

Mesures de sécurité

Version 2.1, en vigueur depuis le 5 octobre 2026

OutLine Digital Agency (entrepreneur individuel), Via Dalmazia 36, 76125 Trani (BT), Italie — TVA IT08978680729

Comment nous protégeons les données : espaces de travail séparés, chiffrement, contrôle d'accès, sauvegardes — y compris ce que nous ne faisons pas encore.

Références juridiques

Règlement (UE) 2016/679 (RGPD), art. 32 (sécurité du traitement) ·
Règlement (UE) 2016/679 (RGPD), art. 25 (protection des données dès la conception et par défaut)

1. Une base de données par espace de travail

C'est la mesure la plus importante, et peu d'applications infonuagiques l'adoptent parce qu'elle coûte plus cher : **chaque espace de travail dispose de sa propre base de données**, et non d'une colonne « client » dans des tables partagées.

La différence se voit le jour où quelque chose tourne mal. Avec des tables partagées, une requête qui oublie le filtre client affiche les données de tout le monde ; ici, une telle requête n'existe pas, car les données des autres clients se trouvent dans une autre base de données. Il en va de même des sauvegardes, qui peuvent être restaurées un espace de travail à la fois sans toucher à personne d'autre.

2. Chiffrement

Quoi	Comment
Trafic vers le site et l'application	HTTPS avec des certificats renouvelés automatiquement. Le trafic non chiffré est redirigé.
Mots de passe des utilisateurs	Jamais conservés sous forme lisible ni avec un chiffrement réversible : uniquement un hachage calculé avec bcrypt , avec un sel aléatoire pour chaque utilisateur et une comparaison à temps constant. Même nous ne pouvons pas les lire ni vous les communiquer.
Jetons de session	La base de données ne conserve qu'une empreinte du jeton, jamais la valeur stockée dans le cookie.
Identifiants des connecteurs d'API	Chiffrés au repos avec AES-256-GCM , au moyen d'une clé dédiée conservée séparément des données. Une personne qui obtiendrait une copie de la base de données n'obtiendrait pas vos clés d'API.

Le modèle de menace, en toute franchise

Le chiffrement des identifiants protège contre les copies de base de données et les sauvegardes qui se retrouveraient là où elles ne devraient pas — de loin l'incident le plus probable. Il ne protège pas contre une compromission complète du serveur, où la clé reste lisible : il faudrait pour cela un service externe de gestion des clés, que nous n'utilisons pas aujourd'hui. Nous préférons le dire plutôt que de vous laisser supposer le contraire.

3. Contrôle d'accès

- Connexion avec une adresse e-mail personnelle et un mot de passe ; les sessions expirent et peuvent être fermées.
- Le cookie de session est **HttpOnly** (illisible par les scripts), **Secure** (envoyé uniquement sur des connexions

chiffrées) et **SameSite=Lax** (non envoyé avec les requêtes provenant d'autres sites).

- **Rôles et autorisations** : propriétaire, administrateur, membre et invité. Les invités ne voient que les projets auxquels ils ont été invités.
- Les clés d'API et les clés d'assistant d'IA (MCP) agissent avec les autorisations de la personne qui les a créées et peuvent être en lecture seule.
- L'accès de l'assistance utilise un **utilisateur temporaire qui expire au bout de 15 minutes** et dispose, pendant ce temps, des droits d'un administrateur ; chaque accès est présenté au propriétaire et aux administrateurs de l'espace de travail dans la console d'administration (Confidentialité et conformité) — quand, pendant combien de temps, par qui, pourquoi et les fichiers téléchargés —, le propriétaire est averti par e-mail à son ouverture, et l'export complet des données est bloqué pendant sa durée.
- Les données d'un espace de travail ne sont accessibles que depuis cet espace de travail : aucun écran, pas même pour nous, n'affiche ensemble les données de travail de plusieurs clients.

4. Infrastructure

- Serveurs chez IONOS SE en Allemagne, dans l'Union européenne.
- La base de données n'est pas exposée à Internet : elle n'écoute que sur le serveur lui-même.
- Les pages privées (l'application, la console d'administration, la prise en main, les API) sont exclues de l'indexation par les moteurs de recherche.
- Les tâches planifiées s'exécutent sur un canal interne protégé par un secret partagé : sans ce secret, le point d'accès refuse toute requête au lieu de rester ouvert.
- Les appels sortants vers les webhooks et les connecteurs d'API ne sont autorisés qu'en HTTPS et uniquement vers des adresses IP publiques, de sorte que le service ne puisse pas servir à atteindre des réseaux internes.
- Les mises à jour du système d'exploitation et des dépendances sont appliquées régulièrement ; les mises en production passent par une compilation vérifiée, et non par des modifications manuelles sur le serveur.

