E-Mail-Adressen, Inhalte der E-Mails · Ort / Garantien: Deutschland

**Versand und Empfang von E-Mails
(Tickets, Bestätigungen, Support)****OpenAI Ireland Ltd**

1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01
YC43, Irland · Daten: Inhalte von Chatnachrichten; keine Bestell- oder
Zahlungsdaten · Ort / Garantien: EU; Verarbeitung in den USA möglich auf
Grundlage der EU-Standardvertragsklauseln; keine Nutzung zum Training

**Automatische Erstantwort im
Live-Chat (Support)****Google Ireland Limited**

Gordon House, Barrow Street, Dublin 4, Irland · Daten: Nutzungsdaten ohne
Namen und E-Mail-Adressen, gekürzte IP-Adressen · Ort / Garantien: EU;
Übermittlung in die USA auf Grundlage des EU-US Data Privacy Framework

**Reichweitenmessung (Google
Analytics 4) – nur nach Einwilligung
des Besuchers**

Physische Tickets (Hardtickets) werden derzeit nicht angeboten. Wird dafür künftig ein Druck- oder Versanddienstleister eingesetzt, kündigt der Auftragnehmer diesen vorher nach § 7 Abs. 3 an.

Abschluss

Abschluss durch Bestätigung im maintix-Dashboard; Zeitpunkt und Benutzer werden protokolliert.
Für den Auftragnehmer: Maximilian Schunk und Nick Schwenderling, Gesellschafter der Maintix.World
GbR.