ACCORD DE TRAITEMENT DE DONNÉES (DPA)

Conforme à l'article 28 du Règlement (UE) 2016/679 (RGPD)

Version : 1.1

Date d'entrée en vigueur : date d'acceptation du Document de commande y faisant référence

ENTRE LES SOUSSIGNÉS

Le Responsable de Traitement (ci-après le « **Client** » ou « **Responsable de Traitement** »)

Le client identifié au devis, au bon de commande ou au formulaire de souscription faisant référence au présent DPA (ci-après le « Document de commande » et le « Client »).

Adresse : celle indiquée au Document de commande

E-mail de contact RGPD : celui indiqué au Document de commande

DPO (si désigné) : le cas échéant, indiqué au Document de commande

ET

Le Sous-Traitant (ci-après le « **Prestataire** » ou « **Sous-Traitant** »)

La société **YOUAI**, SARL au capital de 1 000 €, dont le siège social est situé au 62 boulevard Fauriat, 42000 Saint-Étienne, immatriculée au RCS de Saint-Étienne sous le n° 105 263 735 (SIRET siège 105 263 735 00018), n° TVA intracommunautaire FR54105263735, représentée par ses cogérants Monsieur Joris PELLEGRIN et Monsieur Malcom MOREL.

E-mail de contact RGPD : contact@youai.fr

Ci-après désignés ensemble les « **Parties** ».

PRÉAMBULE

Les Parties sont liées par un contrat de prestation de services (le « **Contrat Principal** ») conclu sur la base d'un Document de commande (devis, bon de commande ou formulaire de souscription en ligne) faisant référence au présent DPA standard. Le DPA est accepté par la signature ou l'acceptation électronique du Document de commande, dont il fait partie intégrante, sans signature séparée. Les spécificités de chaque traitement (finalité, catégories de données, sous-traitants applicables, contact RGPD) figurent au Document de commande. Dans le cadre de l'exécution de ce Contrat Principal, le Prestataire est amené à traiter, pour le compte du Client, des données à caractère personnel.

Le présent Accord de Traitement de Données (ci-après le « **DPA** ») a pour objet de définir les conditions dans lesquelles le Prestataire, agissant en qualité de Sous-Traitant au sens de l'article 28 du RGPD, s'engage à effectuer pour le compte du Client les opérations de traitement de données personnelles décrites ci-après.

ARTICLE 1 — DESCRIPTION DU TRAITEMENT

1.1 Nature et finalité du traitement

La finalité et la description du traitement propres à chaque projet sont précisées au Document de commande (le cas échéant, bloc « RGPD » des conditions particulières du devis). À défaut de précision : hébergement, exploitation et maintenance de la Solution développée par le Prestataire pour le Client.

1.2 Catégories de personnes concernées

Les catégories de personnes concernées propres à chaque projet sont précisées au Document de commande. La liste indicative ci-dessous présente les catégories usuelles.

- Utilisateurs finaux de la Solution (clients, prospects, salariés du Client)
- Visiteurs du site internet
- Contacts commerciaux
- Correspondants et interlocuteurs du Client, participants aux échanges et réunions traités par la Solution
- Candidats à l'emploi, le cas échéant
- Autres : le cas échéant, précisées au Document de commande

1.3 Catégories de données traitées

Les catégories de données traitées propres à chaque projet sont précisées au Document de commande. La liste indicative ci-dessous présente les catégories usuelles.

- Données d'identification : nom, prénom, e-mail, téléphone
- Données de connexion : adresse IP, identifiants, logs, cookies
- Données professionnelles : fonction, société, données de facturation
- Contenus générés par les utilisateurs
- Contenus traités par la Solution : e-mails, documents, enregistrements et transcriptions, requêtes adressées aux outils d'intelligence artificielle
- Données techniques d'usage (statistiques anonymisées ou non)
- Autres : le cas échéant, précisées au Document de commande

Ne sont en principe traitées ni catégories particulières de données (article 9 RGPD : santé, opinions, religion, origine, etc.), ni données relatives aux condamnations (article 10 RGPD). Toute exception doit être expressément documentée par avenant au présent DPA. Le Client s'interdit de transmettre de telles données sans en avoir préalablement informé le Prestataire par écrit.

