POLITIQUE DE CONFIDENTIALITÉ

JUMBER • Dernière mise à jour : 4 novembre 2026

1. Responsable et périmètre

La présente politique concerne les traitements de données personnelles dont Jumber est responsable, notamment l'administration de son site, des comptes, contrats, paiements, contacts commerciaux et de la sécurité de son service. Responsable : JUMBER, société par actions simplifiée (SAS) au capital de 7 500 €, immatriculée au RCS de Rennes sous le numéro 130 585 557, SIRET 130 585 557 00015, TVA intracommunautaire FR67130585557, dont le siège social est situé 21 avenue Germaine Tillion, 35136 Saint-Jacques-de-la-Lande, France. Contact : privacy@jumber.io. Lorsque des données de collaborateurs sont traitées sur instruction d'une organisation cliente, cette organisation est en principe responsable du traitement et Jumber agit comme sous-traitant selon le DPA.

2. Données liées aux comptes et à la relation client

Jumber traite les noms, coordonnées professionnelles, identifiants, adresses email, données d'organisation et de rôles, informations de connexion, tickets de support, paramètres, contrats, factures et historique des paiements. Stripe traite les paiements ; Jumber ne stocke pas les numéros complets de carte. HubSpot est utilisé pour l'hébergement du site et la gestion commerciale, et Mailjet pour les emails applicatifs.

3. Données de suivi et de sécurité traitées pour les clients

Selon les fonctionnalités compatibles, Jumber peut traiter pour le compte des organisations clientes les sites IA de sa bibliothèque visités par les collaborateurs, durées d'utilisation, horodatages, nombre de prompts, modèles, tokens, coûts estimés, alertes et certains prompts après retrait de données sensibles identifiées. L'analyse de prompts ne fonctionne pas nécessairement sur tous les outils suivis. Les documents joints sont envoyés aux serveurs Jumber pour analyse puis ne sont pas conservés. Les analyses sont réalisées dans l'extension et sur les serveurs Jumber, sans fournisseur IA externe pour ces contenus.

4. Accès des administrateurs

Les administrateurs et propriétaires d'organisation disposent de mesures individuelles et agrégées selon leurs droits, sans consultation des prompts complets depuis le tableau de bord. Les membres n'accèdent pas au tableau de bord de l'organisation. Le client définit les règles par équipe et doit informer les collaborateurs de l'existence, de l'étendue et des finalités du suivi.

5. Finalités et bases légales propres à Jumber

Gestion de comptes et fourniture des prestations : exécution du contrat ou intérêts légitimes selon la personne concernée ; facturation et comptabilité : obligation légale et contrat ; protection du service et prévention des abus : intérêt légitime ; traitement des demandes de support : contrat ou intérêt légitime ; prospection commerciale B2B : intérêt légitime lorsque les règles applicables le permettent, ou consentement lorsque requis ; cookies de suivi et mesure marketing HubSpot : consentement lorsqu'exigé. Les bases légales des dispositifs de suivi mis en œuvre par une organisation cliente relèvent de son analyse en qualité de responsable du traitement.

6. Destinataires et hébergement

Les données peuvent être accessibles à des personnes habilitées chez Jumber et aux prestataires strictement nécessaires : Hostinger (VPS applicatif à Paris), MongoDB Atlas (stockage dans l'Union européenne), HubSpot (site hébergé en Europe et CRM), Stripe (paiements) et Mailjet (emails applicatifs). Aucun service externe d'IA ne reçoit les prompts ou documents confiés à Jumber pour l'analyse DLP, selon le fonctionnement déclaré. L'existence éventuelle de sous-traitances et d'accès techniques transfrontières doit être évaluée prestataire par prestataire.

7. Durées de conservation

Pour les données relevant du service client : journaux d'activité IA, 12 mois ; alertes DLP, 12 mois ; statistiques de tokens et de coûts, 24 mois ; prompts expurgés, 30 jours ; documents analysés, supprimés après analyse. Pour les traitements propres à Jumber : journaux techniques de connexion et de sécurité, 6 mois ; tickets de support, 24 mois après leur clôture ; données de prospection sans relation commerciale, en principe 3 ans après le dernier contact émanant du prospect ; factures et pièces comptables, 10 ans

lorsque la réglementation l'exige. Les informations de compte sont conservées pendant la relation contractuelle, puis selon les obligations légales et les délais de suppression applicables. À la fin du contrat, un export JSON reste disponible 14 jours ; les données actives sont ensuite supprimées, sous réserve des obligations légales, tandis que les copies de sauvegarde expirent au plus tard à l'issue de leur rétention de 30 jours. Les statistiques véritablement anonymes peuvent être conservées plus longtemps.

8. Sécurité

Jumber utilise des mesures de sécurité proportionnées aux risques : contrôles d'accès et de rôle, protections des communications, authentification multifacteur obligatoire pour Owner et Admin, sauvegardes chiffrées quotidiennes conservées 30 jours, tests trimestriels de restauration, tests de sécurité automatisés lors des déploiements et revue trimestrielle des habilitations. Les accès internes sont limités aux personnes autorisées. Malgré ces mesures, aucun service numérique n'est totalement exempt de risques.

9. Transferts internationaux

Le serveur applicatif principal est situé à Paris et la base de données est hébergée dans une région de l'Union européenne. Les contenus des prompts et documents analysés ne sont pas transmis à un fournisseur externe d'IA. Certains prestataires internationaux utilisés pour le site, les paiements, les emails ou l'assistance peuvent néanmoins impliquer des accès ou traitements depuis des pays tiers dans les conditions de leurs contrats. Jumber encadre les transferts soumis au chapitre V du RGPD par un mécanisme légal approprié, notamment une décision d'adéquation ou des clauses contractuelles types lorsque nécessaire.

10. Droits et réclamations

Dans les conditions de la loi, les personnes disposent des droits d'accès, de rectification, d'effacement, de limitation, d'opposition et de portabilité quand celle-ci est applicable. Elles peuvent retirer leur consentement lorsqu'il fonde un traitement. Pour les traitements propres à Jumber : privacy@jumber.io. Pour le suivi professionnel décidé par un employeur, contacter d'abord l'employeur responsable du traitement ; Jumber l'assiste.

11. Cookies et modifications

Les cookies HubSpot et les autres traceurs du site sont régis par la Politique cookies et traceurs. La présente politique peut évoluer pour refléter des changements légaux, techniques ou organisationnels ; les informations requises seront fournies lors des changements significatifs.

12. Transparence pour les collaborateurs

Lorsqu'une entreprise utilise Jumber pour suivre les outils IA employés par son personnel, l'entreprise détermine les finalités et moyens essentiels de ces traitements et demeure responsable de l'information préalable des collaborateurs. Elle peut obtenir une notice type pour expliquer les catégories de données, les destinataires, les périodes de conservation, les droits et les limitations des dispositifs de suivi. Les demandes relatives à ces données sont adressées en priorité à l'entreprise concernée.

13. Précisions sur la conservation des prompts

Les contenus expurgés peuvent conserver des informations permettant d'identifier directement ou indirectement une personne ; ils ne sont pas systématiquement anonymes. Les collaborateurs doivent éviter d'introduire des données personnelles ou professionnelles non nécessaires dans les services d'IA. Les règles de suivi des outils de la bibliothèque ne signifient pas que les prompts sont inspectés sur chaque service référencé.