upster

DATA PROCESSING AGREEMENT - UPSTER.AI - 2026

ENTRE

La société SOARLY, SARL au capital de 2.000 €, dont le siège social est situé au 1 rue de la gare, 40100 Dax, immatriculée au greffe de DAX sous le n°939 920 591 R.C.S.

Ci-après dénommée le « Prestataire » ou «UPSTER »,
DE PREMIERE PART,

ET

Toute personne physique ou morale utilisant la plateforme Upster.ai

Ci-après dénommée le « Client »,
DE SECONDE PART.

PRÉAMBULE

Le présent contrat est conclu dans le cadre de l'exécution du contrat principal relatif à la fourniture de la solution SaaS Upster.ai (les "Conditions Générales de Vente").

Ce contrat vise à définir les conditions dans lesquelles UPSTER, agissant en qualité de Sous-Traitant, traite des données à caractère personnel pour le compte du Client, Responsable du Traitement, en conformité avec le Règlement (UE) 2016/679 (RGPD) et la loi française Informatique et Libertés.

LE PRÉSENT CONTRAT EST OBLIGATOIRE ET INDISSOCIABLE DES CGV.

CECI EXPOSÉ, IL A ETE CONVENU CE QUI SUIT :

ARTICLE 0 – DÉFINITIONS

Au sens du présent contrat :

- "Données à Caractère Personnel" ou "Données" : toute information se rapportant à une personne physique identifiée ou identifiable
- "Traitement" : toute opération appliquée à des données (collecte, enregistrement, conservation, modification, extraction, consultation, utilisation, communication, effacement, destruction)
- "Responsable du Traitement" : le Client, qui détermine les finalités et les moyens du traitement
- "Sous-Traitant" : UPSTER, qui traite des données pour le compte du Responsable du Traitement
- "Violation de Données" : violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données
- "Personne Concernée" : toute personne physique dont les données sont traitées
- "CNIL" : Commission Nationale de l'Informatique et des Libertés
- "DPO" : Data Protection Officer / Délégué à la Protection des Données
- "Sous-Traitant Ultérieur" : tout prestataire engagé par UPSTER pour traiter des données

ARTICLE 1 – OBJET DU TRAITEMENT

1.1 Nature du traitement

UPSTER traite des données à caractère personnel pour le compte du Client dans le cadre de la fourniture de la solution SaaS Upster.ai, permettant :

- L'automatisation des réponses aux messages directs (DM) Instagram
- La génération de réponses via intelligence artificielle
- La gestion des conversations avec les prospects du Client
- L'analyse de performance et statistiques d'usage

1.2 Finalités du traitement

Les données sont traitées exclusivement aux fins suivantes :

1. Génération automatique de réponses aux messages Instagram via IA
2. Personnalisation des réponses en fonction du contexte conversationnel
3. Stockage temporaire de l'historique des conversations (2 mois maximum)
4. Fourniture de statistiques agrégées au Client
5. Support technique et résolution d'incidents
6. Amélioration de la solution (données anonymisées uniquement)

1.3 Durée du traitement

Le traitement des données est effectué pendant toute la durée du contrat principal (CGV).

À l'issue du contrat, les données sont :

- Soit restituées au Client dans un format exploitable (.csv, .json, .xml)
- Soit supprimées définitivement sous 30 jours

ARTICLE 2 – CATÉGORIES DE DONNÉES TRAITÉES

2.1 Données traitées par UPSTER

UPSTER traite les catégories de données suivantes :

Données d'identification :
- Prénom / Nom
- Pseudonyme Instagram
- Identifiant Instagram (ID utilisateur)

Données de contenu :
- Messages directs (DM) Instagram échangés
- Contenu textuel des conversations
- Métadonnées des messages (date, heure, statut)

Données comportementales :
- Historique des interactions avec le compte Instagram du Client
- Fréquence des messages
- Engagement (taux de réponse)

Données techniques :
- Tokens OAuth Instagram
- Logs de connexion API
- Adresse IP (uniquement pour l'acceptation du contrat)

2.2 Données exclues

UPSTER ne traite AUCUNE donnée sensible au sens de l'article 9 du RGPD :
- Origine raciale ou ethnique
- Opinions politiques, religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques ou biométriques
- Données de santé

En cas de détection de telles données dans les messages, le Client s'engage à les supprimer immédiatement.

