



# Brainsight Data Processing Addendum

Last updated: 2 October 2026

This Data Processing Addendum ("DPA") forms an integral part of the Brainsight Terms & Conditions (the "Terms") between Brainsight B.V., Amsterdam, the Netherlands ("Brainsight") and the Customer. It applies automatically, without separate signature, whenever Brainsight processes Personal Data contained in Customer Content. A countersigned copy is available on request at [support@brainsight.app](mailto:support@brainsight.app). Capitalised terms not defined here have the meaning given in the Terms or the GDPR.

## 1. Roles and Scope

1.1. Customer acts as controller or, where it processes Personal Data on behalf of its own clients, as processor. Brainsight acts as processor or, respectively, sub-processor. Where Customer acts as processor, Customer warrants that its instructions and this DPA are authorised by the relevant controller, and Brainsight assumes the obligations required by Article 28(4) GDPR as set out in this DPA.

1.2. This DPA applies only to Personal Data contained in Customer Content. Account, contact, usage and billing data of Authorized Users are processed by Brainsight as controller under its Privacy Policy and are outside the scope of this DPA.

1.3. The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of data subjects are described in Annex 1.

## 2. Customer Obligations

2.1. Customer is solely responsible for the lawfulness of the Personal Data it submits, including the legal basis for processing, transparency towards data subjects, any required consents and image or portrait rights. Customer will not submit special categories of Personal Data (Article 9 GDPR) or Personal Data of children unless strictly necessary and lawful.

2.2. Customer manages Customer Content through the self-service functions of the Services, including upload, retention and deletion.

### 3. Instructions

3.1. Brainsight processes Personal Data only on documented instructions from Customer, unless required otherwise by EU or Member State law, in which case Brainsight will inform Customer before processing where legally permitted.

3.2. Customer instructs Brainsight to: (i) process Personal Data to provide the Services in accordance with the Terms, including via the API and integrations; (ii) generate Derived Data, which does not contain Personal Data; and (iii) anonymise Customer Content before any use under clause 5.2(d) of the Terms, in line with the standard set out in Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques.

3.3. Brainsight will not process Personal Data for its own purposes. Brainsight does not use Personal Data for biometric identification of natural persons: the Services may detect the presence of faces as a driver of visual attention, but do not identify or recognise individuals.

3.4. Brainsight will inform Customer if, in its opinion, an instruction infringes the GDPR.

### 4. Confidentiality

Brainsight ensures that persons authorised to process Personal Data are bound by confidentiality obligations or are under an appropriate statutory obligation of confidentiality. Contractors without such obligations have no access to Customer Content.

### 5. Security

Brainsight implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in Annex 2 (Article 32 GDPR). Brainsight may update these measures, provided the overall level of security is not reduced.

### 6. AI and Model Providers

Where Brainsight uses third-party AI or model providers as sub-processors, Brainsight uses business or API offerings under which the provider does not use Customer Content to train its own models.

## 7. Sub-processors

7.1. Customer grants Brainsight general written authorisation to engage sub-processors. The current list is set out in Annex 3 and published at [brainsight.app/help-center-articles/compliance-security-policies](https://brainsight.app/help-center/articles/compliance-security-policies).

7.2. Brainsight will notify Customer of any intended addition or replacement of a sub-processor at least thirty (30) days in advance, by e-mail or through a notification mechanism to which Customer may subscribe.

7.3. Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, Customer's sole remedy is to terminate the affected Services before the change takes effect, with a refund of any prepaid fees for the period after termination.

7.4. Brainsight imposes data protection obligations on each sub-processor that are substantially equivalent to those in this DPA, and remains responsible to Customer for the performance of its sub-processors' obligations.

## 8. International Transfers

Customer Content is stored in the European Union. Where a sub-processor processes Personal Data outside the European Economic Area, Brainsight ensures an appropriate transfer mechanism under Chapter V GDPR, such as an adequacy decision (including the EU-US Data Privacy Framework) or the European Commission's Standard Contractual Clauses. The mechanism per sub-processor is listed in Annex 3.

## 9. Assistance

9.1. Taking into account the nature of the processing, Brainsight assists Customer by appropriate technical and organisational measures in responding to requests from data subjects. Customer can access, export and delete Customer Content through the self-service functions of the Services. Brainsight will promptly forward any request it receives directly from a data subject relating to Customer Content, without responding itself unless authorised.

9.2. Brainsight provides reasonable assistance to Customer with data protection impact assessments and prior consultations (Articles 35 and 36 GDPR), to the extent Customer cannot reasonably fulfil these with the information available to it. Brainsight may charge reasonable costs for assistance beyond providing its standard documentation.

## 10. Personal Data Breach

10.1. Brainsight will notify Customer without undue delay, and in any event within forty-eight (48) hours after becoming aware of a Personal Data Breach affecting Customer Content.

10.2. The notification will include, to the extent available, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed. Information may be provided in phases.

10.3. Brainsight will take reasonable steps to contain and remediate the breach. Notification is not an acknowledgement of fault or liability.

## 11. Deletion and Return

11.1. Customer can return (export) and delete Customer Content at any time through the self-service functions of the Services. Deletion by the user is permanent in production systems.

11.2. On Customer's written request to support@brainsight.app, Brainsight will delete all Customer Content of Customer's account from its production systems within ten (10) business days.

