

Accord de traitement des données (DPA)

Dernière mise à jour : 20 juin 2026 · enrow.io/fr/legal/dpa

SOMMAIRE

Article 1 — Objet	Article 9 — Droit d'audit
Article 2 — Définitions	Article 10 — Conformité internationale
Article 3 — Rôles des Parties	Article 11 — Responsabilité
Article 4 — Description du traitement	Article 12 — Durée et résiliation
Article 5 — Obligations d'ENROW en qualité de Sous-Traitant	Article 13 — Dispositions finales
Article 6 — Obligations du Client	Annexe 1 — Description du traitement
Article 7 — Sous-Traitants Ultérieurs	Annexe 2 — Mesures techniques et organisationnelles (MTO)
Article 8 — Transferts hors EEE	Annexe 3 — Liste des Sous-Traitants Ultérieurs

Le présent Accord de Traitement des Données (ci-après « DPA ») est conclu entre :

SCHRUTE FARMS, SARL au capital de 500 euros, siège social au 123 Rue De Rome, 75017 Paris, RCS Paris 981 316 300, représentée par ses co-gérants Thomas LUCY et Louis CONGARD, exploitant le service « ENROW » (ci-après « ENROW » ou « le Prestataire »),

et

Le Client, personne morale ayant souscrit au Service et accepté les Conditions Générales de Vente et d'Utilisation (CGV) d'ENROW (ci-après « le Client »),

ci-après désignés individuellement une « Partie » et collectivement les « Parties ».

Le présent DPA est conclu en application de l'article 28 du Règlement (UE) 2016/679 (RGPD) et de la Loi n°78-17 du 6 janvier 1978 modifiée (Loi Informatique et Libertés). Il fait partie intégrante du Contrat conclu entre les Parties, tel que défini dans la hiérarchie documentaire de l'article 1 des CGV.

Le Délégué à la Protection des Données (DPO) d'ENROW est Monsieur Louis CONGARD, joignable à dpo@enrow.io.

Article 1 — Objet

Le présent DPA a pour objet de définir les conditions dans lesquelles ENROW traite des données à caractère personnel pour le compte du Client dans le cadre de la fourniture du Service d'enrichissement de données professionnelles B2B, et de préciser les obligations de chaque Partie en matière de protection des données.

Article 2 — Définitions

Les termes utilisés dans le présent DPA ont la même signification que dans les CGV, sauf définition spécifique ci-dessous :

- « **Données à Caractère Personnel** » ou « **DCP** » : toute information relative à une personne physique identifiée ou identifiable au sens de l'article 4(1) du RGPD.
- « **Responsable de Traitement** » : la personne physique ou morale qui détermine les finalités et les moyens du traitement de DCP (article 4(7) RGPD).

- « **Sous-Traitant** » : la personne physique ou morale qui traite des DCP pour le compte du Responsable de Traitement (article 4(8) RGPD).
- « **Sous-Traitant Ulérieur** » : tout sous-traitant engagé par ENROW pour traiter des DCP pour le compte du Client.
- « **Violation de Données** » : toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des DCP (article 4(12) RGPD).
- « **Personne Concernée** » : toute personne physique identifiée ou identifiable dont les DCP sont traitées.
- « **Autorité de Contrôle** » : toute autorité publique indépendante chargée de surveiller l'application de la réglementation relative à la protection des données (en France : la CNIL).

Article 3 — Rôles des Parties

3.1 — Double qualification d'ENROW

Les Parties reconnaissent qu'ENROW intervient dans deux rôles distincts :

(a) Responsable de Traitement indépendant : ENROW agit en qualité de Responsable de Traitement pour les DCP qu'il collecte, agrège et maintient dans sa propre base de données d'enrichissement (emails professionnels, numéros de téléphone, profils LinkedIn, informations d'entreprise). Ce traitement est fondé sur l'intérêt légitime d'ENROW (article 6.1(f) RGPD), documenté dans une LIA révisée annuellement.

(b) Sous-Traitant : ENROW agit en qualité de Sous-Traitant au sens de l'article 28 du RGPD lorsqu'il traite les Données Client (données transmises par le Client pour être enrichies) pour le compte et sur instruction du Client.