1.4 Durée du traitement

Le traitement est effectué pendant toute la durée du Contrat Principal, étendue le cas échéant au délai de restitution ou de destruction des données prévu à l'article 9 ci-après.

ARTICLE 2 — OBLIGATIONS DU SOUS-TRAITANT

Conformément à l'article 28 du RGPD, le Prestataire, en qualité de Sous-Traitant, s'engage à :

2.1 Instructions documentées — Ne traiter les données personnelles que sur instruction documentée du Client, y compris en cas de transfert vers un pays tiers. Le présent DPA et le Contrat Principal valent instructions initiales documentées. Toute instruction complémentaire fera l'objet d'un écrit (e-mail accepté). Si le Prestataire estime qu'une instruction du Client constitue une violation du RGPD ou d'autres dispositions applicables, il en informera immédiatement le Client.

2.2 Confidentialité — Garantir que les personnes autorisées à traiter les données personnelles sont soumises à une obligation contractuelle de confidentialité ou à une obligation légale appropriée.

2.3 Sécurité — Prendre toutes mesures techniques et organisationnelles requises au titre de l'article 32 du RGPD, et notamment celles décrites à l'article 4 du présent DPA.

2.4 Sous-traitance en cascade — Respecter les conditions prévues à l'article 5 ci-après pour le recours à d'autres sous-traitants.

2.5 Coopération avec les droits des personnes — Aider le Client à donner suite aux demandes des personnes concernées exerçant leurs droits (accès, rectification, effacement, opposition, limitation, portabilité, retrait du consentement). Le Prestataire transmettra au Client, dans les meilleurs délais, toute demande adressée directement à lui par une personne concernée.

2.6 Assistance à la conformité — Aider le Client à respecter ses obligations en matière de sécurité, de notification de violation, d'analyse d'impact (AIPD) et de consultation préalable de la CNIL, dans la mesure raisonnable et compte tenu de la nature du traitement et des informations dont dispose le Prestataire. L'assistance excédant la fourniture des informations disponibles peut être facturée au tarif en vigueur.

2.7 Notification des violations — Notifier au Client toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance, par e-mail à l'adresse de contact RGPD du Client. La notification précise, dans la mesure où ces informations sont disponibles :

- La nature de la violation et les catégories et nombre approximatifs de personnes concernées et d'enregistrements ;
- Les conséquences probables de la violation ;
- Les mesures déjà prises ou envisagées pour atténuer ses effets ;
- Le point de contact pour obtenir des informations complémentaires.

2.8 Restitution ou destruction — À l'issue du traitement, restituer ou détruire les données personnelles selon les modalités prévues à l'article 9.

2.9 Documentation — Mettre à disposition du Client toute information nécessaire à la démonstration du respect des obligations du présent article 28 RGPD, dans la limite raisonnable et sous réserve de confidentialité.

ARTICLE 3 — OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

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

3.1 Disposer de la base légale appropriée pour les traitements confiés au Prestataire (consentement, contrat, obligation légale, intérêt légitime, etc.) et garantir qu'il a effectué les démarches nécessaires en matière d'information des personnes concernées.

3.2 Tenir le registre des activités de traitement le concernant (article 30 RGPD).

3.3 Réaliser, le cas échéant, l'analyse d'impact (AIPD) requise par l'article 35 du RGPD pour les traitements à risque élevé.

3.4 Communiquer au Prestataire toute instruction relative aux traitements de manière documentée et conforme au RGPD.

3.5 Informer sans délai le Prestataire de toute évolution susceptible d'affecter le traitement (modification des finalités, changement de base légale, élargissement des catégories de personnes ou de données, etc.).

