

Data Processing Agreement (DPA)

The terms under which Etropo processes personal data on a customer's behalf, with the EU Standard Contractual Clauses incorporated and the subprocessor list as an annex. Takes effect with the Terms of Service; a countersigned copy is available on request.

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

This Data Processing Agreement ("DPA") forms part of the agreement between the customer named in the Etropo account ("Customer") and Etropo, Trakt Napoleoński 31/1, 04-809 Warsaw, Poland, VAT ID PL5842721889 ("Etropo") for the use of the Etropo service (the "Agreement"). It applies wherever Etropo processes personal data on the Customer's behalf.

It needs no signature. It takes effect when the Customer accepts Etropo's Terms of Service, or on the date a Customer and Etropo sign it, whichever is earlier. A Customer that needs a countersigned copy can request one from security@etropo.com; the signature page is at the end of this document.

1. Definitions

- **"Data Protection Law"** means every law that applies to the processing of personal data under this DPA, including the EU General Data Protection Regulation (EU) 2016/679 ("GDPR"), the GDPR as it forms part of the law of the United Kingdom ("UK GDPR") and the UK Data Protection Act 2018, and the Swiss Federal Act on Data Protection ("FADP").
- **"Customer Personal Data"** means personal data that the Customer, or a person using the Service on the Customer's behalf, submits to the Service, and that Etropo processes on the Customer's behalf. It is described in Annex I.
- **"Service"** means the Etropo marketing budget software at app.etropo.com, its API, the assistants in Slack, Microsoft Teams and HubSpot, and the integrations a Customer connects to it.
- **"Subprocessor"** means a third party that Etropo engages to process Customer Personal Data as part of running the Service. The current list is Annex III.
- **"Standard Contractual Clauses" or "SCCs"** means the standard contractual clauses for the transfer of personal data to third countries annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **"UK Addendum"** means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner, version B1.0, in force 21 March 2022.
- **"Restricted Transfer"** means a transfer of Customer Personal Data to a country that Data Protection Law does not treat as providing adequate protection, where the transfer would be unlawful without a transfer mechanism such as the SCCs.

- "Controller", "processor", "data subject", "personal data", "personal data breach", "processing" and "supervisory authority" have the meanings given in the GDPR.

2. Roles

2.1 Customer Personal Data. For the content a Customer puts into the Service, budgets, line items, actuals, invoices, comments, Marketing Brain entries, the data flowing through connected integrations, and the account details of the Customer's users, the Customer is the controller (or a processor acting for its own controller) and Etropo is the processor. Etropo processes this data only to provide the Service, on the Customer's documented instructions.

2.2 Etropo as controller. For the data Etropo needs to run its own business, billing records, support conversations, product analytics and error reports, Etropo is an independent controller. That processing is described in Etropo's Privacy Policy at www.etropo.com/legal and is not covered by this DPA.

2.3 The Customer's instructions. The Customer's complete and final instructions are: the Agreement, this DPA, and the use of the Service's features by the Customer's users (including a user's question to the AI assistant, a file a user uploads, and an integration a Customer's admin connects). Additional instructions require Etropo's written agreement. Etropo will tell the Customer, without legal analysis, if it believes an instruction infringes Data Protection Law.

2.4 The Customer's responsibilities. The Customer is responsible for the lawfulness of the Customer Personal Data and of its instructions, for any notice to or consent from data subjects that its use of the Service requires, and for the accounts, roles and category permissions it grants its users. The Customer will not submit special categories of personal data (GDPR Article 9), criminal-offence data or payment card numbers to the Service; the Service is not designed for them.

3. Details of processing

The subject matter, duration, nature and purpose of the processing, the categories of data subjects and the categories of personal data are set out in Annex I.

4. Etropo's obligations as processor

Etropo will:

(a) Follow instructions. Process Customer Personal Data only on the Customer's documented instructions (clause 2.3), including with regard to transfers to a third country, unless required to do otherwise by law to which Etropo is subject; in that case Etropo will inform the Customer of the legal requirement before processing, unless that law prohibits it on important grounds of public interest.

(b) Keep it confidential. Ensure that every person Etropo authorises to process Customer Personal Data has committed to confidentiality, under a signed confidentiality agreement or a statutory obligation, and has access only to the data they need for their role, as set out in Etropo's Access Control Policy and Human Resource Security Policy.