3.2 — Le Client, Responsable de Traitement

Le Client agit en qualité de Responsable de Traitement pour :

- Les Données Client qu'il transmet à ENROW pour enrichissement ;
- L'utilisation qu'il fait des Données Enrichies restituées par le Service.

Le Client détermine seul les finalités et les moyens de l'utilisation des Données Enrichies en aval du Service et est seul responsable du respect de ses obligations au titre du RGPD et de la Loi Informatique et Libertés dans ce cadre.

Article 4 — Description du traitement

Le détail du traitement est décrit en Annexe 1 du présent DPA. Il comprend notamment :

- **Finalité du traitement** : Enrichissement de données professionnelles B2B pour le compte du Client.
- **Catégories de Personnes Concernées** : Contacts professionnels (prospects, clients potentiels) du Client : salariés, dirigeants, associés de personnes morales.
- **Catégories de DCP traitées** : Nom, prénom, adresse email professionnelle, numéro de téléphone professionnel et/ou personnel, intitulé de poste, nom de l'entreprise, URL du profil LinkedIn, informations d'entreprise (secteur, taille, localisation).
- **Données sensibles** : Aucune donnée sensible au sens de l'article 9 du RGPD n'est traitée.
- **Durée du traitement** : Durée de l'Abonnement. Les Données Client sont conservées 90 jours maximum puis supprimées automatiquement. Le cache technique est de 48 heures.
- **Localisation du traitement** : Union européenne — AWS Paris (eu-west-3).

Article 5 — Obligations d'ENROW en qualité de Sous-Traitant

5.1 — Instructions du Client

ENROW ne traite les Données Client que sur instructions documentées du Client. Les présentes CGV et le présent DPA constituent les instructions initiales du Client. Toute instruction supplémentaire doit être transmise par écrit (email à dpo@enrow.io).

Si ENROW estime qu'une instruction constitue une violation du RGPD ou de toute autre réglementation applicable, il en informe immédiatement le Client par écrit.

5.2 — Confidentialité

ENROW garantit que les personnes autorisées à traiter les DCP se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale de confidentialité appropriée. Seules les personnes dont l'accès est strictement nécessaire à l'exécution du Service y ont accès.

5.3 — Sécurité du traitement

ENROW met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD. Ces mesures sont décrites en Annexe 2 du présent DPA. ENROW procède à des vérifications régulières de l'efficacité de ces mesures.

5.4 — Notification de Violation de Données

En cas de Violation de Données affectant les Données Client, ENROW s'engage à :

- Notifier le Client dans les meilleurs délais et au plus tard dans les soixante-douze (72) heures après en avoir pris connaissance ;
- Fournir les informations suivantes : description de la nature de la violation (catégories et nombre approximatif de Personnes Concernées et d'enregistrements), conséquences probables, mesures prises ou proposées pour y remédier, coordonnées du DPO ;
- Documenter la violation dans un registre interne et coopérer avec le Client pour lui permettre de respecter ses propres obligations de notification (articles 33 et 34 RGPD) ;
- Notifier la CNIL dans les 72 heures en sa qualité de Responsable de Traitement pour les données de sa propre base d'enrichissement.

5.5 — Assistance au Client

ENROW assiste le Client, dans la mesure du possible et compte tenu de la nature du traitement, pour :

- Répondre aux demandes d'exercice des droits des Personnes Concernées (accès, rectification, effacement, opposition, portabilité, limitation) ;
- Respecter ses obligations au titre des articles 32 à 36 du RGPD (sécurité, notification de violation, analyse d'impact) ;
- Répondre aux demandes et contrôles d'une Autorité de Contrôle.

Si ENROW reçoit directement une demande d'une Personne Concernée portant sur les Données Client, il en informe le Client dans les meilleurs délais et ne répond pas directement sauf instruction contraire du Client.

