

Dispendo — App Privacy Notice

privacy-2026-10-app-review-draft-1 · 2026-10-07 · EN

DRAFT • LEGAL REVIEW PENDING

Legal/tax details and contractual checks remain incomplete. This document does not certify service compliance.

Contents

Scope and document status

1. Controller and contacts

2. Data and sources

3. Purposes and legal bases

4. Categorisation, AI and merchant search

5. Recipients and providers

6. International transfers

7. Retention and deletion

8. Cookies, tracking and device permissions

9. Security

10. Your rights

11. Account deletion and subscription

12. Children

13. Changes

14. AIS provider and bank flow

Scope and document status

DRAFT FOR PROFESSIONAL REVIEW — NOT THE FINAL PUBLIC-LAUNCH NOTICE Version: privacy-2026-10-app-review-draft-1 Revision: 7 October 2026

This notice covers the Dispendo app, backend and app support, including the private beta. Browsing the website alone is covered by a separate website notice. Language follows the app selection. Acknowledgement is not blanket consent: Terms, bank authorization, AI preferences and device permissions are separate controls.

1. Controller and contacts

The controller is Alberto Schianni, a natural person, at [FULL PUBLIC ADDRESS], Italian tax code [TAX CODE] and, if issued before launch, VAT number [VAT NUMBER AND EXACT REGISTERED BUSINESS/PROFESSIONAL NAME].

- Privacy and rights: privacy@dispendo.app
- Support: support@dispendo.app

Whether a DPO is required, and their contacts if applicable, must be checked before launch. This draft does not claim an appointment that has not occurred.

2. Data and sources

Data you provide

- email, display name, language, preferences and optional profile picture;
- credentials handled by the authentication system; we cannot read your plaintext password;
- entered/imported transactions, amounts, currencies, dates, descriptions, categories, notes, budgets, recurrences and shared-wallet data;
- CSV/XLSX/JSON files selected for import: the app parses them, and the source file is not retained as a server attachment;
- requests, feedback and data you choose to send to support. Do not send passwords, one-time codes, bank credentials or complete exports unless a secure route has been expressly agreed.

Bank and open-banking data

If you voluntarily connect an account through Enable Banking and your bank, we may receive bank and account identifiers, available balance, transactions, descriptions, amounts, currencies, dates, counterparty information (such as name or IBAN), operation/MCC codes and consent/sync metadata. Availability depends on the bank. You enter bank credentials in the bank/provider flow and must not give them to Dispendo.

Transaction descriptions can incidentally reveal highly sensitive information and sometimes special-category facts (for example health, religion or political views). We protect them at a high-confidentiality level and limit use to requested features; the final legal review must confirm the basis and safeguards for any special-category processing.

Apple, Google and device data

Depending on your choices and active features, we may receive:

- identifier, email/name and authentication metadata from Apple or Google;
- notification token and device-permission status;
- subscription product, technical transaction identifiers, status, expiry, renewal, refund or revocation from Apple. We do not receive the payment-card number used in the App Store;
- app/OS version, time, request/session identifiers, errors, IP and technical security/reliability data generated by systems and providers.

Other people's data

A social account does not necessarily need a Dispendo password: access and recovery may depend on Apple or Google. We do not request GPS location to manage spending. A town already present in a bank description is not device geolocation.

Authorized group members see group data and expense attribution. "Add also to group" creates a copy of the supported details in your name, without sharing the entire account or removing the personal source. The copy is separate: do not assume later changes propagate. Check recipients and details before sharing; other members may have retained copies or exports.

A transaction description, counterparty or shared wallet can contain another person's data. Only use data you are entitled to process, keep notes/descriptions necessary, and inform others where required. Dispendo minimises this use and publishes this Notice; the final review must validate the processing and any exception from individual notice for the final use case.

3. Purposes and legal bases

Purpose: Create, authenticate, secure and recover the account · Main data: contact, provider identity, session, security · Proposed basis and decision: contract; legitimate interests for security/abuse prevention [LIA/LEGAL REVIEW]

Purpose: Provide ledger, import/export, budgets, charts, recurrences and sharing · Main data: finance and configuration · Proposed basis and decision: contract

Purpose: Connect accounts and sync requested movements · Main data: bank, consent and connection · Proposed basis and decision: contract; PSD2 consent with the bank/provider is distinct from GDPR consent [ROLE/BASIS REVIEW]

Purpose: Categorise using internal rules and detect refunds/transfers · Main data: transaction signals, categories, corrections · Proposed basis and decision: contract