2.3 Personnes concernées

Les personnes concernées par le traitement sont :
- Les prospects du Client (utilisateurs Instagram entrant en contact via DM)
- Les clients du Client (ayant interagi via Instagram)

ARTICLE 3 – OBLIGATIONS DU RESPONSABLE DU TRAITEMENT (CLIENT)

3.1 Base légale du traitement
Le Client garantit disposer d'une base légale valide pour le traitement des données, conformément à l'article 6 du RGPD :

- Consentement de la personne concernée, OU
- Exécution d'un contrat, OU
- Intérêt légitime du Client (marketing direct, prospection commerciale)

Le Client est seul responsable de la vérification et du respect de cette base légale.

3.2 Information des personnes concernées
Le Client s'engage à informer les personnes concernées du traitement de leurs données, conformément aux articles 13 et 14 du RGPD.
Cette information doit mentionner :

- L'identité du Client (Responsable du Traitement)
- L'identité d'UPSTER (Sous-Traitant)
- Les finalités du traitement
- La durée de conservation (2 mois)
- Les destinataires des données (notamment transferts USA vers OpenAI/Mistral/Gemini)
- Les droits des personnes (accès, rectification, effacement, portabilité, opposition)

UPSTER met à disposition du Client un modèle de politique de confidentialité conforme.

3.3 Respect des droits des personnes
Le Client est responsable de la gestion des demandes d'exercice des droits des personnes concernées :

- Droit d'accès (article 15 RGPD)
- Droit de rectification (article 16 RGPD)
- Droit à l'effacement (article 17 RGPD)
- Droit à la limitation du traitement (article 18 RGPD)
- Droit à la portabilité (article 20 RGPD)
- Droit d'opposition (article 21 RGPD)

UPSTER s'engage à assister le Client dans le traitement de ces demandes dans un délai de 72 heures après réception de la demande transmise par le Client.

3.4 Instructions documentées
Le Client donne les instructions suivantes à UPSTER :

1. Traiter les données uniquement aux fins définies à l'article 1.2
2. Ne pas transférer les données en dehors de l'Union Européenne sauf vers les sous-traitants ultérieurs listés à l'Annexe 1
3. Conserver les données pendant 2 mois maximum
4. Supprimer ou restituer les données à la fin du contrat

Toute instruction supplémentaire doit être communiquée par écrit à : contact@upster.ai

ARTICLE 4 – OBLIGATIONS DU SOUS-TRAITANT (UPSTER)

4.1 Traitement conforme aux instructions
UPSTER s'engage à :

- Traiter les données uniquement sur instruction documentée du Client
- Ne pas utiliser les données à des fins autres que celles définies dans le présent contrat
- Ne pas communiquer les données à des tiers non autorisés

4.2 Confidentialité
UPSTER garantit que les personnes autorisées à traiter les données :

- Sont soumises à une obligation de confidentialité contractuelle
- N'ont accès qu'aux données strictement nécessaires à l'exécution de leur mission

4.3 Sécurité des données
UPSTER met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD.
Ces mesures sont détaillées à l'Article 5 (Sécurité).

4.4 Sous-traitance ultérieure
UPSTER peut faire appel à des Sous-Traitants Ultérieurs pour exécuter certaines opérations de traitement.
La liste des Sous-Traitants Ultérieurs est fournie en Annexe 1 du présent contrat.
Le Client autorise expressément le recours à ces Sous-Traitants Ultérieurs.

UPSTER s'engage à :

- Informer le Client de tout changement (ajout/remplacement) avec un préavis de 30 jours
- Imposer aux Sous-Traitants Ultérieurs les mêmes obligations de protection des données
- Rester pleinement responsable vis-à-vis du Client en cas de manquement d'un Sous-Traitant Ultérieur

Le Client dispose d'un droit d'opposition à l'ajout d'un nouveau Sous-Traitant Ultérieur. En cas d'opposition motivée, le Client pourra résilier le contrat sans pénalité.