5.6 — Sort des données en fin de contrat

Conformément à l'article 14.3 des CGV, à la cessation du Contrat :

- **Export** : le Client dispose de trente (30) jours pour exporter ses Données Client au format CSV et/ou JSON via le Logiciel, l'API ou sur demande à support@enrow.io ;
- **Suppression** : passé ce délai, ENROW procède à la suppression définitive de l'ensemble des Données Client, y compris les copies et sauvegardes, dans un délai maximal de trente (30) jours supplémentaires ;

- **Certification** : ENROW fournit au Client, sur demande, une attestation écrite de suppression.

La suppression des Données Client n'affecte pas les données anonymisées et agrégées utilisées conformément à l'article 9.6 des CGV.

Article 6 — Obligations du Client

Le Client, en sa qualité de Responsable de Traitement, s'engage à :

- Disposer d'une base légale valide pour transmettre les Données Client à ENROW et pour utiliser les Données Enrichies (article 8.2 des CGV) ;
- Informer les Personnes Concernées conformément aux articles 13 et 14 du RGPD ;
- S'assurer que ses instructions à ENROW sont conformes à la réglementation applicable ;
- Ne transmettre aucune donnée sensible au sens de l'article 9 du RGPD ;
- Coopérer avec ENROW en cas de Violation de Données, de contrôle ou de demande d'une Autorité de Contrôle.

Article 7 — Sous-Traitants Ultérieurs

7.1 — Autorisation générale

Le Client autorise de manière générale ENROW à recourir à des Sous-Traitants Ultérieurs pour la fourniture du Service (notamment les Fournisseurs Tiers d'enrichissement et les prestataires d'hébergement). La liste des Sous-Traitants Ultérieurs en vigueur figure en Annexe 3 du présent DPA et est également disponible sur demande auprès du DPO.

7.2 — Notification et droit d'opposition

Conformément à l'article 12.2 des CGV, ENROW notifie le Client de tout changement de Sous-Traitant Ulérieur (ajout ou remplacement) au moins quinze (15) jours avant la prise d'effet. Le Client peut s'opposer par écrit dans les 15 jours. À défaut d'accord, l'opposition vaut résiliation du Contrat conformément à l'article 12.2 des CGV.

7.3 — Obligations imposées aux Sous-Traitants Ultérieurs

ENROW impose contractuellement à chaque Sous-Traitant Ulérieur des obligations de protection des données substantiellement équivalentes à celles prévues dans le présent DPA, notamment en matière de confidentialité, de sécurité, de limitation de finalité et de suppression des données.

7.4 — Responsabilité

ENROW demeure pleinement responsable envers le Client de l'exécution par ses Sous-Traitants Ultérieurs de leurs obligations en matière de protection des données.

Article 8 — Transferts hors EEE

L'ensemble des données est hébergé au sein de l'Espace Économique Européen (EEE), sur les serveurs d'AWS à Paris (eu-west-3).

Dans l'hypothèse où un transfert de DCP vers un pays tiers serait nécessaire, notamment dans le cadre du recours à un Sous-Traitant Ulérieur établi hors de l'EEE, ENROW s'assure préalablement que des garanties appropriées sont mises en place conformément au chapitre V du RGPD :

- **Décision d'adéquation** de la Commission européenne (article 45 RGPD) ;
- **Clauses Contractuelles Types (CCT)** adoptées par la Commission européenne (Décision d'exécution 2021/914), le cas échéant complétées par des mesures supplémentaires (article 46(2)(c) RGPD) ;
- **Tout autre mécanisme de transfert reconnu** par le RGPD (règles d'entreprise contraignantes, dérogations de l'article 49).

Le Client est informé de tout transfert hors EEE via la liste des Sous-Traitants Ultérieurs (Annexe 3) qui précise, pour chaque sous-traitant, sa localisation et le mécanisme de transfert applicable.

Si les CCT sont requises, elles sont réputées conclues entre ENROW et le Sous-Traitant Ultérieur concerné. Le Client peut en obtenir copie sur demande auprès du DPO.

