

POLITIQUE DE CONFIDENTIALITÉ

Responsable du Traitement : Faciliter AI, une Société par Actions Simplifiée Unipersonnelle (SASU)

Siège Social : 100 chemin de Mireille, 13300 Salon-de-Provence, France

N° TVA Intracommunautaire : FR14938793775

Contact : contact@myfaq.ai

Délégué à la Protection des Données : dpo@faciliter.ai

Version : 2.3

Date d'entrée en vigueur : 2 novembre 2026

1. INTRODUCTION

Faciliter AI ("nous", "notre") s'engage à protéger votre vie privée et vos données personnelles. La présente Politique de Confidentialité explique comment nous collectons, utilisons, stockons, partageons et protégeons vos informations personnelles lorsque vous utilisez la plateforme MyFAQ et les services associés, y compris l'application Microsoft Teams MyFAQ Assistant (nom complet : MyFAQ Knowledge Base Assistant) (le "Service").

MyFAQ fournit des réponses assistées par IA à partir des connaissances de l'entreprise et accompagne les processus des projets RFx. MyFAQ Assistant permet d'utiliser ces fonctions dans Microsoft Teams, notamment les questions et réponses avec références aux sources, le contexte des projets et les notifications de revue, selon vos droits d'accès MyFAQ.

Cette politique couvre l'utilisation du Service via un navigateur web, les agents pris en charge, les API et les applications connectées telles que Microsoft Teams. Elle s'applique aux administrateurs d'organisation, aux membres d'équipe invités et aux autres utilisateurs du Service, ainsi qu'aux visiteurs de notre site web.

Pour les données personnelles contenues dans le Contenu Client, le Client détermine les finalités et moyens essentiels du traitement et Faciliter AI traite les données sur ses instructions documentées conformément à l'Annexe 1 des Conditions. Ainsi, selon la législation applicable, le Client est responsable du traitement et Faciliter AI sous-traite au titre du RGPD ; le Client est le « Business » et Faciliter AI son « Service Provider » ou « Contractor » au titre du CCPA/CPRA ; le Client est le « Controlador » et Faciliter AI l'« Operador » au titre de la LGPD brésilienne. Faciliter AI agit comme responsable de traitement indépendant pour les données de compte, facturation, sécurité et relation directe décrites dans la présente Politique.

2. DONNÉES QUE NOUS COLLECTONS

2.1 Informations de Compte

Lors de votre inscription ou de votre invitation à utiliser le Service, nous collectons :

- Nom (prénom, nom de famille)
- Adresse e-mail
- Nom et site web de l'entreprise
- Pays de résidence
- Préférences linguistiques
- Intitulé de poste (facultatif)

2.2 Données d'Utilisation

Nous collectons automatiquement des informations sur votre utilisation du Service :

- Données de connexion (adresse IP, type de navigateur, informations sur l'appareil)
- Utilisation des fonctionnalités et schémas d'interaction
- Volumes de requêtes et métriques de performance du service
- Journaux d'erreurs pour le débogage et l'amélioration

2.3 Données de Contenu

Nous traitons le contenu que vous téléchargez sur le Service, notamment :

- Documents (appels d'offres, PDF, fichiers Excel)
- Paires de questions et réponses
- Contenu de base de connaissances

2.4 Informations de Facturation et Fiscales

Lorsque cela est nécessaire pour fournir un abonnement payant, émettre des factures ou respecter nos obligations fiscales et comptables, nous collectons :

- Nom et adresse e-mail du contact de facturation
- Dénomination sociale, adresse de facturation et pays de l'entreprise
- Numéro de TVA, numéro fiscal ou autre identifiant professionnel
- Informations relatives aux bons de commande, factures et au statut de paiement

2.5 Enregistrements de Consentement

Nous conservons des enregistrements de votre consentement pour la conformité légale :

- Horodatage d'acceptation des Conditions d'Utilisation
- Horodatage d'acceptation de la Politique de Confidentialité
- Horodatage d'acceptation de la Politique d'Utilisation Acceptable
- Versions des politiques acceptées

2.6 Applications connectées. Lors de l'utilisation d'agents ou de messageries pris en charge, nous traitons les identifiants d'utilisateur et d'organisation liés, permissions, jetons d'authentification et traces de connexion et d'activité nécessaires à l'authentification, au routage et à la sécurité. Les instructions, contenus sélectionnés, résultats et pièces jointes peuvent transiter par la plateforme connectée.