(c) Secure it. Implement and maintain the technical and organisational measures in Annex II, and keep them under review. Etropo may change a measure, but not so that the overall level of protection falls.

(d) Use Subprocessors only as clause 5 allows.

(e) Help with data subject requests. Taking into account the nature of the processing, assist the Customer with appropriate technical and organisational measures in meeting the Customer's obligation to respond to requests from data subjects. The Service lets the Customer's admins view, correct, export and delete the data themselves. Where a data subject writes directly to Etropo about Customer Personal Data, Etropo will not answer on the merits; it will pass the request to the Customer within 5 business days and tell the data subject it has done so.

(f) Help with security, breach notification and impact assessments. Taking into account the nature of the processing and the information available to Etropo, assist the Customer in meeting its obligations under GDPR Articles 32 to 36. The Trust Center at trust.etropo.com, this DPA and the documents listed under Resources there are the first source of that assistance.

(g) Delete or return the data as clause 8 provides.

(h) Demonstrate compliance as clause 9 provides.

5. Subprocessors

5.1 General authorisation. The Customer gives Etropo general written authorisation to engage the Subprocessors listed in Annex III, and to engage new ones under this clause. The authoritative, current list is published at trust.etropo.com/subprocessors.

5.2 Notice of changes. Etropo will announce the addition or replacement of a Subprocessor on the Updates page of the Trust Center (trust.etropo.com/updates, also available as an RSS feed) at least **30 days before** the Subprocessor first receives Customer Personal Data. A Customer may also subscribe to receive these announcements by email on the Trust Center.

5.3 Objection. A Customer may object, on reasonable grounds relating to data protection, by emailing security@etropo.com within 30 days of the announcement. Etropo will discuss the objection in good faith and, where it can, offer a way to avoid the new Subprocessor processing that Customer's data. Where Etropo cannot accommodate the objection within a further 30 days, the Customer may terminate the Agreement for the affected part of the Service, with written notice, and Etropo will refund any prepaid fees for the period after termination.

5.4 Flow-down and responsibility. Etropo will impose on each Subprocessor, by a written agreement, data protection obligations that provide at least the level of protection of this DPA, in particular on security and confidentiality. Etropo remains fully liable to the Customer for a Subprocessor's performance of those obligations.

5.5 Customer-connected integrations are not Subprocessors. A service the Customer itself connects to Etropo (for example Google Ads, Google Sheets, LinkedIn, Meta, TikTok, Slack, Microsoft Teams, Notion, HubSpot or Attio) receives data only after a Customer admin authorises the connection, and only the data that connection is for. Etropo sends that data on the Customer's instruction; the Customer's agreement with that provider governs the provider's processing, and the Customer can stop the flow at any time by disconnecting the integration in the Service.

6. International transfers

6.1 Where the data is stored. Etropo stores Customer Personal Data in the European Union: the database, file storage and backups run in Frankfurt, Germany (AWS eu-central-1, via Supabase), and the Service's application functions run in Frankfurt (Vercel fra1). Etropo will not move this storage outside the European Economic Area without giving notice under clause 5.2.

6.2 Subprocessors outside the EEA. Some Subprocessors in Annex III process Customer Personal Data outside the EEA, chiefly in the United States. For each of them Etropo relies on a lawful transfer mechanism: the SCCs (Module Three, processor to processor) concluded with that Subprocessor, or an adequacy decision of the European Commission, including the EU-U.S. Data Privacy Framework for a certified Subprocessor. Etropo assesses each Subprocessor's transfer before adding it, as its Third-Party and Vendor Management Policy requires.

6.3 Transfers from the Customer to Etropo. Etropo is established in Poland, in the EEA, so a Customer in the EEA makes no Restricted Transfer by using the Service. Should a transfer from the Customer to Etropo nevertheless be a Restricted Transfer, including because the Customer is established in the United Kingdom or Switzerland, or because Etropo later processes the data outside the EEA, then:

(a) **EU.** The SCCs, Module Two (controller to processor), are incorporated into this DPA and apply to that transfer, completed as follows: Clause 7 (docking clause) is included; in Clause 9, Option 2 (general written authorisation) applies with the notice period in clause 5.2 of this DPA; the optional language in Clause 11 is not included; in Clause 13, the supervisory authority is the one determined by the Customer's establishment; in Clause 17, Option 1 applies and the governing law is the law of Poland; in Clause 18, the courts of Poland have jurisdiction; Annexes I, II and III of the SCCs are Annexes I, II and III of this DPA. Where this DPA and the SCCs conflict, the SCCs prevail for the transfer they govern.