Article 9 — Droit d'audit

Conformément à l'article 28(3)(h) du RGPD, le Client peut demander un audit des pratiques d'ENROW en matière de traitement et de sécurité des DCP, dans les conditions suivantes :

- **Préavis de 30 jours** par écrit à dpo@enrow.io ;
- **1 audit par an maximum**, sauf violation avérée ou demande d'Autorité de Contrôle ;
- **Périmètre** : conformité RGPD et DPA uniquement. Exclusion du code source, des algorithmes propriétaires et des secrets d'affaires ;
- **Réalisation** : par le Client ou un tiers indépendant sous obligation de confidentialité. ENROW peut récuser un auditeur concurrent ;
- **Coûts à la charge du Client**, sauf manquement substantiel d'ENROW.

Alternative : ENROW peut satisfaire la demande d'audit en fournissant au Client un ou plusieurs des documents suivants, de moins de 12 mois : rapport de test d'intrusion (pentest) par un tiers indépendant, questionnaire de sécurité CSA CAIQ (Consensus Assessments Initiative Questionnaire) dûment complété, ou tout autre rapport de certification ou d'audit de sécurité reconnu le cas échéant. La fourniture de ces documents dispense ENROW de l'obligation d'accepter un audit sur site pour la période couverte, sauf violation avérée ou demande d'Autorité de Contrôle.

ENROW met à la disposition du Client toute information nécessaire pour démontrer le respect de ses obligations au titre de l'article 28 du RGPD.

Article 10 — Conformité internationale

Le présent DPA s'applique dans le cadre des réglementations suivantes, dans la mesure où elles sont applicables au traitement :

- **RGPD** (Règlement (UE) 2016/679) et Loi Informatique et Libertés (Loi n°78-17) ;
- **UK GDPR** et Data Protection Act 2018 (pour les Personnes Concernées au Royaume-Uni) ;
- **nLPD** (nouvelle Loi Fédérale suisse sur la Protection des Données) ;
- **CCPA / CPRA** : ENROW agit en qualité de « service provider » au sens du CCPA/CPRA. ENROW ne vend ni ne partage les DCP au sens de cette réglementation.

Article 11 — Responsabilité

La responsabilité de chaque Partie au titre du présent DPA est soumise aux limitations et exclusions prévues à l'article 16 des CGV, sous réserve des exceptions applicables (faute lourde, dol, manquement en matière de protection des données).

Chaque Partie est responsable du respect de ses propres obligations au titre de la réglementation applicable en matière de protection des données. Le Client reste seul responsable de l'utilisation qu'il fait des Données Enrichies en aval du Service.

Article 12 — Durée et résiliation

Le présent DPA entre en vigueur à la date d'acceptation des CGV par le Client et reste en vigueur aussi longtemps que le Contrat est actif. Les obligations d'ENROW relatives à la suppression des Données Client (article 5.6) et à la

confidentialité survivent à la cessation du Contrat.

Article 13 — Dispositions finales

13.1 — Hiérarchie

Le présent DPA fait partie intégrante du Contrat. En cas de contradiction entre le DPA et les CGV, le DPA prévaut pour toute question relative au traitement des DCP. Pour toute autre question, les CGV prévalent.

13.2 — Modification

ENROW peut modifier le présent DPA pour se conformer aux évolutions de la réglementation. Toute modification substantielle est notifiée au Client trente (30) jours avant son entrée en vigueur.

13.3 — Droit applicable

Le présent DPA est régi par le droit français. Compétence exclusive des tribunaux de Paris.

Annexe 1 — Description du traitement

- **Responsable de Traitement (Données Client) :** Le Client.
- **Sous-Traitant :** SCHRUTE FARMS / ENROW.
- **DPO du Sous-Traitant :** Louis CONGARD — dpo@enrow.io.
- **Finalités du traitement :** Enrichissement de données professionnelles B2B (recherche d'emails, de téléphones, de profils LinkedIn, d'informations d'entreprise) à partir des Données Client transmises par le Client.
- **Nature du traitement :** Collecte, consultation, rapprochement, structuration, stockage temporaire, restitution, suppression.
- **Catégories de Personnes Concernées :** Contacts professionnels (salariés, dirigeants, associés, indépendants) de personnes morales ciblées par le Client dans le cadre de sa prospection B2B.
- **Catégories de DCP :** Nom, prénom, adresse email professionnelle, numéro de téléphone professionnel, numéro de téléphone personnel (le cas échéant), intitulé de poste, nom et informations de l'entreprise (secteur, taille, localisation, site web), URL du profil LinkedIn.
- **Données sensibles (art. 9 RGPD) :** Aucune.
- **Base légale (traitement par ENROW en tant que RT) :** Intérêt légitime (article 6.1(f) RGPD) — LIA documentée.
- **Fréquence du traitement :** En continu, à la demande du Client via le Logiciel, l'API ou l'Extension.
- **Durée de conservation des Données Client :** 90 jours maximum après transmission, puis suppression automatique.
- **Cache technique :** 48 heures (justifié par la performance et la vérification ; purgé sous 24h en cas de demande d'opposition).
- **Localisation :** UE — AWS Paris (eu-west-3).