3. COMMENT NOUS UTILISONS VOS DONNÉES

3.1 Fourniture du Service (Base juridique : Exécution du contrat)

- Fournir et maintenir le Service
- Traiter vos demandes et requêtes
- Gérer votre compte et abonnement
- Envoyer des communications liées au service

3.2 Amélioration du Service (Base juridique : Intérêt légitime)

- Analyser les schémas d'utilisation pour améliorer les fonctionnalités
- Développer de nouvelles fonctionnalités
- Résoudre les problèmes techniques
- Optimiser les algorithmes de recherche et de récupération IA

3.3 Conformité Légale (Base juridique : Obligation légale)

- Respecter les lois et réglementations applicables
- Répondre aux demandes légitimes des autorités
- Maintenir des pistes d'audit pour la conformité
- Émettre des factures, calculer et déclarer les taxes applicables, et conserver les documents comptables

3.4 Marketing (Base juridique : Consentement)

- Envoi de newsletters et mises à jour produit (avec votre consentement)
- Informations sur les nouvelles fonctionnalités ou services

4. PARTAGE DES DONNÉES

4.1 Prestataires de Services

Nous partageons des données avec des prestataires de confiance qui nous aident à exploiter le Service :

Région de données sélectionnée : Le Client choisit la région de données UE/EEE ou Amérique du Nord lors de l'inscription. Ce choix détermine le lieu où le Contenu Client et les données principales du Service sont hébergés et traités, sous réserve des informations relatives aux fournisseurs et aux transferts ci-dessous.

- **Infrastructure Cloud** : OVH et d'autres fournisseurs de cloud et d'infrastructure sélectionnés, dans l'UE/EEE, aux États-Unis ou dans d'autres pays selon les besoins
- **Traitement des Paiements** : Stripe (conforme PCI-DSS)
- **Traitement IA** : Google (Gemini), Mistral, modèles hébergés OVH et autres fournisseurs d'IA sélectionnés, y compris des fournisseurs aux États-Unis lorsque nécessaire - contractuellement tenus de ne pas utiliser vos données pour entraîner leurs modèles
- **Services Email** : Pour les e-mails transactionnels et marketing

Nous pouvons ajouter, remplacer ou utiliser d'autres fournisseurs lorsque cela est nécessaire pour exploiter, sécuriser, assister ou améliorer le Service, sous réserve d'une diligence appropriée et d'obligations contractuelles de protection des données. Les fournisseurs peuvent traiter des données dans l'UE/EEE, aux États-Unis ou dans d'autres pays. Pour les transferts de données personnelles hors de l'EEE, nous utilisons un mécanisme de transfert juridiquement valable, tel qu'une décision d'adéquation (y compris le Cadre de protection des données UE-États-Unis lorsque applicable), les clauses contractuelles types de la Commission européenne avec des mesures supplémentaires lorsque requises, ou un autre mécanisme autorisé par le droit applicable de la protection des données.

4.2 Exigences Légales

Nous pouvons divulguer des données lorsque la loi, une procédure judiciaire l'exige, ou pour protéger nos droits et notre sécurité.

4.3 Pas de Vente de Données

Nous NE VENDONS PAS vos données personnelles à des tiers.

4.4 Applications choisies par le Client. Lorsqu'un utilisateur autorisé connecte une application externe telle que ChatGPT, Claude ou Microsoft Teams, nous transmettons le contenu et les résultats nécessaires aux fonctions autorisées sur instruction du Client. Les conditions et paramètres du destinataire régissent sa conservation distincte, ses lieux de traitement et tout entraînement permis. Examinez-les avant connexion. Nos engagements de région et de non-entraînement concernent nos traitements et ceux de nos fournisseurs engagés, pas un service distinct choisi par le Client. La déconnexion ne supprime pas les copies externes. Nos obligations RGPD, garanties de transfert et restrictions de données de tiers demeurent applicables.

