

Accord sur le Traitement des Données (DPA)

Date d'entrée en vigueur : 01/01/2026

Le présent Accord sur le Traitement des Données (ci-après le « DPA ») fait partie intégrante des Conditions Générales d'Utilisation (les « CGU ») du service MedCopilot.

Il définit les obligations respectives des parties concernant le traitement des données à caractère personnel, conformément au Règlement (UE) 2016/679 (le « RGPD »). En souscrivant au service MedCopilot et en acceptant les CGU, le Client accepte expressément et sans réserve les termes du présent DPA.

LES PARTIES :

- **Le Responsable de Traitement** : Tout professionnel de santé, cabinet ou établissement souscrivant aux services de MedCopilot et agissant en tant que Responsable de Traitement au sens du RGPD (ci-après le « Client » ou le « Responsable de Traitement »).
- **Le Sous-traitant** : Oscar & Caroline, société par actions simplifiée au capital de 133 992 euros, immatriculée au RCS de Versailles sous le numéro 942 141 995, dont le siège social est situé au 1 avenue du Belvédère 78100 Saint-Germain-en-Laye, éditeur de la solution MedCopilot, agissant en tant que Sous-traitant au sens du RGPD (ci-après le « Sous-traitant » ou « MedCopilot »).

Préambule

Dans le cadre de la fourniture du Service (tel que défini dans les CGU), le Sous-traitant est amené à traiter des Données à Caractère Personnel, et notamment des Données de Santé, pour le compte et sur instruction du Responsable de Traitement. Le présent Accord a pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer les opérations de traitement de Données à Caractère Personnel définies ci-après..

Article 1 : Objet de l'accord

Le présent Accord régit le traitement des Données à Caractère Personnel (telles que définies en Annexe 1) confiées par le Responsable de Traitement au Sous-traitant pour l'exécution du Service.

Article 2 : Description du traitement

Le Sous-traitant est autorisé à traiter pour le compte du Responsable de Traitement les Données à Caractère Personnel nécessaires pour fournir le Service. Les détails de ce traitement (finalités, types de données, personnes concernées, durée) sont décrits en Annexe 1 du présent Accord.

Article 3 : Obligations du sous-traitant (MedCopilot)

Le Sous-traitant s'engage à :

3.1. Instructions du responsable de traitement

Traiter les Données à Caractère Personnel uniquement pour les finalités décrites en Annexe 1 et conformément aux instructions documentées du Responsable de Traitement. Les CGU et l'utilisation du Service par le Responsable de Traitement constituent les instructions documentées.

3.2. Confidentialité

Veiller à ce que les personnes autorisées à traiter les Données à Caractère Personnel soient soumises à une obligation légale ou contractuelle de confidentialité. Le Sous-traitant applique une politique de « Eyes-Off » : aucune personne physique de l'équipe MedCopilot ni de son partenaire technique de développement (Coreoz) n'est autorisée à accéder au contenu des données de santé (matière clinique, audio ou synthèses). Le Sous-traitant garantit qu'aucune réécoute humaine des flux audio ni aucune relecture humaine des transcriptions n'est effectuée, que ce soit par MedCopilot ou ses sous-traitants ultérieurs, sauf demande expresse, ponctuelle et documentée du Responsable de Traitement pour des besoins exclusifs de support technique.

3.3. Sécurité des données (Art. 32 RGPD)

Mettre en œuvre toutes les mesures techniques et organisationnelles (les « TOMs ») appropriées pour garantir un niveau de sécurité adapté au risque, telles que décrites en Annexe 2 du présent Accord. Cela inclut notamment l'hébergement des Données de Santé sur une infrastructure certifiée Hébergeur de Données de Santé (HDS) en France.

3.4. Sous-traitance ultérieure (Art. 28.2 et 28.4 RGPD)

Ne pas engager de sous-traitant ultérieur sans l'autorisation écrite, spécifique ou générale, préalable du Responsable de Traitement.

En signant le présent Accord, le Responsable de Traitement donne une autorisation générale pour l'engagement des sous-traitants ultérieurs listés en Annexe 3.

Le Sous-traitant s'engage à informer le Responsable de Traitement de tout ajout ou remplacement de sous-traitant ultérieur par écrit (ex: email) au moins trente (30) jours à l'avance, donnant ainsi au Responsable de Traitement la possibilité d'émettre des objections.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

3.5. Exercice des droits des personnes concernées (Patients)

Aider le Responsable de Traitement, dans la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Note importante : Les Parties reconnaissent que la politique de suppression automatique et définitive des Données de Santé après **1 mois** (telle que décrite en Annexe 1) rendra impossible l'exercice de ces droits (accès, rectification, portabilité) via l'interface MedCopilot au-delà de ce délai. Le Responsable de Traitement gérera ces demandes via son propre système (DPI).

