

Record of Processing Activities

Orbiq Record of Processing Activities (RoPA)

Document Status: Version 1.2 (Official)
Effective Date: April 13, 2026 (rev. June 1, 2026 — cloud migration + Plaid; rev. August 16, 2026 — LunchFlow BYO-key aggregation)
Supersedes: v1.1 — retained at `archive/RoPA_v1.1_effective_2026-06-01.md`
Data Controller: FINARO CAPITAL SERVICES INC., Toronto, Ontario, Canada — contact: support@orbiq.online
Privacy Officer: Sumeet Chaurasia (on behalf of FINARO CAPITAL SERVICES INC.)
Governing Laws: PIPEDA (Canada), GDPR-aligned best practices

1. Introduction

This Record of Processing Activities (RoPA) identifies and documents the data processing operations conducted by **FINARO CAPITAL SERVICES INC.** (the data controller) through its **Orbiq** application. This document serves as a core artifact for demonstrating accountability under the Personal Information Protection and Electronic Documents Act (PIPEDA).

2. Data Processing Inventory

ID	Activity Name	Purpose of Processing	Data Subjects	Data Categories	Recipients / Third Parties	Cross-Border Transfer	Retention Period	Legal Basis
01	Identity & Account Management	User authentication, profile maintenance, and secure session management [cite: user-guide.html].	App Users	Email address, OAuth tokens, session identifiers, hashed credentials [cite: 26, 28].	Cloudflare (Network Security), Google (IdP)	None (Primary storage in Canada)	15 days after profile closure (per user request).	Contractual Necessity
02	Transaction Import & Management	Processing uploaded financial files for cash flow tracking and analysis [cite: 98].	App Users	Merchant strings, transaction amounts, dates, and account identifiers [cite: user-guide.html].	Internal (Cloud SQL for PostgreSQL, Canada region; CMEK encrypted, RLS-isolated)	None (Primary storage in Canada)	Persistent while account is active; user-initiated "wipe" functionality supported [cite: user-guide.html].	Contractual Necessity
03	AI Expense Categorization	Automated tagging of transactions using Large Language Models [cite: 52].	App Users	Sanitized merchant keywords, generalized amount ranges (PII stripped via local logic) [cite: 1, 3].	Groq Inc. (via API)	USA (Processed under Zero Data Retention) [cite: 1, 3]	Transient (Processed in RAM; Zero Data Retention enabled) [cite: 3].	Consent / Contractual Necessity

04	Operational Logging & Auditing	Debugging, security monitoring, and regulatory compliance [cite: 4].	Users, Admins	IP addresses, login timestamps, admin action logs.	Axiom, Google Cloud Storage (GCS) [cite: 4]	USA (Encrypted archive)	1 year (Minimum requirement) [cite: 4].	Legal Obligation / Legitimate Interest
05	Billing & Subscription	Managing monthly payments for service access [cite: user-guide.html].	App Users	Name, billing address, payment method tokens (No raw card data) [cite: 43].	Stripe	USA / Global	Defined by Stripe and tax regulations (7 years).	Contractual Necessity
06	Currency Conversion	Real-time balance conversion for multi-currency support [cite: 109].	App Users	Transaction amounts and dates (anonymized) [cite: user-guide.html].	Frankfurter API	EU / Global	Transient	Contractual Necessity
07	Bank Sync (Plaid — Connect tier)	Consumer-permissioned import of bank account metadata, balances, and transactions for automatic cash-flow tracking (paid Connect subscribers, US/CA only).	App Users (paid Connect)	Bank account metadata, balances, transactions; Plaid item/account identifiers; encrypted Plaid access token.	Plaid Inc. (via API + Plaid Link)	USA (DPA + SCCs; consumer-consented)	Until user disconnects bank or loses Connect entitlement; access token auto-reaped via <code>/item/remove</code> + revoke on downgrade/lapse/idle. Synced transactions follow ID 02 rules.	Consent / Contractual Necessity

08	Bank Account Aggregation (Core — user-supplied LunchFlow key)	Import of bank account metadata, balances, and transactions from an aggregation account the user holds directly with LunchFlow , read on the user's behalf using an API key the user generates there and pastes into Orbiq. Available on Orbiq Core; no region gate, because a pasted key works wherever LunchFlow reaches.	App Users (Core, opt-in)	Bank account metadata (institution, account name, type, currency), balances, transaction records (date, description, amount), LunchFlow account identifiers, and the user's LunchFlow REST API key (encrypted at rest).	LunchFlow — <i>not an Orbiq processor</i> . The user contracts with LunchFlow directly; Orbiq has no commercial or data-processing agreement with them. See §2.1 for the controller determination.	Determined by the user's own LunchFlow account , not by Orbiq. Orbiq's outbound leg is an authenticated read to LunchFlow's API; the upstream bank rails (GoCardless, Akahu, Pluggy, Finverse, MX/Finicity) sit under LunchFlow's contract with the user, not Orbiq's.	API key retained until the user removes the connection or the key stops authenticating; deleted with the connection row. Imported transactions follow ID 02 rules and survive disconnection — they are the user's ledger, not a cache of LunchFlow's.	Consent (explicit, per-connection) / Contractual Necessity
----	--	--	--------------------------	---	---	---	---	--

2.1 Controller determination for activity 08 (LunchFlow)

This determination is stated explicitly because it changes what Orbiq must disclose, and leaving it implied would be the single easiest inconsistency to find in a published record.

