

POUR LES DÉCIDEURS, LES DPO ET LES ACHETEURS

Sécurité, conformité et souveraineté des données : ce que nous affirmons, et ce que nous ne prétendons pas

Où sont vos données, qui y accède, comment elles sont protégées, ce que fait SheeplA, ce que dit la loi : des faits vérifiables, leurs limites, et les points que l'éditeur doit encore compléter.



France

données hébergées sur les serveurs de l'éditeur, à Lingolsheim

AES-256

chiffrement par l'application des documents, jetons et secrets

0 publicité

ni publicité ni revente de données

Des faits vérifiables, chacun avec sa source

Les limites écrites en toutes lettres

Les points non documentés signalés, pas masqués



Cloisonnement des données entre organisations

- ✓ Les données de chaque organisation sont isolées dans la base par des politiques de sécurité au niveau des lignes (Row Level Security de PostgreSQL), en plus des contrôles de l'application.
- ✓ Le contexte de l'organisation est posé à chaque transaction, et le compte de la base utilisé par l'application n'est ni superutilisateur ni autorisé à contourner ces politiques.
- ✓ Des tests automatiques vérifient l'isolation : la suite découvre elle-même les tables qui portent l'identifiant d'organisation et n'exempte que des tables justifiées.
- ⚠ Quelques tables techniques (sessions, appartenances, file d'événements) sont exemptées de ces politiques par conception : l'isolation ne se présente donc pas comme valant pour « toutes les tables ».



Chiffrement

- ✓ Les connexions à SheepOS sont chiffrées (HTTPS). Une boîte mail IMAP ne se relie qu'en connexion chiffrée.
- ✓ Les mots de passe sont hachés avec Argon2id et ne sont jamais stockés en clair.
- ✓ Les jetons des services reliés (Microsoft, par exemple) et les secrets de double authentification sont chiffrés en base (AES-256-GCM), avec une clé qui n'est pas dans la base.
- ✓ Les documents sont chiffrés avant d'être écrits sur les serveurs, avec une clé de données par organisation, une par espace privé de membre et une par fichier. Les copies de mails et les identifiants des boîtes sont chiffrés avec une clé propre au membre.
- ✓ L'IBAN d'un fournisseur est chiffré et n'apparaît que sur demande.
- ⚠ Limite : la clé maîtresse est détenue par le serveur. Ce n'est pas un chiffrement de bout en bout dont l'éditeur ne pourrait pas lire le contenu ; il protège les données stockées, et l'éditeur n'y accède pas en pratique.
- ⚠ Limite : les PDF de factures, les justificatifs de dépense et les logos ne sont pas chiffrés par l'application. Ne dites pas que « tous les fichiers » sont chiffrés.



Accès et authentification

- ✓ Mot de passe de 12 caractères au moins, comparé aux fuites connues par une méthode qui n'envoie que 5 caractères d'une empreinte. Si ce service est indisponible, l'inscription n'est pas bloquée.
- ✓ Double authentification par application (TOTP) avec dix codes de secours à usage unique. Elle est facultative pour les membres ; elle est obligatoire pour la console de l'éditeur.
- ✓ Limitation des tentatives de connexion avec verrouillage progressif, appareils connectés consultables et révocables, e-mail d'alerte lors d'une connexion depuis un nouvel appareil.
- ✓ Rôles prêts à l'emploi (propriétaire, administrateur, membre, lecteur, assistant, comptable, copropriétaire, ménage) et rôles sur mesure par module, avec une portée des données. Les permissions sont vérifiées côté serveur : l'interface ne fait que masquer ce que le serveur refuse.
- ✓ Un module coupé pour une organisation est fermé côté serveur en lecture comme en écriture, y compris pour les tâches de fond ; ses données sont conservées.
- ✓ Les notes privées ne sont visibles que de leur auteur. La boîte mail d'un membre est privée : les autres membres, administrateurs compris, n'y ont pas accès par l'application.
- ✓ La console de l'éditeur ne montre, pour chaque espace, que des indicateurs globaux (offre, date d'inscription, dernière activité, nombre de membres, volumes) : le contenu de votre espace n'y est pas visible, et chaque consultation est journalisée.