ARTICLE 4 — MESURES TECHNIQUES ET ORGANISATIONNELLES

Le Prestataire met en œuvre des mesures techniques et organisationnelles appropriées au sens de l'article 32 du RGPD, adaptées à la nature de chaque Solution et aux risques du traitement, notamment :

- Accès aux données limités aux personnes qui en ont besoin, au moyen de comptes nominatifs, et retirés en fin de mission ;
- Chiffrement des données en transit (HTTPS / TLS) ;
- Hébergement auprès des fournisseurs listés en Annexe 1, dans l'EEE sauf indication contraire au Document de commande ;
- Sauvegardes régulières des données hébergées par le Prestataire ;
- Application des mises à jour de sécurité dans des délais raisonnables ;
- Engagement de confidentialité des personnes autorisées à traiter les données.

Le Client reconnaît que ces mesures, considérées comme appropriées au regard de la nature du traitement et des risques pour les personnes concernées, peuvent évoluer dans le temps pour rester conformes à l'état de l'art, sans diminution du niveau global de sécurité.

ARTICLE 5 — SOUS-TRAITANCE EN CASCADE

5.1. Le Client autorise le Prestataire à recourir à des sous-traitants ultérieurs pour l'exécution du traitement, sous réserve du respect des conditions prévues à l'article 28-2 et 28-4 du RGPD.

5.2. La liste des sous-traitants ultérieurs actuels figure en Annexe 1 du présent DPA. Cette liste pourra être mise à jour par le Prestataire ; toute modification (ajout ou remplacement) est portée à la connaissance du Client, par e-mail ou par la mise à jour de la liste publiée à l'adresse https://www.youai.fr/dpa, au moins quinze (15) jours avant son entrée en vigueur.

5.3. Le Client dispose d'un délai de quinze (15) jours à compter de la notification pour s'opposer pour motif légitime à l'ajout d'un nouveau sous-traitant. En cas d'opposition légitime que les Parties ne parviennent pas à résoudre, le Client pourra résilier le Contrat Principal pour la partie concernée par le traitement, sans indemnité.

5.4. Le Prestataire conclut avec chaque sous-traitant ultérieur un contrat lui imposant des obligations de protection des données équivalentes à celles du présent DPA, et reste pleinement responsable vis-à-vis du Client de l'exécution par ledit sous-traitant ultérieur de ses obligations.

5.5. Nouveaux fournisseurs d'intelligence artificielle — Le recours à un nouveau fournisseur d'intelligence artificielle établi dans l'EEE, ou dans un pays bénéficiant d'une décision d'adéquation de la Commission européenne (y compris les entités certifiées EU-US Data Privacy Framework), suit la procédure de l'article 5.2. Le recours à un fournisseur établi dans un pays ne bénéficiant pas d'une décision d'adéquation requiert une mention expresse au Document de commande ou l'accord écrit préalable du Client.

ARTICLE 6 — TRANSFERTS HORS UE

6.1. Les transferts de données personnelles vers un pays tiers à l'Espace Économique Européen sont limités à ceux qui résultent du recours aux sous-traitants ultérieurs listés en Annexe 1 ou au Document de commande, que le Client autorise par l'acceptation du présent DPA. Aucun autre transfert n'est effectué sans instruction documentée du Client.

6.2. Tout transfert hors EEE est encadré par les garanties appropriées prévues aux articles 44 et suivants du RGPD : décision d'adéquation (notamment EU-US Data Privacy Framework pour les sous-traitants certifiés) ou Clauses Contractuelles Types de la Commission européenne.

ARTICLE 7 — AUDIT

7.1. Le Client peut, à ses frais et au maximum une (1) fois par an, demander au Prestataire de démontrer le respect du présent DPA, par la fourniture de documentation pertinente (politique de sécurité, certifications, rapports d'audit externes, registre des traitements) ou par la réalisation d'un audit sur site. Le temps consacré par le Prestataire à un audit sur site est facturé au Client au tarif en vigueur.