Purpose: Anthropic enrichment of unresolved cases · Main data: minimised fields described below · Proposed basis and decision: open decision; launch recommendation: separate, specific, revocable consent, off by default

Purpose: Service/security/budget notifications · Main data: token, minimised event, preference · Proposed basis and decision: contract/legitimate interests depending on message; revocable OS permission [LEGAL REVIEW]

Purpose: Manage subscription and entitlement · Main data: product, transaction, status/renewal · Proposed basis and decision: contract and legal obligations

Purpose: Security, limits, diagnostics and incidents · Main data: minimised technical logs · Proposed basis and decision: legitimate interests and legal obligation where applicable [LIA]

Purpose: Prove Terms/Privacy version shown and accepted · Main data: versions, hash, language, source, timestamp · Proposed basis and decision: contract/accountability legitimate interests [LEGAL REVIEW]

Purpose: Respond to rights, complaints and obligations · Main data: request and minimal verification · Proposed basis and decision: legal obligation

Where data is necessary for the contract, the related feature cannot work without it. Bank linking, notifications, avatar, social sign-in and external enrichment are optional and must be separately controllable.

Current state: the beta enables external AI by default, with an opt-out. The switch is not represented as prior consent. Before launch, approve the legal basis and choice flow; an opt-in also needs a technical change. Reading this draft does not replace or remedy that assessment.

4. Categorisation, AI and merchant search

Most movements are processed in the Dispendo backend using deterministic rules. When advanced categorization is on, a still-unrecognised movement may be sent to Anthropic (Claude models) to suggest a category or identify a merchant through web search.

Fields are limited to what is necessary, such as normalised merchant, direction, amount/currency, day of month, recurrence, MCC/operation code and cleaned remittance. Public merchant search uses a normalised descriptor and limited context, not exact amount/date. Before sending, controls strip IBANs, card numbers, phone numbers, email addresses and tax codes and replace names that appear to identify private people. We do not send user ID, the user's IBAN or account balance. Redaction is heuristic and cannot guarantee identification of every personal identifier: information is minimized and potentially personal/pseudonymized, not necessarily anonymous.

Turn the option off in Privacy to prevent new external requests without disabling rules, corrections or private memory. It does not recall requests a provider has already received. Withdrawal of any consent does not affect earlier lawful processing.

Check the applicable Anthropic agreement, data-use settings and retention for Dispendo before promising absolute non-retention or no training.

Google Places is currently observation-only experimental processing and must not be active for public users until separately approved, configured and disclosed. Community learning is disabled and will not be activated without a new assessment, notice and user choice where required.

Categories remain editable suggestions. We do not make solely automated decisions producing legal or similarly significant effects under GDPR Article 22.

5. Recipients and providers

Only services relevant to the selected feature are used. The current technical list includes:

- Supabase: authentication, database, storage, functions and backend operations;
- Enable Banking and the selected bank/ASPSP: open-banking connection and data;
- Anthropic: external categorisation/search only where enabled and applicable;
- Google: optional sign-in, Firebase Cloud Messaging and Places only if later approved;
- Apple: distribution, purchases, optional sign-in and APNs notification transport;
- Resend: transactional and security emails;
- Cloudflare: DNS/TLS and email-link landing pages;
- Netlify: public pages and the separate admin-console host;
- email routing and the operator's mailbox service: inbound support;
- advisers or authorities only where necessary and legally based.

[PRE-LAUNCH: state the contracting entity, role, DPA/agreement, regions, subprocessors, retention, deletion, incident contact and transfer for each party. Do not automatically label every party a processor without review.]

We do not sell personal data or use it for behavioural advertising. No advertising or third-party analytics SDK was identified in the current source audit; this must be rechecked against the final signed binary.

6. International transfers

The main project is configured in a European region, but some providers/subprocessors may process data outside the EEA. Before public launch, this section will identify each destination and applicable safeguard, such as an adequacy decision, Standard Contractual Clauses and supplementary measures.

[BLOCKER: complete provider contracts and the transfer assessment in the vendor register. Do not publish this as final until verified.]