Journal d'audit

- ✓ Les actions métier sont journalisées (qui, quoi, quand, valeurs avant et après, adresse IP). Le journal est en ajout seul : le compte de la base utilisé par l'application ne peut ni modifier ni supprimer une ligne.
- ✓ Les propriétaires et les administrateurs consultent le journal et l'exportent en CSV ; les secrets en sont exclus, et le détail d'une entrée est masqué à qui n'a pas le droit de voir la donnée concernée.
- ⚠ Limite : « ajout seul » vaut pour le compte de l'application, pas face à un administrateur de la base de données ; le journal n'est pas présenté comme inviolable. Seuls les événements de signature électronique et de devis forment une chaîne d'empreintes.



Sauvegardes et continuité



Les procédures d'exploitation prévoient des sauvegardes de la base de données (toutes les 15 minutes, avec contrôle de l'archive, et copies journalières, hebdomadaires et mensuelles) et des fichiers.



À compléter par l'éditeur : cadence réellement en service, lieu de stockage des sauvegardes, chiffrement des sauvegardes, durée de conservation et date du dernier test de restauration. Aucun de ces points n'est attesté dans les documents du dépôt : ne les affirmez pas.



Hébergement et souveraineté



Les données (base, documents, copies de mails, modèle de SheeplA) sont hébergées en France, sur les serveurs propres de l'éditeur, TB-IT, à Lingolsheim (Bas-Rhin).



Pas de réseau de diffusion de contenu (CDN) ni de service de polices tiers : les polices du site et de l'application sont embarquées.



L'envoi des e-mails de l'application passe par Infomaniak (Suisse).



À compléter par l'éditeur : lieu des sauvegardes, hébergeur du serveur mandataire inverse (reverse proxy), fournisseur du nom de domaine et du réseau. Ces points ne sont pas documentés.



Aucune certification d'hébergement ou de sécurité (ISO 27001, HDS, SecNumCloud...) n'est revendiquée.



Facture électronique



SheepOS n'est pas une plateforme agréée et n'émet pas de facture électronique à ce jour. Une option, désactivée par défaut, joint le format Factur-X (un PDF qui contient aussi les données de la facture, profil Basique ou EN 16931) aux factures et aux avoirs ; elle ne dépose rien sur une plateforme agréée et, si une donnée manque, le PDF simple part tel quel.



La réception puis l'émission par une plateforme agréée sont prévues, sans date garantie. D'après le calendrier publié, l'obligation d'émettre s'appliquerait aux petites entreprises à partir du 1er septembre 2027 : à vérifier sur les sites officiels, qui seuls font foi.



RGPD : rôles, droits, durées et sous-traitants

- ✓ Pour les données de vos propres clients, voyageurs et correspondants, vous êtes responsable du traitement et l'éditeur agit comme sous-traitant. Pour votre compte, votre connexion, la sécurité, la démo publique et le support, l'éditeur est responsable du traitement.
- ✓ Droits exercés en libre-service : export de vos données (profil), suppression du compte (effacement définitif 30 jours après la demande, annulable), voir, corriger et effacer ce que SheepIA sait de vous, effacement d'un contact marketing, anonymisation des voyageurs des locations après la durée que vous fixez.
- ✓ Durées de conservation publiées : factures et avoirs émis au moins 10 ans (obligation comptable) ; corbeille de Documents 30 jours ; visites de la démo 30 jours ; mesures d'arrivée sur le site 30 jours ; sessions 30 jours au plus ; texte généré par SheepIA en attente de relecture effacé 10 minutes après le traitement (2 heures au plus).
- ✓ Destinataires listés par la politique de confidentialité : envoi d'e-mails (Infomaniak, Suisse), itinéraires (OpenRouteService, Allemagne), fonds de carte (OpenStreetMap, Royaume-Uni), annuaire public des entreprises, vérification des mots de passe (Have I Been Pwned, Australie, préfixe d'empreinte seulement), taux de change (Banque centrale européenne), notifications du navigateur, et, si vous les reliez, Microsoft ou votre fournisseur de messagerie.
- ✓ Selon les modules activés, d'autres services interviennent : paiement des abonnements (PayPal, Stripe), boutique en ligne (Stripe Connect et les transporteurs Boxtal, Colissimo, DPD, GLS), connexion avec Google, vérification de TVA intracommunautaire (VIES).
- ⚠ À compléter par l'éditeur : la liste détaillée de ces services (rôle, données transmises, lieu de traitement) dans la politique de confidentialité, qui ne les décrit pas tous aujourd'hui. Ne dites jamais « aucun sous-traitant hors Union européenne ».
- ✓ Selon la politique de confidentialité, hors Union européenne : la Suisse et le Royaume-Uni (décisions d'adéquation), l'Australie (préfixe d'empreinte de mot de passe, sans donnée identifiante) et les services de notification du navigateur si vous les activez. Aucun contenu de votre espace n'est transféré hors de l'Union, sauf service extérieur que vous reliez vous-même.
- ⚠ À compléter par l'éditeur : le registre des traitements, la procédure de notification d'une violation (la politique s'engage à informer dans les délais légaux, notification à la CNIL sous 72 heures quand elle est requise) et le modèle d'accord de sous-traitance. Ces documents ne sont pas dans le dépôt.
- ✓ Mesure d'audience du site : une requête par visite, sans cookie ni adresse IP enregistrée, effacée après 30 jours, et rien si le navigateur demande de ne pas être suivi. Aucun cookie publicitaire. Une mesure par un tiers (Google Analytics), lorsqu'elle est activée, ne s'exécute qu'avec votre consentement, refusable aussi simplement qu'acceptable.