4.5 Assistance au Client
UPSTER s'engage à assister le Client dans le respect de ses obligations RGPD, notamment :

- Gestion des demandes d'exercice des droits (délai : 72h)
- Réalisation d'analyses d'impact sur la protection des données (AIPD) si nécessaire
- Notification des violations de données (article 33 RGPD)
- Audit de conformité (sur demande écrite du Client)

4.6 Registre des activités de traitement
UPSTER tient un registre des catégories d'activités de traitement effectuées pour le compte du Client, conformément à l'article 30.2 du RGPD.
Ce registre est tenu à la disposition du Client et de la CNIL sur demande.

4.7 Suppression ou restitution des données
À l'issue du contrat, UPSTER s'engage à :

Option 1 - Restitution :

- Restituer toutes les données dans un format exploitable (.csv, .json, .xml)
- Délai de demande : 15 jours après la fin du contrat
- Délai de livraison : 7 jours après réception de la demande

Option 2 - Suppression :

- Supprimer définitivement toutes les données
- Méthode : écrasement sécurisé (norme DoD 5220.22-M ou équivalent)
- Délai : 30 jours maximum après la fin du contrat

Certificat de suppression fourni sur demande.

ARTICLE 5 – MESURES DE SÉCURITÉ

5.1 Mesures techniques

UPSTER met en œuvre les mesures de sécurité techniques suivantes :

Chiffrement :
- Chiffrement des données en transit : TLS 1.3 minimum
- Chiffrement des données au repos : AES-256
- Chiffrement des sauvegardes : AES-256

Authentification et contrôle d'accès :
- Gestion granulaire des accès (principe du moindre privilège)
- Révocation immédiate des accès en cas de départ d'un collaborateur
- Revue trimestrielle des droits d'accès

Surveillance et détection :
- Surveillance continue des infrastructures (24/7)
- Détection automatique d'intrusion (IDS/IPS)
- Logs d'audit centralisés et conservés 12 mois
- Alertes automatiques en cas d'activité suspecte

Sauvegardes :
- Sauvegardes quotidiennes automatisées
- Rétention : 30 jours minimum
- Sauvegardes chiffrées (AES-256)

5.3 Hébergement sécurisé

Les données sont hébergées sur des serveurs situés en France (Union Européenne) :

- Hébergeur : Hostinger VPS (datacenters certifiés ISO 27001)
- Localisation : France
- Certification : ISO 27001, HDS (si applicable)
- Contrat de sous-traitance signé avec l'hébergeur

5.4 Revue de sécurité

Les mesures de sécurité sont revues et mises à jour :

- Annuellement dans le cadre d'un audit interne
- Immédiatement en cas de violation de données
- À la demande du Client (audit externe aux frais du Client)

ARTICLE 6 – NOTIFICATION DES VIOLATIONS DE DONNÉES

6.1 Définition
Une Violation de Données désigne toute violation de la sécurité entraînant, de manière accidentelle ou illicite :

- La destruction
- La perte
- L'altération
- La divulgation non autorisée
- L'accès non autorisé à des données transmises, conservées ou traitées

6.2 Obligation de notification à la CNIL
En cas de violation de données susceptible d'engendrer un risque pour les droits et libertés des personnes, UPSTER s'engage à notifier la CNIL dans un délai de 72 heures après en avoir pris connaissance, conformément à l'article 33 du RGPD.
Cette notification comprendra :

- La nature de la violation
- Les catégories et le nombre approximatif de personnes concernées
- Les catégories et le nombre approximatif d'enregistrements de données concernés
- Les conséquences probables de la violation
- Les mesures prises ou proposées pour remédier à la violation

6.3 Obligation d'information du Client
UPSTER s'engage à informer le Client de toute violation de données dans un délai maximum de 24 heures après en avoir pris connaissance.
Cette information sera communiquée par :

- Email à l'adresse du Client enregistrée dans le compte
- Téléphone (si numéro renseigné)
- Interface de la plateforme (alerte dans le tableau de bord)

