Data Processing Agreement

qualcode.ai

Version: 1.0
Effective Date: January 2026

AI Research & Technology Lab GmbH
Enzersdorfer Strasse 25
A-2340 Modling, Austria

Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Terms of Service between you ("Controller", "Customer") and AI Research & Technology Lab GmbH ("Processor", "qualcode.ai", "we") for the provision of the qualcode.ai service.

This DPA reflects the requirements of Article 28 of the General Data Protection Regulation (GDPR) and applies to the processing of personal data that you, as data controller, entrust to us for processing.

1 Definitions

- **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.
- **"Processing"** means any operation performed on Personal Data, as defined in Article 4(2) GDPR.
- **"Data Subject"** means the individual to whom Personal Data relates (in this context, typically your survey respondents).
- **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **"Customer Data"** means the survey responses, coding guides, and related data you upload to the Service.

2 Scope and Roles

2.1 Controller

You are the Controller for all Customer Data you upload to the Service. You determine the purposes and means of processing survey respondent data.

2.2 Processor

We are the Processor for Customer Data. We process this data solely to provide the Service to you, in accordance with your documented instructions.

2.3 Our Own Processing

For data we collect directly (your account information, usage data), we are the Controller. See our Privacy Policy for details.

3 Details of Processing

Subject matter	AI-assisted classification of open-ended survey responses
Duration	For the duration of your use of the Service, plus retention periods specified in Section 8
Nature of processing	Storage, transmission to AI services for classification, aggregation, export

Purpose	To provide qualitative coding services as described in the Terms of Service
Categories of Data Subjects	Survey respondents whose responses you upload
Types of Personal Data	Free-text survey responses, which may contain any personal data you choose to upload

4 Controller Obligations

As Controller, you are responsible for:

- Ensuring you have a valid legal basis for processing respondent data (consent, legitimate interest, etc.)
- Providing appropriate privacy notices to Data Subjects, including disclosure of AI processing
- Responding to Data Subject requests (we will assist as described in Section 6)
- Ensuring uploaded data complies with applicable laws
- Not uploading special category data (Article 9 GDPR) without explicit consent and appropriate safeguards
- Implementing appropriate anonymization or pseudonymization where feasible

5 Processor Obligations

We commit to the following obligations:

5.1 Processing Instructions

We will process Customer Data only on your documented instructions, unless required by EU or Austrian law. The Service's standard operation constitutes your instructions. If we believe an instruction violates GDPR, we will inform you.

5.2 Confidentiality

All personnel processing Customer Data are bound by confidentiality obligations.

5.3 Security Measures

We implement appropriate technical and organizational measures including:

- Encryption of data in transit (TLS) and at rest
- Access controls and authentication requirements
- Secure development practices
- Physical security at hosting facilities (AWS Frankfurt data center)

5.4 Sub-processors

We may engage Sub-processors to assist in providing the Service. The current list is in Section 7. We will:

- Maintain written contracts with Sub-processors imposing equivalent data protection obligations

- Notify you of any intended changes to Sub-processors with at least 30 days' notice
- Provide you with the opportunity to object to new Sub-processors
- Remain liable for Sub-processor compliance

5.5 Data Subject Rights

We will assist you in responding to Data Subject requests (access, rectification, erasure, etc.) by:

- Providing you with tools to export and delete data
- Promptly informing you of any requests received directly
- Providing relevant information upon request

5.6 Data Protection Impact Assessments

We will provide reasonable assistance if you need to conduct a DPIA for your processing activities.

6 Data Subject Requests

If we receive a request from a Data Subject regarding Customer Data, we will:

1. Notify you without undue delay
2. Not respond directly unless required by law or with your authorization
3. Provide you with information needed to respond

You can fulfill most requests directly through the Service interface (export data, delete projects, etc.).

7 Sub-processors

We use the following Sub-processors for Customer Data:

Sub-processor	Purpose	Location	Transfer Mechanism
Amazon Web Services EMEA SARL	Infrastructure hosting (servers, storage, databases)	Frankfurt, Germany (eu-central-1)	EU-based, no transfer
OpenAI, Inc.	AI classification (Rater A)	USA	EU Standard Contractual Clauses
Anthropic, PBC	AI classification (Rater B)	USA	EU Standard Contractual Clauses
Stripe, Inc.	Payment processing	Ireland/USA	EU Standard Contractual Clauses
Resend, Inc.	Transactional email	USA	EU Standard Contractual Clauses

7.1 AI Sub-processor Details

Survey data sent to OpenAI and Anthropic for classification:

- Is transmitted via encrypted connections
- Is processed transiently and not used for model training. OpenAI and Anthropic may retain request logs for abuse detection (up to 30 days) per their API terms.
- Is not used to train their AI models
- Is subject to their data processing agreements with us

7.2 Changes to Sub-processors

We will notify you via email of any intended addition or replacement of Sub-processors at least 30 days before the change takes effect. You may object in writing within 14 days. If we cannot reasonably accommodate your objection, either party may terminate the affected services.