SheepIA, l'assistant

- ✓ Le modèle de SheepIA fonctionne sur des machines que l'éditeur contrôle. Selon la politique de confidentialité, le contenu de votre espace n'est envoyé à aucun fournisseur d'intelligence artificielle tiers et vos contenus ne servent pas à entraîner un modèle commun.
- ✓ SheepIA ne lit rien à votre insu et ne reçoit aucun outil d'action : elle écrit du texte que vous relisez. Par défaut, rien n'est envoyé ni appliqué sans votre accord ; vous pouvez ensuite autoriser, action par action, ce qu'elle fait seule, et annuler pendant un délai.
- ✓ Les documents classés « secret » ne lui sont jamais fournis ; un dossier ou un document peut lui être fermé ; un administrateur peut la désactiver pour toute l'organisation et chaque membre peut exclure sa boîte mail. Elle ne lit que ce que le rôle de l'utilisateur lui permet déjà de lire.
- ✓ Chaque appel est étiqueté et vérifié avant d'atteindre le modèle (deux organisations ne partagent aucun contenu). Le journal technique ne contient ni messages, ni consignes, ni brouillons. Un journal des actions de SheepIA montre ce qu'elle a préparé ou fait, et permet d'annuler.
- ✓ Sa mémoire privée (préférences d'écriture, corrections) est chiffrée avec la clé du membre, invisible des autres membres, administrateurs compris, et de l'éditeur ; l'apprentissage est activé par défaut et se désactive d'un clic ; tout se voit, se corrige et s'efface.
- ✓ Des crédits quotidiens, selon l'offre, limitent l'usage ; un appel qui échoue rend ses crédits. SheepIA peut se tromper : relisez toujours.
- ⚠ Limite : le code n'interdit pas techniquement de pointer le modèle vers un service extérieur ; l'absence de fournisseur tiers repose sur la configuration de production, que l'éditeur doit confirmer.

Mentions légales, conservation et prospection

- ✓ Une facture émise est figée et ne se corrige que par avoir ; la numérotation est continue ; une facture ne part pas tant qu'une mention obligatoire manque ; les factures et avoirs émis sont conservés au moins 10 ans.
- ✓ Prospection : avant chaque envoi marketing, le serveur vérifie l'éligibilité du destinataire (liste de suppression, désinscrits, consentement valide pour un particulier, intérêt légitime justifié pour un professionnel) ; la désinscription se fait en un clic ; la base légale d'un prospect s'enregistre avec sa date et sa preuve, et l'enregistrer n'envoie rien. SheepOS n'envoie jamais de message de prospection de lui-même.
- ⚠ Limite : SheepOS aide à respecter les règles de prospection mais n'est pas un conseil juridique et ne dit jamais qu'un message est « conforme à la CNIL » : le contenu du message et la base légale restent de la responsabilité de l'organisation qui écrit. Il ne vérifie pas les listes d'opposition à la prospection téléphonique.

QUESTIONS À POSER À VOTRE INTERLOCUTEUR

Une liste à parcourir avec n'importe quel éditeur

Les réponses de SheepOS à ce jour ; posez les mêmes questions à tout autre éditeur.