5. IA ET VOS DONNÉES

5.1 Fournisseurs de LLM tiers

Les fournisseurs de LLM tiers que nous engageons ont l'interdiction contractuelle d'utiliser le Contenu Client pour entraîner ou affiner leurs modèles. Notre utilisation interne pour améliorer le Service est décrite à l'article 5.3 et à l'article 8.2 des Conditions. Les applications externes choisies par le Client relèvent de l'article 4.4.

5.2 Traitement pour la Fourniture du Service

Nous traitons le contenu pour fournir, sécuriser, assister et améliorer le Service dans les finalités et instructions de cette Politique et de l'Annexe 1 des Conditions. Les fournisseurs IA que nous engageons le traitent uniquement pour nos finalités autorisées précisées ; les applications externes choisies par le Client relèvent de l'article 4.4.

5.3 Améliorations internes du Service

Nous pouvons utiliser le Contenu Client en interne pour évaluer et améliorer fonctionnalités, recherche, qualité des réponses, fiabilité et sécurité dans les finalités convenues et instructions documentées du Client, en respectant confidentialité, droit de protection des données et restrictions des sources. Les usages hors de ces instructions exigent une anonymisation irréversible ou une autorisation licite distincte et toute base légale requise, selon l'article 8.2 des Conditions.

5.4 Politique relative aux données utilisateur des services d'API Google

Lorsque vous choisissez de connecter votre Google Drive au Service, notre accès, utilisation, transfert, protection et conservation des données utilisateur Google sont régis par les déclarations suivantes :

- **Accès aux données** : Nous accédons aux informations de profil de votre compte Google (notamment votre adresse e-mail et vos informations de profil de base) pour authentifier la connexion. Nous accédons également aux fichiers et dossiers Google Drive (métadonnées telles que les noms de fichiers, les identifiants, les tailles et le contenu des fichiers) que vous sélectionnez explicitement à l'aide de notre intégration de sélecteur de fichiers.
- **Utilisation des données** : Nous utilisons vos fichiers Google Drive exclusivement pour les importer dans votre base de connaissances isolée et utiliser notre agent IA pour répondre à vos questions sur la base de ces documents. Nous n'utilisons pas ces données à d'autres fins.
- **Transfert de données** : Les données Google sont traitées dans la région du Service choisie, sous réserve des transferts licites divulgués. Le contenu sélectionné peut être transmis à nos fournisseurs IA pour générer les réponses autorisées sous restrictions contractuelles de non-entraînement. La divulgation aux applications choisies par le Client n'est permise que pour des fonctions visibles, divulguées et autorisées et dans le respect des exigences Google Limited Use applicables ; elle n'autorise ni publicité, ni revente, ni entraînement général. Tout changement d'usage exige les informations et consentements requis par Google et la loi.
- **Protection des données** : Les données utilisateur Google sont protégées conformément aux normes de sécurité les plus strictes de l'industrie, notamment le chiffrement en transit (TLS 1.3) et au repos (AES-256), un partitionnement strict entre clients (tenant isolation) et des audits de sécurité réguliers.
- **Conservation et suppression des données** : Nous conservons le contenu des fichiers Google Drive importés uniquement tant que votre compte est actif ou jusqu'à ce que vous supprimiez le document de la base de connaissances. Si vous supprimez un document, il est immédiatement retiré des systèmes actifs et définitivement purgé des sauvegardes sous 90 jours. Si vous déconnectez votre compte Google, tous les jetons associés sont immédiatement supprimés.
- **Conformité d'utilisation limitée (Limited Use)** : L'utilisation et le transfert par MyFAQ vers toute autre application d'informations reçues des API Google respecteront la politique relative aux données utilisateur des services d'API Google, y compris les exigences d'utilisation limitée (Limited Use). En particulier : Nous n'utilisons pas les données Workspace (telles que les fichiers Google Drive) pour développer, améliorer ou entraîner des modèles d'IA/ML (y compris les grands modèles de langage). Nous ne transférons pas les données Workspace à des services d'IA/ML tiers qui utiliseraient ces données pour entraîner leurs propres modèles d'IA/ML.

6. CONSERVATION DES DONNÉES

6.1 Comptes Actifs

Nous conservons vos données aussi longtemps que votre compte est actif et selon les besoins pour fournir le Service.

