

Brainsight IT Security & Compliance Overview

Last updated: 2 October 2026

1. Introduction

Brainsight is a secure, cloud-based SaaS platform that predicts visual attention on content uploaded by its users, such as images, videos and websites. It does not generate content. The platform runs on Google Cloud's EU-based infrastructure, which maintains ISO 27001 and SOC 2 certifications.

Brainsight B.V. is a Dutch company operating under EU law, including the General Data Protection Regulation (GDPR).

2. Security & Data Protection

2.1 Infrastructure & Data Handling

- Brainsight is fully cloud-based and hosted on Google Cloud. Customer content is stored in the EU.
- No local installations are required.
- Selected sub-processors process data for specific functions, such as AI interpretation and website screenshots, under our Data Processing Addendum with appropriate transfer safeguards. The current list is published on our compliance page.
- AI providers are used under business API terms that exclude training on customer content.
- Brainsight does not generate content. It provides analytical insights on uploaded media.

2.2 Encryption

- Data in transit: encrypted using HTTPS (TLS 1.2/1.3).
- Data at rest: encrypted using AES-256, with keys managed through Google Cloud Key Management Service (KMS).

2.3 Access Control

- Users sign in via Google authentication (OAuth 2.0) with 2FA. Brainsight does not store user passwords.
- Production access is restricted to three named roles, based on least privilege, with multi-factor authentication enforced.
- Development takes place in a separate staging environment. Production access is limited to incident analysis and is logged.
- Contractors have no access to customer content.

2.4 Network & System Security

- Brainsight operates in an isolated cloud environment, with no corporate network dependencies.

- Google Cloud's built-in anti-malware and security frameworks protect all access points.
- Access logs are stored securely, and inactive accounts are locked automatically.
- Security patches and updates are applied automatically.
- Enterprise customers may perform penetration tests in a dedicated test environment, by prior agreement. Findings are remediated with priority.

2.5 User & Account Management

- Each client designates an admin user who manages users, roles and licences.
- Users can download their analysed creatives with Brainsight overlays, such as heatmaps and peekthroughs. Once downloaded, securing these files is the user's responsibility.

3. Personal Data

- Brainsight is designed for business creative assets. Uploaded content may contain images of identifiable persons. For such content, Brainsight acts as processor under its Data Processing Addendum, which forms part of the Terms & Conditions and applies automatically.
- Brainsight does not perform biometric identification. Faces are detected only as a driver of visual attention, without identifying individuals.
- Account and billing data of users are processed by Brainsight as controller, as described in the Privacy Policy.

4. Compliance & Certifications

4.1 Policies

The Terms & Conditions, Data Processing Addendum, Developer Terms, Acceptable Use Policy, Privacy Policy and the list of sub-processors are available at:

brainsight.app/help-center/articles/compliance-security-policies

4.2 Infrastructure Certifications

Brainsight runs on Google Cloud and Google Workspace, which maintain the following internationally recognised certifications and reports:

- ISO/IEC 27001: Information Security Management System.
- ISO/IEC 27017: Cloud security controls.
- ISO/IEC 27018: Protection of personal data in public clouds.
- ISO/IEC 27701: Privacy Information Management System.
- ISO 9001: Quality management system.
- SOC 2 and SOC 3: Security, availability and confidentiality.

Brainsight inherits these infrastructure controls under Google's shared responsibility model and is responsible for application-level security, as described in this document.

5. Incident Management & Business Continuity

5.1 Incident Response

- Brainsight is a non-critical analytical tool. Temporary unavailability does not affect clients' operational systems.
- Security incidents are handled through Brainsight's incident response process, supported by Google Cloud's security operations and monitoring.
- Personal data breaches affecting customer content are notified to the customer within 48 hours, as set out in the Data Processing Addendum.

5.2 Data Exposure

- Uploaded content typically consists of marketing materials, such as ads, images and videos, rather than confidential corporate data.
- Once a user has downloaded analysed creatives, securing those files is the user's responsibility.

5.3 Backups & Disaster Recovery

- Automated, encrypted backups are made exclusively for disaster recovery, within Google Cloud (EU).
- Backups are not accessible to users and are overwritten within a maximum of 90 days.

5.4 Deletion

- Users can permanently delete their content at any time.
- Full account deletion is completed within 10 business days of a request to support@brainsight.app, in line with NIST SP 800-88 media sanitisation guidelines as implemented by Google Cloud.

6. Remote Working & Device Security

- Access is secured with Google authentication and 2FA.
- Google Workspace is used for secure e-mail communication.
- External storage devices (USB, HDDs, etc.) are not used for customer data.
- Mobile access is restricted to authenticated devices with strong password protection and automatic lockout enabled.

7. Contact

Questions about security or compliance can be sent to support@brainsight.app.