(b) **United Kingdom.** The SCCs as completed in (a) apply, amended by the UK Addendum. Table 1 of the Addendum is completed with the parties' details from Annex I; Table 2 with the SCCs as completed in

(a); Table 3 with Annexes I to III of this DPA; and in Table 4 either party may end the Addendum as its section 19 provides.

(c) **Switzerland.** The SCCs as completed in (a) apply with these adaptations: references to the GDPR include the FADP; the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for transfers governed by the FADP; "member state" includes Switzerland, so that Swiss data subjects may bring claims in Switzerland; and the SCCs also protect the data of legal entities until the FADP no longer does.

6.4 Customer's acceptance. By accepting the Agreement the Customer, as data exporter, and Etropo, as data importer, are each deemed to have signed the SCCs and the UK Addendum where clause 6.3 makes them apply.

7. Personal data breach

7.1 Notification. Etropo will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and in any event in time for the Customer to meet its own 72-hour notification obligation under GDPR Article 33. Notice goes by email to the Customer's organisation admins, and for incidents affecting several customers also to the Updates page of the Trust Center.

7.2 Content. The notice will, so far as Etropo knows it at the time, describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures Etropo has taken or proposes to take, and a point of contact. Information Etropo does not yet have will follow without undue delay as it becomes available.

7.3 Cooperation. Etropo will take reasonable steps to contain the breach and reduce its effects, and will cooperate with the Customer's own investigation and notifications. Etropo's notice is not an admission of fault or liability. Its procedure is the Security Incident Response Plan published on the Trust Center.

8. Return and deletion

8.1 During the term. The Customer can export any budget as an XLSX file from the Service at any time, mirror budgets to Google Sheets or Notion, and delete content through the Service.

8.2 On termination or request. Within 30 days of the end of the Agreement, or of a written request from the Customer's admin to team@etropo.com, Etropo will delete the Customer's organisation, its budgets, versions, line items, comments, dashboards, Marketing Brain entries, integration connections and tokens, and its users' personal data, from the live database. Before deletion, and on request, Etropo will provide a full export of the organisation's data in a machine-readable form within 30 days.

8.3 Backups. Encrypted backups that still hold the data are overwritten by the backup cycle within a further 90 days. Backups are used only to restore the Service and are never read for any other purpose.

8.4 Subprocessors. Data already passed to a Subprocessor (for example a support conversation, or an invoice email) is deleted from that Subprocessor by request or by its own published retention schedule, as listed on the Subprocessors page.

8.5 Exceptions. Etropo may retain Customer Personal Data to the extent and for the period that law requires, keeping it confidential and processing it only for that purpose.

9. Information and audits

9.1 Information. Etropo makes available all information reasonably necessary to demonstrate compliance with this DPA. The Trust Center publishes Etropo's controls with their status, its policies, its subprocessor list and its FAQ; the documents marked "shared on request" there, and the SOC 2 and ISO 27001 reports of the platforms the Service runs on (Vercel and Supabase), are available through it. Etropo will answer a reasonable written security questionnaire within 30 days.

9.2 Audit. Where the information in clause 9.1 is not enough to meet a Customer's legal obligation, the Customer, or an independent auditor it appoints who is bound by confidentiality and is not a competitor of Etropo, may audit Etropo's compliance with this DPA, under these conditions: at most once in any 12-month period, unless a supervisory authority requires it or an audit follows a personal data breach affecting the Customer; on at least 30 days' written notice to security@etropo.com; during business hours, in a way that does not unreasonably disrupt Etropo's business or compromise the security of other customers' data; and limited to the systems and records that process Customer Personal Data. Etropo's Subprocessors' own facilities and systems are audited through those Subprocessors' audit reports, not in person. Each party bears its own costs.

9.3 Findings. The parties will agree the scope, timing and duration of an audit in advance and will discuss its findings in good faith. Etropo will address any material non-compliance an audit shows within a reasonable time.

10. Liability

Each party's liability under this DPA, including the SCCs where they apply, is subject to the exclusions and limitations of liability in the Agreement, except that nothing in the Agreement limits a data subject's rights under the SCCs or a party's liability to a data subject that Data Protection Law does not allow to be limited.

