

# Data Processing Agreement (DPA)

Modèle d'accord de sous-traitance — article 28 du RGPD · version 2026.04.28-v1 · mis à jour le 2026-04-28

## Préambule

Le présent Data Processing Agreement (« DPA ») encadre, en application de l'article 28 du règlement (UE) 2016/679 (« RGPD »), les conditions dans lesquelles l'éditeur du service Scope traite des données à caractère personnel pour le compte de l'Organisation cliente. Il complète et fait partie intégrante des Conditions Générales d'Utilisation et de Vente. En cas de contradiction, le présent DPA prévaut sur les CGU/CGV pour toute disposition relative à la protection des données.

## Parties

**Sous-traitant :** Amir KELLOUSIDHOUM, entrepreneur individuel — 133 rue du Général de Gaulle, 94350 Villiers-sur-Marne, France · SIRET 917 709 024 00017 (« Scope »).

**Responsable de traitement :** L'Organisation cliente ayant souscrit un abonnement Scope (« le Client »), à compléter avec sa raison sociale, son adresse et son numéro de TVA intracommunautaire.

**Point de contact :** Délégué à la Protection des Données — dpo@getscope.dev. Notification d'incident : security@getscope.dev (24/7).

## Article 1 — Objet et durée

Scope traite les Données du Client aux seules fins de fournir le Service défini aux CGU/CGV. La durée du traitement correspond à la durée de l'abonnement, augmentée du délai de suppression prévu à l'article 8.

## Article 2 — Nature et finalité du traitement

Le traitement consiste à ingérer, structurer, transformer (via IA tierce sous clause de non-entraînement), stocker, afficher, exporter et signer les Documents de cadrage produits à partir du Contenu fourni par le Client. La finalité est strictement opérationnelle : exécuter le pipeline IA et permettre au Client de produire et partager ses livrables.

## Article 3 — Catégories de données

- Données d'identification professionnelle des collaborateurs et contacts cités dans les briefs.
- Contenu professionnel libre : texte, audio transcrit, PDF, notes.
- Métadonnées techniques : horodatage, nom de fichier, taille, IP de connexion.

Aucune catégorie particulière de données au sens de l'article 9 du RGPD (santé, religion, orientation, etc.), ni donnée relative aux condamnations (article 10), n'est attendue. Le Client s'engage à ne pas charger de telles données dans le Service.

## Article 4 — Catégories de personnes concernées

- Collaborateurs et utilisateurs du Client habilités à utiliser le Service.
- Clients finaux du Client et leurs interlocuteurs cités dans les briefs, notes de cadrage ou propositions commerciales.
- Signataires des documents soumis à signature électronique.

## Article 5 — Obligations de Scope

- Ne traiter les Données que sur instruction documentée du Client (l'acceptation des CGU/CGV constitue ces instructions, sauf instruction spécifique communiquée par écrit à dpo@getscope.dev).

- Garantir que les personnes autorisées à traiter les Données sont soumises à une obligation de confidentialité contractuelle ou légale.
- Mettre en œuvre les mesures techniques et organisationnelles décrites en Annexe 2 (article 32 du RGPD).
- N'engager aucun sous-traitant ultérieur sans information préalable du Client, dans les conditions de l'article 6.
- Assister le Client pour répondre aux demandes d'exercice des droits des personnes concernées (articles 12 à 22 du RGPD).
- Notifier au Client toute violation de Données dans un délai maximum de 72 heures après en avoir pris connaissance (article 33.2).
- Au choix du Client, supprimer ou restituer les Données à la fin de la prestation (article 8).
- Mettre à disposition du Client toutes les informations nécessaires pour démontrer sa conformité aux obligations de l'article 28 et permettre la réalisation d'audits (article 9).

## Article 6 — Sous-traitants ultérieurs

Le Client autorise Scope à recourir aux sous-traitants ultérieurs listés en Annexe 3. Toute évolution de cette liste (ajout ou remplacement) est notifiée par email aux clients abonnés au moins 30 jours avant son entrée en vigueur, en application de l'article 28.2 du RGPD. Le Client peut s'opposer à un nouveau sous-traitant pour des motifs légitimes liés à la protection des Données ; à défaut d'accord, le Client peut résilier sans pénalité son abonnement avant l'entrée en vigueur du changement.

## Article 7 — Transferts hors Union européenne

Les Données du Client sont stockées en Union européenne. Certains traitements peuvent toutefois impliquer un transfert vers un pays tiers, encadré par les Clauses Contractuelles Types adoptées par la Commission européenne (décision d'exécution (UE) 2021/914 du 4 juin 2021), incorporées par référence dans les contrats avec chaque sous-traitant ultérieur, et complété par les mesures supplémentaires décrites en Annexe 2.

