

Data Management, Classification and Retention Policy

Data classes, handling rules, retention periods, deletion and export.

Version 1.1 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/data-management-policy>

1. Purpose

This policy classifies the data Etropo holds, sets handling rules for each class, and states how long data is kept, how it is deleted, and how customers get it back.

2. Classification

Class	Examples	Handling
Highly Confidential	Budget plans and actuals, invoices, integration tokens, passwords and session tokens, encryption keys, personal data	Encrypted in transit and at rest; access through Row Level Security or the Access Control Policy only; never on personal devices; never in chat, email or tickets except as the customer sends it
Confidential	Organisation details, user names and emails, audit logs, architecture documentation, vendor contracts	Access limited to personnel who need it; shared outside Etropo only under agreement
Internal	Application logs without customer content, performance metrics, aggregated analytics	Available to Etropo personnel
Public	Marketing site, documentation, this Trust Center, product descriptions	No restriction

3. Roles under the GDPR

- For **budget data, invoices, comments and the content of connected integrations**, the customer is the controller and Etropo is the processor, acting on the customer's instructions through the product.
- For **account, billing, support and usage data**, Etropo is the controller. The lawful bases are performance of the contract and legitimate interest in running and improving the service.

4. Where data is

Customer data is stored in Frankfurt (AWS eu-central-1 via Supabase). The vendors that receive data, the data each receives and the region are listed on the Subprocessors page, which is the authoritative list and is updated before a change takes effect.

5. Retention

Data	Kept for	Then
Account, organisation and budget data	While the organisation has an account	Deleted on request, see §6
Deleted accounts and organisations	Up to 30 days after the request	Removed from the live database
Backups	Up to 90 days after deletion from the live database	Overwritten by the backup cycle
Integration token audit logs (who connected or disconnected an integration, token events)	1 year	Deleted by a daily scheduled job
Integration sync logs	90 days	Deleted by a daily scheduled job
Webhook events	90 days	Deleted by a daily scheduled job
Authentication and database logs (Supabase)	7 days (Supabase Pro)	Deleted by the provider
Application and function logs (Vercel)	30 days (Vercel Pro with Observability Plus)	Deleted by the provider
Error reports and session replays (Sentry, Mixpanel)	Per the vendor's retention (90 days for Sentry replays)	Deleted by the vendor
Billing records (Stripe)	As required by tax law, typically 5 years	Deleted

Deletion at the end of these periods is automated for the integration, token-audit and webhook tables: a scheduled job runs once a day and deletes every row older than its period (in place since 22 October 2026).

6. Deletion

- A user or an organisation admin can request deletion of an account or a whole organisation by emailing team@etropo.com. Identity is verified against the account's email before deletion.
- Deletion is completed within 30 days. It removes the organisation's budgets, versions, line items, comments, dashboards, Marketing Brain entries, integration connections and tokens, and the users' personal data, from the live database.
- Backups that still contain the data are overwritten within a further 90 days.
- Data already passed to a vendor (for example a support conversation in Intercom, or an invoice email in Resend) is deleted from that vendor by request to the vendor or by its own retention schedule, as listed on the Subprocessors page.
- Self-service deletion inside the product is on the roadmap.

7. Export and portability

- Any budget can be exported to XLSX from the budget editor by any member with access to it.
- Budgets can be mirrored continuously to Google Sheets or Notion.
- A full export of an organisation's data in a machine-readable form is provided within 30 days of a request to team@etropo.com.

8. Data subject rights

Requests to access, correct, delete, restrict or port personal data, and objections to processing, are sent to team@etropo.com and answered within 30 days. Where Etropo is the processor, the request is passed to the customer, who decides.

9. Minimisation and analytics

- Sign-up collects name, email and password, or a Google account.
- Product analytics events are sent server-side and carry user and organisation identifiers and feature names, not budget content.
- Session replay is used to diagnose problems. Sentry masks text by default. Mixpanel replay masks all page text and typed input (since 2026-10-22); the organisation name entered at sign-up is the one unmasked field.
- AI model providers receive data when a user asks a question or uploads a file, and only the data that user is allowed to see; two scheduled Marketing Brain jobs (line-item names daily, brain entries weekly) run for organisations with Budget Buddy enabled. Every AI call is traced to Braintrust. The "AI in Etropo" paper, available on request, has the details.

10. Media and devices

Customer data is accessed through the browser and is not downloaded to or stored on personal devices, removable media or personal cloud accounts. See the Acceptable Use Policy.

11. Review

Reviewed annually. Version 1.1, October 2026: log tables kept for 1 year (token audit) or 90 days (sync logs, webhook events) with daily automated deletion; provider log retention corrected to the current plans (§5).

This PDF is a snapshot. The page at <https://trust.etropo.com/resources/data-management-policy> is the current version.