FINAREO

LÉGAL & CONFORMITÉ

ACCORD DE TRAITEMENT DES DONNÉES

Pour vos données. Notre engagement contractuel.

Modèle de référence Finareo — conforme au Règlement Général sur la Protection des Données (RGPD) Article 28. Diffusion publique.

VERSION	DATE	CADRE	CONTACT
1.0	14 mai 2026	RGPD Art. 28	security@finareo.io

00 PRÉAMBULE

Préambule et définitions

EN CLAIR

Ce document est un contrat annexe au Mandat principal. Il décrit comment Finareo traite vos données à caractère personnel et formalise nos engagements RGPD. Il est obligatoire pour tout client traitant des données personnelles.

Le présent Accord de Traitement des Données (« **DPA** ») encadre les conditions dans lesquelles **Finareo**, agissant en qualité de **sous-traitant** au sens de l'article 4(8) du Règlement (UE) 2016/679 (« **RGPD** »), traite les données à caractère personnel pour le compte de ses clients, agissant en qualité de **responsables du traitement** au sens de l'article 4(7) du RGPD.

Ce DPA est conclu en complément du contrat principal liant Finareo et le Client (le « **Contrat** » ou « **Mandat** ») et constitue une annexe contractuelle obligatoire. En cas de contradiction entre le DPA et le Contrat sur les questions de protection des données, le DPA prévaut.

Le présent DPA est mis à disposition publique sur `finareo.io/dpa`. Toute évolution est notifiée aux clients selon les modalités prévues à l'article 16.

Définitions

RGPD	Règlement (UE) 2016/679 du 27 avril 2016
Loi Informatique et Libertés	Loi française n° 78-17 du 6 janvier 1978 modifiée
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (RGPD Art. 4(1))
Traitement	Toute opération effectuée sur des données à caractère personnel (RGPD Art. 4(2))
Responsable du traitement	Le Client, qui détermine les finalités et les moyens du traitement
Sous-traitant	Finareo, qui traite les données pour le compte du Client
Sous-traitant ultérieur	Toute personne physique ou morale à qui Finareo confie tout ou partie du traitement
Violation de données	Violation de la sécurité entraînant destruction, perte, altération, divulgation non autorisée ou accès non autorisé à des données
CNIL / CNDP	Commission Nationale de l'Informatique et des Libertés (France) / Commission Nationale de Protection des Données à caractère Personnel (Maroc)
CCT / SCC	Clauses Contractuelles Types adoptées par la Commission européenne
Mesures TOM	Mesures techniques et organisationnelles décrites en Annexe 3

Art. 1 OBJET

Objet du DPA

Le présent DPA a pour objet de définir les conditions dans lesquelles Finareo s'engage à effectuer, pour le compte du Client, les opérations de traitement de données à caractère personnel décrites en **Annexe 1**, dans le cadre de l'exécution du Contrat.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel, notamment le RGPD et la Loi Informatique et Libertés.

Art. 2 DURÉE

Durée d'application

Le présent DPA prend effet à la date de signature du Contrat. Il s'applique pendant toute la durée d'exécution du Contrat et reste en vigueur pour les obligations relatives au sort des données après la fin du Contrat (article 13).

Art. 3 NATURE ET FINALITÉ

Nature et finalité du traitement

Finareo est autorisé à traiter, pour le compte du Client, les données à caractère personnel nécessaires à la fourniture du service Finareo : détection d'anomalies financières, analyse de documents (factures, contrats, paiements, abonnements), production de rapports d'audit et accompagnement à la récupération de pertes financières.

La nature et la finalité du traitement, le type de données et les catégories de personnes concernées sont décrits en détail en **Annexe 1**.

Art. 4 OBLIGATIONS DE FINAREO

Obligations du sous-traitant

EN CLAIR

Ce sont les 8 obligations imposées à Finareo par le RGPD Article 28. Chacune est détaillée dans une sous-section. C'est le cœur du DPA.

