Data Processing Agreement

Kaizan Limited · Last updated 7 August 2026 · kaizan.ai/data-processing-agreement/

THIS AGREEMENT is dated from the activation of the License Agreement ("**Agreement**")

BETWEEN:

(1) **KAIZAN LIMITED** incorporated and registered in England and Wales with company number 13082820 whose registered office is at Runway East, 189 Shaftesbury Avenue, London, England, WC2H 8JR ("**Processor**").

(2) the party entering into a licence agreement for the use of Kaizan AI software("**Controller**"); and

collectively the, "**Parties**" and each a, "**Party**".

BACKGROUND

This Agreement is intended to ensure that Controller and the Processor comply with applicable Data Protection Laws.

AGREED TERMS

1. INTERPRETATION

1.1 In this Agreement, the following capitalised terms shall have the meanings set out below:

Applicable Laws	the laws of England and Wales and any other laws which apply to Controller Personal Data;
Controller Personal Data	any Personal Data of Controller Processed by Processor;
Data Protection Laws	1. To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data. 2. To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Controller or Processor is subject, which relates to the protection of personal data.
EEA	the European Economic Area;
EU Data Protection Laws	the GDPR and laws implementing or supplementing the GDPR (including the Data Protection Act 2018) and EU Directive 2002/58/EC, as transposed into domestic legislation of the UK and each Member State and as amended, replaced or superseded from time to time;
EU GDPR	EU General Data Protection Regulation 2016/679;
Licence Agreement	an agreement under which the Processor licenses the use of its Kaizan AI software to the Controller made pursuant to the terms of service found here: https://kaizan.ai/license-agreement/
Personal Data	means any information relating to an identified or identifiable living individual that is processed by the Processor on behalf of the Controller as a result of, or in connection with, the provision of the services under the Licence Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

Personal Data Breach	a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data;
Services	the services supplied to or carried out by (or on behalf of) Processor for Controller from time to time;
Restricted Transfer	A transfer of Personal Data from the UK to any country outside of the UK that has not received an adequacy decision from the United Kingdom Secretary of State. Where such transfers occur under this Agreement, the parties shall implement appropriate safeguards, which may include the UK International Data Transfer Agreement (IDTA) or other valid transfer mechanisms under UK GDPR
Transfer Mechanism	means the UK International Data Transfer Agreement (IDTA) issued by the UK Information Commissioner's Office on 21 March 2022, the UK Addendum to the EU Standard Contractual Clauses, or any other appropriate safeguard recognised under Article 46 of the UK GDPR for transfers of personal data to countries outside the UK;
Subprocessor	any person or entity (excluding an employee of the Processor) appointed by or on behalf of the Processor to Process Personal Data on behalf of Controller or otherwise in connection with the provision of the Services;
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 The terms, "**Commission**", "**Data Subject**", "**Member State**", "**Processing**" and "**Supervisory Authority**" shall have the meanings given to them in the Data Protection Laws. In the event of any discrepancy between the terms of the EU GDPR and the UK GDPR, the UK GDPR will apply.

1.3 By entering into the Licence Agreement, agreeing to the terms of service applicable to the Processor's software, or by using the Processor's software, the Controller is agreeing to be bound by the terms of this Agreement.

2. PROCESSING OF CONTROLLER PERSONAL DATA

2.1 Processor shall:

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

2.1.2 not Process Controller Personal Data other than on Controller's documented instructions unless Processing is required by Applicable Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by Applicable Laws, inform Controller of that legal requirement before the relevant Processing of that Controller Personal Data.

2.2 The Controller and the Processor agree and acknowledge that for the purpose of the Data Protection Laws:

2.2.1 the Controller is the Data Controller and the Processor is the Data Processor; and

2.2.2 the Controller retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Processor.

2.3 Controller instructs the Processor to Process Controller Personal Data as reasonably necessary for the provision of the software pursuant to the Licence Agreement.

2.4 The Processor will promptly notify the Controller if, in its opinion, the Controller's instructions do not comply with the Data Protection Laws.

2.5 The Processor must comply promptly with any Controller written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

2.6 The Processor will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Controller or this Agreement specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) requires the Processor to process or disclose the Personal Data to a third-party, the Processor must first inform the Controller of such legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

2.7 Schedule 1 to this Agreement sets out certain information regarding the Processors' Processing of Controller Personal Data as required by Article 28(3) of the UK GDPR.

