RULIORA

Accord de Traitement des Données (DPA)

Conditions de sous-traitance des données personnelles conformément à l'article 28 du RGPD — Responsable de traitement : le Client ; Sous-traitant : Ruliora SAS.

Dernière mise à jour : 22 juin 2026

> Extrait automatiquement de la page en ligne `legal/dpa` — la page publiée fait foi.

Version PDF du DPA

Document contractuellement opposable — signez et retournez à legal@ruliora.com

-

Télécharger DPA PDF

1. Définitions

Au sens du présent Accord :

- **Responsable de traitement** : le Client, personne morale ayant souscrit un abonnement Ruliora, qui détermine les finalités et les moyens du traitement des données personnelles de ses utilisateurs.

- **Sous-traitant** : Ruliora SAS (ci-après « Ruliora »), qui traite des données personnelles pour le compte et sur instruction du Responsable de traitement.

- **RGPD** : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

- **Données personnelles** : toute information se rapportant à une personne physique identifiée ou identifiable, traitée dans le cadre de la fourniture de la Plateforme.

- **Violation de données** : violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données personnelles.

- **Sous-traitant ultérieur** : tout tiers auquel Ruliora recourt pour effectuer des activités de traitement spécifiques pour le compte du Client.

2. Objet et durée du traitement

Le présent Accord de Traitement des Données (« DPA ») encadre le traitement par Ruliora des données personnelles confiées par le Client dans le cadre de l'utilisation de la plateforme Ruliora, conformément à l'article 28 du RGPD. Le DPA fait partie intégrante des Conditions Générales de Vente (CGV). En cas de contradiction, le DPA prévaut pour les questions relatives au traitement des données personnelles.

Le DPA prend effet à la date de souscription et reste applicable pendant toute la durée du contrat principal ainsi que pendant 30 jours suivant son terme (délai de récupération des données ou suppression

confirmée).

3. Nature et finalité des traitements

- **Nature :** hébergement, stockage, sauvegarde, indexation, analyse, restitution et traitement par des modèles d'intelligence artificielle des données du Client.

- **Finalité exclusive :** fourniture des fonctionnalités de la Plateforme Ruliora (gouvernance d'entreprise, décisions, conseil d'administration, conformité réglementaire, ESG/CSRD, assistant IA Synapse).

- Ruliora n'utilise pas les données du Client à des fins de prospection commerciale, de profilage publicitaire ou d'entraînement de modèles d'IA sans accord écrit exprès du Client.

4. Types de données traitées

- Données d'identification et de contact (nom, prénom, adresse email professionnelle, fonction, numéro de téléphone professionnel)
- Données de connexion et de traçabilité (logs d'accès, adresses IP, sessions, empreintes de dispositif, audit trail horodaté)
- Données métier saisies par le Client (décisions stratégiques, procès-verbaux de réunions, documents contractuels, dataroom, données ESG/CSRD, questionnaires fournisseurs)
- Données de configuration et de personnalisation (préférences d'interface, paramètres d'organisation, intégrations tierces)
- Métadonnées de traitement IA (prompts, réponses générées, scores de conformité)

Données sensibles (art. 9 RGPD) : le périmètre contractuel n'inclut pas de traitement de données sensibles. Si le Client en saisit volontairement dans les interfaces de la Plateforme, il en assume l'entière responsabilité de traitement. Le Client est expressément invité à ne pas saisir de telles données dans les interfaces IA (voir CGU art. 3).

5. Catégories de personnes concernées

- Employés et collaborateurs du Client autorisés à utiliser la Plateforme
- Administrateurs et membres du conseil d'administration désignés par le Client
- Tiers dont les données sont saisies par le Client (fournisseurs, partenaires, parties prenantes, clients du Client)
- Utilisateurs invités et intervenants ponctuels (auditeurs externes, conseils)

6. Obligations de Ruliora en tant que sous-traitant (art. 28 §3 RGPD)

Ruliora s'engage à :

- **Instruction documentée :** traiter les données uniquement sur instruction documentée du Client, conformément au contrat principal et aux fonctionnalités de la Plateforme. Si Ruliora estime qu'une instruction constitue une violation du RGPD, elle en informe immédiatement le Client par écrit.

- **Confidentialité :** garantir que les personnes autorisées à traiter les données ont souscrit à une obligation de confidentialité appropriée et sont formées aux exigences du RGPD.