11. General

11.1 Term. This DPA lasts as long as Etropo processes Customer Personal Data, and ends when deletion under clause 8 is complete.

11.2 Precedence. Where this DPA conflicts with the Agreement, this DPA prevails for the processing of Customer Personal Data. Where the SCCs apply and conflict with this DPA, the SCCs prevail.

11.3 Changes. Etropo may update this DPA to reflect a change in Data Protection Law, a change in the Service, or a new version of the SCCs, by publishing the new version on the Trust Center and announcing it on the Updates page. A change that reduces the Customer's protection takes effect only after 30 days' notice; a Customer who objects within that period may terminate as clause 5.3 provides.

11.4 Governing law. This DPA is governed by the law of Poland, and the courts of Poland have jurisdiction, except where the SCCs or Data Protection Law provide otherwise.

11.5 Severability. If a provision of this DPA is invalid, the rest remains in force and the invalid provision is replaced by a valid one that comes closest to its intent.

11.6 Contact. Questions about this DPA go to security@etropo.com. Data subject requests and deletion requests go to team@etropo.com.

Annex I: Description of the processing

A. The parties

	Data exporter (Customer)	Data importer (Etropo)
Name and address	The Customer, as named in its Etropo account and billing details	Etropo, Trakt Napoleoński 31/1, 04-809 Warsaw, Poland. VAT ID PL5842721889
Contact	The admins of the Customer's organisation in the Service	Security Lead, security@etropo.com
Role	Controller (or processor on behalf of its own controller)	Processor
Signature and date	Deemed signed on acceptance of the Agreement (clause 6.4)	Deemed signed on acceptance of the Agreement (clause 6.4)

B. Description of the transfer

Categories of data subjects.

- The Customer's employees, contractors and other users who are given an Etropo account.
- People named in the Customer's budget data: line item owners, people a comment mentions, named contractors, agencies and vendors.
- Contact persons named in invoices the Customer uploads or forwards to the Service.
- Users of the Customer's Slack, Microsoft Teams or HubSpot workspace who talk to the Etropo assistant there.

Categories of personal data.

- Account data: name, business email address, password hash or Google account identifier, optional avatar, two-factor enrolment, organisation membership and role, category permissions.
- Budget content as the Customer enters it: budget, level, category and line item names, planned and actual amounts, currencies, owners, reminders, comments, dashboards, Marketing Brain entries.
- Invoice content: the text extracted from an uploaded or forwarded PDF, which may include the names and contact details of the issuer's staff.
- Integration data: encrypted OAuth tokens for the services the Customer connects, the ad spend imported from them, sync logs.
- Assistant conversations: the questions a user asks the AI assistant in the Service, Slack, Teams or HubSpot, the answers, and the platform user identifiers.
- Technical data: IP address, browser and request metadata, in logs and for rate limiting.

Special categories of data. None. The Customer agrees not to submit any (clause 2.4).

Frequency. Continuous, for the term of the Agreement.

Nature of the processing. Hosting, storage, backup, retrieval, display, computation (totals, variances, currency conversion), analysis by AI models when a user asks a question or uploads a file, synchronisation to integrations the Customer connects, and sending of email and chat notifications.

Purpose. Providing the Service to the Customer under the Agreement, and nothing else.

Retention. For the term of the Agreement, then deletion under clause 8: 30 days from the live database, a further 90 days from backups.

Transfers to Subprocessors. As listed in Annex III: subject matter, nature and duration as above, for the purpose each Subprocessor is engaged for.

C. Competent supervisory authority

For the SCCs, Clause 13: the supervisory authority of the EU member state in which the Customer is established. Where that rule gives no answer, the President of the Personal Data Protection Office of Poland (Urząd Ochrony Danych Osobowych, UODO), ul. Stawki 2, 00-193 Warsaw.

Annex II: Technical and organisational measures

These measures are in place today. Each is also listed, with its evidence, on trust.etropo.com/controls, where the status of every control is kept current. Measures that are planned but not yet operating are not listed here.

