Agreement on Data Processing

between ReDem GmbH, Hafenstraße 47-51, 4020 Linz, FN 530708 d (hereinafter: “Processor”), and its customers, who use ReDem's web software to analyze and optimize the quality of surveys (hereinafter: “Controller”)

PREAMBLE

This agreement is an integral part of the General Terms and Conditions (GTC) concluded between the Processor and the Controller (Main Agreement). It becomes effective upon the conclusion of the Main Agreement and replaces all previous agreements on data processing between the parties.

1. SCOPE AND DEFINITIONS

1.1. This agreement governs the rights and obligations of the Controller and Processor (hereinafter: "Parties") regarding the processing of personal data.

1.2. This agreement applies to all activities in which the Processor's employees or subcontractors process personal data on behalf of the Controller.

1.3. Terms used in this agreement are to be understood as defined in the EU General Data Protection Regulation (Regulation [EU] 2016/679 – GDPR).

2. SUBJECT AND DURATION OF PROCESSING

2.1. Tasks
The subject of this agreement is the execution of the following tasks by the Processor:

- Analysis and optimization of survey quality using web software.

2.2. Processing Subject
This agreement pertains to the processing of the following categories of personal data by the Processor:

- Imported or uploaded content and data from the Controller.

The following categories of individuals are affected by the data processing:

- Customers of the Controller.

2.3. Purpose of Processing
Personal data will be processed by the Processor for the following purposes:

- Analysis of survey data quality.
- Data cleansing.

2.4. Processing Location
The Processor generally processes personal data within the EU/EEA. Any transfers to third countries will be conducted solely based on Articles 44 et seq. of the GDPR.

2.5. Duration

Unless expressly agreed otherwise, the term of this agreement corresponds to the term of the Main Agreement.

3. OBLIGATIONS OF THE PROCESSOR

3.1. The Processor confirms its awareness of the relevant data protection regulations and adheres to the principles of proper data processing.

3.2. The Processor commits to processing personal data exclusively based on the instructions of the Controller and this agreement, ensuring compliance with all data protection regulations.

3.3. Should the Processor deem an instruction from the Controller unlawful, it must immediately inform the Controller in writing.

3.4. The Processor will implement all appropriate technical and organizational measures as outlined in Article 32 of the GDPR to ensure the security of data processing.

3.5. The Processor will assist the Controller in responding to requests from data subjects regarding their rights. If such a request is directed to the Processor, it will immediately forward it to the Controller.

3.6. The Processor will support the Controller in fulfilling obligations under Articles 32 to 36 of the GDPR, particularly regarding security measures, notification of data breaches, and the preparation of data protection impact assessments.

3.7. Upon the termination of processing or at the request of the Controller, the Processor must delete or return all personal data in its possession.

3.8. The Processor will provide all details necessary for demonstrating compliance with Article 28 GDPR and will assist the Controller in conducting audits.

3.9. The Processor maintains a written or electronic record of all categories of processing activities carried out on behalf of the Controller as required by Article 30(2) GDPR.

3.10. The Processor commits to appointing a qualified Data Protection Officer under Article 37 GDPR, if applicable.

3.11. The Processor must handle all personal data disclosed or made available to it with confidentiality. This obligation extends to any processing outcomes.

4. OBLIGATIONS OF THE CONTROLLER

4.1. The Controller is responsible for the lawful collection, processing, and transfer of data to the Processor and indemnifies the Processor in this respect.

5. TECHNICAL AND ORGANIZATIONAL MEASURES

5.1. The security measures described in Annex 2 are binding and define the minimum owed by the Processor.

5.2. The Processor must implement appropriate measures to ensure an adequate level of data protection.

5.3. The Processor will inform the Controller about measures before commencing processing.

5.4. The Processor regularly reviews the adequacy of implemented measures and informs the Controller of significant changes.

6. CORRECTION, DELETION, AND BLOCKING OF DATA

6.1. The Processor processes data corrections, deletions, or restrictions as instructed by the Controller.

7. SUB-PROCESSORS

7.1. The Controller explicitly consents to the use of sub-processors listed in Annex 1.

7.2. The Processor remains liable for any breaches of obligations by sub-processors.

8. NOTIFICATION OBLIGATIONS

8.1. The Processor will promptly notify the Controller of any data breaches or significant disruptions.

9. INSTRUCTIONS

9.1. The Controller retains a comprehensive right to issue instructions regarding processing.

10. TERMINATION

10.1. Upon termination of this agreement, the Processor will delete or return all data as instructed by the Controller.

11. COMPENSATION

11.1. The Processor may charge for services related to this agreement at the applicable hourly rate.

12. CONFIDENTIALITY

12.1. Both parties agree to maintain the confidentiality of information obtained during this agreement.

13. MISCELLANEOUS

13.1. This agreement is governed by Austrian law, with the exclusive jurisdiction of the competent court in Linz.

Data Processing Table

Recipient	Purpose	Legal Basis for Transfer	Location of Data Processing	Basis for Transfer to a Third Country
Amazon Web Services (AWS)	IT infrastructure and data storage	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Frankfurt, Germany	No third-country transfer
Atlassian Corporation plc	Improvement of workflows, promotion of collaboration, increase in productivity	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	London, United Kingdom	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures
Brevo (Sendinblue GmbH)	Creation of email, SMS, and chat campaigns; managing leads, customer relationships, and marketing automation	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Berlin, Germany	No third-country transfer
Dr. Sebastian Berger	Business consulting	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional consulting services for business development	Krems, Austria	No third-country transfer
Google Cloud EMEA Limited	Collaboration, communication, email, document processing, and file storage	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT	USA, with data stored in the EU	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures; see: https://cloud.google.com/terms/data-processing-addendum/

