

AUFTRAGSVERARBEITUNGSVERTRAG

AVV- RAHMEN

Rahmenbedingungen für B2B-Kunden gemäß Art. 28 DSGVO

1. Gegenstand und Umfang der Verarbeitung

Für den Betrieb der FurtherSales-Auktionslösung verarbeiten wir im Auftrag unserer Kunden personenbezogene Daten, beispielsweise von Bietern oder Nutzern der Plattform. Der AVV regelt insbesondere die Verarbeitung personenbezogener Daten im Auftrag, den Einsatz unserer technischen Infrastruktur, die Verpflichtungen von Further Sales als Auftragsverarbeiter, die Pflichten des Kunden als Verantwortlicher sowie technische und organisatorische Maßnahmen (TOM).

2. Kategorien betroffener Personen und Datenkategorien

- **Betroffene Personen:** Nutzer der Plattform, Bieter, Kunden-Mitarbeiter.
- **Datenkategorien:** Stammdaten, Kontaktdaten, Gebotsdaten, Transaktions- und Protokolldaten.

3. Technische und Organisatorische Maßnahmen (TOM)

Wir verpflichten uns zur Einhaltung angemessener technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko entsprechendes Schutzniveau zu gewährleisten. Diese Maßnahmen umfassen Schutzvorkehrungen in den Bereichen Zutritts- und Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle sowie Verfügbarkeit und Belastbarkeit.

ANLAGE 1: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Aktualisierte Fassung gemäß Anforderungen V3

Diese technischen und organisatorischen Maßnahmen beschreiben die Sicherheitsmaßnahmen der FurtherSales GmbH zur Gewährleistung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO. Die Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang und Zweck der Verarbeitung umgesetzt.

1. Zutrittskontrolle

Ziel: Verhinderung des unbefugten physischen Zugangs zu Systemen, auf denen personenbezogene Daten verarbeitet werden.

- Hosting der Plattform erfolgt über Cloud-Infrastruktur eines professionellen Hosting-Anbieters (Base44).
- Die physische Sicherheit der Rechenzentren wird durch den jeweiligen Cloud-Infrastrukturbetreiber gewährleistet.
- Rechenzentren verfügen über strenge Zugangskontrollen, Überwachungssysteme und physische Sicherheitsmaßnahmen.
- Zugriff auf Serverhardware durch FurtherSales selbst erfolgt nicht.

2. Zugangskontrolle

Ziel: Verhinderung der unbefugten Nutzung von IT-Systemen.

- Zugriff auf Administrationssysteme erfolgt ausschließlich durch autorisierte Personen.
- Der Zugriff auf das Base44-System sowie die Plattformadministration der Auktionssoftware erfolgt über gesicherte, personalisierte Benutzerkonten.
- Mehrfaktor-Authentifizierung (2FA) wird für kritische Systeme eingesetzt, insbesondere für Zahlungsdienste (Stripe) sowie administrative Zugänge.
- Alle Benutzerkonten sind passwortgeschützt.
- Zugangsdaten werden streng vertraulich behandelt und nicht an unbefugte Dritte weitergegeben.

3. Zugriffskontrolle

Ziel: Sicherstellung, dass berechtigte Benutzer nur auf die Daten zugreifen können, die sie für ihre jeweiligen Aufgaben benötigen.

- Der Zugriff auf personenbezogene Daten erfolgt ausschließlich durch autorisierte Personen im Rahmen ihrer Aufgaben und Berechtigungen.
- Der Zugriff auf Kundendaten durch Endnutzer erfolgt ausschließlich regelbasiert über die Plattformsoftware.
- Die Verwaltung der Plattformdaten erfolgt über ein rollenbasiertes Benutzerkonten- und Berechtigungssystem.
- Ein direkter, unkontrollierter Zugriff auf die zugrundeliegenden Datenbanken wird durch die Plattformarchitektur verhindert.

4. Weitergabekontrolle

Ziel: Verhinderung des unbefugten Übertragens, Kopierens oder Offenlegens personenbezogener Daten.

- Datenübertragung zwischen Browser und Plattform erfolgt über verschlüsselte HTTPS-Verbindungen (TLS).
- Kommunikation mit externen Diensten erfolgt über gesicherte API-Verbindungen.
- Weitergabe von Daten erfolgt streng zweckgebunden und ausschließlich im Rahmen der vertraglichen Leistungserbringung an beauftragte Dienstleister.
- Mit allen externen Dienstleistern (Unterauftragsverarbeitern) werden datenschutzkonforme Verträge zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen.

5. Eingabekontrolle

Ziel: Nachvollziehbarkeit von Datenverarbeitungen innerhalb der Systeme.

- Plattformsysteme protokollieren technische Systemereignisse und Fehlerlogs automatisiert.
- Systemlogs werden vom Hosting- und Plattformanbieter zweckgebunden zur Fehlersuche und Systemüberwachung gespeichert.
- Jegliche Änderungen an produktiven Plattformdaten können nur über authentifizierte und rückverfolgbare Benutzerkonten vorgenommen werden.

