

Vendor security pack

Answers to the questions of vendor security questionnaires, in the order of the usual sections (inspired by CAIQ-Lite and SIG-Lite).

Version 1.1, 27 October 2026

Security and personal data contact: contact@finozio.com

This pack describes the Finozio service as of its version date. Each answer was checked against the service's source code, configuration or technical documentation. When the answer is "no" or "not yet", we say so. The privacy policy (www.finozio.com/en/politique-confidentialite) is authoritative for the list of sub-processors and retention periods.

- | | |
|---|---|
| 1 Governance and organisation | 8 Logging and monitoring |
| 2 Hosting and data location | 9 Backups and continuity |
| 3 Sub-processors and artificial intelligence | 10 Incident response |
| 4 Encryption | 11 Vulnerability reporting and management |
| 5 Access to your Azure and Microsoft 365 environments | 12 Retention, reversibility and end of contract |
| 6 Authentication and access control | 13 Personal data protection (GDPR) |
| 7 Separation between clients | 14 Sub-processors |

1. Governance and organisation

Who is the vendor?

FINOZIO SAS, 47 rue Vivienne, 75002 Paris, France, Paris Trade and Companies Register (RCS) 109 096 388.
Security and personal data contact: contact@finozio.com.

Do you hold a security certification (ISO 27001, SOC 2...)?

IN PROGRESS

In progress for ISO 27001: the process started in October 2026 – gap assessment against the standard's 93 controls and action plan completed –, with a certification audit targeted for 2027 by a COFRAC-accredited body. Finozio does not yet hold a certification and has not yet been audited by an independent third party. SOC 2: not planned at this stage.

Has a third party performed a penetration test?

NOT YET

Not yet. No penetration test has been performed by an independent provider. An internal security review of the code and configuration was carried out in October 2026; its fixes are tracked in the code repository.

Have you appointed a DPO (GDPR, Article 37)?

NO

No, no DPO has been appointed. Personal data requests go to contact@finozio.com.

Do you have a written information security policy?

PARTIAL

Partially. There is no formal, published security policy. Security rules and procedures (key rotation, protection of server access, backup, restore) are written in the service's technical documentation, and part of them is enforced by automated tests.

Are code changes checked before going to production?

YES

Yes. Every change goes through a merge request and an automated verification chain before deployment: unit, integration and end-to-end tests, static analysis, secret scanning, audit of known-vulnerable dependencies (npm audit, pip-audit) and a 72-hour quarantine for any dependency version that is too recent.

2. Hosting and data location

Where is the data hosted?

In the European Union: the database and authentication at Supabase, in Paris (AWS region eu-west-3); the website, the platform and their cache at Railway, in Amsterdam (Netherlands); error traces at Sentry, in Frankfurt (Germany); the off-site copy of the backups at Microsoft Azure, France Central region, replicated to the paired France South region.

Does any data leave the European Union?

YES

Yes, to some sub-processors (section 3): Cloudflare, whose network carries all traffic to the website and the platform; Anthropic, for the Aurora AI assistant, from the Pilot plan; Resend, for emails; Stripe, for payment; and, only with the visitor's consent and on the public pages of the website, Google, LinkedIn and Apollo. Supabase, Railway and Sentry keep the data in the EU but are companies established outside the EU: access from outside remains possible, governed by standard contractual clauses.

Is the service multi-tenant?

Yes: a single instance of the service and a single database for all clients, logically separated per client (section 7). There is no dedicated hosting and no per-client instance.

3. Sub-processors and artificial intelligence

Who are your sub-processors, and what do they receive?

See the table at the end of this pack. It follows the list in the privacy policy, which is authoritative.

What data does the Aurora AI assistant send to Anthropic?

Aurora is Anthropic's Claude model (United States), called through its API from our servers, from the Pilot plan. Sent: conversation content (questions, answers, and the context entered to assess a recommendation); the client's name and plan; aggregated Azure costs (total, per service, per resource group and per subscription, with its name or, failing that, its identifier) and their forecast; recommendations; the name, type, resource group, region, SKU and state of unused resources; the name, size and usage metrics of virtual machines; for Microsoft 365, aggregated counts and amounts. Never sent: connection secrets, resource tags, or any per-user Microsoft 365 data (no name, email or UPN). Basis: standard contractual clauses.

Do the free scan and Audit Spring send data to Anthropic?

No. The Free and Audit Spring plans do not include Aurora, and free scans call no AI: the server checks the client's plan before any call to Anthropic.

