BAI Analytics EU and UK Data Processing Addendum

Version 2.7 - Revised 2 November 2026

This Data Processing Addendum (DPA) forms part of the agreement governing the customer's use of the BAI Analytics services (Agreement). It is entered into between the customer identified in the Agreement (Customer) and the BAI Analytics legal entity identified in the applicable order form, subscription agreement, or invoice (Company). If no entity is identified there, Company means: (a) BAI Analytics Inc., a corporation incorporated under the Canada Business Corporations Act, where Customer is located in the European Union, the United Kingdom, or Canada; (b) BoundaryAI, Inc., a Delaware corporation, where Customer is located in the United States; and (c) where Customer is located in any other country, the BAI Analytics entity that is party to the Agreement. Customer's location is the country of the Customer address stated in the Agreement. This DPA applies when Company processes Customer Personal Data on behalf of Customer.

If this DPA conflicts with the Agreement on the protection or processing of Customer Personal Data, this DPA controls. The EU Standard Contractual Clauses and UK Addendum control over inconsistent terms where they apply.

1. Definitions

1.1 Applicable Data Protection Law means privacy and data-protection law applicable to the processing, including the EU GDPR, UK GDPR, UK Data Protection Act 2018, Swiss Federal Act on Data Protection, and applicable Canadian and United States privacy laws.

1.2 Customer Personal Data means personal data contained in content submitted to, collected through, or generated for Customer by the Services. It excludes business-contact, billing, security, and service-usage data for which Company acts as an independent controller as described in the Privacy Policy.

1.3 Personal Data Breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data.

1.4 Sub-processor means a third party engaged by Company to process Customer Personal Data to provide the Services.

1.5 EU SCCs means the standard contractual clauses adopted by European Commission Implementing Decision (EU) 2021/914. UK Addendum means the ICO International Data Transfer Addendum to the EU SCCs, as revised from time to time.

2. Roles, instructions, and purpose limitation

2.1 Customer is a controller or processor of Customer Personal Data. Company is Customer's processor or sub-processor, except for data Company processes as an independent controller under the Privacy Policy.

2.2 Company will process Customer Personal Data only to provide, secure, support, and improve the reliability of the Services, in accordance with the Agreement, this DPA, Customer's documented instructions, and Applicable Data Protection Law. Company will notify Customer if, in Company's reasonable opinion, an instruction infringes Applicable Data Protection Law, unless prohibited by law.

2.3 Company will not sell Customer Personal Data. Company will not use Customer content, prompts, audio, transcripts, inputs, or outputs to train or fine-tune shared or general-purpose artificial-intelligence models. Aggregated telemetry that cannot reasonably be linked to Customer or a person may be used to operate and improve the Services.

2.4 Customer is responsible for the lawfulness, accuracy, and quality of Customer Personal Data and for providing all required notices and obtaining all required authorisations. The Services do not require special-category data as a default. Before intentionally processing special-category or similarly sensitive data, Customer must notify Company and ensure that the Agreement documents the required safeguards.

3. Confidentiality and personnel

Company will ensure that personnel authorised to process Customer Personal Data are bound by confidentiality obligations, receive role-appropriate privacy and security training, and access Customer Personal Data only where necessary under least-privilege controls. Personnel screening is applied according to role, access, applicable law, and documented risk.

4. Security

4.1 Company will maintain technical and organisational measures appropriate to the risk, including encryption in transit and at rest, identity and access controls, multi-factor authentication for privileged systems, logging and monitoring, vulnerability management, secure development practices, incident response, backups, business continuity, and supplier risk management.

4.2 Company has completed a SOC 2 Type I examination. The report may be made available to eligible customers under appropriate confidentiality controls. Type II monitoring is ongoing. The examination does not expand the scope of the Services or replace Customer's own risk assessment.

4.3 Customer acknowledges that no system is completely secure. Customer must configure access, retention, integrations, and optional features consistently with its requirements and promptly notify Company of suspected misuse or compromise.

