

Politique de confidentialité

Introduction.....	2
Champ d'application.....	2
Rôles et responsabilités.....	2
Base légale du traitement.....	3
Types de données collectées.....	3
Comment nous utilisons vos données.....	4
Transferts internationaux.....	4
Conservation et suppression des données.....	5
Cookies et technologies de suivi.....	6
Sécurité des données.....	6
Dispositions spécifiques à l'extension Chrome MedCopilot.....	7
Utilisation limitée des données (Limited Use).....	7
Transparence sur les permissions demandées.....	7
Engagements stricts de MedCopilot.....	8
Vos droits selon la RGPD.....	8
Éditeur et Contact.....	8

Date d'entrée en vigueur : 01/01/2026

Introduction

Oscar & Caroline (« MedCopilot », « nous », « notre » ou « nos »), éditeur de la solution MedCopilot, s'engage à protéger les données personnelles des utilisateurs situés dans l'Union européenne (UE), conformément au Règlement général sur la protection des données (RGPD) (UE) 2016/679.

Cette politique de confidentialité explique comment nous collectons, utilisons, stockons et protégeons vos données personnelles, et expose vos droits en vertu du RGPD.

MedCopilot est un outil d'assistance à la documentation administrative et clinique. Il ne constitue pas un Dispositif Médical au sens du Règlement (UE) 2017/745. Les synthèses documentaires générées par l'IA ne sont jamais des diagnostics et doivent impérativement être relues, vérifiées et validées par le professionnel de santé, qui demeure seul responsable de la prise en charge du patient.

Champ d'application

Cette politique s'applique aux personnes situées dans l'UE qui utilisent la plateforme MedCopilot, y compris les professionnels de santé et les patients dont les données peuvent être traitées dans le cadre des services de MedCopilot.

Elle couvre notre rôle en tant que sous-traitant agissant pour le compte des professionnels de santé (qui demeurent les responsables du traitement pour les données de leurs patients), ainsi que notre rôle en tant que responsable du traitement pour nos propres besoins administratifs (gestion de vos comptes utilisateurs).

Rôles et responsabilités

MedCopilot en tant que Responsable du Traitement : MedCopilot (Oscar & Caroline) agit en tant que responsable du traitement pour les données administratives des

professionnels de santé (par exemple, la création de comptes utilisateurs, la facturation, la communication de support).

MedCopilot en tant que Sous-traitant : MedCopilot agit en tant que sous-traitant pour le compte des professionnels de santé (les responsables du traitement) lorsqu'elle traite les données de santé des patients (textes, documents PDF, images) que vous importez dans le service pour générer des synthèses.

Base légale du traitement

Nous traitons les données personnelles selon les bases légales suivantes :

- **Exécution d'un contrat (Art. 6.1.b du RGPD)** : Pour la création du compte, l'accès à la plateforme, la gestion des abonnements et la facturation du professionnel de santé.
- **Intérêt légitime (Art. 6.1.f du RGPD)** : Pour assurer la sécurité de notre plateforme (journaux de sécurité), fournir un support technique de qualité, et utiliser des cookies strictement nécessaires au fonctionnement de la session.
- **Données de Santé (Sous-traitance – Art. 9.2.h du RGPD)** : Dans le cadre de son rôle de sous-traitant, MedCopilot traite les données de santé des patients uniquement sur instructions documentées du professionnel de santé. Ce dernier garantit disposer de la base légale appropriée (liée aux soins de santé ou diagnostics médicaux) pour utiliser l'outil dans sa pratique.

Types de données collectées

Selon votre utilisation de MedCopilot, nous pouvons traiter :

- Données d'identité du professionnel (Utilisateur) : Noms, prénoms, email, numéro de téléphone, mot de passe hashé (soumis à une politique de robustesse de 8 caractères minimum comprenant majuscule, minuscule, chiffre et caractère spécial).
- Données cliniques (en tant que sous-traitant) :
 - Données de santé du patient (état civil, diagnostics, antécédents...) contenues dans les fichiers (PDF, Word, images) ou les textes que vous importez.

- Transcriptions textuelles de dictées vocales (issues de votre fonctionnalité "Réflexion personnelle").
- Données techniques : Adresse IP, type de navigateur, journaux d'utilisation et d'audit (logs).
- Données de support : Informations fournies volontairement à nos canaux d'assistance.