****Orbiq is a controller for the data it receives, and is neither a controller nor a processor for the bank-to-LunchFlow leg. Orbiq and LunchFlow are not joint controllers.****

Reasoning:

1. Orbiq is not LunchFlow's processor. A processor acts on the controller's

documented instructions under a contract. Orbiq has no contract with LunchFlow of any kind — no DPA, no SCCs, no commercial relationship, no reseller arrangement. Orbiq presents a key the *user* issued.

1. LunchFlow is not Orbiq's processor. Orbiq does not instruct LunchFlow,

cannot vary its retention, cannot audit it, and cannot terminate the user's relationship with it. Naming LunchFlow as an Orbiq processor would assert a control Orbiq does not have — which is worse than naming it accurately.

1. Not joint control. Joint control requires jointly determining purposes

and means. LunchFlow determines how it collects from banks and on what terms; Orbiq determines what happens to the data once it arrives. There is

no shared decision and no common purpose set by both parties.

1. **Orbiq is a controller downstream.** From the moment data crosses into

Orbiq's systems, Orbiq alone determines purposes and means (categorization, FX conversion, retention, deletion) and is accountable for it under PIPEDA Principle 1 / 4.1.3, exactly as for imported files (ID 02).

Consequent disclosure obligations, which Orbiq meets:

- The user must be told, *before* choosing this path, that it requires a

separate account with a third party who will bill them directly, and that Orbiq's own coverage is Canada and the US only. This is stated on the homepage pricing card, the comparison table, the features page, the FAQ, and the setup guide, and is enforced continuously by `scripts/claims-audit.py`.

- The user must be told Orbiq holds the API key and how it is protected. See

the Vendor Risk Assessment for LunchFlow and Tier 4 of the Data Classification Policy.

- Orbiq must **not** claim to have vetted LunchFlow's processing on the user's

behalf, because it has no contractual standing to do so. See the residual risk section of the LunchFlow VRA.

2.2 Contrast with activity 07 (Plaid)

The two aggregation paths are governed differently and must never be documented as one row:

	07 — Plaid (Connect)	08 — LunchFlow (Core, BYO key)
Who contracts with the vendor	Orbiq	The user
DPA / SCCs in place	Yes, Orbiq↔Plaid	None — Orbiq is not a party
Who is billed	Orbiq bills the user, one bill	LunchFlow bills the user directly, second bill
Vendor is an Orbiq processor	Yes	No
Credential held by Orbiq	Plaid <code>access_token</code> (Fernet)	User's LunchFlow API key (Fernet)
Region	US / CA only	Wherever the user's LunchFlow account reaches
Orbiq's leverage on incident	Contractual (DPA, <code>/item/remove</code>)	Operational only (stop polling, delete key)

3. Data Transfer Safeguards

For activities involving cross-border transfers (ID 03, 04, 05, 07, 08), Orbiq employs the following safeguards:

- **Zero Data Retention (ZDR):** Explicitly enabled for AI processing to prevent persistent storage on foreign infrastructure [cite: 3, 4].
- **Data Minimization:** Local prompt sanitization strips names and account numbers before transfer [cite: 1, 3].
- **Encryption:** All data in transit is protected via TLS 1.2+ [cite: 4].
- **Aggregator credentials at rest:** Plaid `access_tokens` (ID 07) and user-supplied LunchFlow API keys (ID 08) are Fernet-encrypted at the application layer before persistence, under a key held in GCP Secret Manager. Neither is ever logged or returned to a client.
- **Safeguard asymmetry, stated plainly:** ID 07's transfer rests on a DPA and SCCs between Orbiq and Plaid. **ID 08 has no**

such instrument, because the contract is between the user and LunchFlow and Orbiq is not a party to it. The compensating controls for ID 08 are (a) informed, per-connection consent, (b) the disclosure obligations in §2.1, and (c) the user's own ability to revoke the key at LunchFlow at any moment without involving Orbiq. Orbiq does not represent this as equivalent to a DPA.

4. Individual Rights Fulfillment

Orbiq facilitates the following rights through the application UI and dedicated support channels:

- **Right to Erasure:** Users can initiate a data "wipe" within the application settings; account closure deletes identity records within 15 days; disconnecting a bank revokes and deletes the Plaid access token via `/item/remove`, and removing a LunchFlow connection deletes the stored encrypted API key. Erasure of the account **at LunchFlow** is the user's own action with their own vendor — Orbiq cannot perform it and does not claim to. See the [Data Retention & Deletion Policy](#) [cite: user-guide.html].
- **Right to Access:** Data Subject Access Requests (DSAR) are handled via `support@orbiq.online` or `support@orbiq.online` [cite: 3, 78].
- **Consent Withdrawal:** Users can disable AI-driven features to prevent further categorization processing [cite: 1, 3].

5. References

1. Orbiq Terms of Service (Effective March 22, 2026).
2. Orbiq Legal, Privacy, and Safeguards (Data Sovereignty Clauses).
3. Orbiq User Guide (Feature Overview and Data Management).
4. Orbiq SecOps Implementation Feedback (Security Controls and Logging).