Question	Réponse de SheepOS à ce jour
Où sont hébergées mes données, et par qui ?	En France, sur les serveurs propres de l'éditeur (TB-IT, Lingolsheim). Les e-mails de l'application partent par Infomaniak (Suisse). Lieu des sauvegardes et fournisseur du réseau : à compléter par l'éditeur.
Qui peut voir le contenu de mon espace chez l'éditeur ?	La console de l'éditeur ne montre que des indicateurs globaux ; le contenu (clients, factures, documents, mails, mémoire de SheepIA) n'y est pas visible et chaque consultation est journalisée. Le chiffrement n'est pas de bout en bout : la clé maîtresse est détenue par le serveur.
Puis-je récupérer et supprimer mes données ?	Oui : export depuis le profil, suppression du compte (effacement 30 jours après la demande, annulable), export toujours possible même à la limite d'une offre. Les factures émises sont conservées au moins 10 ans.
Quels sont vos sous-traitants et où traitent-ils mes données ?	La politique de confidentialité en liste une partie, avec les transferts hors Union européenne ; d'autres services interviennent selon les modules (paiement, boutique, transport, connexion Google, TVA). La liste complète est à compléter par l'éditeur : demandez-la.
L'intelligence artificielle envoie-t-elle mes données à un tiers ?	Selon la politique de confidentialité, non : le modèle fonctionne sur des machines de l'éditeur. Demandez la confirmation écrite de la configuration de production.
SheepIA peut-elle agir sans mon accord ?	Par défaut non : elle prépare, vous validez. Vous pouvez autoriser, action par action, ce qu'elle fait seule, avec un délai d'annulation et un journal.
Quelles sauvegardes, et la restauration est-elle testée ?	Des procédures de sauvegarde sont prévues (base toutes les 15 minutes, fichiers). La cadence en service, le chiffrement et la date du dernier test de restauration sont à compléter par l'éditeur.
Avez-vous un registre des traitements et un accord de sous-traitance à signer ?	À compléter par l'éditeur : ces documents ne sont pas dans le dépôt. Demandez-les par écrit avant de signer.
Avez-vous des certifications de sécurité ?	Aucune n'est revendiquée (ISO 27001, HDS, SecNumCloud...). Les contrôles décrits ici sont conçus et testés par l'éditeur ; aucun audit externe n'est revendiqué.
Que se passe-t-il en cas de violation de données ?	La politique de confidentialité s'engage à vous informer dans les délais prévus par la loi, avec notification à la CNIL sous 72 heures quand elle est requise. Aucun système n'est infaillible.
SheepOS est-il prêt pour la facture électronique ?	Pas encore de plateforme agréée connectée : SheepOS reçoit déjà les factures électroniques de vos fournisseurs et une option Factur-X prépare vos fichiers, sans les déposer. L'émission via la plateforme suivra, sans date garantie ; vérifiez le calendrier sur les sites officiels.

Questions fréquentes

Où sont hébergées les données de SheepOS ?

En France, sur les serveurs propres de l'éditeur, TB-IT, à Lingolsheim. Les e-mails de l'application sont envoyés par Infomaniak, en Suisse.

SheepOS chiffre-t-il mes documents et mes mails ?

Les documents sont chiffrés avant d'être écrits sur les serveurs, et les copies de mails et les identifiants des boîtes le sont avec une clé propre au membre. La clé maîtresse est détenue par le serveur : ce n'est pas un chiffrement de bout en bout.

L'assistant SheeplA envoie-t-il mes données à un fournisseur d'IA ?

Selon la politique de confidentialité, non : le modèle fonctionne sur des machines que l'éditeur contrôle, et vos contenus ne servent pas à entraîner un modèle commun. Par défaut, rien n'est envoyé sans votre accord.

SheepOS a-t-il une certification de sécurité ?

Aucune certification (ISO 27001, HDS, SecNumCloud...) n'est revendiquée. Les contrôles décrits sont conçus et testés par l'éditeur, avec leurs limites écrites en toutes lettres.

À savoir

- ⚠ Cette plaquette décrit ce que SheepOS fait aujourd'hui. Elle n'est ni un avis juridique, ni une attestation de conformité, ni une certification.
- ⚠ Aucun système n'est infallible ; les points marqués « à compléter par l'éditeur » ne sont pas encore documentés.

DONNÉES PERSONNELLES
contact@tb-it.fr

QUESTIONS SUR LE SERVICE
support@tb-it.fr

ÉDITEUR
TB-IT, 6 rue Simone
de Beauvoir, 67380
Lingolsheim, France