FINAREO

CENTRE DE CONFIANCE

SECURITY OVERVIEW

Vos données financières. Notre engagement.

Document de référence pour vos équipes métier, IT et sécurité.
Présenté à deux niveaux — accessible et technique — sans NDA.

VERSION	DATE	DIFFUSION	CONTACT
2.1	14 mai 2026	Publique	security@finareo.io

SOMMAIRE

Le plan du document.

Ce que vous allez lire : 13 sections couvrant l'ensemble de notre posture sécurité, de la synthèse exécutive aux annexes techniques. Comptez 15 minutes pour une lecture complète.

01 VUE D'ENSEMBLE

Synthèse

EN CLAIR

Finareo détecte les pertes financières invisibles — factures dupliquées, sur-facturation, abonnements inutilisés, anomalies contractuelles. Comme nous traitons des documents sensibles (factures, contrats, RIB, paiements), la sécurité n'est pas une couche ajoutée plus tard : elle est intégrée dans l'architecture depuis le premier jour.

DÉTAIL TECHNIQUE

L'architecture repose sur trois principes structurants, complémentaires et appliqués sur toutes les couches.

Isolation stricte

Un schéma PostgreSQL distinct par client, isolation enforcée au niveau middleware. Aucun mélange technique possible.

Moindre privilège

Chaque accès humain ou applicatif est strictement limité au périmètre nécessaire, sur tous les fronts.

Anonymisation IA

Aucune donnée nominative n'est jamais envoyée à un fournisseur d'intelligence artificielle. La table de mapping reste chez nous.

- Architecture alignée sur le référentiel `ISO 27001` — mesures de l'Annexe A en place
- Stack : `Python 3.12` / `Django 5` / `DRF` côté API ; `React 19` / `Vite` / `TypeScript` côté front
- Revue de code obligatoire avant fusion, aucune fusion automatique sur `main`
- Couverture OWASP Top 10 documentée (matrice détaillée sous NDA)

02 INFRASTRUCTURE

Hébergement et résidence des données

EN CLAIR

Vos données sont hébergées dans votre zone géographique. Pour les clients marocains : datacenter **N+ONE** au Maroc, conforme aux exigences de la **CNDP**. Pour les clients européens : datacenters **Hetzner** en Allemagne ou Finlande, opérateur certifié ISO 27001 et conforme au RGPD. Elles ne quittent jamais leur zone.

MA

N+ONE Datacenters (Maroc)

Datacenter Tier III conforme aux exigences de la CNDP. Hébergement local pour la clientèle marocaine.

UE

Hetzner (Allemagne / Finlande)

Datacenters Hetzner Online GmbH, certifiés ISO 27001, conformes RGPD. DPA signé avec l'hébergeur.

DÉTAIL TECHNIQUE

- N+ONE Datacenters (Maroc, Casablanca) — Tier III, conformité CNDP
- Hetzner Online GmbH (Allemagne, Finlande) — certifié ISO 27001
- Settings Django séparés : `production.py`, `development.py`, `test.py` — bases de données et secrets distincts
- Orchestration Docker Compose + Dokploy, déploiements zero-downtime versionnés
- Pare-feu opérateur + UFW sur le VPS. Ports ouverts : 443 (HTTPS) et 22 (SSH par clé)
- DNS Cloudflare avec DNSSEC, anti-DDoS, WAF. SPF / DKIM / DMARC configurés

03 IDENTITÉ

Authentification et contrôle d'accès

EN CLAIR

Vous vous connectez par un code unique reçu par email à chaque connexion — pas de mot de passe à retenir, pas de risque de réutilisation. Côté Finareo, seules les personnes habilitées à votre dossier y accèdent, avec authentification renforcée par second facteur.

10 min	5	8 h	60/min
Durée de vie d'un code OTP	Tentatives avant verrouillage	Expiration de session inactive	Rate limit IP anonyme

DÉTAIL TECHNIQUE

Côté portail client

- OTP par email, TTL `10 min`
- Max 3 demandes / 10 min, 5 vérifications
- Rate limiting global : 60 req/min IP, 300 req/min user
- Session expirable 8 h, invalidation à la fermeture navigateur
- Cookies `Secure`, `HttpOnly`, `SameSite`

Côté Finareo (interne)

- RBAC : analyste, administrateur, superadmin (orthogonal)
- MFA TOTP obligatoire pour admin et superadmin (`django-otp`)
- Isolation par schéma PostgreSQL (`django-tenants`)
- Hash mots de passe PBKDF2-SHA256
- Désactivation immédiate au départ via procédure RH

04 CRYPTOGRAPHIE

Chiffrement

EN CLAIR

Toutes les communications sont chiffrées de bout en bout. Les données sensibles stockées en base sont chiffrées séparément. Aucun mot de passe n'est jamais lisible, même par nos équipes.

TLS

En transit

TLS 1.3 obligatoire, HSTS preload, désactivation des versions inférieures à 1.2 au niveau Nginx et Cloudflare.