5. Sauvegardes et restauration

- Sauvegarde **quotidienne** de toutes les bases de données, compressée ; la taille de chaque copie est contrôlée lors de sa création.
- **Rotation : 7 copies quotidiennes, 4 hebdomadaires et 3 mensuelles.** Les copies plus anciennes sont supprimées automatiquement.
- Les copies sont conservées sur la même infrastructure européenne, avec des autorisations limitées à l'utilisateur système qui les produit.
- Les restaurations se font **par espace de travail** : un client peut être ramené en arrière sans toucher aux autres.
- Les restaurations sont effectuées à la main. Nous nous engageons à tester la procédure au moins deux fois par an, sur une copie : une sauvegarde jamais restaurée n'est pas une sauvegarde.

Ce que cela signifie pour vous

Si vous supprimez par erreur quelque chose d'important, la fenêtre utile pour le récupérer au niveau quotidien est normalement de sept jours. Plus vite vous nous écrivez, plus il est probable que nous puissions tout récupérer : écrivez à amministrazione@outlinedigital.it en indiquant le nom de l'espace de travail et, si vous le savez, quand cela s'est produit.

6. Comment le logiciel est écrit

- Les saisies des utilisateurs sont validées avant d'être enregistrées ; les requêtes à la base de données sont paramétrées et ne peuvent pas être manipulées de l'extérieur.
- Les opérations qui écrivent des données passent par des actions côté serveur avec contrôle du rôle : on ne peut pas les atteindre en appelant une adresse à la main.
- Les liens publics des formulaires utilisent des **codes impossibles à deviner** et révocables : régénérer un code

invalide immédiatement le précédent.

- Les secrets ne se trouvent pas dans le code mais dans les variables d'environnement du serveur.
- Avant chaque mise en production, des contrôles automatisés vérifient le bon fonctionnement des fonctionnalités et la cohérence des configurations.

7. En cas d'incident

Les violations de données personnelles sont notifiées au client **dans les 48 heures** après que nous en avons pris connaissance, avec les informations nécessaires pour évaluer la notification aux autorités. La procédure est décrite à la section 6 de l'Accord de traitement des données (<https://work.omegasuiteapp.com/legal/dpa>).

Si vous découvrez une vulnérabilité, écrivez à amministrazione@outlinedigital.it. Nous nous engageons à répondre dans un délai de 5 jours ouvrés et à n'engager aucune action contre quiconque signale de bonne foi, sans accéder aux données d'autrui, sans dégrader le service et sans divulguer le problème avant sa correction.

8. Ce que nous ne faisons pas (encore)

Une liste de mesures sans ses limites relève de la publicité. Voici ce **quin'est pas** en place aujourd'hui, pour que vous le sachiez avant plutôt qu'après :

- **Authentification à deux facteurs** : non disponible. Utilisez un mot de passe long que vous n'utilisez nulle part ailleurs, ainsi qu'un gestionnaire de mots de passe.
- **Chiffrement de l'ensemble de la base de données au repos** : non activé. Les mots de passe et les identifiants des services connectés sont protégés ; le reste des données est protégé par le contrôle d'accès et l'isolement du système, et non par le chiffrement.
- **Certifications** (ISO/IEC 27001, SOC 2) : nous n'en avons aucune. Nous ne revendiquons pas de normes pour lesquelles nous n'avons pas été audités.
- **Restrictions par adresse IP et journal des connexions par utilisateur consultable par le client** : non disponibles.
- **Sauvegarde des fichiers et copies conservées ailleurs** : non en place. Les sauvegardes couvrent les bases de données ; elles sont conservées sur le même serveur, protégées par les droits d'accès aux fichiers et non chiffrées, et aucune copie n'est conservée sur un autre site. Les fichiers que vous téléversez — pièces jointes, documents — sont stockés sur le serveur et ne font pas partie des sauvegardes : conservez votre propre copie des fichiers que vous ne pouvez pas vous permettre de perdre.
- **Identifiants de base de données distincts pour chaque espace de travail** : non en place. Chaque espace de travail a sa propre base de données, mais l'application accède à toutes avec le même compte de base de données.
- **Chiffrement des adresses de canaux** : non en place. Les adresses et les secrets de signature des canaux que vous connectez pour les notifications (Slack, Microsoft Teams, Discord, Google Chat, Telegram, webhooks) sont stockés sans chiffrement supplémentaire dans la base de données de l'espace de travail.

Lorsque l'une de ces mesures sera mise en place, elle passera dans les sections ci-dessus et la version du présent document sera relevée.

9. Votre part

Au moins la moitié de la sécurité d'un logiciel de travail se joue en dehors du logiciel :

- utilisez des mots de passe robustes et ne réutilisez pas ceux d'autres services ;
- créez un utilisateur par personne : les comptes partagés rendent impossible de savoir qui a fait quoi ;
- accordez les autorisations minimales nécessaires et **retirez immédiatement** les personnes qui partent ;
- régénérez les liens publics si vous soupçonnez qu'ils ont circulé, et révoquez les clés d'API que vous n'utilisez plus ;
- tenez à jour les appareils depuis lesquels vous vous connectez ;
- exportez régulièrement les données que vous ne pourriez pas vous permettre de perdre.

Le texte intégral à jour est toujours disponible à l'adresse <https://work.omegasuiteapp.com/legal/security?lang=fr>.
Pour toute question : amministrazione@outlinedigital.it.