- **Mesures de sécurité :** mettre en œuvre et maintenir les mesures techniques et organisationnelles décrites à l'article 9 du présent DPA, conformément à l'article 32 du RGPD.

- **Sous-traitance ultérieure :** ne recourir à un sous-traitant ultérieur qu'avec l'autorisation générale préalable du Client (matérialisée par acceptation des présentes) et avec un préavis de 14 jours pour tout ajout ou remplacement de sous-traitant, permettant au Client de s'y opposer.

- **Assistance au responsable :** aider le Client à respecter ses obligations au titre des articles 32 à 36 du RGPD (sécurité, notification de violations, AIPD, consultation préalable CNIL) ainsi qu'à répondre aux demandes d'exercice des droits des personnes concernées.

- **Notification de violation :** notifier le Client de toute violation de données dans les meilleurs délais, et au plus tard dans les 24 heures suivant sa découverte (délai inférieur à l'obligation légale de 72h de l'art. 33 RGPD, voir art. 12 ci-après).

- **Sort des données en fin de contrat :** à la fin du contrat, restituer au Client l'ensemble des données (export JSON/CSV/XLSX) et procéder à leur suppression sécurisée dans un délai de 30 jours suivant la demande confirmée, sauf obligation légale de conservation (voir art. 11 ci-après).

- **Audit et documentation :** mettre à disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations du présent article et permettre la réalisation d'audits ou d'inspections sur préavis écrit raisonnable (voir art. 10 ci-après).

7. Sous-traitants ultérieurs

Le Client autorise Ruliora à recourir aux sous-traitants ultérieurs suivants. Ruliora leur impose des obligations de protection des données équivalentes aux présentes :

Sous-traitant | Localisation | Finalité | Garanties RGPD |

Anthropic Inc. | États-Unis | Modèles d'IA Claude (Synapse) | SCC Module 2 (Décision UE 2021/914) + TIA Schrems II |

OVH SAS | France (Gravelines, Strasbourg) | Hébergement, infrastructure cloud, backups chiffrés | ISO 27001 certifié, HDS (zones), SecNumCloud (zones), RGPD natif |

Sentry (Functional Software Inc.) | États-Unis | Monitoring d'erreurs applicatives (traces anonymisées) | SCC + DPA Sentry, données PII scrubbées avant envoi |

OpenAI LLC | États-Unis | Modèles d'IA GPT (fonctionnalités IA en fallback) | SCC Module 2 (Décision UE 2021/914) + TIA Schrems II — désactivable via allow_external_fallback = false |

Stripe Inc. | États-Unis | Traitement des paiements (données de facturation uniquement) | SCC Module 2 (Décision UE 2021/914) — données limitées aux informations de facturation (nom, email, montant) |

Resend (Functional Software) | États-Unis | Envoi d'e-mails transactionnels (notifications, alertes) | SCC Module 2 (Décision UE 2021/914) — données limitées à l'adresse email et au contenu de la notification |

Datadog Inc. | États-Unis (New York) | Monitoring applicatif, métriques de performance, journaux d'infrastructure | SCC Module 2 (Décision UE 2021/914) + DPA Datadog — logs pseudonymisés, rétention 15 jours, option EU residency activée |

Liste complète et à jour disponible sur demande à dpo@ruliora.com. Tout ajout ou remplacement de sous-traitant fait l'objet d'une notification avec préavis minimum de 14 jours, le Client pouvant s'y opposer par écrit pour motif légitime.

8. Transferts hors Union Européenne

Ruliora recourt à des sous-traitants basés aux États-Unis (Anthropic, OpenAI, Stripe, Resend, Sentry). Pour ces transferts, Ruliora applique les Clauses Contractuelles Types (CCT) Module 2 (responsable de traitement vers sous-traitant) adoptées par la Décision d'exécution de la Commission UE 2021/914 du 4 juin 2021.

Pour Anthropic en particulier, les CCT Module 2 encadrent les transferts de données soumises aux fonctionnalités d'IA de la Plateforme. Une Analyse d'Impact des Transferts (TIA) au sens de l'arrêt Schrems II (CJUE, C-311/18) a été réalisée et est disponible sur demande à dpo@ruliora.com.