L'information comprendra :

- La nature de la violation
- Les données concernées
- Le nombre de personnes potentiellement affectées
- Les mesures correctives immédiates prises
- Les recommandations pour le Client

6.4 Rapport détaillé
UPSTER fournira au Client un rapport détaillé de la violation dans un délai maximum de 15 jours après la découverte, comprenant :

- L'analyse des causes (techniques, humaines, organisationnelles)
- La chronologie des événements
- L'évaluation de l'impact
- Les mesures correctives mises en place
- Les mesures préventives pour éviter toute récurrence
- Les éventuelles recommandations pour le Client

6.5 Assistance à la notification
Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, UPSTER assistera le Client dans ses obligations de communication aux personnes concernées (article 34 RGPD).

UPSTER fournira :
- Un modèle de communication aux personnes concernées
- La liste des personnes affectées (si disponible)
- Les coordonnées de contact pour les questions des personnes

6.6 Documentation des violations
UPSTER tient un registre des violations de données comprenant :
- Les faits concernant la violation
- Les effets de la violation
- Les mesures prises pour y remédier

Ce registre est tenu à la disposition de la CNIL et du Client.

ARTICLE 7 – TRANSFERTS INTERNATIONAUX DE DONNÉES

7.1 Principe
Les données sont principalement traitées et stockées au sein de l'Union Européenne (France).

Toutefois, certains Sous-Traitants Ultérieurs sont situés hors UE, notamment aux États-Unis.

7.2 Sous-Traitants hors UE
Les transferts de données vers des pays tiers sont effectués vers les prestataires suivants :

Sous-Traitant	Pays	Traitement	Garanties
OpenAI	USA	Génération de réponses IA	Clauses Contractuelles Types (CCT) UE + API Zero Retention
Mistral AI	France/USA	Génération de réponses IA	CCT UE + API Zero Retention
Google Gemini	USA	Génération de réponses IA	CCT UE + API Zero Retention
Anthropic (Claude)	USA	Génération de réponses IA	CCT UE + API Zero Retention
Stripe	Irlande/USA	Paiements	CCT UE + Certification PCI-DSS niveau 1

Annexe 1

7.3 Garanties appropriées
UPSTER s'engage à ce que tous les transferts hors UE soient encadrés par des garanties appropriées au sens de l'article 46 RGPD :
Clauses Contractuelles Types (CCT) :
- Version approuvée par la Commission Européenne (Décision 2021/914)
- Signées avec chaque Sous-Traitant Ultérieur situé hors UE
- Copies disponibles sur demande du Client

API Zero Retention Policy :
- Les fournisseurs d'IA (OpenAI, Mistral, Gemini, Anthropic) s'engagent contractuellement à ne pas stocker les données traitées via API
- Les données sont traitées en temps réel puis immédiatement supprimées
- Aucune réutilisation des données pour l'entraînement des modèles d'IA

7.4 Analyse d'impact des transferts
Conformément aux recommandations du CEPD (Comité Européen de la Protection des Données), UPSTER a réalisé une analyse d'impact des transferts (Transfer Impact Assessment) pour chaque Sous-Traitant hors UE.
Cette analyse est disponible sur demande du Client.

7.5 Surveillance des transferts

UPSTER surveille en permanence :

- Les évolutions législatives dans les pays tiers (notamment USA)
- La jurisprudence de la CJUE relative aux transferts internationaux
- Les recommandations de la CNIL et du CEPD

En cas d'invalidation des CCT ou de modification substantielle du cadre juridique, UPSTER informera le Client dans les 48 heures et proposera des mesures alternatives.

7.6 Droit d'opposition du Client

Le Client peut s'opposer à tout moment aux transferts vers un Sous-Traitant hors UE.

En cas d'opposition, UPSTER proposera une alternative (autre prestataire ou limitation fonctionnelle).

Si aucune alternative n'est techniquement possible, le Client pourra résilier le contrat sans pénalité.

