ACCORD DE TRAITEMENT DES DONNÉES (DPA)

Le présent Accord de traitement des données (« **DPA** ») est conclu entre (a) Hexagone AI, SAS immatriculée sous le numéro 989 062 849 au R.C.S. de Nanterre, dont le siège social est situé 32 Rue De Paris, 92100 Boulogne-Billancourt (le « **Sous-traitant** »), et (b) l'entité ayant accepté les Conditions Générales d'Hexagone AI faisant référence au présent DPA, agissant en qualité de responsable de traitement des données personnelles (le « **Client** »).

Le présent DPA définit les modalités applicables aux activités de traitement réalisées par le Sous-traitant pour le compte du Client, conformément aux instructions de ce dernier, dans le cadre des services mis à disposition du Client par le Sous-traitant (les « **Services** ») en vertu des Conditions Générales et de tout bon de commande entre les Parties (ensemble le « **Contrat** »). Le Client et le Sous-traitant sont désignés individuellement comme une « **Partie** » et collectivement comme les « **Parties** ». Dans le cadre du présent DPA, les termes « **responsable du traitement** », « **personne concernée** », « **données personnelles** », « **violation de données personnelles** », « **traitement** », « **sous-traitant** », « pseudonymisation » et « **autorité de contrôle** » ont la même signification que dans le Règlement général sur la protection des données (UE) 2016/679 (« **RGPD** »).

1. Traitement des données personnelles.

1.1. Obligations du Sous-traitant. Le Sous-traitant s'engage à:

1.1.1. traiter les données personnelles en conformité avec le RGPD et notamment, opérer ce traitement pour les seules finalités prévues aux présentes et conformément aux instructions du Client documentées dans le Contrat et le présent DPA, ainsi que pour répondre à toute obligation légale ou réglementaire, auquel cas le Sous-traitant en informe préalablement le Client sauf si cette information lui est interdite;

1.1.2. assister le Client, le cas échéant, pour la réalisation d'analyses d'impact relatives à la protection des données et pour la consultation préalable de l'autorité de contrôle compétente.

1.2. Obligations du Client. Le Client :

1.2.1. donne instruction au Sous-traitant de traiter les données personnelles et de donner instruction à chacun de ses sous-traitants ultérieurs de traiter ces données, dans les conditions définies aux présentes et dans la limite des besoins nécessaires à l'exécution du Contrat;

1.2.2. garantit qu'il dispose de tous les droits nécessaires concernant les données personnelles et qu'il a fourni aux personnes concernées les informations requises au moment de la collecte de leurs données.

1.3. Chaîne de Sous-traitance. Dans le cas où le Client intervient lui-même en tant que sous-traitant d'un responsable de traitement tiers, le Client garantit que ce dernier a autorisé les instructions documentées dans le Contrat et le présent DPA, la désignation du Sous-traitant en tant que sous-traitant ultérieur, ainsi que la désignation par le Sous-traitant de ses propres sous-traitants ultérieurs dans les conditions de l'Article 4. Le Client s'engage à transmettre sans délai au responsable de traitement concerné toute notification reçue du Sous-traitant relative à une violation de données dans les conditions de l'Article 6, ou à un changement de sous-traitant ultérieur dans les conditions de l'Article 4.2, ainsi que toute information mise à sa disposition en matière de sécurité ou de transferts. Le Client répercute ses obligations au titre du présent DPA au responsable de traitement tiers.

1.4. Les détails concernant les catégories de données personnelles faisant l'objet du traitement par le Sous-traitant, conformément à l'article 28(3) du RGPD, sont fournis en Annexe 1 des présentes**.**

2. Personnel du Sous-traitant. Le Sous-traitant s'engage à limiter l'accès aux données personnelles aux seules personnes (a) ayant besoin d'en connaître ou d'y accéder aux fins de la fourniture des Services ou du respect de la législation applicable, et (b) soumises à des obligations contractuelles, professionnelles ou légales de confidentialité.

3. **Mesures de sécurité techniques et organisationnelles**. Le Sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles appropriées décrites en Annexe 3 des présentes, et à les adapter aux risques du traitement, en tenant compte de l'état de l'art, des coûts de mise en œuvre, des risques de violation des données personnelles dans le contexte du traitement, ainsi que des catégories de données personnelles concernées, de l'étendue du traitement, de son contexte et de ses finalités, et du niveau et de la probabilité de risque pour les droits et libertés des personnes concernées.

4. Sous-traitants ultérieurs

4.1. Le Client autorise le Sous-traitant à désigner les sous-traitants ultérieurs dont la liste à la date du DPA figure en Annexe 2, ainsi que tout nouveau sous-traitant ultérieur désigné postérieurement au DPA.

