



FOV Pro — Security & Data Handling Statement

How FOV Pro handles data, and what it deliberately never holds.

Self-contained by design

FOV Pro runs entirely on the user's device. Field of view simulations, captures, site positions and coverage information are created on the phone and stay on the phone: captures save to the device's own photo library, under the user's control and the platform's standard protections. Makalen Pty Ltd operates no cloud service that receives, stores or can access this material. For organisations whose camera placements and coverage constitute security design information, this is the core assurance: FOV Pro is a tool used on site, not a repository of your sites.

What FOV Pro never collects

- Captures, images or video produced with the app, and any site or coverage information they contain
- GPS positions, mounting locations or any record of where the app has been used
- Payment card details (payments are processed entirely by Apple, Google or Stripe — see below)
- User accounts, passwords or personal profiles — no account is required to use FOV Pro

Data flows, in full

Camera specification database. The app retrieves camera specification data (published manufacturer figures) from Makalen's database over TLS-encrypted connections. This flow is inbound reference data only; nothing about the user's activity, position or captures travels the other way.

Subscriptions. Purchases are made through Apple App Store and Google Play billing, with entitlements managed via RevenueCat. Apple and Google are the merchants of record: card data is collected and processed solely by them and never touches Makalen systems. Website and enterprise purchases are processed by Stripe, a PCI DSS Level 1 certified payment processor; card details are entered directly into Stripe-hosted checkout and are never received, stored or accessible by Makalen. Subscription state is tracked against an anonymous identifier, not a personal profile.

Diagnostics. Platform-standard crash reporting only, as disclosed in the app store listings. No capture content or location data is included.

Operational practices

Administrative access to Makalen systems (app store consoles, database, hosting, build infrastructure) is protected by multi-factor authentication and least-privilege credentials. Application builds are signed and distributed exclusively through the Apple App Store and Google Play, with their review and integrity protections. Database access from the application is read-only and scoped, with credentials held server-side and never embedded in the client. The FOV Pro website is served exclusively over TLS with HSTS and hardened security headers. Email from FOV Pro domains is authenticated with SPF, DKIM and enforced DMARC. The camera specification database is backed up routinely, and dependencies are monitored for published vulnerabilities as part of the release process.

Privacy and contact

Makalen Pty Ltd voluntarily aligns its handling of personal information with the Australian Privacy Principles. Because the application is self-contained, the personal information Makalen actually holds is limited to what users choose to send us directly (for example, support correspondence). Security questions, vulnerability reports and privacy enquiries: security@fovpro.app, as published at fovpro.app/.well-known/security.txt. We respond to responsible disclosure in good faith and acknowledge reports promptly.

This statement describes the application and practices current at the date shown and is reviewed as the product develops. It is provided for supplier assessment and procurement purposes and may be reproduced for that use.