DPA RGPD · ART. 28

Data Processing Agreement. Entre Korva, sous-traitant, et le Client, responsable du traitement.

Le présent accord encadre le traitement par Korva des données à caractère personnel confiées par le Client, conformément à l'article 28 du Règlement (UE) 2016/679 (RGPD) et à la loi Informatique et Libertés modifiée. Il s'applique à toute donnée transmise via la plateforme Korva, y compris les fichiers FEC, CAMT.053, DRM ProDouane, DSN, et toute donnée d'authentification ou d'usage liée à l'exploitation du service.

Korva SAS · siège Bordeaux · contact RGPD bonjour@korva.me.

1. Préambule

Parties.

Korva SAS, société par actions simplifiée, sise à Bordeaux, représentée par son président, ci-après désignée « le Sous-traitant ». Le Client, personne morale signataire du contrat commercial Korva, ci-après désigné « le Responsable du traitement ».

Objet.

Le présent accord définit les conditions dans lesquelles Korva traite, pour le compte du Responsable du traitement, les données à caractère personnel nécessaires à l'exécution du service Korva (consolidation financière multi-entités wine, pack PE, surveillance covenants, audit log, MCP).

Durée.

Le présent accord prend effet à la date de signature du contrat commercial Korva et reste applicable pour toute la durée d'exécution du service, augmentée des durées de conservation légales (sept ans pour les données comptables FEC, conformément à l'article L.123-22 du Code de commerce).

2. Périmètre du traitement

Catégories de données.

Données d'identification (nom, prénom, email professionnel, rôle), données comptables et financières du Responsable (écritures FEC, relevés CAMT.053, déclarations DRM ProDouane, DSN), données de configuration tenant (référentiels comptables, entités, covenants), métadonnées d'audit log (action, horodatage, hash chaîné).

Finalités.

Exécution du service Korva · ingestion et parsing des fichiers, consolidation P&L multi-entités, génération du pack PE, surveillance des covenants, exposition MCP, audit log immuable. Aucun traitement à des fins commerciales tierces. Aucune réutilisation pour entraîner un modèle de langage.

Durée de conservation.

FEC, CAMT.053, DRM, DSN · sept ans (obligation légale française). Logs d'authentification · trois ans. Sessions actives · six mois. Métadonnées d'audit log · sept ans, immuables (chaînage hash). Données utilisateur supprimables sous trente jours sur demande, hors données comptables sous obligation de conservation.

3. Obligations du sous-traitant

Korva s'engage à respecter, sans exception, les obligations suivantes ·

Hébergement EU strict.

L'intégralité des données est hébergée en Union européenne · Postgres Railway Frankfurt ou Belgique, storage Scaleway Paris, monitoring Sentry self-hosted EU. Aucun transfert hors UE par défaut.

Chiffrement at-rest et in-transit.

AES-256 sur Postgres et Scaleway. TLS 1.3 sur tous les flux client-serveur et serveur-serveur. Secrets stockés chiffrés (Railway secret manager, Vercel encrypted env).

Isolation multi-tenant FORCE RLS.

Postgres ENABLE + FORCE ROW LEVEL SECURITY sur toutes les tables tenant-scoped. Rôle applicatif sans SUPERUSER ni BYPASSRLS. SET LOCAL app.current_tenant à chaque requête. Tests d'isolation cross-tenant exécutés en CI.

Accès restreint.

Accès aux données limité aux personnes ayant besoin d'en connaître dans le cadre de la maintenance ou du support. Authentification Clerk EU obligatoire. Aucun accès direct base de données en production hors incident.

Audit log immuable.

Toute action sensible est loggée AVANT exécution, chaînée par hash. Conservation sept ans. Aucune modification rétroactive techniquement possible (triggers BEFORE UPDATE/DELETE).

Confidentialité du personnel.

Tout collaborateur ayant accès aux données est tenu à une obligation de confidentialité de durée illimitée, formalisée contractuellement.

Coopération CNIL.

Korva coopère avec la CNIL en cas de contrôle. Les registres de traitement et la documentation d'architecture sont produits sous huit jours ouvrés à toute demande motivée.

4. Sous-traitants ultérieurs

Korva s'appuie sur les sous-traitants ultérieurs listés ci-dessous. Tout ajout ou remplacement fait l'objet d'une notification écrite au Responsable du traitement au moins trente jours avant prise d'effet, avec possibilité d'opposition motivée.

`Vercel` · Hébergement frontend (Next.js) · région EU · DPA signé.

`Railway` · Hébergement backend + Postgres · Frankfurt / Belgique · DPA signé.

`Scaleway` · Object storage · Paris · DPA signé · souveraineté française.

`Clerk` · Authentification · région EU · DPA signé.

`Anthropic` · API LLM · États-Unis · DPA signé + Zero Data Retention activé · aucune réutilisation des requêtes pour l'entraînement.

`Resend` · Email transactionnel · région EU · DPA signé.

`Sentry` · Monitoring erreurs · instance self-hosted EU · pas de tiers.