Infrastructure and encryption

- The Service runs on cloud platforms that hold SOC 2 Type II reports: Vercel (application, build pipeline, edge network) and Supabase on AWS (database, authentication, storage, backups). Etropo operates no physical servers.
- Customer Personal Data is stored in Frankfurt, Germany (AWS eu-central-1); application functions run in Frankfurt (Vercel fra1).
- Encryption in transit: TLS on every connection, with HTTP Strict Transport Security set for two years and applied to subdomains; connections to third-party APIs are HTTPS only.
- Encryption at rest: database volumes, file storage and backups are encrypted by the provider with AES-256.
- Application-level encryption: OAuth tokens for connected services are encrypted with AES-256-GCM, with a per-record random IV and authentication tag, before they are written to the database; the key exists only in the production environment.
- Secrets (API keys, the token-encryption key, database credentials) are held in the hosting provider's encrypted environment settings, separate for production and preview, and never in source control.
- Every response carries a Content Security Policy, X-Frame-Options, X-Content-Type-Options and a Referrer-Policy.
- Authentication, billing, AI, integration and data-changing endpoints are rate-limited per user or IP address.
- Sign-in and sign-up are protected by a bot challenge verified server-side; sign-ups from disposable email domains are refused.
- Non-production deployments require a team login; only the production domain is public.
- Operating systems, databases and runtimes are patched by the platform providers.

Access control and tenant isolation

- Every table in the application database has PostgreSQL Row Level Security enabled. Each row belongs to one organisation and the policies check the caller's membership on every query, so the database refuses cross-tenant access even if the application has a bug.
- Within an organisation, two roles (admin and user) and category-level permissions decide what each user may see and change; the restriction is enforced in the database. The AI features and the

Slack, Teams and HubSpot assistants see only the data the asking user is allowed to see.

- Two-factor authentication with an authenticator app is available to every user, up to two devices; once enrolled, every page, API call and database query requires the second factor.
- Passwords are hashed with bcrypt, must be at least 12 characters, and are rejected if they appear in known breach corpora.
- Sessions: an idle browser is signed out after 15 minutes, every session cookie expires after at most 14 days, and the authentication provider ends sessions after 168 hours without a refresh and at 720 hours at the latest.
- Etropo personnel access to the production consoles (hosting, database, source control) requires multi-factor authentication. Access is granted on a least-privilege basis under the Access Control Policy and reviewed every quarter.
- Personnel devices have full-disk encryption, a screen lock and automatic updates; customer data is accessed through the browser and is not stored on personal devices.

Secure development and change management

- Every change to the Service goes through a pull request; automated type checking, linting, the unit test suite and the integration test suite run on every pull request before it is merged. Sensitive areas receive human review.
- Dependencies are monitored continuously for known vulnerabilities; fixes follow the service levels in the Secure Development and Change Management Policy.
- Every release can be rolled back to any previous deployment.
- Webhooks from third parties are verified by signature; OAuth integrations use cryptographically random state and encrypted token storage; every input is validated on the server.
- A Responsible Disclosure Policy invites vulnerability reports to security@etropo.com, acknowledged within 48 hours.

Operations, monitoring and resilience

- Errors and uptime are monitored with alerting.
- The production database is backed up daily, encrypted. Documented recovery objectives: application restored within 1 hour with no data loss; database restored within 4 hours with at most 24 hours of data loss. The Business Continuity and Disaster Recovery Plan is published on the Trust Center.
- Authentication events, integration syncs, token operations and inbound webhooks are logged; retention periods are in the Data Management, Classification and Retention Policy.
- Security incidents are handled under the published Security Incident Response Plan, with severity levels, containment steps and the notification duties in clause 7.

Organisation and people

- An Information Security Policy and the supporting policies (access control, secure development, incident response, business continuity, cryptography, data management, vendor management, risk management, acceptable use, human resource security) are maintained, published on the Trust Center and reviewed annually.
- Personnel complete security awareness training on joining and annually. Their access to production systems is reviewed every quarter and removed when they leave.
- Subprocessors are assessed before use for the data they receive, the region, their security evidence and their data protection terms, and reviewed annually under the Third-Party and Vendor Management Policy.

Data minimisation and AI

- Product analytics events carry user and organisation identifiers and feature names, not budget content. Session replay masks all page text and typed input.
- AI model providers receive data only when a user asks a question, builds something or uploads a file, and only the data that user may see; all providers are used under API terms that exclude training on customer data. Two scheduled jobs for organisations with the AI assistant enabled send budget line item names (never amounts) daily and Marketing Brain entries weekly. A Customer can ask to be excluded from AI call tracing.
- Payment card data is handled by Stripe only and never reaches Etropo.