11.3. Deleted Customer Content may persist in backups until overwritten in the regular backup cycle, which does not exceed ninety (90) days. Backups are not accessed for any purpose other than disaster recovery.

11.4. Cancelling a Subscription does not terminate the account. Customer Content remains stored until deleted by Customer, at Customer's request, or under clause 12.4 of the Terms. Derived Data and models trained under clause 5.2(d) of the Terms do not contain Personal Data and are not subject to deletion.

## 12. Audits and Information

12.1. Brainsight makes available to Customer the information necessary to demonstrate compliance with Article 28 GDPR, including this DPA, its security documentation and, on request, written answers to a reasonable security questionnaire once per year.

12.2. Where this information is insufficient, Customer may conduct security testing under clause 4.8 of the Terms, or an audit by an independent auditor bound by confidentiality, on at least thirty (30) days' written notice, during business hours, no more than once per year, and at Customer's cost. On-site audits are limited to cases where required by a supervisory authority or following a Personal Data Breach. Audits will not cover other customers' data or Brainsight's proprietary methodologies.

12.3. Infrastructure audits are covered by the certifications and reports of Google Cloud, which Customer accepts as sufficient evidence for the infrastructure layer.

## 13. Liability

Each party's liability under or in connection with this DPA is subject to the exclusions and limitations of liability in the Terms or the applicable Order Form. Nothing in this DPA limits either party's liability towards data subjects under Article 82 GDPR.

## 14. Term and Precedence

14.1. This DPA applies for as long as Brainsight processes Personal Data contained in Customer Content.

14.2. In case of conflict regarding the processing of Personal Data, this DPA prevails over the Terms and the Developer Terms, but not over a signed Order Form that expressly deviates from it.

## Annex 1: Description of Processing

| Item           | Description                                                                                 |
|----------------|---------------------------------------------------------------------------------------------|
| Subject matter | Prediction of visual attention and related analyses of Customer Content                     |
| Duration       | For as long as Customer Content is stored in the Services (see clause 11)                   |
| Nature         | Storage, automated analysis, generation of Output and Derived Data, anonymisation, deletion |
| Purpose        | Providing the Services to Customer under the Terms, Developer Terms and any Order Form      |

| Item                   | Description                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Types of Personal Data | Images and likenesses of persons appearing in Customer Content (photos, video frames, website screenshots), and any names or text visible in it |
| Special categories     | None intended. No biometric identification is performed                                                                                         |
| Data subjects          | Persons depicted in advertising, design or web content submitted by Customer, such as models, actors, employees or other individuals            |
| Location               | European Union (Google Cloud); transfers per Annex 3                                                                                            |

## Annex 2: Technical and Organisational Measures

**Infrastructure.** Brainsight runs on Google Cloud (EU), which maintains ISO 27001 and SOC 2 certifications. Brainsight inherits these infrastructure controls under Google's shared responsibility model and is responsible for application-level security as described below.

**Encryption.** Customer Content is encrypted in transit using HTTPS (TLS 1.2/1.3) and at rest using AES-256, with encryption keys managed by Google Cloud.

**Access control.** Access to production systems is restricted to three named roles: CTO/Tech Lead, Product Owner and Research & Platform Lead, based on least privilege. Multi-factor authentication is enforced for all administrative and production access. Users sign in via OAuth or authenticated credentials. Contractors have no access to Customer Content.

**Development.** Development and testing take place in a separate staging environment. AI-assisted development tools operate on staging. Read-only production access is limited to incident and bug analysis, and is logged.

**Customer control.** Customers manage upload, retention and permanent deletion of Customer Content through self-service functions, and can request full account deletion.

**Model providers.** Third-party AI providers are used under business or API terms that exclude training on Customer Content.

**Testing.** Enterprise customers may perform penetration tests in a dedicated test environment under clause 4.8 of the Terms. Findings are remediated with priority.

**Incident response.** Personal Data Breaches are notified within 48 hours under clause 10.

**Confidentiality.** Personnel with access to Customer Content are bound by confidentiality obligations.

**Network and system security.** Brainsight operates in an isolated cloud environment without corporate network dependencies. Google Cloud's built-in anti-malware and security frameworks protect access points. Security patches and updates are applied automatically. Access logs are stored securely, and inactive accounts are locked automatically.

**Backups.** Automated, encrypted backups are made exclusively for disaster recovery and are not accessible to users.

**Secure deletion.** Deletion of Customer Content on request follows NIST SP 800-88 media sanitisation guidelines, as implemented by Google Cloud.

## Annex 3: Sub-processors

| Sub-processor                                   | Purpose                                                       | Location       | Transfer mechanism           |
|-------------------------------------------------|---------------------------------------------------------------|----------------|------------------------------|
| Google Cloud (Google Cloud Platform / Firebase) | Hosting, storage, database                                    | EU             | Not applicable               |
| Google (Gemini API)                             | AI analysis and interpretation                                | EU (Vertex AI) | Not applicable               |
| OpenAI                                          | AI analysis and interpretation                                | US             | Standard Contractual Clauses |
| Anthropic                                       | Development, maintenance and incident analysis                | US             | Standard Contractual Clauses |
| Website screenshot API provider                 | Rendering website screenshots from URLs submitted by Customer | US             | Standard Contractual Clauses |