8 Data Retention and Deletion

8.1 During Service

Customer Data is retained while your account is active. You can delete individual projects or data files at any time through the Service interface. Deleted data enters a 30-day trash period, then is permanently deleted.

8.2 Upon Termination

When you close your account or we terminate the Service:

- You have 30 days to export your data
- After 30 days, we will delete or anonymize all Customer Data
- We may retain data as required by law (e.g., audit logs for 7 years per Austrian tax law)
- Accounts with credit transaction history are soft-deleted (deactivated) rather than fully deleted to maintain financial audit integrity; personal identifiable information in such accounts is anonymized

8.3 Deletion Confirmation

Upon request, we will provide written confirmation that Customer Data has been deleted, except for legally required retention.

9 Data Breach Notification

In the event of a Personal Data breach affecting Customer Data, we will:

1. **Notify you** without undue delay, and where feasible within 72 hours of becoming aware
2. **Provide details** including:
   - Nature of the breach
   - Categories and approximate number of affected Data Subjects
   - Likely consequences
   - Measures taken or proposed to address the breach
3. **Cooperate** with your investigation and any regulatory notification
4. **Document** the breach and remediation for audit purposes

10 Audit Rights

You have the right to audit our compliance with this DPA. We will:

- Make available information necessary to demonstrate compliance
- Allow for and contribute to audits conducted by you or an independent auditor

Audits shall be conducted with reasonable notice (at least 7 business days), during business hours, and in a manner that minimizes disruption. You shall bear your own audit costs.

11 International Transfers

Customer Data is primarily stored in the EU (Frankfurt, Germany). When transferred to the USA (for AI processing), we rely on:

- **Standard Contractual Clauses (SCCs)** - EU Commission approved (Commission Implementing Decision 2021/914), Module 2 (Controller to Processor) and Module 3 (Processor to Processor) as applicable
- **Supplementary measures** including encryption and contractual commitments from processors

We conduct Transfer Impact Assessments (TIAs) to evaluate and document the risks of international transfers. Our TIA document is available at qualcode.ai/tia and provides detailed analysis of the legal framework and supplementary measures for each sub-processor.

12 Liability

Each party's liability under this DPA is subject to the limitations set out in the Terms of Service, except that these limitations do not apply to:

- Breaches of confidentiality obligations
- Violations of applicable data protection laws
- Indemnification obligations

13 Term and Termination

This DPA remains in effect for the duration of your use of the Service. Upon termination:

- Sections 8 (Retention and Deletion), 10 (Audit Rights), and 12 (Liability) survive
- We will fulfill our deletion obligations as specified in Section 8

14 Governing Law

This DPA is governed by Austrian law. For disputes, the courts of Modling, Austria shall have exclusive jurisdiction.

15 Contact

For questions or requests regarding this DPA, contact:

AI Research & Technology Lab GmbH
Attn: Data Protection
Enzersdorfer Strasse 25
A-2340 Modling
Austria
Email: legal@qualcode.ai

By using the Service, you acknowledge that you have read, understood, and agree to this Data Processing Agreement.

Annex 1: Processing Details

This Annex provides detailed information about the processing of Personal Data under this DPA.

1 Categories of Data Subjects

Category	Description
Survey Respondents	Individuals who have participated in surveys conducted by the Controller and whose free-text responses are uploaded to the Service
Customer Users	Employees or representatives of the Controller who access and use the Service

2 Types of Personal Data Processed

Data Type	Description
Free-text survey responses	Open-ended answers provided by survey respondents, which may contain names, opinions, experiences, or other personal information
Respondent identifiers	Any identifiers included in uploaded data files (e.g., respondent IDs, demographic information)
Coding results	AI-generated classifications and codes applied to survey responses
Project metadata	Project names, coding guide categories, file names, timestamps

3 Processing Activities

Activity	Description
Storage	Secure storage of uploaded data files and processing results in EU-based infrastructure
AI Classification	Transmission of survey responses to AI providers for automated classification
Aggregation	Compilation of coding results and agreement metrics

Export	Generation of downloadable result files for the Controller
Display	Presentation of data and results through the Service interface

4 Sensitive Data

The Controller should avoid uploading special categories of personal data as defined in Article 9 GDPR (racial or ethnic origin, political opinions, religious beliefs, health data, etc.) unless:

- Explicit consent has been obtained from Data Subjects
- Appropriate safeguards are in place
- Processing is otherwise lawful under Article 9(2) GDPR

Annex 2: Technical and Organizational Measures

This Annex describes the technical and organizational security measures implemented by the Processor in accordance with Article 32 GDPR.