2.8 The Processor shall not use Controller Personal Data, or any data derived from or aggregated from Controller Personal Data, to provide services to any other customer of the Processor, or to train, improve or develop any artificial intelligence or machine learning models

(whether the Processor's own or a third party's). The Processor may produce and use aggregated and anonymised data — including technical and usage telemetry and cross-customer statistics and benchmarks — provided that such data contains no Controller Personal Data and that neither the Controller, its clients, nor any individual can be identified from it.

3. PROCESSOR PERSONNEL

3.1 The Processor will ensure that all of its employees:

3.1.1 are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

3.1.2 have undertaken training on the Data Protection Laws and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

3.1.3 are aware both of the Processor's duties and their personal duties and obligations under the Data Protection Laws and this Agreement.

4. SECURITY AND CONFIDENTIALITY OF DATA

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 Controller Personal Data, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR.

4.2 In assessing the appropriate level of security, Processor shall in particular take account of the risks that are presented by Processing, including from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Controller Personal Data transmitted, stored or otherwise Processed.

5. SUBPROCESSING

5.1 Controller authorises the Processor to appoint Subprocessors in accordance with this Clause 5 and as listed in Schedule 2 to this Agreement.

5.2 Processor shall give Controller at least 45 days' prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 45 days of receipt of that notice, Controller notifies Processor in writing of any objection (on reasonable grounds relating to data protection) to the proposed appointment, Processor shall not appoint (nor disclose any Controller Personal Data to) the proposed Subprocessor until reasonable steps have been taken to address the objection and Controller has been provided with a reasonable written explanation of those steps. If the objection cannot be resolved, Controller may, by written notice to Processor, terminate those Services which cannot be provided without the use of the proposed Subprocessor.

5.3 With respect to each proposed Subprocessor, Processor shall:

5.3.1 before the Subprocessor first Processes Controller Personal Data, carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Controller Personal Data;

5.3.2 ensure that the arrangement between Processor and Subprocessor, is governed by a written contract including (i) terms which offer at least the same level of protection for Controller Personal Data as those set out in this Agreement and (ii) meet the requirements of Article 28(3) of the UK GDPR;

5.3.3 provide to Controller, for review such copies of the agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Agreement) as Controller may request from time to time; and

5.3.4 ensure the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

6. DATA SUBJECT RIGHTS

6.1 The Processor must, at no additional cost to the Controller, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with:

6.1.1 the rights of Data Subjects under the Data Protection Laws, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

6.1.2 information or assessment notices served on the Controller by the Commissioner or other relevant regulator under the Data Protection Laws.

6.2 The Processor must notify the Controller immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Laws.

6.3 The Processor must notify the Controller within 7 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Laws.

6.4 The Processor will give the Controller, at no additional cost to the Controller, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

6.5 The Processor must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Controller's written instructions, or as required by domestic or EU law.

7. PERSONAL DATA BREACH

7.1 The Processor shall:

7.1.1 notify Controller without undue delay and in any event no later than 48 hours upon becoming aware of a Personal Data Breach affecting Controller Personal Data ("**Controller Data Breach**");

7.1.2 provide Controller with sufficient information to allow Controller to meet any obligations to report or inform Data Subjects of an Controller Data Breach under or in connection with the Data Protection Laws;

7.1.3 meaningfully consult with Controller in respect of the external communications and public relations strategy related to an Controller Data Breach;

7.1.4 subject to Applicable Law, not notify any Supervisory Authorities or other data protection regulator of an Controller Data Breach without having obtained prior written approval by Controller; and

7.1.5 not issue a press release or communicate with any member of the press in respect of a Controller Data Breach, without having obtained prior written approval by Controller.

7.2 The notification set out in Clause 7.1.1 above, shall as a minimum:

7.2.1 describe the nature of the Controller Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

7.2.2 communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;

7.2.3 describe the likely consequences of the Controller Data Breach; and

7.2.4 describe the measures taken or proposed to be taken to address the Controller Data Breach.

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

7.4 the Processor agrees that the Controller has the sole right to determine:

7.4.1 whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the contents and delivery method of the notice; and

7.4.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

8. DATA PROTECTION IMPACT ASSESSMENT

The Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller 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 Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

9. DELETION OR RETURN OF CONTROLLER PERSONAL DATA

9.1 The Processor shall, at the written direction of Controller, securely delete or return Controller Personal Data and copies thereof to Controller upon the cessation of any Services involving the Processing of Controller Personal Data.