Is your data used to train an AI model?

NO

Finozio trains and fine-tunes no model: Aurora calls the Claude model through Anthropic's API, with no fine-tuning on your data.

4. Encryption

Is data encrypted in transit?

YES

Yes. HTTPS everywhere, with a one-year HSTS header (subdomains included) and httpOnly, Secure session cookies. Between Cloudflare and our servers, the connection is encrypted with certificate verification ("Full (strict)" mode). The application server refuses any unencrypted connection to the database. Between the website and the application server, traffic uses Railway's private network, with no public address.

Is data encrypted at rest?

PARTIAL

Partly by Finozio. Azure connection secrets and Microsoft tokens are encrypted field by field before entering the database (Fernet: AES-128-CBC and HMAC-SHA256), with a key kept outside the database, which can be rotated without downtime. Two-factor backup codes and API keys are stored hashed. Backups are encrypted (AES-256-GCM) before leaving the machine that produces them. Other data (costs, inventory, recommendations) receives no additional application-level encryption: its encryption at rest is that of the database host, Supabase.

Who manages keys and secrets?

Finozio. Encryption keys and production secrets are not in the source code: they are host configuration variables, and automated secret scanning blocks any change that would contain one. The private key that decrypts backups is not on the machine that produces them.

5. Access to your Azure and Microsoft 365 environments

Which rights does Finozio request on Azure?

Two ways to connect a subscription. A Service Principal you create, to which you assign, per subscription, two built-in read-only Azure roles: Reader and Cost Management Reader; optionally, for commitments, two more read-only roles: Reservations Reader (scope /providers/Microsoft.Capacity) and Savings plan reader (scope /providers/Microsoft.BillingBenefits). Or your Microsoft account (OAuth, delegated user_impersonation permission): Finozio then acts with your own rights. No custom role is requested.

And on Microsoft 365?

Microsoft Graph Application permissions, read-only: Organization.Read.All, Reports.Read.All and Directory.Read.All; optionally AuditLog.Read.All, for users' last sign-in date. No mailbox, file or conversation content is read.

Can Finozio change your environment?

No, except on the Custom plan. The requested rights are read-only. On Custom, the automation rules your administrator enables can stop, resize and restart virtual machines, delete orphaned disks and release public IP addresses, with the account connected to the subscription: your Microsoft account, or a Service Principal to which you yourself granted write rights. Remediation scripts (Azure, and Microsoft 365 license removal) are generated by Finozio, then reviewed and run by your administrator: Finozio never runs them.

Are the credentials stored?

YES

Yes. The Service Principal secret or the Microsoft token is stored, encrypted (section 4), until you delete it; it is used for subsequent readings, including the nightly one from Pilot. The free scan stores none: it keeps only the tenant and subscription identifiers, for 90 days — unless the prospect opts into the free monthly report (unchecked by default): their access is then stored encrypted the same way, for 12 reports at most, and deleted as soon as it stops (one-click stop link, purchase of a plan or access failure).

Do you install an agent in our environment?

NO

No. Finozio reads the Azure (Azure Resource Manager, Cost Management) and Microsoft Graph APIs; nothing is installed.

How do we revoke access?

At any time, on both sides: by deleting the connection from your Finozio workspace, and, at Microsoft, by deleting the Service Principal or its role assignments, or by revoking the consent granted to the application.

6. Authentication and access control

How do users authenticate?

With an email address and password (Supabase's authentication service), or with enterprise SAML single sign-on (SSO), from the Scale Up plan, on domains whose ownership is verified. Passwords are at least 12 characters long and stored hashed by Supabase; a password found in known breaches is refused (checked against Have I Been Pwned, which receives only the first 5 characters of its SHA-1 fingerprint).

Is two-factor authentication available, and mandatory?

PARTIAL

Available to every account (TOTP authenticator app, with 10 backup codes stored hashed). Mandatory for Finozio's administration accounts, whose powers exist only after the second factor. Not yet: a client cannot enforce it on the members of its workspace. With SSO, your identity provider's rules apply, two-factor authentication included.

Are you protected against brute-force attacks?

YES

Yes. CAPTCHA (Cloudflare Turnstile) at sign-up, sign-in and password reset; sign-in lock after 5 failures in 15 minutes from the same IP address, and after 50 attempts in one hour on the same account, all addresses combined — so a third party cannot lock a customer's account from their own address (for the two-factor code: 5 in 15 minutes and 20 in 24 hours); rate limiting of sign-in attempts per IP address.