ARTICLE 8 – AUDITS ET CONTRÔLES

8.1 Droit d'audit du Client
Le Client dispose d'un droit d'audit des traitements effectués par UPSTER.
Modalités :

- Fréquence : 1 fois par an maximum (sauf incident de sécurité)
- Préavis : 30 jours calendaires
- Périmètre : mesures de sécurité, procédures RGPD, registre des traitements
- Réalisé par : le Client ou un auditeur indépendant certifié (ISO 27001, CNIL, etc.)
- Coûts : à la charge du Client
- Durée : maximum 2 jours ouvrés
- Conditions : ne doit pas perturber l'exploitation normale de la plateforme

UPSTER s'engage à collaborer pleinement et à fournir toutes les informations nécessaires.

8.2 Audits de sécurité internes
UPSTER réalise des audits internes :

- Tests de vulnérabilité : semestriels
- Tests d'intrusion : annuels
- Revue de code : trimestrielle (code critique)
- Audit de conformité RGPD : annuel

Les rapports d'audit (anonymisés) sont disponibles sur demande du Client.

8.3 Certifications
UPSTER s'engage à obtenir et maintenir les certifications suivantes :

- ISO 27001 (Sécurité de l'information) : objectif 2027
- SOC 2 Type II (Contrôles de sécurité) : objectif 2027

Les certificats seront communiqués au Client dès obtention.

8.4 Droit de contrôle de la CNIL
UPSTER accepte les contrôles de la CNIL à tout moment.
En cas de contrôle, UPSTER informera le Client dans les 48 heures

ARTICLE 9 – RESPONSABILITÉ ET INDEMNISATION

9.1 Responsabilité générale
Chaque partie est responsable du respect de ses obligations au titre du RGPD :

- Le Client en tant que Responsable du Traitement
- UPSTER en tant que Sous-Traitant

9.2 Responsabilité en cas de violation
En cas de violation du RGPD imputable à UPSTER :

- UPSTER assume l'intégralité de la responsabilité vis-à-vis des personnes concernées et de la CNIL
- UPSTER indemnisera le Client de tout préjudice subi (amendes CNIL, dommages et intérêts, frais de justice)

9.3 Exclusions de responsabilité
UPSTER ne saurait être tenue responsable :

- Des violations résultant d'instructions du Client non conformes au RGPD
- Des violations causées par le non-respect par le Client de ses obligations (ex : absence de base légale)
- Des violations résultant d'un acte d'un tiers (piratage, force majeure)
- Des violations résultant d'une défaillance d'un Sous-Traitant Ultérieur autorisé par le Client

9.4 Limitation des dommages indirects
Conformément aux CGV, UPSTER ne saurait être tenue responsable des dommages indirects (perte d'exploitation, perte de clientèle, atteinte à l'image, etc.), sauf faute intentionnelle ou dolosive.

ARTICLE 10 – DURÉE ET RÉSILIATION

10.1 Durée
Le présent contrat entre en vigueur à la date d'acceptation des CGV et du présent DPA par le Client.
Il demeure en vigueur pendant toute la durée du contrat principal (CGV).

10.2 Résiliation
Le présent DPA prend fin automatiquement à la résiliation du contrat principal (CGV).

10.3 Sort des données après résiliation
Voir Article 4.7 (Suppression ou restitution des données).

ARTICLE 11 – DISPOSITIONS GÉNÉRALES

11.1 Modification du DPA
UPSTER se réserve le droit de modifier le présent DPA en cas :

- D'évolution de la réglementation (RGPD, loi française)
- De recommandations de la CNIL ou du CEPD
- D'évolution des Sous-Traitants Ultérieurs

Toute modification sera notifiée au Client avec un préavis de 30 jours.

11.2 Ordre de priorité
En cas de contradiction entre les présentes et les CGV, les dispositions du présent DPA prévalent en matière de protection des données personnelles.

11.3 Divisibilité
Si une clause du présent DPA est déclarée nulle ou inapplicable, les autres dispositions demeurent pleinement en vigueur.

11.4 Loi applicable
Le présent DPA est soumis au droit français et au RGPD.

11.5 Juridiction compétente
Tout litige relatif au présent DPA relève de la compétence exclusive du Tribunal de Commerce de DAX.