4.1 — Traiter les données uniquement sur instruction du Client

Finareo traite les données à caractère personnel **uniquement sur instruction documentée du Client**, y compris en ce qui concerne les transferts de données hors Union européenne. Toute instruction est réputée documentée dès lors qu'elle est formulée par écrit (email, ticket, document contractuel).

Si Finareo considère qu'une instruction du Client constitue une violation du RGPD, il en informe le Client sans délai et peut suspendre l'exécution de l'instruction.

4.2 — Garantir la confidentialité

Finareo garantit que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou sont soumises à une obligation légale appropriée de confidentialité. Cet engagement est formalisé par contrat de travail, charte interne ou accord de confidentialité.

4.3 — Mettre en œuvre les mesures de sécurité

Finareo met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD. Ces mesures sont décrites en **Annexe 3** et dans le document public *Security Overview* (`finareo.io/security`).

Les mesures incluent notamment : chiffrement TLS 1.3 et AES-256, anonymisation systématique avant traitement IA, isolation par tenant, authentification renforcée (OTP, MFA TOTP), journalisation horodatée, sauvegardes quotidiennes chiffrées géolocalisées hors-site.

4.4 — Recourir à un sous-traitant ultérieur uniquement avec autorisation

Finareo ne recrute pas un autre sous-traitant sans **l'autorisation écrite, préalable et spécifique ou générale du Client**.

Le Client autorise par le présent DPA le recours aux sous-traitants ultérieurs listés en **Annexe 2**. Toute modification de cette liste (ajout, suppression, changement de région) est notifiée au Client **au moins 30 jours à l'avance**, par email et publication sur `finareo.io/subprocessors`.

Le Client dispose d'un droit d'opposition motivé à ce changement, à exercer dans les 30 jours suivant la notification. À défaut d'opposition, le changement est réputé accepté. En cas d'opposition légitime, Finareo s'efforce de proposer une alternative ; à défaut, le Client peut résilier le Contrat sans pénalité.

Finareo demeure pleinement responsable, devant le Client, de l'exécution par le sous-traitant ultérieur de ses obligations.

4.5 — Assister le Client dans le respect des droits des personnes concernées

Finareo met en place, dans la mesure du possible, les mesures techniques et organisationnelles appropriées pour aider le Client à répondre aux demandes d'exercice des droits des personnes concernées (droit d'accès, de rectification, d'effacement, de limitation, de portabilité, d'opposition — articles 15 à 22 du RGPD).

Lorsqu'une personne concernée s'adresse directement à Finareo, Finareo transmet la demande au Client dans les meilleurs délais et n'y répond pas directement, sauf à la demande expresse du Client.

4.6 — Assister le Client dans la sécurité et la gestion des violations

Finareo assiste le Client dans la mise en œuvre des obligations prévues aux articles 32 à 36 du RGPD, notamment : sécurité du traitement (Art. 32), notification des violations à l'autorité de contrôle (Art. 33) et à la personne concernée (Art. 34), analyse d'impact (DPIA, Art. 35) et consultation préalable (Art. 36) si applicable.

4.7 — Notifier les violations de données

Finareo notifie au Client toute violation de données à caractère personnel **dans les meilleurs délais et au plus tard sous 72 heures** après en avoir pris connaissance, par email à l'adresse de contact technique fournie par le Client.

La notification comporte :

- La nature de la violation, y compris les catégories et le nombre approximatif de personnes concernées et de données concernées
- Les conséquences probables de la violation
- Les mesures prises ou proposées par Finareo pour remédier à la violation et atténuer ses effets négatifs

Un post-mortem détaillé est communiqué au Client sous **7 jours ouvrés** suivant la résolution de l'incident.

4.8 — Restituer ou supprimer les données en fin de prestation

À l'issue de la prestation, **au choix du Client**, Finareo :

- **Restitue** au Client toutes les données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine (Excel, CSV, JSON), *et/ou*
- **Supprime** définitivement les données à caractère personnel et copies existantes, sauf obligations légales de conservation

La restitution ou la suppression intervient dans un délai de **30 jours** à compter de la demande écrite du Client. Un certificat de destruction peut être fourni sur demande.