Assistance to the controller

- Self-service export (XLSX, Google Sheets, Notion), self-service correction and deletion of content, and deletion of accounts and organisations on request within 30 days.
- The Trust Center, this DPA, the published policies and the provider audit reports support the Customer's data protection impact assessments and audits.

Annex III: Subprocessors

The authoritative list, with each vendor's purpose, data and region, is trust.etropo.com/subprocessors. Changes are announced on trust.etropo.com/updates at least 30 days in advance (clause 5.2). The list below is current as of the date of this document.

Subprocessor	Purpose	Data received	Processing location
Vercel Inc.	Application hosting, build and deployment,	All application traffic in transit, function logs. Budget data	Germany (functions),

Subprocessor	Purpose	Data received	Processing location
	edge network, AI Gateway routing of model requests	passes through; it is stored in Supabase	global edge network, USA (control plane)
Supabase Inc.	PostgreSQL database, authentication, file storage, daily backups	All Customer Personal Data	Germany (AWS eu-central-1, Frankfurt)
Amazon Web Services (via Supabase)	Underlying cloud infrastructure for the database and storage	Same as Supabase, encrypted at rest	Germany (eu-central-1)
Stripe Inc.	Subscription billing and the billing portal	Billing contact name and email, subscription and invoice records; payment method held by Stripe only	USA
Anthropic PBC (via Vercel AI Gateway)	AI models for the assistant, dashboards, Marketing Brain and the Slack and Teams assistants	A user's question and the budget data that user may see, when the user asks; line item names (daily) and Marketing Brain entries (weekly) for organisations with the assistant enabled. Not used for training	USA
OpenAI	Analysis of uploaded spreadsheets during budget import	The uploaded file and the structure extracted from it, only when a user imports a file. Not used for training	USA
Mistral AI	Text extraction from PDF invoices a user uploads or forwards	The uploaded PDF, only when a user submits one	EU (France)
Resend	Transactional email; receipt of invoices forwarded to a Customer's inbound address	Email addresses, names, email content including forwarded invoices	USA
Upstash	Rate limiting; short-lived chat state for the Slack and Teams assistants	User and organisation identifiers, IP addresses as rate-limit keys, conversation state. No budget content	Germany (AWS eu-central-1, Frankfurt)

Subprocessor	Purpose	Data received	Processing location
Cloudflare	Bot protection on sign-in and sign-up	Browser and request metadata	Global
Sentry (Functional Software Inc.)	Error monitoring and performance traces; session replay with text masked	Error stack traces, request metadata, user identifier, IP address	EU (Germany)
Mixpanel	Product analytics and session replay with all text and typed input masked	User and organisation identifiers, feature events, masked session recordings	USA
Segment (Twilio)	Server-side analytics event pipeline	User identifier, email, organisation identifier, product events	USA
Intercom	In-app support messenger	Name, email, organisation, conversation content and attachments	USA
Linear	Bug reports submitted from inside the Service	Reporter email, report text, attached screenshot	USA
Braintrust	Tracing of AI calls for quality evaluation; an organisation can ask to be excluded	Prompt, tools used and output of each AI call, including the budget data in the request and the content of uploaded files	USA

For every Subprocessor outside the EEA, Etropo relies on the SCCs concluded with that Subprocessor or on an adequacy decision, including the EU-U.S. Data Privacy Framework where the Subprocessor is certified (clause 6.2).

Not Subprocessors. The integrations a Customer connects itself, Google (Ads, Sheets, sign-in), LinkedIn, Meta, TikTok, Slack, Microsoft Teams, Notion, HubSpot and Attio, receive data only on the Customer's authorisation and under the Customer's own agreement with each provider (clause 5.5). GitHub hosts the Service's source code and receives no Customer Personal Data.

Signature page

This DPA takes effect without signature when the Customer accepts the Terms of Service (clause 6.4). Customers whose procedures require a countersigned copy may complete this page and send it to security@etropo.com; Etropo will return it countersigned.

Customer	Etropo
Legal name	Etropo
Registered address	Trakt Napoleoński 31/1, 04-809 Warsaw, Poland
VAT ID	PL5842721889
Signed by (name)	
Title	
Date	
Signature	

Version 1.0, January 2026. The current version is published at trust.etropo.com/resources/data-processing-agreement.

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