1 Encryption

Measure	Implementation
Data in Transit	All data transmitted over networks is encrypted using TLS. HTTPS is enforced for all web traffic. API calls to sub-processors use encrypted connections.
Data at Rest	Stored data is encrypted at the infrastructure level using industry-standard encryption.

2 Access Control

Measure	Implementation
Authentication	Password requirements, secure session management, HTTPS-only cookies.
Authorization	Role-based access control. Users can only access their own data. Administrative access is restricted.
Principle of Least Privilege	Staff access to production systems is limited to essential personnel only.

3 Infrastructure Security

Measure	Implementation
Hosting	AWS Frankfurt (eu-central-1) data center located within the European Union.
Network Security	Security groups and firewall rules restrict access to necessary ports and services.

4 Data Integrity and Availability

Measure	Implementation
Backups	Regular automated backups of Customer Data.
Monitoring	Infrastructure monitoring to detect and respond to issues.

5 Organizational Measures

Measure	Implementation
Confidentiality	Personnel with access to Customer Data are bound by confidentiality obligations.
Vendor Management	Contractual data protection requirements for sub-processors.
Secure Development	Security-conscious software development practices and code reviews.
Audit Logging	Comprehensive access logs for authentication events, admin actions, and data exports. Logs retained for 90 days for security monitoring and incident response.

6 Data Separation

- Customer Data is logically separated by customer account
- Each customer can only access their own projects and data
- Administrative access is restricted to essential personnel
- No cross-customer data access is possible through the application

Annex 3: Approved Sub-Processors

This Annex lists all approved Sub-processors as of the effective date of this DPA.

1 Amazon Web Services EMEA SARL

Legal Entity	Amazon Web Services EMEA SARL
Address	38 Avenue John F. Kennedy, L-1855 Luxembourg
Purpose	Cloud infrastructure hosting including compute, storage, and database services
Data Location	Frankfurt, Germany (eu-central-1 region)
Transfer Mechanism	EU-based processing, no international transfer
Certifications	ISO 27001, SOC 1/2/3, PCI DSS, GDPR compliant

2 OpenAI, Inc.

Legal Entity	OpenAI, Inc.
Address	3180 18th Street, San Francisco, CA 94110, USA
Purpose	AI-powered text classification (Rater A in dual-rater methodology)
Data Location	United States
Transfer Mechanism	EU Standard Contractual Clauses (Commission Decision 2021/914)
Data Retention	Transient processing only; data not retained or used for training

3 Anthropic, PBC

Legal Entity	Anthropic, PBC
Address	548 Market Street, PMB 90375, San Francisco, CA 94104, USA
Purpose	AI-powered text classification (Rater B in dual-rater methodology)

Data Location	United States
Transfer Mechanism	EU Standard Contractual Clauses (Commission Decision 2021/914)
Data Retention	Transient processing only; data not retained or used for training

4 Stripe, Inc.

Legal Entity	Stripe, Inc.
Address	354 Oyster Point Blvd, South San Francisco, CA 94080, USA
EU Entity	Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Dublin 2, Ireland
Purpose	Payment processing and subscription management
Data Location	Ireland (primary), United States (backup)
Transfer Mechanism	EU Standard Contractual Clauses (Commission Decision 2021/914)
Note	Processes payment data only; does not process Customer survey data

5 Resend, Inc.

Legal Entity	Resend, Inc.
Address	2261 Market Street 4012, San Francisco, CA 94114, USA
Purpose	Transactional email delivery (account notifications, password resets)
Data Location	United States
Transfer Mechanism	EU Standard Contractual Clauses (Commission Decision 2021/914)
Note	Processes email addresses and notification content only; does not process Customer survey data

6 Changes to Sub-Processors

The Controller will be notified via email at least 30 days before any changes to this list take effect. The Controller may object to changes in accordance with Section 7.2 of this DPA.

End of Data Processing Agreement