4.9 — Mettre à disposition la documentation et permettre les audits

Finareo met à la disposition du Client toute la documentation nécessaire pour démontrer le respect de ses obligations, notamment : le présent DPA, le document *Security Overview*, la liste à jour des sous-traitants, l'extrait d'audit du périmètre Client (sur demande), et le récépissé de déclaration CNDP (pour les clients hébergés au Maroc).

Finareo autorise et contribue aux audits, y compris aux inspections, réalisés par le Client ou un auditeur tiers mandaté par le Client, dans les limites prévues à l'article 14.

Art. 5 OBLIGATIONS DU CLIENT

Obligations du responsable du traitement

Le Client s'engage à :

- Fournir à Finareo les données à caractère personnel nécessaires à l'exécution du Contrat
- Documenter par écrit toute instruction relative au traitement
- Respecter ses propres obligations en tant que responsable du traitement, notamment l'information des personnes concernées, le respect de leurs droits, et la tenue du registre des traitements
- Garantir, préalablement et pendant toute la durée du traitement, le respect par les personnes concernées des informations relatives au traitement et des droits leur permettant de s'opposer à celui-ci
- Superviser le traitement, y compris en réalisant des audits selon les modalités prévues à l'article 14

Art. 6 SOUS-TRAITANTS ULTÉRIEURS

Recours à des sous-traitants ultérieurs

La liste des sous-traitants ultérieurs autorisés est en **Annexe 2** et publiée à `finareo.io/subprocessors`.

Tout sous-traitant ultérieur est tenu de respecter les mêmes obligations de protection des données que celles définies dans le présent DPA, notamment en ce qui concerne la sécurité, la confidentialité et la coopération. Finareo s'assure de cette équivalence par des engagements contractuels écrits.

Art. 7 TRANSFERTS INTERNATIONAUX

Transferts de données hors Union européenne

Lorsque Finareo recourt à des sous-traitants ultérieurs situés en dehors de l'Espace Économique Européen (EEE), les transferts sont encadrés par : une décision d'adéquation de la Commission européenne, lorsqu'elle existe ; les Clauses Contractuelles Types (CCT) adoptées par la décision d'exécution 2021/914 du 4 juin 2021 ; ou les règles d'entreprise contraignantes (BCR) approuvées par une autorité de contrôle.

La liste des sous-traitants ultérieurs en Annexe 2 précise, pour chacun, la base juridique du transfert applicable.

Pour les clients hébergés au **Maroc**, les transferts hors Maroc sont encadrés conformément à la **Loi marocaine 09-08** et aux autorisations délivrées par la **CNDP**.

Art. 8 DROITS DES PERSONNES

Droits des personnes concernées

Finareo notifie au Client, dans les meilleurs délais et au plus tard sous **3 jours ouvrés**, toute demande émanant d'une personne concernée et relative à l'exercice de ses droits (accès, rectification, effacement, limitation, portabilité, opposition, retrait du consentement).

Finareo aide le Client à répondre à ces demandes, notamment par la mise à disposition d'outils d'export et de suppression accessibles depuis le portail client.

Art. 9 VIOLATIONS DE DONNÉES

Notification des violations

Conformément à l'article 4.7, toute violation est notifiée au Client sous **72 heures maximum**.

Finareo conserve un registre interne des violations de données conformément à l'article 33(5) du RGPD, accessible au Client sur demande.

Art. 10 POINT DE CONTACT DPO

Délégué à la Protection des Données

Finareo a désigné un point de contact unique pour les questions relatives à la protection des données : `security@finareo.io`.

Toute communication officielle relative au présent DPA, y compris les instructions, notifications, demandes d'audit et notifications de violations, est adressée à cette adresse.

