FINDINGS

Consumer Health Data Privacy Notice

UNIT01 d.o.o.
Vodovodska 75, 11030 Belgrade, Serbia
hello@unit01.dev

Version: 8 July 2026
Canonical web version:
https://getfindings.com/consumer-health-privacy

Official PDF export. This document matches the web version at the URL above as of the version date. We may update the web version from time to time; check the canonical URL for the latest text.

1. Scope

This notice supplements our Privacy Policy (https://getfindings.com/privacy) for United States residents whose consumer health data may be subject to state laws — including Washington's My Health My Data Act (MHMDA), Nevada's consumer health privacy laws, Connecticut's health-data provisions, and similar statutes in other states.

Findings is personal health intelligence software. We help you organize lab results, track biomarkers, log optional daily readings, and follow a profile-based health plan informed by published screening guidance. We do not provide medical diagnosis, treatment, or emergency care.

Findings is software membership. You arrange laboratory draws at any lab worldwide; we do not sell or bundle blood tests, operate laboratories, or provide clinical services.

2. Categories of consumer health data

Depending on how you use Findings, we may collect, process, and store the following categories of consumer health data:

- Laboratory reports and biomarker values you upload (including OCR-extracted values you confirm)
- Health profile information: chronic conditions, surgeries, family history, medications, and related context
- Daily tracker readings (e.g. blood pressure, blood glucose, SpO ,, weight) and custom trackers
- AI chat messages, conversation history, and generated summaries related to your health context
- AI Health Context memories (short factual statements you add or we extract from chat)
- Optional consumer genetics files you choose to import — for educational discussion topics only, not diagnosis
- Retest reminders, notification preferences, and related wellness scheduling metadata

We do not intentionally collect government ID numbers unless you include them in an uploaded document. We do not use continuous GPS tracking.

3. Sources of consumer health data

- Directly from you — registration, profile, uploads, trackers, medications, chat, and settings
- Automatically when you use the Service — OCR, trend calculations, retest scheduling, AI context assembly
- From subprocessors under our instructions — authentication (Supabase), AI inference (Anthropic, OpenAI embeddings), subscription status (RevenueCat)
- Optional future health-platform sync (Apple Health / Google Health Connect) only for tracker types you authorize

4. How we use consumer health data

Purpose	Examples
Service delivery	OCR, biomarker storage, charts, personalized plan items, reminders, medications module

AI features	Chat coach, scoped overviews, memory extraction, embeddings for memory search
Account & support	Authentication, subscription access, customer support
Security	Fraud prevention, rate limits, abuse detection, audit logs
Improve reliability	Aggregated or de-identified error and performance analysis — not sale of identifiable health data

We do not sell your consumer health data. We do not share it with third parties for their independent marketing. We do not use your health data to train general-purpose AI foundation models.

We share data with subprocessors who process it on our behalf under contract. The current list is published at https://getfindings.com/trust#subprocessors and in our Privacy Policy (Section 8).

5. Consent for uploads

Before processing special-category health data from lab uploads or optional genetics imports, we require your explicit consent in the product:

- I confirm this is my own health information (or I have permission to upload it), and I consent to Findings processing it to extract biomarker values — as described in the Privacy Policy.
- I confirm this is my own genetic export (or I have permission to upload it), and I consent to Findings processing it to surface educational discussion topics — as described in the Privacy Policy.
- Encrypted in transit and at rest. Original files are processed for OCR and removed from storage after successful extraction; unfinished uploads are purged within 6 hours. Verify extracted values before relying on trends or AI.
- Encrypted in transit and at rest. Raw files are parsed once and not kept after review. Consumer genotyping can be wrong — confirm with a clinical laboratory before medical decisions.

You may withdraw consent by deleting uploaded data, disabling features, or deleting your account. Withdrawal does not affect the lawfulness of processing before withdrawal.

6. How we share consumer health data

We disclose consumer health data only as described in our Privacy Policy, including:

- Subprocessors listed below and in Privacy Policy Section 8
- When required by law, court order, or to protect rights, safety, and security
- In a merger or acquisition, subject to equivalent protections and notice where required

We do not sell or share consumer health data for cross-context behavioral advertising.