AES

Au repos

Chiffrement disque AES-256 LUKS, chiffrement applicatif Fernet sur les champs sensibles via `django-fernet-fields`.

KEY

Secrets

Variables d'environnement Dokploy uniquement, jamais dans le code. Rotation Fernet supportée sans downtime.

DÉTAIL TECHNIQUE

En transit

- TLS 1.3 sur toutes les terminaisons externes
- HSTS `max-age=31536000`, `includeSubDomains`, `preload` activés
- Redirection HTTP → HTTPS systématique
- TLS < 1.2 désactivé au niveau Nginx / Cloudflare

Au repos

- Hash mots de passe PBKDF2-SHA256
- Chiffrement Fernet sur champs sensibles
- Chiffrement disque AES-256 (LUKS) côté hébergeur
- Sauvegardes chiffrées avec clé distincte des disques
- URLs documents signées, durée de vie limitée

05 TRAÇABILITÉ

Audit et journalisation

EN CLAIR

Chaque accès à vos données et chaque action sur votre dossier est tracé dans un journal horodaté. Nous pouvons vous fournir sur demande l'extrait d'audit de votre périmètre.

DÉTAIL TECHNIQUE

- `django-auditlog` actif sur tous les modèles métier (clients, mandats, factures, anomalies, paiements, utilisateurs)
- Journal exposé via `/api/v1/audit-logs/`, filtrable par tenant, utilisateur, action
- Évènements tracés : authentifications, accès documents, mutations, actions admin
- Logs applicatifs structurés (Django `LOGGING`), niveau INFO en production
- Erreurs remontées dans Sentry (PII expurgée avant envoi)
- Appels LLM tracés : modèle, durée, tokens — jamais le contenu
- Webhooks Stripe : signature HMAC SHA-256 vérifiée, rejet immédiat des invalides
- Extrait du journal de votre périmètre disponible sur demande

06 CONTINUITÉ

Sauvegardes

EN CLAIR

Vos données sont sauvegardées chaque jour, chiffrées, et stockées dans un emplacement géographiquement distinct du serveur principal.

DÉTAIL TECHNIQUE

- Sauvegardes quotidiennes chiffrées de la base PostgreSQL (`pg_dump`), pilotées par Dokploy
- Chiffrement AES-256 des archives, clé distincte des disques de production
- Copie quotidienne transférée hors-site, emplacement géographiquement distinct
- Procédure de restauration documentée et testée à la demande

07 ANONYMISATION

Gouvernance de l'intelligence artificielle

● EN CLAIR

Pour analyser vos documents, l'IA doit les lire. Mais **avant chaque envoi**, nous remplaçons automatiquement les noms de fournisseurs, RIB, et identifiants sensibles par des codes anonymes. L'IA voit la structure et les montants — jamais qui est qui.

AVANT — VOTRE DONNÉE BRUTE

```
{
  "fournisseur": "ALPHA TECH SARL",
  "iban": "FR76 3000 4001 234",
  "contact": "marie@alphatech.fr",
  "montant_ht": 14250.00
}
```

→

APRÈS — ENVOYÉ À L'IA

```
{
  "fournisseur": "FOURNISSEUR_a8f2c1",
  "iban": "IBAN_5e9b3a7c",
  "contact": "CONTACT_72f1e8",
  "montant_ht": 14250.00
}
```

— DÉTAIL TECHNIQUE

Anonymisation

- Module `TenantAnonymizer` (`api/apps/llm/anonymizer.py`)
- Substitution déterministe par tokens HMAC-SHA256
- Table de correspondance jamais transmise — ré-injection locale
- Obligatoire pour `MANDATORY_COUNTRIES` (FR, MA, RGPD)

Fournisseur LLM

- OpenAI : `gpt-4o-mini` pour les tâches légères, `gpt-4o` pour l'extraction
- Compte entreprise, DPA signé
- Appels stateless — aucune conversation côté fournisseur
- Métadonnées seulement (modèle, durée, tokens)

08 OWASP

Sécurité applicative

EN CLAIR

L'application est conçue pour résister aux attaques courantes du web (injection, vol de session, force brute) et son code est revu avant chaque déploiement.

DÉTAIL TECHNIQUE

- Rate limiting via DRF throttles : 60/min IP anon, 300/min user, 5 OTP/10min/email
- CORS whitelist stricte : `admin.finareo.io`, `app.finareo.io`
- CSRF actif, cookies `Secure` + `HttpOnly`, `CSRF_TRUSTED_ORIGINS` explicite
- Headers : HSTS, `X-Frame-Options: DENY`, `X-Content-Type-Options: nosniff`, `Referrer-Policy`
- Webhooks Stripe vérifiés via `stripe.Webhook.construct_event()`
- ORM Django uniquement — pas de SQL brut avec inputs utilisateurs
- Validation systématique des sorties LLM par Pydantic
- Linter `ruff` exécuté en CI sur chaque commit

09 VEILLE

Gestion des vulnérabilités

EN CLAIR

Nous suivons les annonces de sécurité sur les composants que nous utilisons et nous corrigeons rapidement les failles critiques. Vous pouvez nous signaler une vulnérabilité à **security@finareo.io**.