4.2. Le Sous-traitant notifie au Client la désignation de tout nouveau sous-traitant ultérieur et les principaux détails du traitement concerné, trente (30) jours avant le commencement de la sous-traitance. Le Client dispose de dix (10) jours à compter de cette notification pour s'opposer, pour motif légitime, à la désignation du nouveau sous-traitant ultérieur. Si cette opposition rend impossible la fourniture des Services dans les conditions prévues au Contrat, le Client peut résilier le Contrat sur notification au Sous-traitant. Le Sous-traitant cesse alors de fournir les Services concernés dans un délai de trente (30) jours à compter de la notification de résiliation.

4.3. Concernant chaque sous-traitant ultérieur, le Sous-traitant s'engage à (a) mettre en place un contrat écrit offrant un niveau de protection au moins équivalent à celui prévu par le présent DPA et répondant aux exigences de l'article 28(3) du RGPD, et (b) s'assurer que ce contrat intègre les clauses contractuelles types ou tout autre mécanisme de transfert transfrontalier juridiquement valable, le cas échéant.

5. Droits des personnes concernées

5.1. Le Sous-traitant s'engage à assister dans la mesure du possible le Client dans le traitement des demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, opposition, limitation, portabilité, droit de ne pas faire l'objet d'une décision individuelle automatisée y compris le profilage).

5.2. Lorsqu'une personne concernée exerce une demande directement auprès du Sous-traitant, celui-ci la transmet dès réception au Client.

6. Violation de données personnelles

6.1. En cas de violation de données personnelles, le Sous-traitant notifie le Client dans les quarante-huit (48) heures et lui fournit toute documentation utile à l'accomplissement de ses obligations de notification à l'autorité de contrôle ou d'information aux personnes concernées le cas échéant. Les Parties s'engagent à coopérer de manière raisonnable et le Sous-traitant tient le Client informé de toute enquête interne et des mesures prises pour remédier à la violation.

6.2. Sauf dans les cas prévus par le RGPD, le Sous-traitant s'engage à ne pas informer les personnes concernées par la violation sans le consentement écrit préalable du Client.

7. Restitution ou suppression des données

7.1. Dans les conditions prévues au Contrat, le Sous-traitant restitue au Client ou supprime, dans les meilleurs délais, les données personnelles pouvant être raisonnablement identifiées et extraites par le Sous-traitant, au plus tard à la cessation du Contrat ou du traitement, sous réserve de l'exception ci-dessous.

7.2. Par exception à ce qui précède, un sous-traitant ultérieur peut continuer à traiter les données personnelles dans les conditions prévues par le RGPD, sous réserve du respect de ses engagements de confidentialité et dans la limite des finalités autorisées par le RGPD.

7.3. Le Sous-traitant fournit au Client, sur demande écrite, une attestation écrite confirmant sa conformité au présent Article.

8. **Droit d'audit**. Le Sous-traitant s'engage à démontrer au Client la mise en place des mesures techniques et organisationnelles appropriées pendant la durée du Contrat. Le Client peut exercer son droit d'audit directement ou par l'intermédiaire d'un tiers autorisé par le Sous-traitant et sous réserve que ce tiers soit soumis à des obligations de confidentialité au moins équivalentes à celles

du Client au titre du Contrat, et que le Client demeure responsable des actes de ce tiers. Le droit d'audit s'exerce au moins une fois par an, sous réserve du respect d'un préavis raisonnable, et est limité à l'examen d'un dossier de diligence raisonnable comprenant : les pratiques du Sous-traitant en matière de sécurité de l'information et de gestion des risques, les résultats d'audits éventuels et un accès raisonnable à du personnel compétent pour discuter des contrôles en place. Toute assistance ou information complémentaire à celles décrites ci-dessus fait l'objet d'un plan d'audit séparé entre les Parties, précisant le périmètre, la durée, les honoraires et le calendrier de cet audit complémentaire. Le Client s'interdit, pour lui-même et tout salarié et représentant, tout accès aux systèmes, serveurs, réseaux, journaux ou données susceptibles de compromettre les données personnelles d'autres clients du Sous-traitant.

9. Transferts internationaux de données

9.1. Le Client autorise le Sous-traitant à faire traiter les données personnelles par des sous-traitants ultérieurs situés dans une région géographique différente de celle du traitement initial.

9.2. Dans le cadre de ces transferts, le Sous-traitant s'engage à n'effectuer de transferts transfrontaliers de données personnelles que vers des pays assurant une protection adéquate ou sur la base d'un mécanisme de transfert transfrontalier valable (clauses contractuelles types de la Commission européenne, ou tout autre mécanisme équivalent applicable).

10. Stipulations générales

10.1. Le présent DPA est régi par le droit applicable prévu au Contrat.

10.2. En cas de conflit entre les stipulations du présent DPA et celles du Contrat, les stipulations du présent DPA prévalent en ce qui concerne le traitement des données personnelles.