How are sessions handled?

With an httpOnly, Secure, SameSite=Lax session cookie valid for 2 hours, renewed by a 7-day refresh token that Supabase replaces on each use.

Which roles and API keys?

Separate roles in each client workspace (administrator, reader), and API keys with a limited scope (read, write, delete), stored hashed, which never carry Finozio's administration powers.

Can Finozio staff access our data?

Yes: Finozio's super-administrators, for support and operations, with mandatory two-factor authentication. Each time a super-administrator opens your workspace, it is recorded in the audit log (who, when, IP address), kept for 2 years.

7. Separation between clients

Is client data separated?

YES

Yes, logically: in the shared database, every application server query is filtered server-side on the user's workspace, and any request about another client's workspace is refused. In addition, row-level security (RLS) is enabled on every table, with no access for Supabase's public keys: only the application server reads the database. An automated test replays every migration and checks this rule on each table.

A dedicated database or encryption key per client?

NO

No: a single database and a single secret encryption key for all clients.

8. Logging and monitoring

Are sensitive actions logged?

YES

Yes: Azure credentials, users, API keys, automations, two-factor authentication and a super-administrator opening a client workspace, with the author, date and IP address. The log is kept for 2 years, then deleted automatically.

Do we have access to these logs?

PARTIAL

Not directly: the audit log is restricted to the Finozio team, which provides an extract on request. No export to a SIEM yet, and entries are not signed.

How is the service monitored?

PARTIAL

Availability monitored continuously by external probes (UptimeRobot); technical errors reported automatically to the team (Sentry, traces cleaned of personal data); service health check (database, migrations, secrets, AI). No security operations centre (SOC).

And the hosts' technical logs?

They are kept for the period set by each provider.

9. Backups and continuity

Is the database backed up?

PARTIAL

Yes, every night: a full backup of the database, read back before being kept (an unreadable backup is rejected and reported), encrypted (AES-256-GCM) before leaving the machine that produces it, then uploaded to Microsoft Azure storage in France with a write-only token, which can neither read nor delete. Retention: 30 days, plus one monthly copy for 1 year. An alert is raised if the latest backup is more than 48 hours old. Known limitation, not yet removed: the backup is started from a Finozio administration workstation, not from the production infrastructure.

Are restores tested?

PARTIAL

A full restore was verified on a separate database in September 2026, and the procedure is documented. No scheduled periodic restore exercise yet.

Do you commit to recovery (RPO, RTO) or availability targets?

NO

No: no recovery or availability target is committed contractually, and there is no formal business continuity plan. Support response times: 48 hours (Pilot), 24 hours (Scale Up), 4 hours (Custom).

10. Incident response

What do you do in case of a personal data breach?

For data Finozio is the controller of (accounts, billing, prospects): notification to the CNIL within 72 hours of becoming aware (GDPR art. 33), and information of the data subjects in case of high risk (art. 34). For your tenant's data, which Finozio processes on your behalf: notification to your organisation without undue delay, for your own notifications (art. 33.2).

Do you have a written procedure, and has it been tested?

NOT YET

Not yet: no incident management procedure is published, and no crisis exercise has been carried out.

11. Vulnerability reporting and management

How do we report a vulnerability?

YES

Write to contact@finozio.com, subject "Vulnerability": reply within 5 business days. The same contact is in the security.txt file (RFC 9116), <https://www.finozio.com/.well-known/security.txt>. No bug bounty programme.

Do you track vulnerabilities in your dependencies?

YES

Yes: automated dependency audit (npm audit, pip-audit) on every code check; Python dependencies pinned and installed with hash verification.

12. Retention, reversibility and end of contract

What happens to our data when the plan ends?

When a paid plan ends, the account returns to the free plan and its data is kept as long as it exists. Microsoft 365 readings, which identify users, are deleted 90 days after access to a plan that includes them ends, unless repurchased; they are also limited to a rolling 13 months.

Can you delete our data?

YES

Yes. Account deletion is requested from the My account page; data is erased 7 days after the request, and disappears from backups when they expire (30 days, 1 year for the monthly copy). Billing data is kept for at least 10 years (legal obligation), at Stripe.

Can we get our data back?

PARTIAL

Partly. Your personal data can be exported as JSON from the My account page (GDPR art. 20); depending on the plan, the workspace also offers a CSV export of FinOps data, a cost export in FOCUS format and the Audit Spring audit exports. No single export of all workspace data yet.