7. Retention and deletion

We apply the shortest period compatible with the purpose unless a documented legal duty requires retention:

Data: account, profile, preferences and avatar · Planned rule: until account/content deletion or replacement

Data: manual/imported movements and normalised bank data · Planned rule: until row, connection or account deletion according to the selected control

Data: import source file · Planned rule: not retained as a server attachment; imported rows and necessary provenance remain

Data: raw bank payloads · Planned rule: no more than 12 months from retrieval or 90 days after an expired/revoked connection becomes stale, if earlier

Data: completed/consumed/expired OAuth attempts · Planned rule: no more than 30 days after the last lifecycle event

Data: notification tokens · Planned rule: until logout, invalidation, removal or account deletion

Data: purchase/entitlement records · Planned rule: for contract reconciliation and applicable legal duties [DEFINE PERIOD]

Data: legal acceptances · Planned rule: currently until account deletion; any minimal post-deletion record requires a new documented decision

Data: security/email/provider logs · Planned rule: [VERIFY MAXIMUM PERIOD BY PROVIDER/PLAN]

Data: console authorization audit · Planned rule: 30 days, minimal operator data, not financial content

Data: backups · Planned rule: [INSERT SUPABASE PLAN, RPO, PERIOD AND MAXIMUM DELETION LAG]

Data: privacy requests, complaints and incidents · Planned rule: [DEFINE MINIMISED PERIOD WITH COUNSEL]

“Deletion” means removal from the live system. Residual protected backups/provider logs are not reused in the app and expire under maximum verified periods to be inserted here. After a restore, deletions must be reapplied so deleted data does not silently return.

8. Cookies, tracking and device permissions

There is no implemented general account deletion after 24 months of inactivity. A European database region alone does not guarantee that all processing remains in the EEA.

At launch, public informational pages must not use advertising cookies or unnecessary analytics. Technical confirmation/recovery pages may use only local storage or data strictly necessary to complete and protect the flow, without profiling. If analytics, cookies or SDKs are added later, we will update the assessment, controls, notice and consent before activation.

Notifications and other device permissions are requested in the context of their feature and can be revoked in iOS Settings; the related function may then be unavailable.

9. Security

Controls include TLS, user-scoped authorisation, least privilege, private avatar storage, server-side secrets, minimised logging, dependency review, operator MFA, retention jobs and incident/recovery procedures. No system is completely secure: protect your device/account and contact support@dispendo.app if you suspect abuse. Do not email complete banking data.

10. Your rights

Where applicable, you may request access, correction, erasure, restriction, portability and object to processing; you may withdraw consent without affecting prior processing. Rights are not absolute, and proportionate identity verification may be required.

In the app you can:

- edit various data and preferences;
- export transactions as CSV/Excel/JSON;
- download a versioned JSON account-data archive; and
- delete individual data and the entire account.

The account archive excludes credentials and raw provider payloads but includes normalised finance data and information owned by the user. For other rights, email privacy@dispendo.app. We will respond without undue delay and normally within one month, subject to lawful extensions/notices.

You may complain to the Italian Data Protection Authority at <https://www.garanteprivacy.it/>. Without limiting that right, we invite you to contact us first so we can try to resolve the concern.

11. Account deletion and subscription

“Delete account” in Profile requires explicit confirmation and removes the authentication user and owned live data, including avatar objects, unless documented law requires retention. Shared/other person data is handled according to ownership, roles and applicable duties. Backups/logs expire as described in section 7.

Account deletion does not cancel an Apple subscription. The app must first offer a direct route to manage it but may not block immediate deletion. See the public “Support and account deletion” page for details.

12. Children

The public service is not intended for anyone under 18. If we learn of an underage account, we will assess and take proportionate steps, including deletion where required. Contact privacy@dispendo.app.

13. Changes

We will publish the date and version of every update. For material changes to purposes, providers, transfers or rights, we will provide appropriate notice and collect renewed consent/acceptance where required. Versions linked to acceptance evidence remain immutable.

14. AIS provider and bank flow

We use Enable Banking Oy, Business ID 2988499-7, Otakaari 5, 02150 Espoo, Finland, registered as an AIS provider supervised by FIN-FSA. Where its authorization is used, separate provider terms/notice apply: <https://tilisy.enablebanking.com/terms>. The actual agreement and privacy roles must still be confirmed. Not every recipient is automatically a processor.

Authorization/renewal follow the bank/provider flow. We do not promise a uniform 180-day duration or real-time information. Revocation/disconnection stops new retrieval according to the flow; erasing history is separate. PSD2 consent and GDPR basis are not interchangeable. For third-party or special-category data, minimization and contract do not replace necessary Article 9/14 assessments.

Operational/product console statistics derive from curated, aggregate service surfaces with small-sample suppression, not unrestricted browsing of personal expenses. Thresholds and pseudonymization alone do not guarantee anonymity.