CONTRAT DE SOUS-TRAITANCE

Protection des données personnelles.

Art. 28 du Règlement (UE) 2016/679 — RGPD · Version 1 · 20 avril 2026

Version	v1
Date de référence	20 avril 2026
Base légale	Art. 28 RGPD
Responsable de traitement	Le CIF utilisateur du Service
Sous-traitant	anø — éditeur du SaaS
Mode de signature	Clickwrap / DocuSign / Yousign

00 — PRÉAMBULE

Contexte contractuel.

Le CIF (Conseiller en Investissements Financiers ou Conseiller en Gestion de Patrimoine) exerce une activité réglementée par l'ORIAS, l'ACPR et l'AMF. Il est **responsable de traitement** au sens du RGPD pour les données personnelles de ses clients finaux.

anø fournit un logiciel SaaS de gestion patrimoniale dont l'architecture est **zero-knowledge côté serveur** pour les données clients finaux (stockage local desktop chiffré AES-256-GCM, pas de copie serveur en clair). anø traite néanmoins, au titre de l'exploitation du Service, certaines données personnelles **du CIF lui-même** (email, licence, logs d'audit, proxy LLM).

Le présent contrat encadre les traitements effectués par anø **pour le compte du CIF**, en qualité de **sous-traitant** au sens de l'article 28 RGPD.

01 — OBJET

Ce que couvre ce contrat.

Le présent DPA a pour objet de définir :
- les traitements effectués par anø pour le compte du CIF ;
- les obligations respectives des parties en matière de protection des données ;
- les garanties techniques et organisationnelles (art. 32 RGPD) ;
- les règles applicables aux sous-traitants ultérieurs (art. 28-2 et 28-4) ;
- les conditions de transfert hors Union européenne (art. 44 à 49).

Il complète et prévaut sur les Conditions générales accessibles sur `/conditions` pour tout point relatif à la protection des données personnelles.

02 — NATURE ET FINALITÉ

Ce qui est traité, pourquoi et combien de temps.

2.1 Personnes concernées
- Le CIF lui-même (personne physique utilisatrice du Service) ;
- par transit chiffré, les clients finaux du CIF — anø n'accède pas aux données en clair.

2.2 Données traitées par anø pour le CIF

Donnée	Nature	Traitement
Email CIF	PII	HMAC-SHA256 + AES-256-GCM — jamais en clair
Licence et statut	Contractuel	Stockage postgres scopé license_id
Logs d'audit admin	PII + traçabilité	admin_audit_trail append-only, 3 ans
Prompts LLM (proxy)	PII potentielle	Transit ⟶ Anthropic, non journalisé, scrubber PII
Preuves consentement	PII + horodatage	Rétention 6 ans (art. 7-1 RGPD)
Backups vault desktop	Ciphertext	Clé dérivée utilisateur, anø ne peut déchiffrer
Métadonnées facturation	Non-PII	Via Stripe, stripe_customer_id uniquement

2.3 Finalités
- Fournir le Service au CIF (authentification, licence, sync, support) ;
- journalisation d'audit (obligations art. 30 et 32 RGPD) ;

- assistance IA via proxy LLM (art. L.541-1 CMF — recommandation CIF) ;
- maintenance, sécurité, amélioration du Service.

2.4 Durée

La durée des traitements correspond à la durée du contrat de licence, augmentée des durées de rétention légales : preuves consentement 6 ans, admin audit trail 3 ans, factures 10 ans (obligation comptable), données de licence durée contrat + 1 an puis anonymisation.

03 — OBLIGATIONS DU SOUS-TRAITANT

Ce qu'anø garantit au CIF (art. 28-3).

3.1 Traitement conforme aux instructions (art. 28-3-a)

anø s'engage à ne traiter les données qu'aux seules fins décrites à l'article 2 et selon les instructions documentées du CIF. Toute instruction contraire au droit de l'Union ou d'un État membre sera immédiatement signalée.

3.2 Confidentialité (art. 28-3-b)

Les personnes autorisées à traiter les données sous l'autorité d'anø sont soumises à une obligation contractuelle de confidentialité. En phase beta privée, anø exploite le Service en mode solo dev ; toute extension d'équipe fera l'objet d'une mise à jour de l'**annexe C**.

3.3 Mesures de sécurité (art. 28-3-c, art. 32)

anø met en œuvre les mesures techniques et organisationnelles détaillées en **annexe B** : chiffrement AES-256-GCM app-layer, HMAC-SHA256 sur les lookups, RLS PostgreSQL multi-tenant, audit trail append-only, scrubber PII whitelist, TLS 1.3 en transit, backups chiffrés age (Ed25519), rotation des clés documentée.

