

Loops Data Processing Addendum (DPA)

Effective Date: July 2026

This Data Processing Addendum ("DPA") forms part of the Agreement between LYT Soft Inc. ("Loops", "Processor") and the Customer ("Controller") and governs Loops' processing of Personal Data on behalf of Customer.

Capitalized terms not defined herein have the meanings set forth in the Agreement.

1. Purpose and Scope

This DPA applies where Loops processes Personal Data on behalf of Customer in connection with the Services.

It supplements the Terms of Service and governs the processing of Customer Personal Data in accordance with applicable data protection laws, including the GDPR and UK GDPR where applicable.

2. Roles of the Parties

Customer acts as the **Controller** of Customer Personal Data.

Loops acts as the **Processor** of Customer Personal Data.

Loops shall process Personal Data only:

- On documented instructions from Customer;
 - As necessary to provide the Services;
 - As required by applicable law.
-

3. Customer Instructions

Customer instructs Loops to process Customer Personal Data for the following purposes:

- Providing the Services

- Aggregating and displaying review data
- Generating analytics and insights
- Providing AI-assisted features
- Providing customer support
- Ensuring system security and integrity

Customer is responsible for ensuring that its instructions comply with applicable law.

4. Confidentiality

Loops ensures that all personnel authorized to process Personal Data are bound by confidentiality obligations.

Access to Personal Data is limited to personnel who require access to perform their duties.

5. Security Measures

Loops implements and maintains technical and organizational security measures designed to protect Customer Data, appropriate to the nature and risk of the processing, including:

- Encryption of data in transit;
- Access controls and authentication mechanisms restricting access to Customer Data to authorized systems and personnel.

Loops maintains an ongoing security program and continues to develop additional safeguards, which may include role-based access restrictions, system monitoring and logging, secure infrastructure and hosting practices, and regular security updates and patching.

These measures are designed to provide a level of security appropriate to the risk. Loops does not guarantee that the Services or Customer Data will be free from all security incidents or unauthorized access.

6. Sub-processors

Customer authorizes Loops to engage third-party service providers and sub-processors to process Personal Data in connection with providing the Services.

Current sub-processors used by Loops are identified in the Loops Sub-processor List.

Loops will:

- Select sub-processors that are reasonably appropriate for the services they provide;
- Identify applicable sub-processors in the Sub-processor List;
- Maintain appropriate agreements or arrangements with sub-processors where required by applicable law.

Customer acknowledges that many sub-processors provide services under their own standard commercial terms, privacy policies, and data processing agreements, and that Loops does not control the technical, operational, or security practices of independent third-party providers.

Loops may update its Sub-processor List from time to time. Where required by applicable law, Loops will provide notice of material changes to sub-processors.

7. International Transfers

Loops uses cloud infrastructure hosted in Germany (European Union) and may engage authorized sub-processors located in Canada, the United States, the European Union, or other jurisdictions as necessary to provide the Services.

Where Customer Personal Data is transferred to a country that does not provide an adequate level of protection under applicable data protection laws, Loops will implement appropriate safeguards, including:

- European Commission Standard Contractual Clauses (SCCs)
 - UK International Data Transfer Addendum (where applicable)
 - Other lawful transfer mechanisms recognized under applicable data protection laws
-

10. Personal Data Breach

Loops shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

Such notification shall include, where possible:

- Nature of the breach
- Categories of data affected
- Likely consequences
- Measures taken or proposed

Customer is responsible for fulfilling any regulatory notification obligations.

12. Audit Rights

Loops shall make available information reasonably necessary to demonstrate compliance with this DPA.

Customer may request audits subject to:

- Reasonable notice
- Confidentiality obligations
- Operational and security constraints

Audits shall not unreasonably interfere with Loops' business operations.

13. Liability

Each party's liability under this DPA is subject to the limitation of liability provisions in the Terms of Service.

14. Annex I – Details of Processing

Subject Matter

Provision of the Loops SaaS platform for reputation management and review intelligence.

Duration

For the duration of the Agreement plus applicable retention periods.

Nature of Processing

- Collection
- Storage
- Organization
- Analysis
- Retrieval

- AI-assisted processing
- Display of Customer Personal Data

Purpose of Processing

- Providing the Services
- Generating insights and analytics
- AI-assisted review processing
- System monitoring and security

Categories of Data Subjects

- Customer account users
- Business administrators
- End customers and reviewers appearing in review content

Categories of Personal Data

- Names
- Email addresses
- Profile images
- Review content
- Ratings and metadata
- Authentication and usage data
- Billing-related identifiers (limited)

Special Categories of Data

Loops does not intentionally process special categories of personal data. However, such data may incidentally appear in free-text review content.

15. Annex II – Technical and Organizational Measures (TOMs)

Loops implements the following security measures:

1. Access Control

- Role-based access control
- Least-privilege permissions
- Authentication via secure login systems

2. Data Protection

- Encryption in transit (TLS)
- Encryption at rest (where supported by infrastructure providers)

3. Infrastructure Security

- Loops hosts the Services in a cloud environment and applies tenant isolation mechanisms designed to keep each Customer's data logically separated, including database-level access restrictions scoped to each Customer's organization.
- Loops continues to develop additional infrastructure safeguards over time, which may include additional network security controls and hardening measures.

4. Monitoring and Logging

- System activity logging
- Security monitoring and alerting
- Incident detection mechanisms

5. Data Integrity and Availability

- Backup systems
- Disaster recovery procedures
- Data redundancy where applicable

6. Sub-processor Controls

- Due diligence for vendors
- Contractual data protection obligations
- Ongoing vendor risk monitoring where feasible

16. Annex III – Sub-processors

Customer authorizes Loops to engage sub-processors listed in the Sub-processor List available at:

<https://loopsfeedback.com/legal/subprocessors>

Loops may update this list from time to time in accordance with the Agreement.