6. Auftragskontrolle

Ziel: Sicherstellung, dass Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

- Verarbeitung personenbezogener Daten erfolgt ausschließlich auf Grundlage des AVV und des Hauptvertrags.
- Subdienstleister werden sorgfältig nach datenschutzrechtlichen Kriterien ausgewählt und vertraglich gebunden.
- Die eingesetzten Unterauftragsverarbeiter werden im Rahmen der AVV-Dokumentation transparent offengelegt.

7. Verfügbarkeitskontrolle

Ziel: Schutz personenbezogener Daten vor Verlust oder Zerstörung.

- Hosting erfolgt über eine hochverfügbare, skalierbare Cloud-Infrastruktur.
- Die eingesetzten Plattform- und Hosting-Dienstleister verfügen über etablierte Verfahren zur Datensicherung und Wiederherstellung.
- Ergänzend können automatisierte Sicherungen von Plattformdaten erstellt und vorgehalten werden.
- Ein kontinuierliches Monitoring sowie Systemlogs unterstützen die frühzeitige Erkennung und Behebung technischer Störungen.

8. Trennungskontrolle

Ziel: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Die Verwaltung der Plattformdaten erfolgt logisch getrennt innerhalb der jeweiligen Anwendung bzw. Datenbankstruktur.
- Test- und Sandbox-Umgebungen sind technisch und logisch vollständig von der Live-Produktionsumgebung getrennt.
- Der Zugriff auf Produktionssysteme bleibt streng limitiert und erfolgt nur über gesonderte, autorisierte Administrationskonten.

9. Incident-Management und Sicherheitsvorfälle

Es bestehen strukturierte organisatorische Prozesse zur Behandlung von Sicherheitsvorfällen (unverzügliche Untersuchung und Bewertung, Einbindung der Hoster, gesetzeskonforme Meldung an Aufsichtsbehörden und Kunden gemäß Art. 33, 34 DSGVO).

10. Verschlüsselung und Transportsicherheit

Sämtliche Webzugriffe werden über zeitgemäße Transportverschlüsselung (HTTPS/TLS) abgesichert, API-Kommunikation ist gesichert und Passwörter werden ausschließlich als sichere kryptografische Hashes gespeichert.

11. Authentifizierung und Zugriffssicherheit

Alle administrativen Zugänge sind durch komplexe Kennwörter geschützt, für kritische Systeme (z. B. Stripe) ist die Nutzung von Mehrfaktor-Authentifizierung verpflichtend und Zugriffe erfolgen personengebunden über nachvollziehbare Benutzerkonten.

12. Überprüfung und Aktualisierung

Die technischen und organisatorischen Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst, um dauerhaft ein angemessenes Schutzniveau gemäß Art. 32 DSGVO zu gewährleisten.

ANLAGE 2: LISTE DER UNTERAUFTRAGSVERARBEITER

Stand: Januar 2026

Dienstleister & Kategorie	Zweck der Verarbeitung	Verarbeitete Datenkategorien
Base44 (Hosting & Infrastruktur)	Betrieb der Plattform, Speicherung von Plattformdaten, Sicherstellung der Systemverfügbarkeit, Backup- und Wiederherstellungsmechanismen, technische Protokollierung (Logfiles).	Plattformdaten, Benutzerkonten, Auktionsdaten, technische Log- und Metadaten.
Bidlogix Ltd. (Plattformtechnologie)	Betrieb der Auktionsplattform, Softwarewartung, Fehleranalyse, technische Weiterentwicklung.	Benutzerkonten, Gebots- und Auktionsdaten, technische Nutzungsdaten.
Brevo GmbH (E-Mail-Dienste)	Versand von Systemnachrichten, Registrierungsbestätigungen, Benachrichtigungen und transaktionsbezogenen E-Mails.	Name, E-Mail-Adresse, Kommunikationsinhalte, Zeitstempel und Versandinformationen.
Stripe Payments Europe Ltd. (Zahlungsdienstleister)	Abrechnung von Plattformgebühren, Zahlungsabwicklung, Rechnungsstellung, Betrugsprävention.	Zahlungsdaten, Kundendaten, Rechnungs- und Transaktionsdaten.
CCM19 (Papoo Software) (Cookie-Consent)	Ververwaltung von Cookie-Einwilligungen, Speicherung und Dokumentation von Einwilligungen gemäß Art. 7 Abs. 1 DSGVO.	IP-Adresse, Einwilligungsstatus, Zeitstempel, technische Browser-Informationen.

Hinweis zu Analyse-Diensten

Analyse-Dienste wie Google Analytics werden ausschließlich für die eigene Website-Analyse des Auftragsverarbeiters eingesetzt und erfolgen nicht im Auftrag des Verantwortlichen im Sinne von Art. 28 DSGVO. Sie sind daher nicht Bestandteil der Auftragsverarbeitung im Rahmen dieses AVV.

Aktualisierung der Liste

Der Auftragsverarbeiter kann Unterauftragsverarbeiter hinzufügen oder ändern, sofern der Verantwortliche hierüber vorab informiert wird und ihm ein angemessenes Widerspruchsrecht aus wichtigem datenschutzrechtlichem Grund eingeräumt wird.