Nous ne collectons ni ne stockons aucun fichier audio. L'audio de votre dictée vocale est diffusé de manière sécurisée pour la transcription en temps réel et est immédiatement supprimé après traitement. Seul le texte transcrit est conservé temporairement.

Comment nous utilisons vos données

- Pour alimenter nos services de synthèse IA et de structuration documentaire (y compris transcrire vos dictées vocales et analyser la matière clinique).
- Pour offrir un support client et répondre aux questions des utilisateurs.
- Pour respecter nos obligations légales ou réglementaires (notamment la conformité HDS). Pour maintenir et améliorer la sécurité et les fonctionnalités de la plateforme.
- Pour remplir nos obligations contractuelles envers vous (gestion des comptes et de la facturation).

Conformément à notre positionnement Non-Dispositif Médical, nous garantissons contractuellement que les données de santé et les transcriptions ne sont jamais utilisées pour entraîner ou améliorer les modèles de nos fournisseurs d'IA. Vos données cliniques restent cloisonnées. Nous ne vendons ni ne partageons ces données à des fins de marketing ou de profilage. Aucune réécoute ou relecture humaine (par MedCopilot, Coreoz ou Google) n'est effectuée sur vos flux cliniques.

Transferts internationaux

Les données de santé (données actives et sauvegardes) sont hébergées physiquement en France. Toutefois, pour fournir nos services d'intelligence artificielle, nous faisons appel à un sous-traitant technologique (Google) disposant d'une société mère aux États-Unis. Bien que les données ne soient pas hébergées outre-atlantique, cette structure juridique peut impliquer un transfert technique, lequel est strictement encadré.

Nos garanties de protection :

- Localisation du traitement : Le traitement algorithmique est contractuellement configuré pour s'exécuter au sein de l'Union Européenne. L'infrastructure cible prioritairement la France, avec une bascule possible en Europe uniquement pour assurer la continuité de service selon la charge.
- Sécurité technique : Chiffrement systématique des données en transit et au repos.
- Encadrement juridique : Les transferts sont encadrés par les Clauses Contractuelles Types (CCT) de la Commission Européenne ainsi que par le Data Privacy Framework (DPF) UE-USA, garantissant un niveau de protection pleinement conforme au RGPD.

Liste des sous-traitants principaux :

- Hébergement & Infogérance HDS : Claranet (France) – Certifications HDS, ISO 27001 et ISO 27701.
- Développement & Maintenance technique : Coreoz (France) – Agence partenaire disposant d'accès strictement encadrés et soumis à confidentialité.
- Intelligence Artificielle (LLM) : Google Cloud Platform (Service Vertex AI / Modèle Gemini).

Conservation et suppression des données

Notre politique de conservation est un pilier de notre approche "Privacy by Design" :

- Données Cliniques (Patients et Réflexions) : Pour minimiser l'exposition des données sensibles, toutes les données (matière clinique importée, transcriptions textuelles de vos réflexions, ET synthèses générées) sont automatiquement et définitivement supprimées après 192 heures. Le DPI du professionnel de santé est le lieu de conservation pérenne.
- Données commerciales du Professionnel (Utilisateur) :
 - Données de compte : Conservées pendant la durée de la relation contractuelle, puis 5 ans (prescription légale).
 - Factures : Conservées 10 ans après la clôture de l'exercice comptable (obligation légale).

- Logs de connexion et d'audit : Conservés 1 an maximum (obligation de sécurité). Ces journaux techniques ne contiennent aucune donnée clinique relative aux patients.

Cookies et technologies de suivi

MedCopilot utilise uniquement des cookies "strictement nécessaires" (essentiels).

Ces cookies sont indispensables au fonctionnement de notre plateforme (ex: maintien de votre session de connexion, sécurisation de l'accès). Ils ne sont pas utilisés à des fins d'analyse d'audience, de publicité ou de performance.

- Base légale : Article 6(1)(f) du RGPD (Intérêts légitimes) car ils sont essentiels au service. Ils sont exemptés de recueil de consentement.

Vous pouvez gérer ou désactiver les cookies via les paramètres de votre navigateur, mais cela affectera les fonctionnalités de la plateforme (ex: incapacité à rester connecté).