7.2. Tout audit sur site est planifié avec un préavis minimum de trente (30) jours et conduit pendant les heures ouvrées, de manière à minimiser l'impact sur l'activité du Prestataire. Le Client peut se faire assister d'un auditeur tiers indépendant soumis à un engagement de confidentialité équivalent à celui du présent DPA.

7.3. Les éventuelles non-conformités constatées font l'objet d'un plan d'action concerté entre les Parties dans un délai raisonnable.

ARTICLE 8 — RESPONSABILITÉ ET RÉPARATION

8.1. Chaque Partie reste responsable du respect de ses propres obligations au titre du RGPD.

8.2. La responsabilité du Prestataire au titre du présent DPA est encadrée et limitée dans les conditions prévues au Contrat Principal, sous réserve des dispositions impératives de l'article 82 du RGPD.

8.3. En cas de violation par le Prestataire de ses obligations spécifiques au RGPD entraînant une condamnation du Client par une autorité de contrôle (CNIL ou équivalent européen), le Prestataire indemnisera le Client à hauteur de la part imputable à sa faute, dans la limite des plafonds prévus au Contrat Principal.

ARTICLE 9 — FIN DU TRAITEMENT — RESTITUTION OU DESTRUCTION

9.1. À l'issue de la prestation, et selon l'instruction écrite du Client, le Prestataire procède :

- Soit à la **restitution** des données personnelles au Client, dans un format standard exploitable (CSV, JSON, export SQL, archive, dépôt Git, etc.), dans un délai maximum de **quinze (15) jours ouvrés** à compter de la demande, conformément à l'Article 22.1 des CGP ;
- Soit à la **destruction** définitive et sécurisée des données personnelles dans les systèmes du Prestataire et de ses sous-traitants ultérieurs, dans un délai maximum de **quinze (15) jours ouvrés** à compter de l'instruction.

9.2. À défaut d'instruction du Client dans un délai de quatre-vingt-dix (90) jours suivant la fin du Contrat Principal, le Prestataire procédera à la destruction des données, sauf obligation légale de conservation.

9.3. Sur demande du Client, le Prestataire émettra une attestation de restitution ou de destruction.

9.4. Les données conservées par le Prestataire au titre d'une obligation légale (comptabilité, archivage légal) sont identifiées et conservées dans le respect strict du RGPD pour la seule durée légale.

ARTICLE 10 — DURÉE — RÉSILIATION

10.1. Le présent DPA prend effet à la date d'acceptation du Document de commande et demeure en vigueur tant que le Prestataire traite des données personnelles pour le compte du Client dans le cadre du Contrat Principal.

10.2. La résiliation du Contrat Principal entraîne de plein droit la résiliation du présent DPA, sous réserve de l'application des obligations de restitution / destruction prévues à l'article 9.

ARTICLE 11 — DISPOSITIONS GÉNÉRALES

11.1. **Loi applicable** — Le présent DPA est soumis au droit français et au droit de l'Union européenne.

11.2. **Juridiction** — Tout litige relatif à l'interprétation ou à l'exécution du présent DPA sera soumis à la compétence exclusive du Tribunal de Commerce de Saint-Étienne, sauf disposition d'ordre public contraire.

11.3. **Hiérarchie des documents** — En cas de contradiction entre le présent DPA et le Contrat Principal sur les questions de protection des données personnelles, le présent DPA prévaut.

11.4. **Modifications** — Toute modification du présent DPA fait l'objet d'un avenant écrit signé par les deux Parties. Le Prestataire peut toutefois mettre à jour unilatéralement la liste des sous-traitants ultérieurs (Annexe 1) dans les conditions de l'article 5.

11.5. **Convention de preuve électronique** — Les Parties conviennent que les e-mails échangés aux adresses de contact RGPD et les signatures électroniques au sens du Règlement (UE) n° 910/2014 (eIDAS) constituent des écrits opposables.