Provider	Role	Data involved	Location / notes
Supabase, Inc.	Database, authentication, encrypted storage, Row Level Security	Account, profile, health records, chat, memories, embeddings	EU/US — DPA via Supabase dashboard (Org !' Legal documents)
Fly.io, Inc.	API application hosting (NestJS backend)	Request metadata, operational logs; health payloads in transit to/from API	US/EU regions — pre-signed DPA in Fly dashboard !' Compliance

Vercel, Inc.	Web application hosting (Next.js frontend)	Access logs, IP addresses; may proxy /api/v1 to API when configured	Global edge — DPA incorporated in Vercel terms (vercel.com/legal/dpa)
Anthropic, PBC	OCR, chat, summaries, memory extraction, titles, drug interaction text	Lab images/PDFs, chat content, assembled health context	US — DPA in Anthropic Commercial Terms; no training on API customer data
OpenAI, LLC	Text embeddings for memory search only	Memory text (category, key, value)	US — DPA at openai.com/policies/data-processing-addendum
RevenueCat, Inc.	Subscription management and webhook billing events	User ID, subscription status, product IDs	US — DPA at revenuecat.com/dpa
Apple Inc. / Google LLC	In-app purchases when you subscribe via App Store or Play Store	Payment handled by platform; we receive entitlement status via RevenueCat	Per platform policies
Resend, Inc.	Transactional email (when enabled)	Email address, notification content	US — DPA at resend.com/legal/dpa
Expo (push infrastructure)	Mobile push notifications	Push token, notification payload	US
Upstash, Inc.	Redis job queue (OCR and notification workers)	Job metadata (upload IDs, user IDs); not full health records in queue payloads by design	EU/US — DPA incorporated in Upstash terms (upstash.com/trust/dpa.pdf)
PostHog, Inc.	Optional product analytics (when you opt in)	Pseudonymous device ID, product event names, coarse usage metadata — not lab or health profile content	EU (eu.posthog.com) — DPA at posthog.com/dpa
Meta Platforms, Inc.	Optional campaign measurement (Conversions API via server-side tags when enabled)	Hashed email (SHA-256), pseudonymous event IDs, browser/click identifiers (fbp/fbc), coarse conversion events (e.g. signup, membership) — not lab values or health profile content	US — Meta Business Tools Terms; only when you opt in to campaign measurement where required
Google LLC	Optional Google Tag Manager, Google Ads, and Google Analytics measurement when enabled	Hashed contact info for enhanced conversions where used, gclid, pseudonymous analytics IDs, coarse conversion events — not lab values or health profile content	Global — Google Ads/Analytics terms; only when you opt in to campaign measurement where required
Stape.io	Server-side tag management hosting (routes measurement events when campaign measurement is enabled)	Event payloads for measurement forwarding (hashed contact info, click IDs, coarse conversion metadata) — not lab values or health profile content	EU/US — DPA at stape.io; optional subprocessor for measurement only

7. Your rights

Depending on your state, you may have the right to:

- Confirm whether we collect, share, or sell your consumer health data (we do not sell)
- Access and obtain a copy of your consumer health data
- Delete your consumer health data
- Correct inaccurate consumer health data
- Withdraw consent for future collection or sharing where consent is the legal basis
- Receive a list of categories of third parties with whom we share consumer health data
- Appeal our denial of a rights request where required by law (e.g. Washington MHMDA)

How to exercise rights

- In-app: Settings !’ Privacy & data (cookie preferences, export, delete account); edit profile, memories, and medications. Delete specific data without closing your account: https://getfindings.com/delete-data. Account deletion: https://getfindings.com/delete-account
- Email: hello@unit01.dev from your registered address
- Privacy choices: Settings !’ Privacy & data, or the Privacy choices link in the site footer

We will verify your identity before fulfilling requests. We aim to respond within 45 days (or the period required by your state's law). If we need more time, we will notify you.

Authorized agents

You may designate an authorized agent to submit requests on your behalf where your state allows. We may require proof of authorization and verify your identity directly.

Appeals

If we deny your request, you may appeal by emailing hello@unit01.dev with the subject line "Consumer health data appeal" and describing why you believe the denial was incorrect. We will respond to appeals within the timeframe required by applicable law.

Non-discrimination

We will not discriminate against you for exercising privacy rights under applicable state law, including by denying goods or services, charging different prices, or providing a different level of service — except as permitted by law.

8. Retention

We retain consumer health data while your account is active and as needed to provide the Service. After account deletion, data is deleted or anonymised subject to backup windows and legal retention requirements. Raw lab files are removed after successful OCR; see Privacy Policy Section 7.

9. HIPAA

Findings is generally not a HIPAA covered entity or business associate for typical direct-to-consumer use. We implement security safeguards appropriate to health data but do not represent HIPAA certification unless explicitly agreed in a B2B contract. Contact us about a Business Associate Agreement for covered-entity integrations.

10. Children

The Service is for adults 18 and over. We do not knowingly collect consumer health data from children. Contact us if you believe a child has provided data.

11. Changes

We may update this notice. Material changes will be posted on this page with an updated date. Continued use after the effective date constitutes acceptance where permitted by law.

12. Contact

UNIT01 d.o.o., Vodovodska 75, 11030 Belgrade, Serbia. Data protection contact: Rade Joksimovic. Email: hello@unit01.dev.