DATA PROCESSING AGREEMENT (DPA FRAMEWORK) V3

Framework Conditions for B2B Customers pursuant to Art. 28 GDPR

1. Subject Matter and Scope of Processing

For the operation of the FurtherSales auction solution, we process personal data on behalf of our customers, for example from bidders or users of the platform. This DPA regulates in particular the processing of personal data on behalf, the use of our technical infrastructure, the obligations of FurtherSales as the Processor and obligations of the Customer as the Controller, as well as technical and organizational measures (TOM).

2. Categories of Data Subjects and Data Categories

- Data Subjects: Platform users, bidders, customer employees.
- Data Categories: Master data, contact data, bidding data, transaction and log data.

3. Technical and Organizational Measures (TOM)

We commit to complying with appropriate technical and organizational measures pursuant to Art. 32 GDPR to ensure a level of protection appropriate to the risk. These measures include safeguards in the areas of physical access control, system access control, data access control, transmission control, as well as availability and resilience.

ANNEX 1: TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

Updated Version according to V3 Requirements

These technical and organizational measures describe the security measures implemented by FurtherSales GmbH to ensure an appropriate level of protection pursuant to Art. 32 GDPR. The measures are implemented taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing.

1. Physical Access Control

Objective: To prevent unauthorized physical access to systems where personal data is processed.

- Hosting of the platform is carried out via the cloud infrastructure of a professional hosting provider (Base44).
- The physical security of the data centers is guaranteed by the respective cloud infrastructure operator.
- Data centers feature strict access controls, surveillance systems, and physical security measures.
- FurtherSales itself does not have physical access to the server hardware.

2. System Access Control

Objective: To prevent the unauthorized use of IT systems.

- Access to administration systems is strictly limited to authorized personnel.
- Access to the Base44 system and the platform administration of the auction software is granted via secured, personalized user accounts.
- Multi-factor authentication (2FA) is deployed for critical systems, particularly for payment services (Stripe) and administrative access.
- All user accounts are password-protected.
- Access credentials are treated with strict confidentiality and are not disclosed to unauthorized third parties.

3. Data Access Control

Objective: To ensure that authorized users can only access data that they require for their specific tasks.

- Access to personal data is restricted exclusively to authorized individuals within the scope of their assigned duties and permissions.
- End-user access to customer data is strictly rule-based and managed via the platform software.
- Platform data management relies on a role-based user account and authorization system.
- Direct, uncontrolled access to the underlying databases is prevented by the platform architecture.

4. Transmission Control

Objective: To prevent personal data from being unauthorizedly transmitted, copied, or disclosed.

- Data transmission between the browser and the platform is secured via encrypted HTTPS connections (TLS).
- Communication with external services is conducted via secured API connections.
- Data disclosure is strictly purpose-bound and occurs solely within the scope of contractual service delivery to commissioned service providers.
- Data processing agreements compliant with Art. 28 GDPR are concluded with all external service providers (sub-processors).

5. Input Control

Objective: To ensure the traceability of data processing activities within the systems.

- Platform systems automatically log technical system events and error logs.
- System logs are stored by the hosting and platform provider strictly for troubleshooting and system monitoring purposes.
- Any modifications to production platform data can only be executed via authenticated and traceable user accounts.

6. Job Control

Objective: To ensure that data is processed strictly in accordance with the instructions of the Controller.

- The processing of personal data is carried out exclusively on the basis of the DPA and the main contract.
- Sub-contractors are carefully selected and contractually bound based on data protection criteria.
- The engaged sub-processors are transparently disclosed within the scope of the DPA documentation.

7. Availability Control

Objective: To protect personal data against loss or destruction.

- Hosting is provided via a highly available, scalable cloud infrastructure.
- The deployed platform and hosting service providers maintain established data backup and recovery procedures.
- Automated backups may be created and retained in accordance with the backup procedures of the hosting and platform providers.
- Continuous monitoring and system logs support the early detection and remediation of technical disruptions.

8. Separation Control

Objective: To guarantee that data collected for different purposes are processed separately.

- Platform data is managed logically separated within the respective application or database structure.
- Testing and sandbox environments are technically and logically completely separated from the live production environment.
- Access to production systems remains strictly limited and is granted only via separate, authorized administrator accounts.

9. Incident Management and Security Incidents

Structured organizational processes are in place to handle security incidents (immediate investigation and assessment, involvement of the hosts, compliance-aligned notification to supervisory authorities and customers pursuant to Art. 33, 34 GDPR).

10. Encryption and Transport Security

All web access is safeguarded via up-to-date transport encryption (HTTPS/TLS), API communication is secured, and passwords are stored exclusively as secure cryptographic hashes.

11. Authentication and Access Security

All administrative access points are protected by complex passwords; the use of multi-factor authentication is mandatory for critical systems (e.g., Stripe), and access is user-specific via traceable accounts.

12. Review and Update

The technical and organizational measures are regularly reviewed for their effectiveness and adjusted as necessary to permanently ensure an appropriate level of protection pursuant to Art. 32 GDPR.

ANNEX 2: LIST OF SUB-PROCESSORS

Status: January 2026

Service provider & category	Purpose of processing	Processed data categories
Base44 (Hosting & Infrastructure)	Operation of the platform, storage of platform data, ensuring system availability, backup and recovery mechanisms, technical logging (log files).	Platform data, user accounts, auction data, technical log and metadata.
Bidlogix Ltd. (platform technology)	Operation of the auction platform, software maintenance, error analysis, technical development.	User accounts, bid and auction data, technical usage data.
Brevo GmbH (email services)	Sending system messages, registration confirmations, notifications and transaction-related emails.	Name, email address, communication content, timestamp and shipping information.
Stripe Payments Europe Ltd. (Payment service provider)	Billing of platform fees, payment processing, invoicing, fraud prevention.	Payment data, customer data, invoice and transaction data.
CCM19 (Papoo Software) (Cookie-Consent)	Management of cookie consents, storage and documentation of consents in accordance with Art. 7 para. 1 GDPR.	IP address, consent status, timestamp, technical browser information.

Note regarding analytics services

Analytics services such as Google Analytics are used exclusively for the data processor's own website analysis. These services are used and are not carried out on behalf of the controller within the meaning of Article 28 GDPR. They are therefore not part of the data processing agreement.

List update

The data processor may add or change sub-processors, provided that the data controller is informed about this. is informed in advance and is granted an appropriate right to object on important data protection grounds.