

Third-Party and Vendor Management Policy

How vendors are chosen, reviewed and listed, and how customers are told about changes.

Version 1.0 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/vendor-management-policy>

1. Purpose

Etropo runs on other companies' platforms and sends customer data to a small number of vendors. This policy says how those vendors are chosen, what is checked before and after, how they are listed, and how customers are told about changes.

2. Definitions

- **Subprocessor.** A vendor to which Etropo sends customer data as part of running the service (hosting, database, email, AI models, monitoring, support).
- **Customer-connected integration.** A service the customer authorises from inside the product (Google Ads, Slack, Notion and so on). Data flows only after the customer connects it and stops when they disconnect it. These are listed separately for transparency.
- **Other vendor.** Tools that hold no customer data (source control, design, internal communication). Not listed.

3. Before a vendor is used

The Security Lead records, for every new subprocessor:

1. the purpose and the exact data it will receive, with the least data that does the job;
2. the region where it processes that data;
3. its security evidence: a SOC 2 Type II or ISO 27001 report is preferred; otherwise a published security page and a review of its practices;
4. the contract terms covering data protection: a data processing agreement, and for vendors outside the EU, the Standard Contractual Clauses or an adequacy decision;
5. for AI providers, confirmation that customer data is not used to train models;
6. how Etropo would replace the vendor.

A vendor is added to the Subprocessors page and announced in the Updates feed **before** it receives customer data.

4. Ongoing

- Once a year the Security Lead confirms that each subprocessor's security report is current, that the DPA is in force, and that the data sent is still the minimum needed.
- Vendor security notifications and incident reports are handled under the Security Incident Response Plan.
- A vendor that no longer meets this policy is replaced, and the change is announced.

5. Customer notification

- The Subprocessors page is the authoritative list.
- Additions and material changes are published on the Updates page, which also has an RSS feed, before they take effect.
- Customers who object to a new subprocessor can raise it at security@etropo.com; where Etropo cannot accommodate the objection, the customer may terminate under the terms of service.

6. Current status

The list on the Subprocessors page is complete as of October 2026. Collecting signed DPA records for every vendor is in progress and is recorded as a partial control.

7. Review

Reviewed annually. Version 1.0, October 2026.

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