3.6. Assistance au responsable de traitement

Aider le Responsable de Traitement à garantir le respect de ses obligations au titre des Articles 32 à 36 du RGPD (Sécurité, Notification de violation, AIPD), compte tenu de la nature du traitement et des informations à la disposition du Sous-traitant.

3.7. Notification des violations de données

Notifier au Responsable de Traitement toute violation de Données à Caractère Personnel sans retard injustifié et au plus tard quarante-huit (48) heures après en avoir pris connaissance.

3.8. Sort des données

Conformément à la mesure de minimisation décrite en Annexe 1, le Sous-traitant supprime automatiquement et définitivement toutes les Données de Santé 1 mois après leur génération. **Le Responsable de Traitement reconnaît qu'il lui appartient d'extraire et de sauvegarder les synthèses dans son propre système (DPI) avant l'expiration de ce délai. Passé ce délai, le Sous-traitant sera dans l'incapacité technique de restaurer lesdites données.**

3.9. Audit

Le droit d'audit s'exerce prioritairement par la communication de rapports récents (Certifications HDS, SOC2 ou synthèses de pentests). Un audit sur site ne pourra être envisagé qu'en cas de violation de données avérée.

3.10 Non-entraînement des modèles

Le Sous-traitant s'engage formellement à ce que les Données à Caractère Personnel traitées pour le compte du Client ne soient en aucun cas utilisées par MedCopilot, ni par ses sous-traitants ultérieurs (notamment Google Cloud), pour l'entraînement, l'amélioration ou le « fine-tuning » de modèles d'intelligence artificielle.

3.11 Point de contact RGPD

Pour toute question relative à l'exécution du présent Accord ou en cas d'alerte sécurité, le point de contact privilégié du Sous-traitant est joignable à l'adresse électronique suivante : dpo@medcopilot.fr

Article 4 : Obligations du responsable de traitement (Le client)

Le Responsable de Traitement s'engage à :

4.1. Licéité du traitement

Garantir qu'il dispose de la base légale appropriée (notamment l'Article 9.2.h du RGPD) pour collecter et traiter les Données de Santé de ses patients via le Service.

4.2. Information des personnes concernées

Assumer son obligation d'information (Articles 13 et 14 du RGPD) envers ses patients concernant l'utilisation du Service MedCopilot pour le traitement de leurs données.

4.3. Validation clinique

Reconnaître que MedCopilot est un outil d'aide à la rédaction (Non-Dispositif Médical) et que le Responsable de Traitement conserve l'entière responsabilité de la validation clinique finale de l'exactitude et de la pertinence de toute synthèse générée avant son utilisation.

4.4. Instructions

Fournir au Sous-traitant des instructions licites et documentées (via l'utilisation du Service).

4.5 Limites de l'IA

Reconnaître être informé que les technologies d'IA peuvent générer des résultats inexacts ou biaisés (phénomène dit d'hallucination), même si MedCopilot travaille activement à leur minimisation. Il incombe au Client de vérifier systématiquement chaque synthèse générée.

Article 5 : Entrée en vigueur et droit applicable

Le présent Accord entre en vigueur à la date de souscription au Service par le Responsable de Traitement et reste en vigueur pour la durée des CGU. L'Accord est régi par le droit français. Tout litige sera de la compétence exclusive des tribunaux de Versailles (France).

Annexe 1 : Description du traitement

Objet du traitement : Fourniture du service d'assistance à la rédaction de synthèses et de courriers médicaux par IA (MedCopilot).

Nature des opérations : Collecte de matière clinique, transcription de dictée vocale (traitement en flux sans stockage persistant de l'audio), analyse par IA, génération de synthèse, stockage temporaire sécurisé (HDS), et suppression automatisée.

Finalité(s) : Aider le professionnel de santé (Responsable de Traitement) à structurer l'information et à générer des projets de synthèses cliniques.

Durée du traitement : La durée du contrat (CGU). Toutefois, la durée de traitement et de conservation de tout jeu de Données de Santé est strictement limitée à **1 mois** à compter de sa génération, après quoi il est définitivement supprimé.

Données statistiques d'usage : Le Sous-traitant peut traiter des données statistiques d'utilisation (métadonnées, temps de réponse, fréquence d'usage) à des fins d'amélioration du service, sous réserve que ces données soient strictement anonymisées et ne permettent aucune réidentification des patients ou des praticiens.

Types de données à caractère personnel traitées :

- Données d'état civil du patient : Nom, prénom (tels que présents dans les documents).
- Données de Santé (Article 9 RGPD) : Toute donnée de santé contenue dans la matière clinique importée (PDF, images, textes) ou dictée (transcriptions) par le Responsable de Traitement (ex: diagnostics, antécédents, traitements, comptes-rendus, notes).

Catégories de personnes concernées : Les patients du Responsable de Traitement.