		infrastructure		
Google LLC	Analysis of user behavior on our website	Consent (§ 165(3) TKG 2021, Art. 6(1)(a) GDPR): Analysis of user behavior to improve our web presence	USA	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures and explicit consent via cookie banner (Art. 49(1)(a) GDPR)
Hetzner Online GmbH	Use of professional IT infrastructure	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Gunzenhausen, Germany, data stored in Germany	No third-country transfer
HubSpot, Inc.	Marketing (e.g., re-identification of users for the purpose of personalized advertising); organization management	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Cambridge, USA	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures and explicit cookie consent
Insighture Pty Ltd.	Product development and technical support	Performance of a contract (Art. 6(1)(f) GDPR)	Australia, data stored in the EU	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures
Kickscale GmbH	Optimization of sales processes through data-driven insights and task automation	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Vienna, Austria, data stored in the EU	No third-country transfer
LinkedIn Ireland Unlimited	Display of profile content on the website for advertising	Consent (§ 165(3) TKG 2021, Art. 6(1)(a) GDPR): Analysis of	EU (Ireland) and transfer to US affiliates	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures and explicit consent via cookie banner (Art. 49(1)(a) GDPR)

	purposes; user identification for targeted advertising	user behavior to improve our web presence		
Microsoft Azure	IT infrastructure	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Redmond, Washington, USA	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures
OpenAI LLC	Conducting quality checks using GPT-4 for categorizing and evaluating responses	Performance of a contract (Art. 6(1)(f) GDPR)	San Francisco, USA	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures*
Raml und Partner Steuerberatung GmbH	Tax consulting	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional consulting services in tax and regulatory matters	Linz, Austria	No third-country transfer
Rechtsanwaltskanzlei Bisset	Legal consulting	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional consulting services in legal matters	Mannersdorf am Leithagebirge, Austria	No third-country transfer
sevdesk GmbH	Management of accounting tasks	Legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Offenburg, Germany	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures

Truendo Technologies GmbH	Privacy-compliant design of websites and apps	Performance of a contract and legitimate interests (Art. 6(1)(f) GDPR): Use of professional IT infrastructure	Vienna, Austria	Standard contractual clauses (Art. 46(2)(c) GDPR) with supplementary measures

***Appropriate complementary measures to ensure the protection of personal data following the CJEU's Schrems II decision for OpenAI LLC:**

- Open-ended responses are transmitted individually, each with a fully anonymized ID, to the sub-processor. The sub-processor receives only single responses per API call and never the complete survey.
- The processor acts as the sole user towards the sub-processor. The sub-processor does not, at any point, learn the origin of the transmitted data.
- Data sent by the processor via the API is stored by the sub-processor for a maximum of 30 days and is then completely and irreversibly deleted. The data is not used for training AI models.

ANNEX 2 – TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

1. Confidentiality

The processor ensures that the confidentiality of personal data is maintained at all times. In particular, the following measures are implemented:

- **Access Control**: Regulated key management, security doors, security personnel, or other access barriers to data processing facilities.
- **System Access Control**: Protection of data processing systems through passwords, automatic locking mechanisms, two-factor authentication, encryption of storage media, VPN, and logging of user logins.
- **Data Access Control**: Access to data is managed via authorization profiles based on the "need-to-know" principle, partial access permissions, and logging of access activities.
- **Pseudonymization**: Personal data is pseudonymized where possible.
- **Data Classification**: Data is classified as secret, confidential, internal, or public.
- **Separation of Processing**: Processing for different purposes is performed through separate databases, tenant separation, or distinct servers.

2. Integrity

The processor ensures the integrity of personal data is guaranteed. The following measures are implemented:

- **Transmission Control**: Protection against unauthorized access, copying, alteration, or removal of data during transmission, e.g., through encryption, VPN, ISDN-wall, content filters, or electronic signatures.
- **Input Control**: Ensuring traceability of who entered, modified, or deleted data in the system through logging and electronic signatures.

3. Availability and Resilience

The processor ensures that systems comply with industry standards and state-of-the-art technology. Measures include:

- **Availability**: Safeguards against data loss or destruction, such as safes, secure cabinets, storage networks, software and hardware protection, and regular backups.
- **Resilience**: Measures to protect against technical attacks and ensure smooth operations even during unforeseen stress.

4. Procedures for Regular Review, Assessment, and Evaluation

The processor's technical and organizational measures are regularly reviewed, assessed, and evaluated. The processor permits the controller or an appointed expert to audit security measures.