Sécurité des données

Nous mettons en place des mesures techniques et organisationnelles robustes pour protéger les données personnelles, notamment :

- Certification HDS : Notre infrastructure principale est hébergée et infogérée par Claranet, prestataire certifié Hébergeur de Données de Santé (HDS) en France.
- Politique Eyes-Off étendue : Aucun membre du personnel de MedCopilot ou de son partenaire technique Coreoz n'a accès aux données cliniques, sauf demande expresse de support de votre part.
- Chiffrement de bout en bout : Flux chiffrés en transit (TLS 1.2 ou supérieur) et données chiffrées au repos (AES-256).
- Journaux d'audit : Traçabilité absolue des accès et des actions (logs).

Dispositions spécifiques à l'extension Chrome MedCopilot

La présente section complète nos engagements pour les utilisateurs de l'extension de navigateur MedCopilot, conformément aux politiques de données utilisateur du Chrome Web Store.

Utilisation limitée des données (Limited Use)

L'utilisation et le transfert par MedCopilot vers tout autre application des informations reçues des API Google respecteront la [Politique de données utilisateur du Chrome Web Store](<https://developer.chrome.com/docs/webstore/program-policies/limited-use>), y compris les exigences d'utilisation limitée.

Transparence sur les permissions demandées

L'extension utilise des permissions spécifiques pour assurer son fonctionnement technique :

- **activeTab & scripting** : Utilisées exclusivement pour permettre l'analyse et la capture d'écran du contenu de la page web active, uniquement suite à une action volontaire de l'utilisateur (clic sur l'outil).
- **sidePanel** : Utilisée pour afficher l'interface d'assistance MedCopilot de manière latérale, permettant à l'utilisateur de consulter ses outils d'aide à la décision tout en gardant son logiciel métier (DPI) visible.
- **tabs** : Utilisée pour assurer la communication fluide entre l'interface du panneau latéral et le site web médical ouvert, garantissant que l'assistance fournie correspond bien au contexte de l'onglet actif.
- **storage** : Utilisée pour sauvegarder localement vos préférences de configuration et les jetons d'authentification de session de manière sécurisée.
- **host_permissions (<all_urls>)** : Nécessaire pour permettre à MedCopilot de fonctionner sur la grande diversité de plateformes logicielles médicales (DPI) et de bases de données de santé utilisées par les professionnels, dont les domaines et sous-domaines peuvent varier.

Engagements stricts de MedCopilot

- **Pas de revente :** Aucune donnée collectée via l'extension n'est cédée, louée ou vendue à des tiers, à des courtiers de données ou à des réseaux publicitaires.
- **Pas de publicité :** Vos données et le contexte de votre navigation ne servent jamais à des fins de ciblage publicitaire ou de profilage commercial.
- **Pas d'entraînement de modèles IA :** Les informations lues ou traitées par l'extension ne sont jamais utilisées par MedCopilot ou ses partenaires tiers pour entraîner, améliorer ou affiner des modèles d'intelligence artificielle.
- **Utilisation strictement fonctionnelle :** L'accès aux données est techniquement limité aux seules fonctionnalités nécessaires à la fourniture et à l'exécution directe du service MedCopilot.

Vos droits selon la RGPD

- Pour vos données de Professionnel (Utilisateur) : En tant que résident de l'UE, vous disposez des droits suivants sur vos propres données de compte : accès, rectification, suppression, limitation du traitement, portabilité et opposition. Vous pouvez exercer ces droits via votre espace "Mon Compte" ou en contactant notre DPO.
- Pour les données de vos Patients : Vous êtes le Responsable de Traitement. Si un patient souhaite exercer ses droits (accès, suppression...), il doit s'adresser directement à vous. En raison de notre politique de suppression automatique sous 192h, MedCopilot ne détiendra aucune donnée patient ou réflexion transcrite au-delà de ce délai.

Nous nous engageons à résoudre toute préoccupation ou plainte de manière transparente et rapide. Si vous estimez que vos droits n'ont pas été respectés, vous pouvez introduire une réclamation auprès de la CNIL.

Éditeur et Contact

MedCopilot est un service édité par Oscar & Caroline, société par actions simplifiée (SAS) au capital de 133 992 euros située au 1 avenue du Belvedere 78100

Saint-Germain-en-Laye, France et immatriculée au RCS de Versailles sous le numéro 942 141 995.

Pour toute question relative à cette politique ou pour contacter notre Délégué à la Protection des Données (DPO), veuillez écrire à : **dpo@medcopilot.fr**