Annexe 2 : Mesures techniques et organisationnelles de sécurité (TOMs)

Le Sous-traitant met en œuvre les mesures de sécurité suivantes :

Hébergement : Infrastructure certifiée Hébergeur de Données de Santé (HDS), située exclusivement en France

Chiffrement :

- En transit : Chiffrement systématique de tous les flux par TLS 1.2 ou supérieur.
- Au repos : Chiffrement des bases de données et des espaces de stockage (ex: AES-256).

Contrôle d'accès :

- Authentification forte (2FA) obligatoire pour les utilisateurs.
- Politique de mots de passe robustes. (8 caractères minimums avec majuscule, minuscule, chiffre, caractères spéciaux)
- Accès administrateur (personnel MedCopilot/Coreoz) restreint et traqué.

Minimisation (Mesure de sécurité principale) :

- Suppression automatique et définitive de toutes les Données de Santé (imports, transcriptions, synthèses) après **1 mois**.
- Audio non stocké : Les flux audio de la dictée vocale sont transcrits en temps réel et immédiatement supprimés (seul le texte est traité).

Sécurité applicative : Pare-feu applicatif (WAF),

Traçabilité : Journalisation des accès (logs) et des actions sur la plateforme, conservés 1 an.

Annexe 3 : Liste des sous-traitants ultérieurs autorisés

Le Responsable de Traitement est informé et autorise le Sous-traitant à faire appel aux sous-traitants ultérieurs suivants :

Sous-traitant ultérieur	Finalité	Pays
Coreoz	Développement, maintenance applicative et support technique	France
Google Cloud (GCP)	Fourniture des modèles d'IA (Vertex AI / Gemini)	France / Europe
Claranet	Maintenance et support de l'infrastructure HDS	France
PayZen (Lyra Group)	Gestion sécurisée des paiements et abonnements (Données bancaires uniquement)	France

Encadrement des transferts hors-UE : L'hébergement des données est situé exclusivement en France. Dans le cas où des accès techniques de maintenance ou de support par les sous-traitants ultérieurs (notamment Google Cloud) impliqueraient un flux hors-UE, ces

transferts sont strictement encadrés par les Clauses Contractuelles Types (CCT) de la Commission Européenne et le Data Privacy Framework (DPF) UE-USA, garantissant un niveau de protection pleinement conforme au RGPD.

Annexe 4 : Modèle d'information des personnes concernées (Patients)

Conformément à l'**Article 4.2** du présent Accord, le Responsable de Traitement (le Praticien) doit informer ses patients de l'utilisation du Service. Le Sous-traitant met à disposition le modèle suivant, que le Responsable de Traitement peut utiliser pour remplir son obligation d'information (affichage en cabinet, mention sur le site de prise de rendez-vous ou note d'information).

Note au Responsable de Traitement : *Ce modèle est fourni à titre indicatif. Il vous appartient de l'adapter selon vos propres modalités d'exercice.*

MODÈLE D'INFORMATION PATIENT (À COPIER-COLLER)

Information sur le traitement de vos données de santé Utilisation de l'assistant médical intelligent : MedCopilot

Chère patiente, cher patient,

Dans le cadre de votre prise en charge, votre praticien utilise la solution **MedCopilot**, un assistant de rédaction basé sur l'intelligence artificielle, afin de consacrer plus de temps à l'échange clinique et d'améliorer la précision de votre dossier médical.

1. Quelles données sont traitées ? L'outil aide le praticien à transcrire ses notes ou à synthétiser des documents médicaux (comptes-rendus, analyses, etc). Si une dictée vocale est utilisée, la voix est transformée en texte en temps réel : **aucun enregistrement audio n'est conservé par le service.**

2. Sécurité et Confidentialité

- **Hébergement HDS :** Vos informations sont traitées sur des serveurs sécurisés bénéficiant de la certification « Hébergeur de Données de Santé » (HDS), situés exclusivement en France.

- **Non-entraînement de l'IA :** Vos données de santé ne sont jamais utilisées pour entraîner ou améliorer les modèles d'intelligence artificielle. Elles restent votre propriété exclusive et celle de votre médecin.
- **Suppression automatique :** Par mesure de sécurité, toutes les données traitées par l'assistant sont **définitivement supprimées du service après un délai d'1 mois..** Seul le compte-rendu final validé par votre médecin est conservé dans votre dossier médical.

3. Vos Droits

Conformément au RGPD, vous disposez d'un droit d'accès, de rectification et d'effacement de vos données. Vous disposez également d'un **droit d'opposition** : vous pouvez demander à votre médecin, à tout moment et sans justification, de ne pas utiliser cet outil lors de votre consultation.

4. Responsabilité Médicale

Votre médecin reste votre seul interlocuteur. Il valide systématiquement chaque note générée par l'outil avant de l'intégrer à votre dossier. L'intelligence artificielle n'est ici qu'une aide à la rédaction et ne remplace en aucun cas le jugement de votre praticien.