Palasil is a service of Terahold S.r.l. ("Terahold"). This page describes the security measures that Terahold applies to the Palasil service on the date of this version. Terahold's contractual commitments on security are those in Appendix B of the Data Processing Agreement (the "DPA"), which lists the technical and organisational measures and prevails over this page in case of differences. Capitalised terms not defined on this page have the meaning given in the Terms of Service, available at palasil.com/legal.

This page is published in English and Italian. In case of conflict, the English version prevails.

1. Where data are stored and processed

1.1 The database, the authentication and the file storage of the Service are located in the European Union, in Frankfurt. The server functions of the application run in the European Union, in Frankfurt. The application server of the AI agent and the archive of the technical logs are located in the European Union.

1.2 Requests to the language models used by the AI agent may be processed outside the European Union. The providers that run the models must have their headquarters in the United States or in a country covered by an adequacy decision of the European Commission, based on the information published by OpenRouter, Inc.; the servers they use may be located in other countries. Requests are subject to zero data retention and are not used for training, as described on the AI and Transparency page.

1.3 Some providers of Terahold are established outside the European Union, as indicated on the Sub-processors page. Transfers of personal data to them are covered by the safeguards of Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "GDPR"), as indicated on that page.

1.4 The infrastructure that stores the data of the Service is located in the European Union and is subject to the law of the Member State in which it is located. Some providers of that infrastructure are established outside the European Union, for example in the United States or in Singapore, and may be subject to the law of those countries, including the law on access to data by public authorities. The country of establishment of each provider is indicated on the Sub-processors page.

1.5 To prevent access by authorities of countries outside the European Union, or transfers to them, that would conflict with the law of the European Union or of a Member State, Terahold applies the following measures to all data of the Service, personal and non-personal:

a) technical measures: the data of the Service are stored in the European Union; data are encrypted in transit; the keys of the Connected Tools are encrypted as described in Section 4.1; access is limited as described in Sections 2 and 3;

b) contractual measures: if Terahold receives a request from a public authority to access the data of a Customer, it informs the Customer, unless prohibited by law, and discloses only the minimum data required, as provided in the DPA; Terahold's providers handle such requests under their own data processing agreements;

c) organisational measures: every request from a public authority is examined by Terahold before any disclosure.

2. Access to the Service

2.1 Access is by invitation only. An invitation is a single use link sent to the email address of the invited person and valid for 7 days.

2.2 Two-step verification is mandatory for Terahold staff and optional for the Users of the Customers, who can activate it in the Settings; Users who have not activated it receive a reminder in the Service. Where two-step verification is activated, it is also enforced by the database: a session that has not completed it cannot read the data of the Customers.

2.3 Each Brand Workspace has its own roles: Owner, Manager, Editor and Analyst. Analysts have read-only access, also at database level. Under a Palasil Custom Agreement, Terahold staff join the Brand Workspace with the role "Palasil admin". The data of different Customers are separated in the database by access rules, which Terahold verifies with tests before changing them. The database accepts a record only if the objects it refers to belong to the same Brand Workspace.

2.4 In the internal administration panel, Terahold administrators see service information, such as the status, plan and payments of each Brand Workspace and the list of its Users, and not the content of the Brand Workspace. Terahold staff with the developer role see in that panel only the activity log and the list of the Users of the Brand Workspaces (name, email, Brand Workspace, role, two-step verification status, last access); they enter a Brand Workspace only through the support access described in Section 3.2.

2.5 The following actions require the User to confirm his or her identity again with the second factor, or with the password where two-step verification is not activated, and the confirmation is valid for 10 minutes: deleting or archiving a Brand Workspace, changing the keys of the Connected Tools, changing the Owner, removing members, granting support access and changing the Palasil admins of a Brand Workspace, together with the corresponding actions of Terahold administrators, such as removing two-step verification from a User, inviting or removing administrators, recording payments and changing contracts or prices.

2.6 A password can be changed only with the current password or through the recovery link received by email. After 10 failed attempts to enter the password or the verification code for the same email address or User within 15 minutes, further attempts are blocked for 15 minutes.

3. Access by Terahold

3.1 Terahold does not access the content of a Brand Workspace, except:

a) to perform the services agreed under a Palasil Custom Agreement;

b) to handle a support request, where an Owner, Manager or Editor of the Brand Workspace has granted support access as described in Section 3.2;

c) for technical access to the infrastructure by authorised staff, solely for maintenance, security, incident response and fault resolution;

d) where required by law.