9.2 The Processor may retain Controller Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.3 The Processor shall provide written certification to Controller that it has fully complied with this Clause 9 within 60 (sixty) days of the date of cessation of any Services involving Controller Personal Data. As a minimum such written certification shall include:

9.3.1 confirmation of extent of Controller Personal Data has been deleted;

9.3.2 confirmation of the extent of Controller Personal Data retained as required by Applicable Laws as set out at Clause 9.2, citing the specific law (including provisions) deemed to be applicable and period of retention.

10. AUDIT RIGHTS

10.1 The Processor will keep an accurate and complete record of its Processing of Controller Personal Data. The Processor shall grant Controller and any auditors of or other advisers to Controller, access to its premises, information, systems, personnel and relevant records as may be reasonably required in order to:

10.1.1 fulfil any legally enforceable request by any regulatory body or data subject; or

10.1.2 undertake verification that obligations of the Processor are being performed in accordance with this Agreement and Applicable Laws.

10.2 Processor shall provide Controller (and its auditors and other advisers) with all reasonable co-operation, access and assistance in relation to each audit. If an audit demonstrates that the Processor is failing to comply with obligations under this Agreement then, without prejudice to any other rights and remedies of Controller, Processor shall take the necessary steps to comply with, or procure compliance with, such obligations.

10.3 Audits under Clause 10.1 shall: (i) be carried out no more than once in any 12-month period, except following a Personal Data Breach or where required by a Supervisory Authority; (ii) require at least 30 days' prior written notice; (iii) be conducted during normal business hours in a manner that causes minimal disruption to the Processor's business; and (iv) be subject to reasonable confidentiality obligations. The Parties agree that a current audit report or certification against a recognised standard held by the Processor (such as a SOC 2 report) shall satisfy routine audit requests.

10.4 The Parties shall bear their own costs and expenses incurred in respect of compliance with their obligations under Clauses 10.1 to 10.3.

11. DATA TRANSFERS

11.1 The Controller consents to the Processor (and its Subprocessors) transferring and processing the Personal Data outside the UK and the EEA where the transfer is made in accordance with Clause 11.2, including the transfers to the Subprocessors described in Schedule 2. Any other transfer of the Personal Data outside the UK or the EEA requires the Controller's prior written consent.

11.2 The Processor may only process, or permit the processing of, the Personal Data outside the UK and the EEA under the following conditions:

11.2.1 the Processor is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals; or

11.2.2 the Processor participates in a valid cross-border transfer mechanism under the Data Protection Laws, so that the Processor (and, where appropriate, the Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR; or

11.2.3 the transfer otherwise complies with the Data Protection Laws.

11.3 Where a Restricted Transfer takes place by Kaizan or one of its subprocessors, Kaizan shall rely on the IDTA or other applicable transfer safeguard to legitimise the transfer of Controller's Personal Data, with details documented in Schedule 1.

11.4 Additionally to the requirements set out in Clause 11.1, the Processor must ensure that any transfer of Controller Personal Data, together with other reasonably practicable compliance steps, can take place without breach of applicable Data Protection Law.

11.5 If, due to a change in Data Protection Law, a transfer of Controller Personal Data made in accordance with Clauses 11.1 to 11.3 above, can no longer take place without a breach of applicable Data Protection Law, the Processor must immediately:

11.5.1 notify the Controller in writing;

11.5.2 stop transferring any relevant Controller Personal Data; and

11.5.3 if the reason for the anticipated breach is due to one of the conditions set out in Clause 11.2 no longer meeting the requirements of Data Protection Law, establish compliance by means of an alternative condition at Clause 11.2; and

11.5.4 obtain renewed consent by Controller in accordance with Clause 11.1; and

11.5.5 ensure that the Controller Personal Data that has been transferred is returned or deleted.

12. TERMINATION

12.1 This Agreement will remain in full force and effect so long as:

12.1.1 the Licence Agreement remains in effect; or

12.1.2 the Processor retains any of the Personal Data related to the Licence Agreement in its possession or control.

13. LIABILITY

Each Party's liability arising out of or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, shall be subject to the limitations and exclusions of liability set out in the Licence Agreement.

14. GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed in accordance with English law and the Parties submit to the exclusive jurisdiction of the courts of England and Wales in relation to any dispute arising therefrom.

15. RIGHTS OF THIRD PARTIES

Third parties shall not be entitled to enforce any of the terms of this Agreement.

16. SEVERANCE

Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained in the Agreement.

Schedule 1

PROCESSING DETAILS

This Schedule 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data

Automated analysis and summarisation of internal and external company communications and information in order to provide the Services under the Licence Agreement. Controller Personal Data is not used to train, improve or develop AI or machine learning models (see Clause 2.8). For the duration of any respective supply of services agreement between the Controller and Processor.

