

Data Processing Agreement — Qualiteam.ai

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

[CUSTOMER COMPANY NAME]

[CUSTOMER ADDRESS]

[CUSTOMER CITY, POSTAL CODE, COUNTRY]

(the "**Company**") and

Anton Riabykh

Pere IV 201

Barcelona, 08018, Spain

Email: legal@qualiteam.ai

Trading as: Qualiteam.ai

(the "**Data Processor**")

(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Company Personal Data**" means any Personal Data Processed by an Authorised Subprocessor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Authorised Subprocessor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means the GDPR and any national data protection laws of EU Member States implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Company Personal Data from the Company to an Authorised Subprocessor; or

1.1.8.2 an onward transfer of Company Personal Data from an Authorised Subprocessor to a Subcontracted Processor, or between two establishments of an Authorised Subprocessor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the AI-powered customer support conversation evaluation and analysis services provided via the Qualiteam.ai platform, including conversation analysis, performance evaluation, criteria-based assessment, and AI-powered insights;

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement;

1.1.11 "**LLM Providers**" means artificial intelligence and large language model service providers including but not limited to OpenAI, Google, and other AI service providers used for conversation analysis and evaluation;

1.1.12 "**Conversation Data**" means customer support conversations, chat transcripts, agent identifiers, evaluation results, and related metadata processed through the Services;

1.1.13 "**Evaluation Services**" means the AI-powered analysis, scoring, and assessment of customer support conversations against defined criteria and rules.

1.1.14 "**Analytics Service**" means Google Analytics 4 used to measure website usage on Qualiteam.ai web properties.

1.2 The terms, "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data for the purposes of providing the Services.

2.3 **Processing Details:**

2.3.1 **Categories of Personal Data:** The personal data processed may include:

- Customer support conversation transcripts and content
- Customer names, email addresses, and identifiers contained within conversations
- Support agent names and identifiers
- Conversation metadata (timestamps, channel information, conversation IDs)
- Evaluation results and performance metrics

2.3.2 **Categories of Data Subjects:** The data subjects whose personal data may be processed include:

- End customers seeking support
- Customer support agents
- Other employees involved in customer service interactions

2.3.3 **Data Exclusions:** The Processor will ignore, exclude, or redact any payment card data (PCI-DSS), health information, or other special category personal data that may inadvertently appear in conversations, and does not intentionally process such data.

2.3.4 **Purposes of Processing:**

- Analysis and evaluation of customer support conversations
- Performance assessment against defined criteria and rules
- Generation of insights and recommendations for service improvement
- AI-powered conversation scoring and analysis
- Integration with third-party platforms (such as Intercom)
- Website analytics and performance measurement (limited to website usage data)

2.3.5 **Data Sources:** Personal data is primarily obtained from customer support platforms, including but not limited to Intercom, Zendesk, Salesforce Service Cloud, and other customer service platforms, as well as voice-call transcripts and chat systems. For website analytics, usage data is obtained from the Qualiteam.ai website and related web properties.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Authorised Subprocessor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Authorised Subprocessor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3 **Specific Security Measures:** The Processor implements the following security measures:

- Encryption of personal data in transit (via HTTPS/TLS 1.2+) and at rest
- Access controls and authentication mechanisms for platform access
- Secure API integrations with LLM Providers via encrypted channels
- Secure data storage and backup procedures
- Incident response procedures for data breaches
- Data processing infrastructure hosted in EU regions (DigitalOcean)

4.4 **Ongoing Security Improvements:** The Processor is committed to continuously improving security measures and may implement additional safeguards including monitoring tools, vulnerability assessments, and enhanced data protection measures as the business grows.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

5.2 **Approved Subprocessors:** The Company hereby provides general authorization for the Processor to engage the following Subprocessors:

Subprocessor	Service	Data Processing Location
OpenAI	AI/LLM processing services	United States (covered by Standard Contractual Clauses)
Google AI	AI/LLM processing services	European Union
DigitalOcean	Infrastructure and data storage	European Union regions (unless Customer specifically requests US regions)
Intercom	Customer support platform integration	European Union / United States (as per Customer's Intercom configuration)

5.2.1 **DigitalOcean Regions:** Data storage via DigitalOcean will remain within EU regions unless the Customer specifically requests and authorizes processing in non-EU regions.