3.2 Support access is granted from the Settings of the Brand Workspace, in the "Palasil access" section, by an Owner, Manager or Editor, for 3 or 7 days, and can be turned off at any time. Terahold staff never grant support access, also when they are members of the Brand Workspace. While support access is on, the authorised staff of Terahold can enter the Brand Workspace; each entry requires a reason, without which the data of the Brand Workspace are not shown. The "Palasil access" register of the Brand Workspace records:

a) when support access is turned on and off;

b) each entry of Terahold staff, with the person, the date and time and the reason;

c) each change made by Terahold staff during support access, including those made by the AI agent at their request, with the sole exclusions of Section 6.2 of the DPA;

d) each download of the data with the "Export all data" function;

e) the drafts saved in Klaviyo, the segments created in Klaviyo and the campaigns scheduled or sent by Terahold staff during support access, with the person, the date and the time.

Reads are not recorded. At the first entry of Terahold staff, the Owners, Managers and Editors of the Brand Workspace receive a notification in the Service.

3.3 Owners, Managers and Editors can read the "Palasil access" register in the Settings. Each entry is kept for 12 months from its date, also after the deletion of the Brand Workspace; after the deletion, only Terahold can access it.

3.4 Under a Palasil Custom Agreement, Terahold staff work in the Brand Workspace as identifiable members with the "Palasil admin" role, and their individual entries are not recorded in the "Palasil access" register. The register records, and the Owners receive a notification in the Service, each time a Palasil admin joins or leaves the team of the Brand Workspace and each time the Brand Workspace moves from self-service to a Palasil Custom Agreement or vice versa.

3.5 Terahold staff and collaborators are bound by written confidentiality obligations, process data only on Terahold's instructions and work only with accounts and tools of Terahold or of the Customers. Their access is personal, limited to what their tasks require and revoked at the end of their engagement. On request, Terahold tells the Customer the names of the persons who access its data.

3.6 Technical access to the production database uses separate keys for each use and for each person. The logs of the database and authentication platform are copied to a storage of Amazon Web Services in the European Union, where they cannot be changed and are kept for 12 months. The records of the actions of Terahold staff in the Service are kept for 12 months.

3.7 When Terahold support removes the two-step verification of a User, the User receives a notification in the Service.

4. Protection of data and secrets

4.1 The keys that connect Palasil to the Customer's Klaviyo and Shopify accounts are encrypted with AES-256-GCM and can be read only by server-side components.

4.2 Data are encrypted in transit: the Service is accessible only through encrypted connections (HTTPS). The database and the file storage are encrypted at rest by Supabase. The application server of the AI agent is accessible only to authorised staff and keeps the execution log of the agent for 14 days.

4.3 The files of the Brand Workspaces are kept in private storage, accessible only through the Service to the members of the Brand Workspace and to Terahold staff under Section 3.1. The cookies that store the selected Brand Workspace and the cookies used for the confirmation of identity and for password recovery are httpOnly. Each automated component of the Service uses its own secret.

4.4 The tools of the AI agent are limited to an allow list, and its access to files on the application server is confined to its own working folder. The gateway to the language models accepts only requests made with the key of the agent. The use of the AI agent is limited for each User and for each Brand Workspace.

4.5 The Service downloads the images of the newsletters of the inspiration feed only from public internet addresses.

5. AI processing

5.1 Requests to the language models are sent through OpenRouter, Inc. Palasil asks for zero data retention in each request, and the same condition and the prohibition of training are set in Terahold's account. Providers established in the People's Republic of China and decentralised computing networks are excluded. Images are not sent to the models. The working data of the agent are deleted after 90 days.

5.2 Palasil creates drafts in the Customer's Klaviyo account, creates the segments proposed by the AI agent, and schedules or sends a campaign, only on the explicit action of a User whose role allows it or of Terahold staff during support access (Section 3.2) or with the Palasil admin role (Section 3.4); each draft saved in Klaviyo is recorded with the person who saved it. A segment proposed by the AI agent is created exactly as proposed, after the confirmation in the chat, which is recorded with the person and the time; Palasil does not change or delete segments in the Customer's Klaviyo account. A campaign is sent without a scheduled date and time only after a further confirmation of the person who requests it, and leaves 3 minutes after that confirmation; the AI agent cannot schedule or send campaigns. The AI agent asks the User for confirmation before deleting content or removing a draft from the Customer's Klaviyo account, and inserts links only to the Customer's own website unless the User provides a different address.

6. Availability

6.1 The database is backed up daily and the backups are kept for 7 days.

7. Incidents and vulnerabilities

7.1 Terahold notifies the Customers of personal data breaches affecting their data without undue delay and in any event within 48 hours after becoming aware of them, as provided in Section 13.1 of the DPA.

7.2 Anyone who finds a security vulnerability in Palasil can report it to security@palasil.com. Terahold asks those who report not to access or change data that are not theirs, not to disrupt the Service and not to disclose the vulnerability before Terahold has confirmed that it is fixed. Security reports are handled before the other support requests.

8. Changes

8.1 Terahold updates this page when its security measures change. The current version is available at palasil.com/legal/security, and the previous versions remain available in the archive at palasil.com/legal/archive.