3.4 Sous-traitants ultérieurs (art. 28-3-d, art. 28-2 et 28-4)

anø a obtenu l'autorisation générale préalable du CIF pour recourir aux sous-traitants ultérieurs listés en **annexe A**. anø informera le CIF **30 jours avant** toute modification. Le CIF peut s'opposer par écrit motivé ; à défaut de solution alternative, il peut résilier. anø demeure pleinement responsable des sous-traitants ultérieurs.

3.5 Assistance à l'exercice des droits (art. 28-3-e)

anø met à disposition du CIF, dans l'espace admin `/compte/`, les fonctionnalités techniques nécessaires pour répondre aux demandes d'exercice des droits (accès, rectification, effacement, portabilité, opposition, limitation). Pour les données du CIF lui-même, les droits s'exercent via `/compte/export` (art. 15 et 20) et `/compte/supprimer` (art. 17).

3.6 Notification de violation (art. 28-3-f, art. 33 et 34)

En cas de violation de données, anø notifie le CIF **sans délai injustifié et au plus tard 24 heures** après en avoir pris connaissance, par email. La notification comprend la nature de la violation, les catégories de données concernées, les conséquences probables, et les mesures prises. Ce délai permet au CIF de respecter sa propre obligation CNIL sous 72 h.

3.7 Assistance à l'AIPD (art. 28-3-f, art. 35 et 36)

anø met à disposition, sur demande, les éléments nécessaires à la réalisation de l'AIPD du CIF. L'AIPD anø v0.9 est tenue à disposition interne.

3.8 Sort des données en fin de contrat (art. 28-3-g)

À l'issue de la relation contractuelle, sur choix du CIF : suppression dans 30 jours avec attestation, ou restitution sous format standard. Les données soumises à obligations légales (factures, audit trail) sont anonymisées et conservées pour leur durée légale.

3.9 Audit et inspection (art. 28-3-h)

anø met à disposition toute information nécessaire. Le CIF peut demander un audit, à ses frais, une fois par an ou suite à un incident, sur préavis de 30 jours. L'audit s'effectue sur pièces et, si nécessaire, sur site avec accord préalable.

04 — OBLIGATIONS DU RESPONSABLE

Ce que le CIF s'engage à faire.

- fournir les instructions documentées ;
- garantir la licéité des traitements qu'il réalise au travers du Service (base légale, consentement, information des personnes concernées) ;
- respecter ses propres obligations d'information vis-à-vis de ses clients finaux (art. 13 et 14 RGPD) ;
- signer le DPA avant toute mise en production (clickwrap `/compte/dpa`) ;
- tenir à jour les données de contact pour la notification de violation.

05 — TRANSFERTS HORS UE

Anthropic, Stripe — SCC art. 46.

5.1 Principes

anø privilégie les sous-traitants ultérieurs établis en Union européenne (Brevo FR, Hostinger FR, Stripe IE). Les transferts hors UE sont limités à **Anthropic (États-Unis)** pour le proxy LLM (pas d'équivalent UE à date) et **Stripe (États-Unis)** partiel (flux bancaires internationaux).

5.2 Encadrement

Les transferts hors UE sont encadrés par les **Clauses Contractuelles Types** (SCC) 2021/914, signées avec chaque sous-traitant concerné (module 3 processor-to-processor). Une analyse d'impact des transferts (TIA) est jointe à l'AIPD anø et réévaluée annuellement. Mesure technique complémentaire pour Anthropic : **scrubber PII whitelist** avant envoi des prompts.

5.3 Option BYOK

Le CIF peut activer l'option Bring Your Own Key : il apporte sa propre clé API Anthropic et anø ne voit plus les prompts. La responsabilité du transfert US bascule alors sur le CIF.

---

06 — RESPONSABILITÉ

Vis-à-vis des personnes et entre parties.

6.1 Vis-à-vis des personnes concernées

Chaque partie assume la responsabilité des dommages causés par un traitement en violation du RGPD (art. 82). Le principe de solidarité s'applique ; anø répond des dommages causés par ses propres manquements ou ceux de ses sous-traitants ultérieurs.

6.2 Plafond contractuel

Sans préjudice de l'art. 82 RGPD, la responsabilité contractuelle d'anø envers le CIF, toutes causes confondues, est plafonnée aux sommes versées au titre de la licence dans les **12 mois** précédant le fait générateur. Ce plafond ne s'applique pas en cas de faute lourde, dol, ou manquement à une obligation essentielle du RGPD.

---

07 — DURÉE, MODIFICATION, RÉSILIATION

Cycle de vie du contrat.

7.1 Durée

Le DPA entre en vigueur à la signature et reste valide pendant toute la durée de la licence. Sa version est enregistrée dans `dpa_signatures` avec `document_version = "v1"` et `document_hash = SHA-256(PDF)`.

7.2 Modification

Toute modification substantielle fait l'objet d'une nouvelle version (v2, v3…). anø notifie le CIF **30 jours avant** l'entrée en vigueur. Le CIF peut ré-accepter par clickwrap ou refuser, avec résiliation sans pénalité et restitution/suppression selon 3.8.