5. Personal Data Breaches

Company will notify Customer without undue delay after confirming a Personal Data Breach affecting Customer Personal Data. The notice will include available information reasonably required for Customer to meet its legal obligations, including the nature of the breach, affected data and data subjects where known, likely consequences, and mitigation taken or proposed. Information may be provided in phases as it becomes available. Notification is not an admission of fault or liability.

6. Data-subject rights and regulatory assistance

Taking into account the nature of the processing, Company will provide reasonable assistance to Customer with data-subject requests, data-protection impact assessments, prior consultation, and breach notifications where required by Applicable Data Protection Law and where Customer cannot reasonably fulfil the obligation through the Services. If Company receives a request concerning Customer Personal Data, it will direct the requester to Customer unless law requires otherwise.

7. Sub-processors

7.1 Customer grants Company general written authorisation to use the Sub-processors listed in the BAI Analytics Vanta Trust Center at:

https://app.vanta.com/boundary-ai.com/trust/03tv0efr50z8j0rye83oo/subprocessors

The Trust Center register is the authoritative list and identifies each provider's purpose and processing location. A provider may be feature-specific and process Customer Personal Data only when the corresponding feature is enabled or used.

7.2 Company will impose data-protection obligations on each Sub-processor that are no less protective than the relevant obligations in this DPA, taking account of the services provided. Company remains responsible for a Sub-processor's performance to the extent required by Applicable Data Protection Law.

7.3 Company will provide at least 30 days' advance notice of a new Sub-processor that will process Customer Personal Data, using the Trust Center subscription mechanism or another written channel. Customer may object during that period on reasonable data-protection grounds. The parties will work in good faith on a commercially reasonable alternative. If none is available, Customer may discontinue the affected feature or terminate the affected Services without penalty for the unused prepaid portion, subject to the Agreement.

8. Data location and international transfers

8.1 Primary databases, object storage, and customer-content processing are provisioned in the customer environment stated in the Agreement or order form. For an EU-residency deployment, Company enables only processing routes that are compatible with the documented EU residency commitment.

8.2 Optional functions are enabled only after their provider route has been validated against the customer's documented residency requirements. A function that cannot meet an EU-residency commitment will not be enabled for that deployment. The live Sub-processor register describes the approved purpose and location. Administrative account data and business communications may be transferred under the mechanism described in Section 8.3 without overriding a customer-content residency commitment.

8.3 For a restricted transfer not covered by an adequacy decision, Company will use the EU SCCs, the UK Addendum, or another lawful mechanism. The EU SCCs apply as follows: Module Two where Customer is controller and Company is processor; Module Three where Customer is processor and Company is sub-processor. Option 2 in Clause 9 applies with the notice period in Section 7.3. The optional language in Clause 11 does not apply. Irish law and Irish courts apply for Clauses 17 and 18 unless Applicable Data Protection Law requires otherwise.

8.4 For UK restricted transfers, the EU SCCs are supplemented by the UK Addendum. The tables are completed using Schedules 1 to 3 of this DPA. Neither party may terminate the UK Addendum solely because the ICO issues a revised approved addendum, unless the mandatory terms provide otherwise.

9. Return, deletion, and retention

During the term, Customer may export Customer Personal Data using available Service functionality. On termination or expiry, Company will delete or return Customer Personal Data at Customer's choice, subject to reasonable technical transition periods, backup cycles, and legal retention duties. Data retained by law will remain protected and will not be processed for other purposes. Company will provide a deletion confirmation on reasonable written request where technically and legally possible.

10. Audit and evidence

Company will make available information reasonably necessary to demonstrate compliance with this DPA. Company may satisfy an audit request through current independent reports, certifications, security documentation, questionnaires, and the Trust Center. If those materials are insufficient for a legally required audit, Customer may request a proportionate audit no more than once annually, during normal business hours, subject to confidentiality, security, and non-disruption requirements. Customer bears its audit costs unless Applicable Data Protection Law requires otherwise.