6.2 Après Résiliation

À la résiliation du compte :

- Vous disposez de 30 jours pour exporter vos données
- Après 30 jours, nous supprimons votre contenu des systèmes actifs
- Les copies de sauvegarde peuvent être conservées jusqu'à 90 jours
- Les analyses anonymisées peuvent être conservées indéfiniment

6.3 Exigences Légales

Certaines données peuvent être conservées plus longtemps pour respecter les obligations légales (par ex., les enregistrements de facturation à des fins fiscales).

7. SÉCURITÉ DES DONNÉES

Nous mettons en œuvre des mesures techniques et organisationnelles appropriées :

- Chiffrement en transit (TLS 1.3) et au repos (AES-256)
- Contrôles d'accès et authentification
- Évaluations de sécurité régulières
- Formation des employés et accords de confidentialité
- Procédures de réponse aux incidents

8. VOS DROITS (RGPD)

En tant que personne concernée au titre du RGPD, vous avez le droit de :

- **Accès** : Demander une copie de vos données personnelles

- **Rectification** : Corriger les données inexactes
- **Effacement** : Demander la suppression de vos données ("droit à l'oubli")
- **Portabilité** : Exporter vos données dans un format lisible par machine
- **Limitation** : Limiter la façon dont nous traitons vos données
- **Opposition** : Vous opposer au traitement basé sur l'intérêt légitime
- **Retrait du Consentement** : Lorsque le traitement est basé sur le consentement

Pour exercer ces droits, contactez-nous à dpo@faciliter.ai.

9. TRANSFERTS INTERNATIONAUX

9.1 Région de données sélectionnée

Lors de l'inscription, le Client sélectionne la région de données UE/EEE ou Amérique du Nord. Le Contenu Client et les données principales du Service sont principalement hébergés et traités dans la région sélectionnée.

9.2 Transferts vers des Tiers

Les prestataires de services peuvent traiter des données dans l'UE/EEE, aux États-Unis ou dans d'autres pays lorsque cela est nécessaire au fonctionnement, à la sécurité, au support ou à l'amélioration du Service. Lorsqu'il y a transfert de données à caractère personnel hors de la région sélectionnée ou, le cas échéant, hors de l'EEE, nous appliquons les garanties exigées par le droit applicable en matière de protection des données, telles qu'une décision d'adéquation (y compris le Cadre UE-États-Unis de protection des données lorsqu'il s'applique), les Clauses Contractuelles Types avec des mesures supplémentaires lorsque nécessaire, ou un autre mécanisme de transfert autorisé.

9.3 Exigences locales de transfert du Client

Les Clients professionnels sont responsables d'identifier et d'obtenir, avant de placer des données personnelles dans le Service, toute déclaration, notification, approbation ou autorisation préalable de transfert exigée par l'autorité de protection des données de leur pays d'établissement. Cela comprend toute déclaration ou autorisation requise auprès de la CNDP marocaine en vertu de la loi n° 09-08 pour les transferts du Maroc vers l'Union européenne ou un autre pays étranger. L'Annexe 1 des Conditions précise les modalités d'assistance.

10. COOKIES

Nous utilisons des cookies essentiels pour le fonctionnement du Service et des cookies d'analyse optionnels avec votre consentement. Consultez notre Politique de Cookies pour plus de détails.

11. CONFIDENTIALITÉ DES ENFANTS

Le Service n'est pas destiné aux personnes de moins de 18 ans. Nous ne collectons pas sciemment de données auprès d'enfants.

12. MODIFICATIONS DE CETTE POLITIQUE

Nous pouvons mettre à jour cette Politique de Confidentialité périodiquement. Les modifications substantielles seront notifiées par e-mail ou via le Service. La poursuite de l'utilisation après notification constitue une acceptation.

13. AUTORITÉ DE CONTRÔLE

Vous avez le droit de déposer une plainte auprès de votre autorité locale de protection des données. Pour la France, il s'agit de la Commission Nationale de l'Informatique et des Libertés (CNIL).

14. NOUS CONTACTER

Pour les questions relatives à la confidentialité :

- **Email** : dpo@faciliter.ai
- **Adresse** : Faciliter AI, 100 chemin de Mireille, 13300 Salon-de-Provence, France