## Article 8 — Sort des données en fin de contrat

À la résiliation de l'abonnement, le Client peut, pendant 30 jours, exporter ses Documents de cadrage et son Contenu via les outils du Service. Au terme de ce délai, Scope supprime l'ensemble des Données dans un délai maximum de 30 jours supplémentaires, sauf obligation légale de conservation (par exemple les pièces comptables, conservées 10 ans en application de l'article L.123-22 du Code de commerce). Une attestation de suppression peut être délivrée sur demande à [dpo@getscope.dev](mailto:dpo@getscope.dev).

## Article 9 — Audit et conformité

Scope met à disposition du Client, sur demande motivée, la documentation nécessaire à la démonstration de sa conformité au présent DPA : politique de sécurité, registre des sous-traitants, mesures techniques et organisationnelles, journal des violations de Données. Le Client peut, à ses frais et après préavis raisonnable de 30 jours, conduire une fois par an un audit sur dossier, ou le faire réaliser par un tiers indépendant tenu au secret professionnel et préalablement accepté par Scope (acceptation ne pouvant être refusée sans motif légitime).

## Article 10 — Droit applicable

Le présent DPA est régi par le droit français. Tout litige relatif à son interprétation ou à son exécution est soumis à la compétence du Tribunal Judiciaire de Créteil (94), sous réserve des règles d'attribution de compétence d'ordre public.

## Annexe 1 — Description du traitement

**Activités :** Ingestion, structuration, génération assistée par IA, stockage, export, partage, signature

électronique des Documents de cadrage.

**Catégories de Données :** Identifiants professionnels, contenu libre, métadonnées techniques.

**Personnes concernées :** Collaborateurs du Client, clients finaux du Client cités dans les briefs, signataires.

**Durée :** Durée de l'abonnement, augmentée du délai de suppression de l'article 8.

**Lieu :** Union européenne (Dublin, Frankfurt, Paris, Pays-Bas), avec transferts encadrés vers les États-Unis pour certains sous-traitants (cf. Annexe 3).

## Annexe 2 — Mesures techniques et organisationnelles

- Chiffrement TLS 1.3 en transit, AES-256 au repos (volumes Postgres et Storage).
- Authentification : mots de passe hachés et salés (bcrypt), MFA pour les comptes administrateurs.
- Cloisonnement multi-tenant : politiques Postgres Row Level Security (RLS) systématiques, séparation par org\_id en base et en Storage (chemin {org\_id}/{project\_id}/...).
- Audit logs : journalisation immuable des mutations sensibles (export, signature, débit crédits), conservation 24 mois pour les comptes Enterprise.
- Idempotence : tout webhook (Stripe, DocuSeal) et toute opération de crédits est rejouable sans effet de bord, identifiée par event\_id ou request\_id.
- Gestion des secrets : variables d'environnement chiffrées, rotation des clés API, séparation rôles user / service-role.
- Sauvegardes : snapshots automatiques quotidiens, réplication multi-AZ.
- Sécurité du paiement : aucune donnée de carte traitée par Scope ; tokenisation totale par Stripe (PCI DSS Level 1).
- Réponse aux incidents : notification sous 72 heures conformément à l'article 33, runbook documenté, point de contact unique dpo@getscope.dev.
- Suppression sécurisée : purge programmée à la résiliation, hors obligations comptables.

## Annexe 3 — Sous-traitants ultérieurs

Liste à jour au 2026-04-28, version 2026.04.28-v1. La version vivante est publiée sur <https://getscope.dev/trust> et exposée en JSON sur <https://getscope.dev/api/sub-processors.json>.

### Vercel

**Entité juridique :** Vercel Inc.

**Finalité :** Hébergement de l'application Next.js et exécution des routes serverless.

**Localisation :** Dublin, Irlande (région eu-west-1)

**Juridiction :** EU

**Certifications :** SOC 2 Type II, ISO 27001, PCI DSS

**DPA :** <https://vercel.com/legal/dpa>

### Supabase

**Entité juridique :** Supabase, Inc.

**Finalité :** Base Postgres, authentification, stockage objet et Realtime pour les briefs, documents de cadrage, audit log et exports.

**Localisation :** Dublin, Irlande (région eu-west-1)

**Juridiction :** EU

**Certifications :** SOC 2 Type II, HIPAA-ready

**DPA :** <https://supabase.com/legal/dpa>

## OpenRouter

**Entité juridique :** OpenRouter, Inc.

**Finalité :** Routeur LLM avec clause contractuelle `data_collection=deny` : vos prompts et les réponses générées ne sont jamais utilisés pour entraîner les modèles.