11. Liability and termination

Liability under this DPA is subject to the exclusions and limitations in the Agreement, except where Applicable Data Protection Law or the SCCs prohibit limitation. This DPA remains effective until Company no longer processes Customer Personal Data.

Schedule 1 - Processing details

Subject matter and duration

Processing Customer Personal Data to provide, secure, support, and administer the Services for the Agreement term and the limited retention period described in Section 9.

Nature and purpose

- Receive, import, collect, record, organise, structure, store, retrieve, analyse, classify, summarise, translate, transcribe, embed, display, export, secure, back up, and delete Customer Personal Data.
- Authenticate users and administer organisations, roles, and permissions.
- Connect customer-authorised systems and retrieve selected records.
- Collect publicly available content when Customer enables social-listening or public-source features.
- Generate evidence-backed analysis and other outputs requested by Customer.

Categories of data subjects

- Customer personnel, authorised users, contractors, and business contacts.
- Customer's customers, prospects, survey respondents, students, research participants, end users, and other individuals represented in Customer-provided or customer-authorised data.
- Authors of publicly available content collected through an enabled feature.

Categories of personal data

- Identity and contact data, account identifiers, organisation and role information.
- Survey responses, support records, feedback, reviews, public posts, imported operational metadata, and free-text content.
- Audio or video recordings, transcripts, speaker labels, and derived analysis when Customer uses those functions.
- Prompts, model inputs and outputs, embeddings, classifications, themes, sentiment, summaries, and evidence links.
- Usage, device, IP address, authentication, audit, diagnostic, and security-event data.

Sensitive data

The standard Services do not require special-category data. Free text, recordings, transcripts, or imported records may contain sensitive information at Customer's discretion. Customer must ensure an appropriate lawful basis and safeguards before intentionally submitting it.

Frequency

Continuous or on demand, according to Customer's use and enabled features.

Schedule 2 - Parties and transfer details

Data exporter

Customer and any Customer affiliate permitted under the Agreement. Name, address, contact, registration details, and role are those stated in the Agreement or order form. Customer may act as controller or processor.

Data importer

The BAI Analytics legal entity identified in the Agreement or order form. If none is identified, the entity determined in the introduction of this DPA: BAI Analytics Inc., 1100 Avenue du Docteur-Penfield #504, Montreal, Quebec H3A 1A8, Canada, where Customer is located in the European Union, the United Kingdom, or Canada; BoundaryAI, Inc., 131 Continental Drive, Suite 305, Newark, Delaware 19713, United States, where Customer is located in the United States; or, where Customer is located in any other country, the BAI Analytics entity that is party to the Agreement. Contact: legal@boundary-ai.com. Company acts as processor or sub-processor for Customer Personal Data.

Competent supervisory authority

The supervisory authority determined under Clause 13 of the EU SCCs. For UK transfers, the Information Commissioner's Office.

Sub-processors

The current authorised list is maintained at the Vanta Trust Center URL in Section 7.1. That register forms Annex III of the SCCs.

Schedule 3 - Technical and organisational measures

- Encryption in transit using TLS 1.2 or higher and encryption at rest using cloud-provider managed encryption.
- Role-based access, least privilege, privileged-access protections, and multi-factor authentication.
- Centralised logging, alerting, monitoring, vulnerability scanning, patching, and independent penetration testing.
- Secure development, code review, change control, dependency monitoring, and controlled production deployment.
- Daily backup monitoring for in-scope production databases, encrypted backup storage, and documented restoration and continuity procedures.
- Incident-response roles, escalation, containment, evidence preservation, communication, and post-incident review.
- Data minimisation, configurable retention, export and deletion workflows, and environment separation.
- Supplier due diligence, contractual data-protection terms, ongoing review, and a public Sub-processor register.
- Security and privacy training, confidentiality commitments, access reviews, and role-appropriate personnel screening.

Contact

Privacy: privacy@boundary-ai.com

Legal and DPA requests: legal@boundary-ai.com

Security: security@boundary-ai.com