7.3 Résiliation

Le DPA prend fin automatiquement à la fin du contrat de licence. Les obligations de confidentialité, de restitution/suppression et de conservation des audit trails survivent à la résiliation pour leurs durées respectives.

08 — DROIT ET JURIDICTION

Droit français, Tribunal de Commerce de Paris.

Le présent DPA est régi par le **droit français**. Tout litige non résolu à l'amiable relève de la compétence exclusive du **Tribunal de Commerce de Paris** (contexte B2B).

ANNEXE A

Sous-traitants ultérieurs autorisés.

Autorisation générale préalable du CIF (art. 28-2 et 28-4). Mise à jour avec notification 30 jours avant effectivité (art. 3.4).

Sous-traitant	Finalité	Localisation	Hors UE	Encadrement
Brevo	Email transactionnel	France (Paris)	Non	DPA signé
Anthropic	Proxy LLM (Claude)	États-Unis	Oui	DPA + SCC art. 46
Stripe	Paiement abonnements	Irlande + US	Partiel	DPA + SCC art. 46
Hostinger	Hébergement VPS FR	France	Non	DPA signé

Outils self-hostés (pas de sous-traitant tiers)

Twenty (CRM interne), GlitchTip (erreurs), Uptime Kuma (monitoring) — opérés sur VPS anø.

Services sans transit de PII (pas de DPA requis)

Slack (alertes post-scrubber), GitHub (code source), Let's Encrypt (certificats), Plausible (analytics cookieless managé EU — recommandation CNIL).

ANNEXE B

Mesures techniques et organisationnelles.

Art. 32 RGPD — garanties concrètes mises en œuvre par anø.

B.1 Chiffrement
- **AES-256-GCM** app-layer sur tous les PII CIF (email, backups vault, questionnaires V2) ;
- **HMAC-SHA256** pour lookup email (pas de SHA-256 simple — rainbow table) ;
- **TLS 1.3** sur tous les transports (Caddy 2 + Let's Encrypt) ;
- **age** (Ed25519) pour les backups DB.

B.2 Contrôle d'accès
- Better Auth v1.5+ (CVE-2025-61928 corrigé) ;
- 2FA admin obligatoire ;
- sessions courtes (24 h), rotation cookies ;
- aucun secret hardcodé — fail-fast si env var manquante.

B.3 Isolation multi-tenant
- **RLS PostgreSQL** sur toutes les tables scopées `license_id` ;
- test CI d'isolation cross-tenant obligatoire avant chaque release.

B.4 Journalisation et traçabilité
- Table `admin_audit_trail` append-only (rétention 3 ans) ;
- actions journalisées : `decrypt_email`, `delete_license`, `export_data`, `key_rotation`, `sign_dpa`, `login` / `logout` ;
- table `dpa_signatures` append-only (rétention 10 ans — preuve contractuelle).

B.5 Minimisation et PII scrubber
- **Scrubber whitelist** (et non blacklist) sur GlitchTip / Slack / logs / LLM ;
- les noms clients finaux ne quittent **jamais** le vault local desktop ;
- `customer_name` CIF non stocké côté anø (délégué à Stripe).

B.6 Proxy LLM
- Proxy serveur anø (pas d'OAuth tiers — art. 50 AI Act) ;
- scrubber PII whitelist avant envoi ;
- option BYOK disponible (CIF apporte sa clé Anthropic).

B.7 Sauvegardes et continuité
- Backup DB quotidien chiffré age, rétention 30 jours ;
- backup vault desktop rétention 30 j + 90 j grace period ;
- monitoring Uptime Kuma 24/7 ;
- test de restauration trimestriel.

B.8 Gestion des incidents
- Collecte d'erreurs centralisée (GlitchTip self-hosted) ;
- runbook breach art. 33 formalisé ;
- notification au CIF sous 24 h (art. 3.6).

ANNEXE C

Personnes autorisées.

En phase beta privée (avril 2026) : l'éditeur anø opère seul. Toute extension d'équipe (embauche, sous-traitant IT) fait l'objet d'un avenant à cette annexe, avec mise à jour des contrats de confidentialité.

Contact DPO anø : `privacy@anoplatform.io`.

SIGNATURES

POUR LE SOUS-TRAITANT (anø)	POUR LE RESPONSABLE (CIF)
Nom : **[à compléter]**	Nom : **renseigné par clickwrap**
Qualité : représentant légal	Email : **renseigné par clickwrap**
Date : **[à compléter]** — Lieu : Paris	Date : **timestamp serveur au clic**
Référence pré-signature : hash PDF v1	Méthode : `clickwrap` / `docusign` / `yousign`

v(12pt) text(size: 8.5pt, fill: fg3, style: « italic »)[Référence signature : `dpa_signatures.id` — preuve append-only avec `ip_address`, `user_agent`, `document_hash = SHA-256(PDF v1)`.]