DÉTAIL TECHNIQUE

- Veille sur les composants critiques (Django, DRF, dépendances LLM)
- CVE critiques (CVSS ≥ 7) corrigées sous 48 h
- Programme de divulgation responsable : `security@finareo.io`
- Accusé de réception sous 48 h, mitigation des critiques sous 7 jours

10 RÉPONSE

Gestion des incidents

EN CLAIR

Si quelque chose se passe mal et que vos données sont concernées, vous serez prévenu sous 72 heures maximum, avec ce qui s'est passé, ce que cela implique, et ce que nous faisons.

01	**Détection**	Sentry + sondes externes + signalement
02	**Qualification**	Criticité P0–P3 sous 1 h
03	**Confinement**	Isolation périmètre, snapshot pour analyse
04	**Investigation**	Analyse logs, cause racine
05	**Résolution**	Correctifs + vérification de la non-récurrence
06	**Notification**	Client impacté sous 72 h maximum (obligation RGPD)
07	**Post-mortem**	Documenté et partagé sous 7 jours

P0

Compromission confirmée, fuite de données

`Immédiat (24/7)`

P1

Indisponibilité totale, vulnérabilité critique

`< 1 heure`

P2

Indisponibilité partielle, vulnérabilité haute

`< 4 heures`

P3

Bug fonctionnel, vulnérabilité moyenne

`< 1 jour ouvré`

11 DROITS

Propriété et cycle de vie des données

EN CLAIR

Vos données vous appartiennent. Vous pouvez les exporter à tout moment depuis votre portail. Vous pouvez demander leur suppression. Nous ne vendons jamais vos données et nous ne les utilisons jamais pour autre chose que votre prestation.

DÉTAIL TECHNIQUE

- Propriété : le client reste propriétaire de ses données à tout moment (clause DPA)
- Export self-service depuis le portail : Excel, CSV, PDF d'anomalies, rapports
- Suppression sur demande sous 30 jours (hors obligations légales de conservation)
- Isolation tenant : aucun mélange technique entre clients
- Aucune revente, aucun usage marketing, aucun croisement entre clients

12 TRANSPARENCE

Sous-traitants

EN CLAIR

Voici la liste exhaustive des prestataires qui interviennent dans le traitement de vos données. Toute évolution de cette liste est notifiée 30 jours avant changement. Liste à jour publique : **finareo.io/subprocessors**.

N+ONE Datacenters

HÉBERGEMENT

Hébergement des données — clients marocains

Maroc · Tier III · conformité CNDP

Hetzner Online GmbH

HÉBERGEMENT

Hébergement des données — clients européens

Allemagne · Finlande · ISO 27001 · RGPD · DPA

Cloudflare

RÉSEAU

DNS, anti-DDoS, WAF

Europe (anycast) · SOC 2 · ISO 27001 · DPA

OpenAI

IA

Analyse de documents (anonymisés)

États-Unis (SCC) · Compte entreprise · DPA

Resend

EMAIL

Emails transactionnels (invitations, notifications)

États-Unis (SCC) · SOC 2 · DPA

Stripe

PAIEMENT

Paiements et gestion des abonnements

États-Unis (SCC) · PCI DSS L1 · SOC 2 · DPA

Sentry

OBSERVABILITÉ

Suivi des erreurs applicatives

États-Unis (SCC) · SOC 2 · DPA

Aucun sous-traitant ne traite vos données bancaires : Finareo ne reçoit qu'un identifiant de transaction Stripe et un statut de paiement. Les coordonnées bancaires sont collectées directement par Stripe Elements / Checkout.

13 RÉFÉRENTIELS

Conformité

EN CLAIR

L'architecture est conçue selon les principes RGPD (minimisation, anonymisation, propriété client, droit à l'export et à la suppression) et alignée sur le référentiel ISO 27001. Le DPA est disponible sur demande pour tout client.

RGPD

Conformité applicable

Minimisation, anonymisation IA, propriété client, droits à l'export et à la suppression. DPA disponible.

ISO 27001

Référentiel d'alignement

Architecture alignée sur l'Annexe A. Statement of Applicability (SoA) documenté en interne.

POUR ALLER PLUS LOIN

Une question, un audit, un signalement.

Notre équipe sécurité répond sous 24 h ouvrées sur les questions commerciales et conformité, sous 48 h sur les signalements de vulnérabilités.

security@finareo.io

CONFORMITÉ

Questionnaires fournisseurs, audits RSSI, DPA, matrices de conformité.

VULNÉRABILITÉS

Divulgation responsable, accusé 48 h, mitigation critique 7 j, clé PGP sur demande.

COMMERCIAL

Personnalisation contractuelle, ajout d'engagements spécifiques, négociation DPA.

finareo.io/security · finareo.io/subprocessors · finareo.io/status · finareo.io/access-policy

Finareo · Document v2.1 — 14 mai 2026 · Diffusion publique