The nature and purpose of the Processing of Controller Personal Data

Processing for consolidating, prioritising and summarising activity of a personnel's work streams, in order to improve the personnel's operational efficiency by automating information exchange, written communication and reporting

The types of Controller Personal Data to be Processed

Email content, attachments and metadata (including sender and recipient names and email addresses); meeting audio and video recordings, transcripts, participant names and calendar event data; CRM records, including contact details and account and interaction data;

and other content displayed or stored in the Controller software systems connected to the Service (including third-party hosted systems), in each case to the extent it contains Personal Data.

The categories of Data Subject to whom Controller Personal Data relates

Employees, contractors, agents and officers of the Controller; and other individuals whose personal data appears in the communications and systems processed under the Licence Agreement, including personnel of the Controller's clients, prospective clients, suppliers and other business contacts (for example, participants in meetings and senders and recipients of emails).

Special categories of Personal Data

The Services are not designed or intended to process special categories of personal data (Article 9 UK GDPR) and the Processor does not knowingly process them. The Parties acknowledge that communications content may incidentally contain such data where included in it by data subjects; any such data receives the same protections as all Controller Personal Data under this Agreement.

Schedule 2

AUTHORISED SUBPROCESSORS

This Schedule 2 lists the Subprocessors authorised by the Controller as at the date of this Agreement, in accordance with Clause 5. The Processor shall notify the Controller in writing prior to any addition to or replacement of the Subprocessors listed below, in accordance with Clause 5.2.

Google Cloud Platform (Google LLC) United Kingdom (europe-west2, London)

PROCESSING ACTIVITY

Cloud infrastructure hosting, data storage, managed database services, and compute services for the operation of the Kaizan platform.

PERSONAL DATA PROCESSED

All Controller Personal Data stored and processed within the platform, encrypted at rest (AES-256) and in transit (TLS 1.2+).

TRANSFER MECHANISM

UK Adequacy Decision (United Kingdom).

OpenAI, L.L.C. United States

PROCESSING ACTIVITY

Natural language processing services, including text summarisation, sentiment analysis, and generation of client relationship insights.

PERSONAL DATA PROCESSED

Pseudonymised text data (system-generated identifiers are used in place of names and email addresses). OpenAI does not retain Controller Personal Data after processing and does not use it for model training.

TRANSFER MECHANISM

UK International Data Transfer Agreement (IDTA) / EU-U.S. Data Privacy Framework.

AssemblyAI, Inc. United States

PROCESSING ACTIVITY

Speech-to-text transcription of meeting recordings.

PERSONAL DATA PROCESSED

Meeting audio data for transcription purposes. Data is deleted after processing is complete.

TRANSFER MECHANISM

UK International Data Transfer Agreement (IDTA).

Recall.ai, Inc. United States

PROCESSING ACTIVITY

Meeting recording and capture via bot-based integration with video conferencing platforms.

PERSONAL DATA PROCESSED

Meeting audio and video streams, participant names, and calendar metadata.

TRANSFER MECHANISM

UK International Data Transfer Agreement (IDTA).

Integration.app European Union

PROCESSING ACTIVITY

Integration platform as a service (iPaaS) providing CRM connectors, OAuth management, webhook handling, and data normalisation.

PERSONAL DATA PROCESSED

CRM contact data, OAuth tokens, and integration payloads as required for third-party system synchronisation.

TRANSFER MECHANISM

N/A (EU-based; UK Adequacy Decision applies).

Google LLC (Google Workspace APIs — Gmail API, Google Calendar API) European Union / United Kingdom

PROCESSING ACTIVITY

Email synchronisation and calendar data access via OAuth 2.0 authorised scopes.

PERSONAL DATA PROCESSED

Email content, email metadata, and calendar event data as authorised by the individual user. The storage, use, and transfer of information received from Google Workspace APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements.

TRANSFER MECHANISM

UK Adequacy Decision / Standard Contractual Clauses as applicable.

Microsoft Corporation (Microsoft Graph API — Outlook, Calendar) European Union / United Kingdom

PROCESSING ACTIVITY

Email synchronisation and calendar data access via OAuth 2.0 authorised scopes.

PERSONAL DATA PROCESSED

Email content, email metadata, and calendar event data as authorised by the individual user.

TRANSFER MECHANISM

UK Adequacy Decision for processing in the EU/UK; EU-U.S. Data Privacy Framework for any processing in the United States.