Annexe 2 — Mesures techniques et organisationnelles (MTO)

Conformément à l'article 32 du RGPD, ENROW met en œuvre les mesures suivantes :

A. Chiffrement

- **En transit :** toutes les communications sont chiffrées via TLS 1.2 ou supérieur (HTTPS). Les connexions non chiffrées sont rejetées.
- **Au repos :** les données stockées sont chiffrées via AES-256 (chiffrement natif AWS).
- **Mots de passe :** hachage irréversible par algorithme bcrypt avec salage individuel.

B. Contrôle d'accès

- **Authentification** : identification par email et mot de passe, avec authentification multi-facteurs (MFA) disponible et recommandée.
- **Gestion des accès** : modèle RBAC (Role-Based Access Control) strict. Chaque accès est limité au strict nécessaire (principe du moindre privilège).
- **Sessions** : tokens JWT signés avec expiration automatique.

C. Infrastructure et hébergement

- **Hébergeur** : Amazon Web Services (AWS), région eu-west-3 (Paris). AWS est certifié ISO 27001, SOC 1/2/3, et conforme au RGPD.
- **Isolation réseau** : bases de données et services internes isolés dans un Virtual Private Cloud (VPC) sans accès public direct.
- **Sauvegardes** : sauvegardes automatiques quotidiennes, chiffrées, avec rétention configurée.

D. Journalisation et surveillance

- **Logs d'accès** : traçabilité des actions utilisateurs (identifiant, action, horodatage, adresse IP). Logs chiffrés au repos.
- **Monitoring** : surveillance continue de l'infrastructure et alertes automatisées en cas d'anomalie.

E. Minimisation et durée de conservation

- Seules les données strictement nécessaires à la fourniture du Service sont collectées et traitées ;
- Données Client : 90 jours maximum, puis suppression automatique ;
- Cache technique : 48 heures ;
- Suppression effective et irréversible en fin de période de rétention.

F. Sécurité organisationnelle

- Sensibilisation des équipes à la protection des données ;
- Politique de mots de passe robustes pour les accès internes ;
- Principe du moindre privilège appliqué à toutes les équipes ;
- Engagement de confidentialité signé par chaque collaborateur ayant accès aux DCP.

G. Gestion des incidents

- Procédure interne de gestion des incidents de sécurité ;
- Notification au Client sous 72h (article 5.4 du présent DPA) ;
- Registre des violations tenu à jour.

Ces mesures sont révisées et mises à jour régulièrement pour tenir compte de l'état de l'art, des coûts de mise en œuvre et de la nature des risques.

Annexe 3 — Liste des Sous-Traitants Ultérieurs

Partie A — Sous-Traitants publiés (liste en vigueur au 20 juin 2026)

Sous-Traitant	Finalité	Catégories de DCP	Localisation	Mécanisme de transfert
Amazon Web Services (AWS)	Hébergement infrastructure, bases de données, stockage	Toutes les DCP traitées par le Service	UE (Paris, eu-west-3)	Pas de transfert hors EEE
Stripe, Inc.	Traitement des paiements et facturation	Nom, email, données de paiement du Client	UE (Irlande)	Pas de transfert hors EEE