Art. 11 REGISTRE

Tenue du registre des activités de traitement

Finareo tient un registre des catégories d'activités de traitement effectuées pour le compte du Client, conformément à l'article 30(2) du RGPD. Ce registre est mis à disposition du Client sur demande.

Art. 12 SÉCURITÉ

Mesures de sécurité

Les mesures techniques et organisationnelles mises en œuvre par Finareo sont décrites en **Annexe 3** et dans le document public *Security Overview*.

Finareo se réserve le droit de faire évoluer ces mesures, à condition que le niveau de protection ne soit pas réduit. Toute évolution significative est notifiée au Client.

Art. 13 SORT DES DONNÉES

Sort des données en fin de prestation

À la fin de la prestation, au choix du Client : **restitution** des données dans un délai de 30 jours à compter de la demande écrite, dans un format structuré et exploitable (Excel, CSV, JSON) ; ou **suppression** définitive dans un délai de 30 jours à compter de la demande écrite, à l'exception des éléments dont la conservation est requise par la loi.

Un certificat de destruction est fourni sur demande.

Art. 14 AUDIT

Audit et contrôle

Le Client peut, à ses frais et après préavis raisonnable d'au moins **30 jours**, réaliser un audit du respect par Finareo de ses obligations au titre du présent DPA. L'audit peut être réalisé par le Client ou par un auditeur tiers indépendant mandaté par le Client.

L'audit se déroule sur les heures ouvrées de Finareo, sans perturbation indue de son activité, et dans le respect de la confidentialité des données des autres clients de Finareo. L'auditeur tiers est tenu à un accord de confidentialité préalable.

En alternative à un audit sur site, Finareo peut fournir :

- Un rapport d'audit externe (pentest, audit de conformité ISO 27001)
- Les certifications applicables
- L'extrait d'audit du périmètre Client
- Des réponses détaillées à un questionnaire de conformité (CAIQ, SIG, VSAQ)

Art. 15 RESPONSABILITÉ

Responsabilité

Chaque partie est responsable du respect de ses propres obligations en application du RGPD. La responsabilité de Finareo, en tant que sous-traitant, est limitée aux obligations qui lui sont propres et à ses fautes prouvées.

La responsabilité financière de Finareo au titre du présent DPA est plafonnée selon les modalités prévues au Contrat principal.

Art. 16 MODIFICATIONS

Modifications du DPA

Finareo peut faire évoluer le présent DPA, notamment pour tenir compte des évolutions législatives ou réglementaires, des recommandations des autorités de contrôle, ou de l'évolution de son service.

Toute modification substantielle est notifiée au Client au moins **30 jours avant** sa prise d'effet, par email et publication sur `finareo.io/dpa`. En cas de désaccord, le Client peut résilier le Contrat sans pénalité dans ce délai.

Art. 17 DROIT APPLICABLE

Droit applicable et juridiction compétente

Le présent DPA est régi par le **droit français** pour les clients établis en Union européenne, et par le **droit marocain** pour les clients établis au Maroc. Tout litige sera porté devant les tribunaux compétents du siège social de Finareo.

ANNEXE 1

Description du traitement

Finalités du traitement

- Détection d'anomalies financières dans les factures, contrats, paiements et abonnements du Client
- Analyse de documents par intelligence artificielle (extraction, classification, enrichissement)
- Production de rapports d'audit et de récupération de pertes
- Suivi du mandat client (anomalies, validations, paiements, statuts)
- Communication avec les contacts désignés du Client

Catégories de données traitées

- **Données d'identification professionnelle** : noms, prénoms, fonctions, emails professionnels, téléphones professionnels des contacts du Client et de ses fournisseurs
- **Données financières** : montants de factures, références bancaires (RIB), conditions de paiement, conditions contractuelles
- **Données documentaires** : contenu des factures, contrats, ordres d'achat, abonnements, paiements
- **Données techniques** : adresses IP, horodatages d'accès, identifiants de session, logs d'activité

Catégories de personnes concernées

- Employés du Client habilités à utiliser le service Finareo
- Contacts désignés du Client (référent métier, référent IT)
- Contacts professionnels des fournisseurs du Client (nommés dans les documents traités)

Durée de conservation

Pendant toute la durée du Contrat, et au-delà uniquement pour répondre aux obligations légales de conservation (notamment fiscales et comptables : 10 ans en France).