10.3. Le Sous-traitant peut apporter des modifications ponctuelles au présent DPA, dont seule la version en ligne sur le site Internet du Sous-traitant fait foi. Toute modification substantielle du présent DPA fait l'objet d'une notification par le Sous-traitant au Client, y-compris notamment au moyen d'une bannière sur le site Internet du Sous-traitant, trente (30) jours avant l'entrée en vigueur de la version modifiée. Le Client dispose de dix (10) jours à compter de cette notification pour s'opposer à la nouvelle version du DPA, auquel cas le Sous-traitant disposera d'un délai de trente (30) jours pour mettre fin au Contrat. Dans le cas où le Client continue à utiliser les Services après l'expiration du délai d'opposition, la nouvelle version du DPA sera présumée comme étant acceptée.

10.4. Le présent DPA est régi par les stipulations du Contrat, notamment en ce qui concerne les exclusions et limitations de responsabilité, sous réserve des dispositions du RGPD.

10.5. Si une stipulation du présent DPA est jugée invalide par une juridiction compétente, seule cette stipulation est affectée et les autres stipulations demeurent en vigueur.

10.6. Le présent DPA constitue l'intégralité de l'accord entre les Parties concernant le traitement des données personnelles, et prévaut sur tout accord antérieur entre les Parties ayant le même objet, y compris tout contrat imposé par le Client au Sous-traitant le cas échéant.

Annexe 1 — Description du traitement

Nature et finalité du traitement: tout traitement de données permettant la fourniture du Service selon les instructions du Client, y-compris notamment: utilisation par le Client des documents pseudonymisés par le biais de l'application de bureau Hexagone AI, dans des services d'IA tiers via l'intégration native Azure OpenAI; utilisation des fonctionnalités de Hexagone AI permettant d'entrer du texte libre telles que "Synchronisation", "Chat"; feedback et commentaires du Client; prévention et détection de bugs (troubleshooting) à des fins de sécurisation du Service.

Catégories de personnes concernées : utilisateurs autorisés à utiliser le service par le Client (tels que employés, intérimaires, stagiaires, consultants externes), toutes personnes physiques dont les données sont traitées directement par le Client (ou le responsable de traitement pour lequel le Client intervient en qualité de sous-traitant le cas échéant) lorsqu'il utilise le Service, y-compris notamment, sans que cette liste soit limitative: les contacts marketing, prospects, clients.

Catégories de données : toutes données personnelles transmises par le Client à Hexagone IA, telles que noms, adresses, adresses email, numéros de téléphone, identifiants internes, identifiants pseudonymisés, photos.

Données sensibles : aucune catégorie particulière de données personnelles n'est nécessaire pour utiliser le Service. Le Client s'empêche expressément de fournir toutes données sensibles au Sous-traitant.

Les données personnelles contenues dans les documents du Client soumis à l'application de bureau de Hexagone AI sont traités exclusivement en local sur l'appareil du Client et sous la seule responsabilité du Client. Hexagone AI n'a aucun accès à ces données et ne les traite en aucune manière, y-compris pour l'entraînement de ses propres modèles d'IA.

Contact protection des données du Sous-traitant : Romain Boudet, rb@hexagone.ai.

Annexe 2 — Liste des sous-traitants ultérieurs

À la date du présent DPA, le Sous-traitant recourt aux sous-traitants ultérieurs suivants :

Sous-traitant ultérieur	Service fourni	Localisation du sous-traitant	Mécanisme de transfert applicable
Microsoft Ireland Operations Limited, Irlande (UE)	Fourniture d'Azure OpenAI (option AI Chat)	Irlande (UE)	N/A
Vercel Inc.	Hébergement du site Internet (journaux techniques de requêtes à des fins de sécurité)	États-Unis	Data Privacy Framework, CCT
Resend	Envoi des e-mails transactionnels et des communications produit	États-Unis	Data Privacy Framework, CCT
Stripe Payments Europe, Limited, Irlande (UE)	Traitement des paiements et de la facturation des abonnements Pro	Irlande (UE)	N/A
PostHog Inc., États-Unis	Collecte de la télémétrie agrégée (compteurs anonymes uniquement ; aucun contenu ni adresse IP)	États-Unis	Data Privacy Framework, CCT

Annexe 3 — Mesures techniques et organisationnelles de sécurité

Le Sous-traitant met en œuvre, a minima, les mesures suivantes, adaptées au risque du traitement concerné:

Domaine / Mesures

Gouvernance de la sécurité: Politique de sécurité de l'information révisée périodiquement, diffusée à l'ensemble du personnel; fonction dédiée à la sécurité et à la conformité.

Gestion du personnel: engagement contractuel de confidentialité, sensibilisation et formation à la protection des données, suppression des accès en cas de départ, principe du moindre privilège.

Contrôle d'accès: Authentification par identifiant unique et mot de passe complexe (ou authentification renforcée pour les accès privilégiés), politique de mots de passe, verrouillage en cas d'inactivité ou de tentatives infructueuses, accès restreint et journalisé aux infrastructures.

Sécurité applicative et réseau: chiffrement des données en transit (TLS) de toutes les communications entre l'Application et le backend, architecture « local-first », séparation stricte des environnements de production.