Sous-Traitant	Finalité	Catégories de DCP	Localisation	Mécanisme de transfert
SigNoz	Journalisation, monitoring et observabilité	Identifiants techniques, adresses IP, logs d'utilisation	UE (instance européenne)	Pas de transfert hors EEE
HubSpot, Inc.	CRM — gestion de la relation client et prospects	Nom, prénom, email, entreprise, historique d'interactions	UE (France / Allemagne)	Pas de transfert hors EEE (instance européenne)
Brevo (ex-Sendinblue)	Email marketing et communications transactionnelles	Nom, prénom, email du Client/Utilisateur	France / UE	Pas de transfert hors EEE
Intercom, Inc.	Support client (chat, tickets, base de connaissances)	Nom, prénom, email, contenu des échanges de support	UE (Irlande)	Pas de transfert hors EEE
Anthropic, Inc. (Claude.ai)	Assistance IA pour le traitement et l'analyse de données. Aucune donnée n'est utilisée pour l'entraînement des modèles.	Données traitées ponctuellement sans persistance	USA	Décision d'adéquation (EU-US DPF) + CCT. Clause de non-utilisation pour l'entraînement.
Partnero	Programme d'affiliation et gestion des commissions	Nom, email, données de référencement des affiliés	UE (Estonie)	Pas de transfert hors EEE
Google Workspace	Communication interne (email, documents)	Données internes, potentiellement DCP de clients dans les échanges	UE (serveurs France)	Pas de transfert hors EEE (configuration région France)
Slack Technologies (Salesforce)	Communication interne entre équipes	Données internes, potentiellement DCP de clients dans les échanges	UE (instance européenne)	Pas de transfert hors EEE

Partie B — Fournisseurs d'enrichissement de données (liste confidentielle)

Dans le cadre de la fourniture du Service d'enrichissement, ENROW fait appel à des fournisseurs spécialisés dans les catégories suivantes :

Catégorie	Finalité	Types de DCP
Fournisseurs de données SERP	Extraction de données publiquement accessibles via les moteurs de recherche	Nom, prénom, entreprise, données professionnelles publiquement accessibles
Fournisseurs de données de contact professionnel	Enrichissement complémentaire en emails et téléphones professionnels	Email professionnel, numéro de téléphone professionnel et/ou personnel
Fournisseurs de données firmographiques	Enrichissement en informations d'entreprise (secteur, taille, chiffre d'affaires, localisation, structure juridique)	Dénomination sociale, SIREN/SIRET, secteur d'activité, effectifs, chiffre d'affaires, adresse du siège social
Fournisseurs de signaux	Détection de signaux d'affaires (levées de fonds, recrutements, changements de poste, technologies utilisées, actualités)	Données d'entreprise, noms et fonctions de dirigeants et collaborateurs, événements professionnels publiquement accessibles

Confidentialité de la liste nominative : la liste nominative complète des fournisseurs d'enrichissement, incluant leur identité, leur localisation et le mécanisme de transfert applicable, constitue un secret d'affaires d'ENROW au sens de la Directive (UE) 2016/943 relative à la protection des savoir-faire et des informations commerciales non divulgués, et de la loi n°2018-670 du 30 juillet 2018 transposant cette directive en droit français.

Communication au Client : cette liste est communiquée sur demande écrite au DPO (dpo@enrow.io), sous réserve de la signature préalable d'un accord de confidentialité (NDA) par le Client. Le Client s'engage à ne pas divulguer

cette liste ni les informations qu'elle contient à un tiers, et à l'utiliser uniquement pour vérifier la conformité d'ENROW au RGPD.

Droit d'opposition : le mécanisme de notification et de droit d'opposition prévu à l'article 7.2 du présent DPA et à l'article 12.2 des CGV s'applique intégralement aux fournisseurs d'enrichissement. Le Client est notifié de tout changement au moins quinze (15) jours avant la prise d'effet, même si le nom du nouveau fournisseur est communiqué sous NDA.

Garanties communes : ENROW garantit que chaque fournisseur d'enrichissement (a) est lié contractuellement par des obligations de protection des données substantiellement équivalentes à celles du présent DPA, (b) est situé dans l'EEE ou couvert par un mécanisme de transfert conforme au chapitre V du RGPD, et (c) ne traite les DCP que dans le cadre strict des instructions d'ENROW et aux seules fins d'enrichissement.