FINDINGS

Data Protection & Security Overview

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

Version: 8 July 2026
Canonical web version:
https://getfindings.com/trust

Security

Findings processes sensitive health data. Security is a product requirement — not a marketing badge. We implement technical and organizational measures appropriate to the risk and assess them against common diligence frameworks (see Compliance posture below).

Data in transit and at rest

- Health data is transmitted over TLS (HTTPS) between your devices and our services
- Data at rest is stored in encrypted databases and object storage provided by our infrastructure vendors
- Authentication credentials are managed by Supabase Auth — we do not store plaintext passwords
- Row Level Security (RLS) in PostgreSQL restricts database access so users can only read their own records

Access control

- Production access is limited to personnel who need it to operate the service
- API endpoints require authenticated sessions for user health data
- Gated features enforce subscription and preview tiers server-side — not only in the client

Application security

- OCR and AI features run server-side; model API keys are not exposed to clients
- Upload and chat flows include consent and disclaimer surfaces before processing health data
- AI chat responses may be reviewed by automated safety checks before delivery
- We minimize data in background job queues (metadata only where possible)

Compliance posture (self-assessed)

We map our controls to the frameworks below and review them on an internal cycle. This is our diligence posture — not a substitute for a customer-specific security questionnaire or independent audit report.

Framework	Our posture	Attestation
GDPR	Aligned — privacy notice, explicit consent for health data (Art. 9), transfer safeguards, and user rights in product (access, export, delete).	Self-assessed
CCPA / CPRA & US state health privacy	Aligned — consumer health data notice, no sale of health data, rights and appeal workflows where required.	Self-assessed
ISO 27001	Security program mapped to ISO 27001 Annex A controls (encryption, access control, incident response).	Self-assessed — not ISO 27001 certified
SOC 2	Controls informed by SOC 2 Trust Services Criteria (security and availability) — subprocessors under contract, RLS, server-side gates.	Self-assessed — no SOC 2 report
HIPAA	Health data safeguards informed by HIPAA Security Rule practices. Generally not a HIPAA covered entity for typical direct-to-consumer use.	Self-assessed — BAA available for enterprise on request

Compliance statements on this page reflect our internal control assessments and documented practices. They are not independent third-party certifications. We will update this page if we obtain formal ISO 27001, SOC 2, or other external attestation.

Incident response

If you believe your account has been compromised, contact hello@unit01.dev immediately. UNIT01 d.o.o. maintains internal procedures for assessing and notifying breaches where required by applicable law (including GDPR Articles 33/34 and US state breach notification rules).

AI transparency

Findings uses artificial intelligence for specific features — not as a replacement for clinical judgment. You should know when AI is involved, what it receives, and what it cannot do reliably.

Where we use AI

- OCR — extracting biomarker values from uploaded lab PDFs and images
- Scoped overviews — short summaries on dashboard, biomarker detail, trackers, checkup plan, and related surfaces
- AI chat — conversational explanations using your stored health context
- Memory extraction — optional facts stated in chat, stored for future context (editable by you)
- Memory search embeddings — semantic retrieval of relevant memories in chat (OpenAI embeddings)

Marketing demos on our public website use illustration-only AI copy — not your data.

What data AI features receive

When you use AI features, our servers may send subprocessors a bundle that can include:

- Profile demographics (age, sex, country) and medications
- Recent biomarker values and trends
- Daily tracker readings (typically last 14 days)
- Relevant conversation-derived memories
- Your chat message and prior messages in the same thread
- For OCR — the lab file or image you uploaded

Anthropic processes most AI features; OpenAI processes embeddings only. API terms with these providers prohibit using your data to train their general models.

Limitations

- AI outputs may be incomplete, outdated, or incorrect — verify with your clinician
- AI does not diagnose, prescribe, or perform emergency triage
- OCR may misread values — you must confirm extractions before saving
- Automated safety review may block or flag some chat responses

AI responses are not medical advice. In an emergency, call your local emergency number.

Your choices

- You choose whether to upload labs, use chat, or open AI overviews
- You can edit or delete conversation-derived memories in Profile
- You can delete your account and associated AI history

- Full AI chat send requires an active membership after preview tiers

Regulatory positioning

Findings is personal health data organisation and education software. It helps adults upload laboratory reports, track biomarkers over time, log optional daily readings, and follow a profile-based health plan informed by published screening guidance.

We are the intelligence layer — software membership. Users arrange blood draws at any lab; we do not sell or bundle laboratory services.

What Findings is not

- Not a medical device — not FDA-cleared or CE-marked as a device
- Not a substitute for a qualified healthcare professional
- Not for emergency triage or acute care decisions
- Not a laboratory or provider of diagnostic testing
- Not a drug interaction checker or prescribing system
- Not intended to diagnose, treat, cure, or prevent disease

United States

We position Findings as a general wellness and education tool for informed adults — not as Software as a Medical Device (SaMD) intended to diagnose or treat disease.

European Union and United Kingdom

UNIT01 d.o.o. is established in Serbia. For EEA/UK users, we process special category health data under GDPR Article 9 with explicit consent. We do not market Findings as a medical device under EU MDR.

Subprocessors

We use service providers ("subprocessors") who process personal data on our behalf under written terms. This list is also in our Privacy Policy (https://getfindings.com/privacy#sharing).

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

Questions: hello@unit01.dev.

UNIT01 d.o.o. · hello@unit01.dev · Last updated 8 July 2026

UNIT01 d.o.o. · hello@unit01.dev · Last updated 8 July 2026

UNIT01 d.o.o. · hello@unit01.dev · Last updated 8 July 2026

UNIT01 d.o.o. · hello@unit01.dev · Last updated 8 July 2026