ANNEXE 2

Sous-traitants ultérieurs autorisés

Liste à jour publiée à `finareo.io/subprocessors`. Toute mise à jour est notifiée 30 jours avant tout changement.

Sous-traitant	Rôle	Localisation	Base juridique du transfert
N+ONE Datacenters	Hébergement infrastructure — clients marocains	Maroc	Loi marocaine 09-08, conformité CNDP
Hetzner Online GmbH	Hébergement infrastructure — clients européens	Allemagne / Finlande	Zone EEE, ISO 27001, DPA signé
Cloudflare	DNS, anti-DDoS, WAF	International (anycast)	SOC 2, ISO 27001, CCT
OpenAI	Analyse de documents par IA (sur données anonymisées)	États-Unis	CCT, compte entreprise, DPA
Resend	Envoi d'emails transactionnels	États-Unis	CCT, SOC 2, DPA
Stripe	Gestion des paiements et abonnements	États-Unis	CCT, PCI DSS Niveau 1, SOC 2, DPA
Sentry	Suivi des erreurs applicatives (PII expurgée)	États-Unis	CCT, SOC 2, DPA

ANNEXE 3

Mesures techniques et organisationnelles

Les mesures suivantes sont mises en œuvre par Finareo et décrites en détail dans le document public *Security Overview* (`finareo.io/security`).

Mesures techniques

- **Chiffrement en transit** : TLS 1.3 obligatoire, HSTS preload, désactivation des versions TLS inférieures à 1.2
- **Chiffrement au repos** : AES-256 (LUKS) au niveau hébergeur ; chiffrement applicatif Fernet sur les champs sensibles
- **Authentification** : OTP par email (TTL 10 minutes), MFA TOTP obligatoire pour les administrateurs Finareo, rate limiting strict
- **Isolation par tenant** : schéma PostgreSQL distinct par client, enforcée au niveau middleware
- **Anonymisation IA** : substitution par tokens HMAC-SHA256 avant tout envoi à un fournisseur d'IA
- **Journalisation** : django-auditlog actif sur tous les modèles métier, logs structurés, erreurs remontées dans Sentry
- **Sauvegardes** : quotidiennes, chiffrées AES-256, géolocalisées hors-site
- **Sécurité applicative** : rate limiting, CORS strict, CSRF, en-têtes HSTS, X-Frame-Options DENY, validation HMAC des webhooks

Mesures organisationnelles

- **Moindre privilège** : accès interne strictement limité au périmètre du dossier confié
- **Confidentialité** : engagement contractuel signé par tous les employés, charte sécurité, formation annuelle
- **Désactivation immédiate** des comptes au départ
- **Procédure incidents** : qualification P0–P3 sous 1 h, notification client sous 72 h, post-mortem sous 7 jours
- **Veille sécurité** sur les composants critiques, mises à jour CVE critiques sous 48 h
- **Programme de divulgation responsable** : `security@finareo.io`

ANNEXE 4 — CONTACTS

Une question, une notification, un audit.

security@finareo.io

Point de contact unique Finareo pour toutes les communications relatives à ce DPA : notifications de violations, demandes d'audit, demandes documentaires, signalements de vulnérabilités, instructions documentées.

Réponse sous 24 h ouvrées pour les demandes conformité, sous 48 h pour les signalements de vulnérabilités. Clé PGP disponible sur demande.

Finareo · contact@finareo.io · finareo.io
Document v1.0 — 14 mai 2026 · Diffusion publique

Liens : finareo.io/dpa · finareo.io/security · finareo.io/subprocessors · finareo.io/access-policy