Altertable

Data Processing Agreement

Version 2026-11-20

This Data Processing Agreement (“DPA”) supplements the Altertable Terms of Service and is entered into by and between Altertable SAS, 26 rue du Commerce, 92700 Colombes, France (“Processor”) and the company identified below (“Controller”).

Company

Registered address

Company registration ID

1. Scope & Roles

1.1 Controller. Customer acts as the Data Controller, determining the purposes and means of processing Personal Data.

1.2 Processor. Altertable acts as the Data Processor in connection with the Processing described in Appendix 1, processing Personal Data solely on behalf of and in accordance with Customer’s documented instructions.

1.3 Applicable Law. This DPA is governed by Regulation (EU) 2016/679 (“GDPR”) and any applicable member state data protection legislation. Where this DPA uses the terms defined in the GDPR, those terms shall have the same meaning as in that Regulation.

2. Processing Description

The details of the processing operations subject to this DPA, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller are specified in Appendix 1.

3. Processor Obligations

Processor shall:

- (a) Process Personal Data only on documented instructions from Controller, unless required by Applicable Laws (in which case Processor shall inform Controller prior to processing, unless

prohibited by law);
- (b) Ensure that persons authorized to process Personal Data are bound by confidentiality obligations;
- (c) Implement and maintain appropriate technical and organizational measures as set forth in Section 4;
- (d) Assist Controller in responding to data subject requests (Section 6);
- (e) Assist Controller in ensuring compliance with its obligations under Articles 32–36 of the GDPR;
- (f) At Controller's choice, delete or return all Personal Data upon termination of the Agreement (Section 8); and
- (g) Make available to Controller all information necessary to demonstrate compliance with this DPA and allow for audits as described in Section 9.
- (h) Inform Controller if according to Processor's opinion, Controller's instructions constitute a violation of Applicable Data Protection Laws.

4. Security Measures

Processor shall implement and maintain technical and organizational security measures appropriate to the risk, as described in Appendix 2.

5. Data Transfers

5.1 In the event that any processing requires a transfer of Personal Data outside the EU/EEA, Processor shall ensure that appropriate safeguards are in place in accordance with Chapter V of the GDPR (such as Standard Contractual Clauses (SCCs)).

5.2. This Section only applies if Customer is located in a country outside the EEA or in a country not having been subject to an adequacy decision by the European Commission. By accepting this DPA, Provider and Customer conclude Module 4 (Processor-to-Controller) of the SCCs which applies to any international data transfer conducted by Provider acting as Processor and is hereby incorporated and completed as follows:

- The "data exporter" is Provider and the "data importer" is Customer.
- The optional docking clause in Clause 7 is implemented; the optional redress clause in Clause 11(a) is struck.
- The governing law in Clause 17 is the law of France.
- The courts in Clause 18(b) are the Courts of France; and
- Annex I and II to the Module 4 of the SCCs are Appendices 1 and 2 to this DPA respectively.

6. Data Subject Rights

6.1 Processor shall, taking into account the nature of the processing, assist Controller by appropriate technical and organizational measures in fulfilling Controller’s obligation to respond to data subject requests, including requests for:

- Access (Article 15 GDPR)
- Rectification (Article 16 GDPR)
- Erasure (Article 17 GDPR)
- Restriction of processing (Article 18 GDPR)
- Data portability (Article 20 GDPR)
- Objection (Article 21 GDPR)

6.2 If Processor receives a request directly from a data subject, Processor shall promptly redirect the data subject to Controller and notify Controller of the request.

7. Subprocessors

7.1 Authorization. Controller grants Processor general written authorization to engage subprocessors for the provision of the Services.

7.2 List. The list of authorized subprocessors is available in Appendix 3.

7.3 Notification. Processor shall notify Controller in writing at least fifteen (15) days in advance of any intended addition or replacement of a subprocessor.

7.4 Objection. Controller may object to a new sub-processor on reasonable, data-protection-related grounds, by giving written notice to Processor within ten (10) days following receipt of the relevant notification. If no objection is raised within that period, the new sub-processor shall be deemed approved. If Controller raises an objection and the Parties are unable to resolve it within a reasonable period, Processor may refrain from appointing the relevant sub-processor, take alternative steps reasonably necessary to address the objection, or, if such options are not reasonably possible, terminate the affected Services or, if necessary, the Agreement, without liability. Such termination shall not be deemed a breach of this Agreement. No refunds of prepaid Fees shall be issued in connection with such termination.

7.5 Liability. Processor shall impose on all sub-processors data protection obligations equivalent to those set out in this DPA and Processor shall remain fully liable for the acts and omissions of its subprocessors to the same extent as for its own acts and omissions.

8. Data Deletion & Return

8.1 Export Period. Upon termination or expiration of the Agreement, Customer shall have sixty (60) days to export Customer Data from the Services.

8.2 Deletion. Following the sixty (60) day export period, Processor shall permanently and securely delete all Customer Data from its systems, including backups, within a further thirty (30) days, unless retention is required by Applicable Laws.

8.3 Certification. Upon Controller’s written request, Processor shall provide written confirmation that deletion has been completed.

9. Audits

9.1 Processor shall make available to Controller all information reasonably necessary to demonstrate compliance with this DPA.

9.2 Controller (or an independent third-party auditor appointed by Controller provided it is not a competitor of Processor) may conduct an audit of Processor’s processing activities, subject to:

- At least thirty (30) days' prior written notice;

- Audit limited to the Processing described in Appendix 1 and reasonable audit duration;
- Audit is conducted at Processor's premises during normal business hours and without disrupting operations;
- Industry-standard confidentiality obligations binding the auditor;
- No more than one (1) audit per twelve (12) month period, unless required by a supervisory authority or following a Personal Data breach.