`BetterStack` · Uptime monitoring · EU · DPA signé.

`Plausible` · Analytics · France · sans cookies, sans tracker tiers.

5. Sécurité technique

Korva applique le cadre NIST Cybersecurity Framework (CSF) sur les cinq fonctions Identify, Protect, Detect, Respond, Recover, ainsi que les mitigations OWASP Top 10 2025.

Identify.

Cartographie complète des données traitées · catégories, finalités, durée. Inventaire des sous-traitants. Registre des traitements.

Protect.

FORCE Row-Level Security, chiffrement AES-256 at-rest et TLS 1.3 in-transit, authentification Clerk EU avec MFA disponible, principe du moindre privilège sur tous les accès, secrets jamais en clair.

Detect.

Sentry self-hosted EU pour la capture d'erreurs, BetterStack pour l'uptime, audit log immuable avec hash chaîné, alertes automatiques sur anomalies (échec auth répété, requête cross-tenant tentée).

Respond.

Procédure d'incident documentée · containment, communication, remédiation. Founder joignable 24/7 pendant la phase MVP, équipe Phase 2.

Recover.

Backups Postgres quotidiens chiffrés conservés trente jours. RPO vingt-quatre heures, RTO quatre heures. Tests de restauration trimestriels.

OWASP Top 10.

Injection (Pydantic strict + paramétrage SQLAlchemy), broken access control (FORCE RLS), cryptographic failures (AES-256, TLS 1.3), insecure design (revue d'architecture systématique), security misconfiguration (CSP + HSTS + headers stricts Vercel), vulnerable components (pip-audit, npm audit, trivy en CI), identification failures (Clerk EU), software and data integrity (signatures CI, branch protection), security logging (audit log immuable), SSRF (allowlist stricte sur les outils MCP).

6. Notification de violation

En cas de violation de données à caractère personnel concernant le Responsable du traitement, Korva notifie le Responsable dans un délai maximum de soixante-douze heures à compter de la connaissance de l'incident, par email au correspondant désigné et publication sur status.korva.me. La notification précise la nature de la violation, les catégories et le volume de données concernées, les conséquences probables, les mesures prises ou proposées.

Korva assiste le Responsable dans ses obligations de notification à la CNIL (article 33 RGPD) et aux personnes concernées (article 34 RGPD).

7. Droits des personnes concernées

Korva met à la disposition du Responsable du traitement les fonctions techniques nécessaires à l'exercice des droits prévus aux articles 15 à 22 du RGPD ·

Accès (Art. 15).

Export des données personnelles d'un utilisateur sur demande, format JSON structuré.

Rectification (Art. 16).

Édition des données utilisateur via l'interface Settings.

Effacement (Art. 17).

Suppression sous trente jours, hors données comptables sous obligation légale.

Limitation (Art. 18).

Suspension d'un compte utilisateur via Settings, conservation sans traitement.

Portabilité (Art. 20).

Export FEC, CAMT.053, DRM aux formats standards d'origine.

Opposition (Art. 21).

Désactivation des notifications non essentielles via Settings.

8. Audits et contrôles

Le Responsable du traitement peut demander un audit annuel des mesures techniques et organisationnelles de Korva, après préavis raisonnable (trente jours) et sous réserve de confidentialité bilatérale. L'audit porte sur la conformité au présent accord et au RGPD. Les frais sont à la charge du Responsable, sauf en cas de non-conformité avérée.

Korva s'engage à produire un rapport SOC 2 Type II dès la Phase 2 du produit (objectif fin 2027). Dans l'intervalle, le présent DPA, l'architecture documentée (ARCHITECTURE.md) et la documentation sécurité (docs/) constituent les éléments de preuve.

9. Transferts hors UE

Aucun transfert de données à caractère personnel hors Union européenne n'est effectué par défaut. La seule exception est l'API Anthropic (États-Unis), utilisée pour la couche d'intelligence Korva, encadrée par un DPA signé avec Anthropic et la fonction Zero Data Retention activée. Aucune donnée n'est utilisée pour entraîner un modèle.

Les transferts hors UE supplémentaires nécessitent un accord écrit préalable du Responsable du traitement, accompagné des clauses contractuelles types de la Commission européenne.

10. Résiliation

À la fin du contrat commercial, et selon l'option choisie par le Responsable du traitement, Korva procède au retour ou à la destruction des données dans un délai de trente jours, à l'exception des données comptables soumises à l'obligation de conservation légale de sept ans (article L.123-22 du Code de commerce), conservées dans un stockage isolé jusqu'à expiration du délai puis détruites.

Un certificat de destruction est remis au Responsable sur demande.

11. Signatures

Le présent accord est signé électroniquement par les deux parties à la conclusion du contrat commercial Korva. La signature manuscrite reste recevable. Le DPA prend effet à la date de la signature la plus tardive.

Pour Korva · Antoine, Président de Korva SAS

Date · _____

Pour le Client · [Nom · Fonction · Société]

Date · _____