Mesures complémentaires pour les transferts IA : (i) seules les données nécessaires à la requête sont transmises ; (ii) les données d'identification sont minimisées avant transmission ; (iii) Anthropic est contractuellement lié à ne pas utiliser les données pour entraîner ses modèles dans le cadre du contrat Enterprise.

Option sans transfert hors UE : le Client peut activer le mode allow_external_fallback = false dans les paramètres de son organisation pour désactiver l'ensemble des sous-traitants IA américains.

8bis. Risques liés aux lois extraterritoriales (CLOUD Act, UK GDPR)

US CLOUD Act (2018)

Ruliora recourt à des sous-traitants américains (Anthropic, OpenAI, Stripe, Resend, Sentry) soumis au **US CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018)**. En vertu de cette loi, les autorités américaines peuvent, dans certaines conditions, contraindre ces sous-traitants à communiquer des données hébergées ou accessibles par eux, y compris celles de clients européens, sans notification préalable à Ruliora ou au Client.

Mesures d'atténuation : (i) les données whistleblowing (alertes lanceurs) et les analyses de conformité sont classées données sensibles — le Client est expressément invité à activer le mode allow_external_fallback = false pour ces traitements, ce qui exclut tout traitement par les sous-traitants IA américains ; (ii) les CCT Module 2 et la TIA Schrems II couvrent les transferts de données dans les conditions habituelles d'utilisation ; (iii) Ruliora s'engage à notifier le Client sans délai de toute injonction reçue, dans la mesure permise par la loi applicable.

Recommandation pour les clients traitant des données particulièrement sensibles (défense, santé, whistleblowing) : activer impérativement le mode sans sous-traitants US (paramètre allow_external_fallback = false) ou demander à Ruliora un hébergement sur infrastructure souveraine dédiée (offre VPS dédié — CGV §2.3).

UK GDPR et transferts post-Brexit

Pour les Clients établis au Royaume-Uni, les transferts de données sont encadrés par le **UK Data Protection Act 2018 (UK GDPR)** et l'**International Data Transfer Agreement (IDTA)** adopté par l'ICO (Information Commissioner's Office) le 21 mars 2022, ou l'UK Addendum aux CCT UE 2021/914. L'Union

Européenne bénéficie d'une décision d'adéquation UK depuis juin 2021 — les transferts UE→UK sont donc libres. Les transferts UK→UE (données de clients UK vers l'infrastructure OVH France) sont couverts par cette adéquation réciproque.

Les Clients UK peuvent contacter dpo@ruliora.com pour obtenir l'IDTA signé ou l'UK Addendum applicable à leur situation.

Base légale Art. 9 RGPD — Données sensibles (module Whistleblowing)

Le module de signalement (Loi Waserman n°2022-401) peut traiter des données sensibles au sens de l'Art. 9 RGPD (opinions syndicales, données de santé, données judiciaires). La base légale applicable est l'Art. 9(2)(b) RGPD — obligation légale dans le domaine du droit du travail et de la protection sociale — la Loi Waserman et la Directive 2019/1937 constituant le fondement légal. À titre subsidiaire, l'Art. 9(2)(g) RGPD (intérêt public) peut s'appliquer. Le Client (responsable de traitement) est tenu de documenter cette base légale dans son propre registre des activités de traitement.

8ter. Analyse d'Impact sur la Protection des Données (AIPD — Art. 35 RGPD)

Pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, Ruliora a réalisé ou s'engage à réaliser une AIPD conformément à l'article 35 du RGPD, notamment pour :

- Le **scoring ESG des fournisseurs** (traitement automatisé affectant potentiellement des personnes morales tierces)
- Le **module de signalement Loi Waserman** (traitement de données sensibles de lanceurs d'alerte)
- Les **modules IA à haut risque Annexe III AI Act** (screening anti-corruption, scoring cyber tiers)

Les conclusions des AIPD réalisées sont disponibles sur demande écrite à dpo@ruliora.com. Le Client (responsable de traitement) est informé que le déploiement de Ruliora auprès de ses salariés peut nécessiter sa propre AIPD si le traitement envisagé présente un risque élevé au sens de l'Art. 35 RGPD.