What are the retention periods?

All are listed in the privacy policy. Main ones: audit log 2 years; conversations with Aurora 1 year; SSO sessions 30 days; free scan requests 90 days; free monthly report access until it stops (12 reports at most); backups 30 days, monthly copy 1 year.

13. Personal data protection (GDPR)

What is Finozio's role under the GDPR?

Controller for account, billing, free scan, quote and appointment request, and audience measurement data; processor (art. 28) for the Azure and Microsoft 365 data read in your tenant, for which your organisation remains the controller.

Which personal data do you process in our tenant?

Microsoft 365 data of licensed accounts: Microsoft Entra identifier, email address and UPN, display name, licenses, account status, creation and last sign-in dates, Copilot activity; from Pilot, job title, department and application usage, from Microsoft's reports, which identify users unless your tenant hides user names. On the Azure side: resource and cost metadata.

How are data subject rights exercised?

By writing to contact@finozio.com; account export and deletion are also self-service from the My account page. A complaint can be lodged with the CNIL.

14. Sub-processors

PROVIDER	COMPANY AND DATA LOCATION	ROLE	DATA RECEIVED	TRANSFER BASIS
Supabase	Supabase Pte. Ltd. (Singapore); data in Paris, France (EU)	Database and authentication	All data stored by the platform	Standard contractual clauses (SCCs) of its data processing agreement, for any access from outside the EU
Railway	Railway Corporation (United States); servers in Amsterdam, Netherlands (EU)	Hosting of the website and the platform (interface, application server, cache)	Everything that goes through the website and the platform; technical logs	EU-US Data Privacy Framework, SCCs as a fallback
Sentry	Functional Software, Inc. (United States); servers in Frankfurt, Germany (EU)	Technical error monitoring	Error traces cleaned before sending: no request bodies, secrets, email addresses, cookies or IP addresses	EU-US Data Privacy Framework, supplemented by the SCCs of its data processing agreement
Cloudflare	Cloudflare (United States); Cloudflare's global network	DNS, proxy and protection of the website and the platform, CAPTCHA	IP address, request headers, technical browser signals; content of pages and exchanges with the platform, decrypted to be relayed and re-encrypted towards our servers	EU-US Data Privacy Framework, SCCs as a fallback
Anthropic	Anthropic Ireland, Limited (Ireland); processing in the United States	Aurora AI assistant, from the Pilot plan	Conversations; the client's name and plan; aggregated Azure costs and forecast; recommendations; unused resources and virtual machines (name, type, region, SKU, state, usage); aggregated Microsoft 365 counts and amounts. Never: secrets, tags, per-user Microsoft 365 data	SCCs (Modules 2 and 3) of its data processing agreement
Resend	Resend (United States); emails sent from Ireland (EU)	Transactional emails	Recipient's address and email content (alerts, invitations, reminders, a free scan's PDF report)	EU-US Data Privacy Framework, SCCs as a fallback
Stripe	Stripe (United States)	Payment (PCI DSS certified)	Email address, billing name and address, VAT number, plan purchased; the card is entered at Stripe and never goes through Finozio	SCCs
Microsoft	Microsoft (EU and international); backups in France (France Central region)	Azure and Microsoft Graph APIs (data source), appointment booking, contact@finozio.com mailbox, off-site copy of backups	Tenant metadata, directory and licenses, activity reports; emails exchanged with Finozio; backups encrypted before upload	Microsoft's data processing agreement (DPA)
Google	Google (United States)	Audience measurement, with consent, on public pages, sign-up and plan selection – never the client workspace	Pages viewed, referrer, interactions, device type, approximate location, pseudonymous identifier	EU-US Data Privacy Framework, supplemented by SCCs
LinkedIn	LinkedIn Ireland Unlimited Company (Ireland); possible transfer to LinkedIn Corporation (United States)	Advertising campaign measurement, with consent, on public pages only	Pages viewed, clicks, IP address, device characteristics, cookie identifier	SCCs

PROVIDER	COMPANY AND DATA LOCATION	ROLE	DATA RECEIVED	TRANSFER BASIS
Apollo	ZenLeads, Inc., doing business as Apollo.io (United States)	Identification of the company visiting the website, with consent, on public pages only – never of the person	Pages viewed, referrer, IP address, browser characteristics, random identifier	EU-US Data Privacy Framework, supplemented by the SCCs of its data processing agreement