ANNEXE 1 — LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Le Prestataire est susceptible de recourir aux sous-traitants ultérieurs suivants. Seuls ceux nécessaires à la Solution concernée sont effectivement mobilisés pour un projet ; ils sont indiqués au Document de commande ou communiqués au Client sur simple demande.

Sous-traitant	Localisation des données	Service rendu	Garanties
Hostinger International Ltd	Région EEE (datacenters UE)	Hébergement principal des Solutions (serveurs, stockage, logs)	ISO 27001, DPA, Clauses Contractuelles Types
Vercel Inc.	EEE / États-Unis	Hébergement d'applications web	DPA, CCT
Supabase Inc.	EEE / États-Unis	Base de données et authentification	DPA, CCT
Amazon Web Services EMEA SARL	Région EEE	Hébergement cloud, stockage, calcul	ISO 27001, SOC 2, DPA, CCT
Google Cloud EMEA Ltd	Région EEE	Services cloud (hébergement, stockage)	ISO 27001, SOC 2, DPA, CCT
Microsoft Ireland Operations Ltd	Région EEE	Azure, Azure OpenAI, Microsoft 365	ISO 27001, SOC 2, DPA, CCT
OpenAI Ireland Ltd	EEE / États-Unis	API d'intelligence artificielle (modèles GPT, transcription)	DPA, EU-US Data Privacy Framework, CCT
Anthropic Ireland Ltd	EEE / États-Unis	API d'intelligence artificielle (modèles Claude)	DPA, EU-US Data Privacy Framework, CCT
Google Ireland Ltd (Gemini / Vertex AI)	EEE / États-Unis	API d'intelligence artificielle (modèles Gemini)	DPA, EU-US Data Privacy Framework, CCT
Mistral AI SAS	Région EEE (France)	API d'intelligence artificielle (modèles Mistral)	Hébergement UE, DPA

Recall.ai Inc.	EEE / États-Unis	Bot d'enregistrement et de transcription de réunions	DPA, CCT
Stripe Payments Europe Ltd	Région EEE (Irlande)	Paiement et prélèvement des abonnements	PCI-DSS niveau 1, DPA, CCT

Toute modification de cette liste est notifiée au Client conformément à l'article 5 du DPA. Le recours à un fournisseur établi dans un pays ne bénéficiant pas d'une décision d'adéquation n'est possible que dans les conditions de l'article 5.5.

ANNEXE 2 — RECOMMANDATIONS DE SÉCURITÉ CÔTÉ CLIENT

Pour permettre au Prestataire d'assurer un haut niveau de protection des données, le Client est invité à :

- Veiller à la sécurité des accès délivrés à ses propres collaborateurs (MFA, gestion des départs) ;
- Notifier sans délai au Prestataire tout incident de sécurité côté Client susceptible d'affecter le traitement ;
- Coopérer avec le Prestataire sur les évolutions de sécurité recommandées ;
- Tenir à jour ses propres registres et politiques RGPD.

SIGNATURES

Le présent DPA standard n'est pas signé séparément : il est accepté par la signature ou l'acceptation électronique du Document de commande y faisant référence, qui l'incorpore. Les Parties conviennent que la signature apposée sur le présent document au format PDF — signature électronique simple ou image de signature manuscrite — vaut signature originale et fait pleinement preuve entre elles, conformément aux articles 1366 et 1367 du Code civil et au Règlement (UE) n° 910/2014 (eIDAS). Chaque Partie reçoit une copie électronique du document signé, valant exemplaire.

Pour le Responsable de Traitement (Client)	**Pour le Sous-Traitant — YOUAI**
Nom : le signataire du Document de commande	Nom : Joris Pellegrin
Qualité : voir Document de commande	Qualité : Cogérant
Date :	Date :
Signature, précédée de la mention « Bon pour accord » :	**Signature, précédée de la mention « Bon pour accord » :**