9.3 Processor shall cooperate with and provide reasonable assistance during any audit. Audit costs shall be borne by Controller unless the audit reveals a material breach by Processor. Audit report shall be provided to Provider without undue delay.

10. Breach Notification

10.1 Processor shall notify Controller without undue delay and in any event within seventy-two (72) hours after becoming aware of a Personal Data breach involving Personal Data processed as Processor.

10.2 The notification shall include, to the extent available:

- A description of the nature of the breach, including categories and approximate number of data subjects and records affected;
- The name and contact details of the Processor's data protection contact;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to address the breach.

10.3 Processor shall cooperate with Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of the breach.

11. Obligations of Controller

- Controller is solely responsible for the accuracy of Personal Data and the means by which such Personal Data is acquired in compliance with the Applicable Data Protection Laws. Controller is solely responsible for providing Processor with instructions that comply with this DPA and the Applicable Data Protection Laws.
- Controller undertakes to document in writing any additional instructions regarding the processing by Processor.
- Controller guarantees that the processing is carried out in accordance with the provisions of the Applicable Data Protection Laws and in particular that the data subjects are informed of the processing and have given their consent if applicable.
- Controller expressly prohibits the processing of Prohibited Data.

12. Liability

Each Party shall be liable for its own acts and omissions under this DPA and the liability provisions of the Terms.

Processor shall be liable for damage caused by processing only where it has not complied with this DPA or the lawful instructions of Controller.

13. DPA Term

13.1 This DPA shall remain in effect for the duration of the Agreement and shall automatically terminate upon the completion of all data deletion obligations set forth herein.

13.2 Sections 5, 9, 10, and 11 shall survive termination of this DPA.

Appendix 1 — Description of Processing

Purpose. Processor shall process Personal Data solely for the purpose of providing and maintaining the Services under the Agreement, including analytics, data storage, querying, modeling, and AI-assisted analysis.

Nature of Processing. Collection, storage, organization, structuring, retrieval, consultation, use, disclosure by transmission, and erasure of Personal Data.

Duration. Processing shall continue for the duration of the Agreement, plus any post-termination retention period as set forth in Section 8 above.

Categories of Personal Data. Customer controls what Personal Data is submitted to the Services. Categories of Personal Data may include the following Customer Data:

- Event data — user actions and interactions tracked by Customer
- User identifiers — such as user IDs, email addresses, or anonymized identifiers
- Behavioral data — usage patterns, feature interactions, conversion events
- Technical metadata — IP addresses, device information, browser data, timestamps

Data subjects may include Customer's end-users, employees, contractors, and business contacts.

Special categories. Customer shall not submit special categories of Personal Data (as defined in Article 9 of the GDPR) to the Services unless the Parties have entered into a separate written agreement addressing such processing.

Appendix 2 — Security Measures

Processor shall implement and maintain technical and organizational security measures appropriate to the risk, including:

Measure	Description
Encryption at rest	AES-256 encryption for all stored Customer Data
Encryption in transit	TLS 1.3 for all data transmission

Measure	Description
Access controls	Role-based access control (RBAC) with least-privilege principle
Audit logging	Comprehensive logs of access to and operations on Customer Data
SOC 2 controls	Independently audited SOC 2 Type II controls
Infrastructure-as-code	Reproducible, version-controlled infrastructure deployments
Vulnerability management	Regular security assessments and timely patching

Appendix 3 — List of Subprocessors

Authorized subprocessors are the following:

Subprocessor	Purpose of processing	Address of subprocessor	Data location
Amazon Web Services, Inc.	Cloud provider — infrastructure, hosting, and data storage	410 Terry Avenue North, Seattle, WA 98109, USA	European Union (primary); United States
Hetzner Online GmbH	Cloud provider — infrastructure, hosting, and data storage	Industriestr. 25, 91710 Gunzenhausen, Germany	European Union
Cloudflare, Inc.	CDN, security, and object storage services	101 Townsend St, San Francisco, CA 94107, USA	European Union; United States; global edge network
OpenAI, L.L.C.	AI model inference and processing	548 Market St, PMB 90358, San Francisco, CA 94104, USA	United States

Subprocessor	Purpose of processing	Address of subprocessor	Data location
Anthropic, PBC	AI model inference and processing	548 Market St, PMB 90375, San Francisco, CA 94104, USA	United States
Mistral AI SAS	AI model inference and processing	15 rue des Halles, 75001 Paris, France	European Union
Cerebras Systems Inc.	AI model inference and processing	1237 E Arques Ave, Sunnyvale, CA 94085, USA	United States; European Union
Datadog, Inc.	Cloud monitoring — infrastructure logging and observability	620 Avenue du Général de Gaulle, 59700 Maubeuge, France	European Union
Intercom R&D Unlimited Company	Customer support — in-product messaging and helpdesk	124 St Stephen's Green, Dublin 2, Ireland	European Union; United States
Customer.io, Inc.	Customer messaging and marketing automation	9450 SW Gemini Dr, PMB 90786, Beaverton, OR 97008, USA	United States; European Union
Google LLC (Google Analytics)	Website and product usage analytics	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	United States; European Union
Attio Limited	Customer relationship management — sales and account data	42 St John's Square, 2nd Floor, London, EC1M 4EA, United Kingdom	United States; European Union
Functional Software, Inc. (Sentry)	Engineering — error tracking and performance monitoring	45 Fremont Street, San Francisco, CA 94105, USA	United States

Signatures

Controller	Processor (Altertable SAS)
Signature	Signature
Name	Name Sylvain Utard
Title	Title CEO
Date	Date Effective on the Controller’s signature date

Altertable DPA, version 2026-11-20