9. Mesures de sécurité (art. 32 RGPD)

Chiffrement et protection des données

- Chiffrement at-rest AES-256 sur l'intégralité du stockage NVMe et des sauvegardes
- Chiffrement in-transit TLS 1.3 obligatoire (HSTS preloaded, certificat ECDSA P-256)
- Audit trail cryptographique Ed25519 — toutes les actions sensibles sont signées et horodatées, non falsifiables
- Backups chiffrés cross-VPS via WireGuard (ChaCha20-Poly1305), rétention 30 jours

Contrôle des accès et authentification

- Multi-tenant Row-Level Security PostgreSQL FORCE — isolation complète des données Client par organisation
- Authentification forte : bcrypt cost 12, MFA TOTP/WebAuthn disponible, SSO SAML/OIDC
- HTTPS uniquement (HSTS), authentification par clé Ed25519 sur l'infrastructure

- Sessions courtes avec rotation des tokens, blacklist logout, révocation immédiate
- RBAC granulaire avec principe du moindre privilège

Sécurité applicative et réseau

- Protection CSRF, rate limiting par IP et par utilisateur, headers de sécurité (X-Frame-Options, CSP, X-Content-Type-Options)
- Validation et sanitization de tous les inputs utilisateur
- vRack OVH privé — base de données non exposée sur Internet public
- Firewall UFW restrictif, monitoring 24/7 (Prometheus, Grafana, Alertmanager)

10. Audit et documentation

Ruliora met à disposition du Client, sur demande écrite avec préavis raisonnable (10 jours ouvrés minimum), la documentation permettant de vérifier le respect des obligations du présent DPA, notamment :

- Le registre des activités de traitement (art. 30 RGPD) relatif aux traitements effectués pour le compte du Client
- Les derniers rapports de pentest (anonymisés si nécessaire) et certifications
- Les TIA relatives aux transferts hors UE
- Les contrats conclus avec les sous-traitants ultérieurs (ou résumés de leurs clauses essentielles)

Le Client peut mandater un auditeur indépendant soumis à confidentialité. Les audits sur site sont limités à un par an, sauf en cas de violation avérée. Les frais d'audit sont à la charge du Client, sauf si l'audit révèle un manquement de Ruliora.

11. Sort des données en fin de contrat

À l'expiration ou résiliation du contrat principal, pour quelque cause que ce soit :

- Le Client dispose d'un délai de **30 jours** pour exporter ses données (formats JSON, CSV, XLSX) via l'interface ou en contactant support@ruliora.com.
- À l'issue de ce délai, ou sur demande écrite expresse du Client, Ruliora procède à la suppression sécurisée et irréversible de l'ensemble des données du Client (écrasement multi-passes conformément au standard NIST SP 800-88).
- Ruliora adresse au Client une attestation de suppression dans les 15 jours suivant la suppression effective.
- Exception : les données faisant l'objet d'une obligation légale de conservation (par exemple logs de sécurité) sont conservées pour la durée légale minimale, puis supprimées.

12. Notification de violation (art. 33 RGPD — 72 heures)

En cas de violation de données personnelles, Ruliora s'engage à :

- Notifier le Client **dans les 24 heures** suivant la découverte de l'incident (engagement supérieur à l'obligation légale CNIL de 72h)
- Communiquer au Client, dès que possible, les informations suivantes : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou envisagées
- Fournir au Client les éléments lui permettant de remplir son obligation de notification à la CNIL dans le délai de 72h requis par l'art. 33 RGPD
- Documenter toutes les violations dans un registre interne, conformément à l'art. 33 §5 RGPD

Contact d'urgence violation de données : security@ruliora.com (astreinte 24h/24, 7j/7).

13. Coordonnées du Référent à la protection des données

Référent à la protection des données — Ruliora SAS

Email : dpo@ruliora.com

Délai de réponse maximum aux demandes des personnes concernées : 30 jours (art. 12.3 RGPD), prorogeable une fois pour les demandes complexes.

Délai de réponse aux demandes du Responsable de traitement : 10 jours ouvrés.

Le Client désigne un interlocuteur référent RGPD au sein de son organisation et le communique à Ruliora dans les 30 jours de la souscription.

14. Loi applicable et autorité de contrôle compétente

Le présent DPA est régi par le droit français et le droit de l'Union européenne. L'autorité de contrôle compétente est la **Commission Nationale de l'Informatique et des Libertés (CNIL)**, 3 Place de Fontenoy, 75007 Paris (www.cnil.fr).

Tout litige relatif à l'interprétation ou à l'exécution du présent DPA relèvera, après tentative de résolution amiable (30 jours), de la compétence exclusive du Tribunal de Commerce de Paris.