**Localisation :** Routage privilégié vers les fournisseurs de modèles UE

**Juridiction :** US

**Certifications :** Clauses Contractuelles Types (CCT) UE

**Mitigation Cloud Act :** OpenRouter est un proxy stateless : aucun prompt ni output n'est conservé côté OpenRouter au-delà du temps de traitement. Le contrat impose `data_collection=deny` en aval. Mitigation supplémentaire : routage explicite vers Mistral (FR) pour les comptes Enterprise « Mode IA souverain ».

**DPA :** <https://openrouter.ai/terms>

---

## Gladia

**Entité juridique :** Gladia SAS

**Finalité :** Transcription audio de qualité entreprise avec spécialisation sur le français — utilisée pour les notes de cadrage à partir d'enregistrements de réunion.

**Localisation :** Paris, France

**Juridiction :** EU

**Certifications :** RGPD, ISO 27001 (en cours)

**DPA :** <https://www.gladia.io/privacy>

---

## DocuSeal (self-hosted)

**Entité juridique :** Scope (auto-hébergé — instance DocuSeal)

**Finalité :** Signature électronique conforme eIDAS pour les notes de cadrage, propales et DPA — instance DocuSeal auto-hébergée par l'éditeur, aucune donnée signée n'est partagée avec un tiers.

**Localisation :** Hostinger NL (Pays-Bas, UE)

**Juridiction :** EU

**Certifications :** eIDAS (signature électronique avancée), Auto-hébergé UE

**DPA :** /dpa

---

## Resend

**Entité juridique :** Resend, Inc.

**Finalité :** Envoi des emails transactionnels (notifications, confirmations, magic links, signatures, exports prêts).

**Localisation :** Région eu-west-1 (Irlande)

**Juridiction :** EU

**Certifications :** SOC 2 Type II, HIPAA-ready

**DPA :** <https://resend.com/legal/dpa>

---

## Stripe

**Entité juridique :** Stripe Payments Europe Ltd

**Finalité :** Traitement des paiements, gestion des abonnements et émission des factures clients. Aucune

donnée de carte ne transite par les serveurs de Scope (tokenisation totale).

**Localisation :** Dublin, Irlande

**Jurisdiction :** EU

**Certifications :** PCI DSS Level 1, SOC 1, SOC 2 Type II, ISO 27001

**DPA :** <https://stripe.com/legal/dpa>

---

## Plausible

**Entité juridique :** Plausible Insights OÜ

**Finalité :** Analytics web auto-hébergées sans cookies et sans données personnelles. Activées uniquement après consentement explicite.

**Localisation :** Allemagne (Hetzner)

**Jurisdiction :** EU

**Certifications :** RGPD by design, Sans cookies

**DPA :** <https://plausible.io/dpa>

---

## Sentry

**Entité juridique :** Functional Software, Inc. (Sentry)

**Finalité :** Capture des erreurs runtime côté serveur et navigateur, pour identifier et corriger les régressions. Les payloads sont scrubbés (PII, secrets) avant émission.

**Localisation :** États-Unis

**Jurisdiction :** US

**Certifications :** SOC 2 Type II, ISO 27001, Privacy Shield (CCT UE)

**Mitigation Cloud Act :** Bascule planifiée vers GlitchTip auto-hébergé en UE à M3 (avant le passage SOC 2 Type 1). En attendant : scrubbing agressif côté SDK (PII, tokens, secrets) et durée de rétention abaissée à 30 jours.

**DPA :** <https://sentry.io/legal/dpa/>

---

## Cloudflare

**Entité juridique :** Cloudflare, Inc.

**Finalité :** Résolution DNS du domaine getscope.dev et routage email vers les boîtes professionnelles. Aucune donnée applicative ne transite par Cloudflare.

**Localisation :** Réseau global (anycast)

**Jurisdiction :** GLOBAL

**Certifications :** SOC 2 Type II, ISO 27001, PCI DSS

**Mitigation Cloud Act :** Cloudflare ne traite que des métadonnées DNS et de routage email. Aucune donnée applicative client (briefs, cadrages, exports) n'est exposée. Le DPA Cloudflare incorpore les Clauses Contractuelles Types UE.

**DPA :** <https://www.cloudflare.com/cloudflare-customer-dpa/>

---

## Signatures

Pour rendre ce DPA opposable, contresignez-le via DocuSeal (lien à demander à [dpo@getscope.dev](mailto:dpo@getscope.dev)) ou retournez un exemplaire signé en original à l'adresse postale ci-dessus. Une copie contresignée sous 48 heures ouvrées est garantie.