5.3 **New Subprocessors:** The Processor may engage additional LLM Providers or technical service providers necessary for the Services, provided that:

- The Company is notified at least 30 days in advance
- The new Subprocessor is bound by equivalent data protection obligations
- The Company has the right to object to the engagement within the notification period
- If the Company reasonably objects to a new Subprocessor, the Company may terminate the affected Services or this Agreement with 30 days' written notice

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, and in any case within 24 hours of discovery, to facilitate the

Company's 72-hour notification obligation under GDPR Article 33. The notification shall provide Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 **Article 28(3) Compliance:** The Processor shall assist the Controller in ensuring compliance with Articles 32-36 of the GDPR, taking into account the nature of processing and the information available to the Processor.

8. Data Protection Impact Assessment and Prior Consultation

8.1 Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

8.2 **Article 28(3) Compliance:** The Processor shall assist the Controller in ensuring compliance with Articles 32-36 of the GDPR, including data protection impact assessments and prior consultations with supervisory authorities.

9. Deletion or Return of Company Personal Data

9.1 **Data Retention During Services:** During the term of this Agreement, personal data will be retained for a maximum period of 1 year from the date of initial processing, unless:

- Required by applicable law to be retained for a longer period; or
- The Company requests earlier deletion in writing.

9.2 **Deletion Upon Service Termination:** Subject to this section 9, Processor shall promptly and in any event within 30 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

9.3 **Deletion Upon Request:** The Company may request deletion of specific personal data at any time during the provision of Services, and the Processor shall comply within 30 days of such written request, except where retention is required by applicable law.

9.4 **Deletion Methods:** Deletion will be performed through secure deletion methods including permanent removal from databases, secure erasure from storage systems, and removal from backup systems in accordance with standard data destruction practices.

10. Audit Rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to information requests and documentation reviews, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Processor.

10.2 **Audit Frequency and Notice:** Audits conducted under section 10.1 shall be limited to once per 12-month period, unless there has been a Personal Data Breach or other security incident. The Company shall

provide the Processor with at least 14 days' written notice before conducting any audit.

10.3 **Audit Costs:** Audits shall be conducted at the Company's expense, unless the audit reveals a material breach of this Agreement by the Processor, in which case the Processor shall bear the reasonable costs of the audit.

10.4 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected.

11.2 **Approved Data Transfers Outside EEA:** The Company hereby consents to the following data transfers outside the EEA:

- **OpenAI (United States):** For AI/LLM processing services, covered by Standard Contractual Clauses (Module 2 - Controller to Processor transfers), with the Processor acting as "data importer"
- **Intercom (United States):** Only when Customer's own Intercom account is configured with US data residency

11.3 **EU-Only Processing:** The following subprocessors process data within the EEA only:

- **Google AI:** Processing within European Union
- **DigitalOcean:** EU regions only (Frankfurt, Amsterdam) unless Customer specifically authorizes US regions

11.4 **Standard Contractual Clauses:** For transfers outside the EEA, the Parties rely on EU approved Standard Contractual Clauses (Decision 2021/914) Module 2, with the Processor accepting its role as "data importer" under Annex I of the SCCs.

11.5 **Future Transfer Mechanisms:** The Processor may utilize the EU-US Data Privacy Framework or other adequacy decisions that may become available, provided they remain valid and legally binding, and will notify the Company of any changes to transfer mechanisms.

12. General Terms

12.1 **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law; (b) the relevant information is already in the public domain.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

12.3 **Data Protection Contact.** For all matters relating to data protection under this Agreement, the Company may contact Anton Riabykh directly at the contact details provided in the header of this Agreement.

12.4 **Liability Limitation.** The liability of each Party under this Agreement shall be subject to the liability limitations set forth in the Principal Agreement, if any.

12.5 **Order of Precedence.** In case of any conflict between this DPA and the Principal Agreement, this DPA shall prevail with respect to data protection matters.

13. AI-Specific Provisions

13.1 **AI Processing Transparency.** The Company acknowledges that:

- AI/LLM outputs are probabilistic in nature and may contain inaccuracies
- The Company must apply appropriate human oversight and review of AI-generated evaluations
- AI processing may not be deterministic and results may vary between processing runs

13.2 **EU AI Act Compliance.** The Processor will provide reasonable assistance to help the Company comply with applicable AI regulations, including:

- Documentation of AI models and processing methods used
- Logs of AI processing activities as technically feasible
- Information about AI system capabilities and limitations

14. Governing Law and Jurisdiction

14.1 This Agreement is governed by the laws of **Spain**.

14.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of **Barcelona, Spain**, subject to possible appeal to **the Spanish Supreme Court**.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

[CUSTOMER COMPANY NAME]

Signature: _____

Name: _____ Title: _____ Date Signed: _____

Anton Riabykh (Qualiteam.ai)

Signature: _____

Name: **Anton Riabykh**

Title: **Data Processor / Business Owner**

Date Signed: _____