Matrice des droits (Règles d'accès par rôle)

Pages	Utilisateur anonyme	Utilisateur connecté	Administrateur
Landing Page (Présentation entreprise et CTA)	X	X	X
Page de la liste des espaces	X	X	X
Page de connexion	X	X	X
Page d'inscription	X	X	X
Page RGPD	X	X	X
Page avec les détails d'un espace		X	X
Planning d'un espace		X	X
Page pour confirmer la réservation		X	X
Page pour le paiement de la réservation		X	X
Page de gestion du profil		X	X
Page de l'historique du profil		X	X
Page de gestion des espaces (CRUD)			X
Page de modification d'un espace			X

RGPD : bases légales, durée conservation, droits utilisateurs

Date prise d'effet : 12 décembre 2025

1. Responsable du traitement

Le responsable du traitement des données à caractère personnel est :

Worknest
Worknest – Société par actions simplifiée (SAS)
28 Place de la Bourse, Paris, 75002
Email : support@worknest.fr

2. Données collectées

Dans le cadre de l'utilisation de la plateforme Worknest, les données suivantes peuvent être collectées :

Données fournies directement par l'utilisateur

- adresse e-mail
- nom et prénom
- adresse postale
- organisation
- identifiants de connexion (mot de passe)

Données techniques

- adresse IP
- données de connexion
- journaux techniques (logs)
- données de navigation

3. Finalités du traitement

Les données personnelles sont collectées pour les finalités suivantes :

- création et gestion des comptes utilisateurs,

- authentification et sécurisation des accès,
- réservation d'espaces,
- gestion des paiements,
- amélioration et maintenance de la plateforme,
- détection d'anomalies et d'incidents de sécurité.

4. Fondement juridique du traitement

Les traitements mis en œuvre par Worknest reposent sur :

- l'**exécution d'un contrat** (création de compte, réservation, paiement),
- le **respect d'obligations légales** (facturation),
- l'**intérêt légitime** de Worknest (sécurité, amélioration du service),
- le **consentement**, lorsque requis (ex. cookies non essentiels).

5. Sécurité des données

Worknest met en œuvre des mesures techniques adaptées au stade de développement du projet afin de protéger les données personnelles :

- les mots de passe sont **hachés de manière irréversible**,
- les données nécessaires à la logique métier sont **chiffrées avant stockage**,
- les communications sont protégées par des protocoles sécurisés,
- le SGBD utilisé (MySQL) permet la **journalisation des connexions** et la traçabilité des accès.

À mesure que la plateforme évoluera vers une mise en production à plus grande échelle, des **audits de sécurité** et des **réévaluations régulières** des mesures de protection seront mis en place afin d'adapter le niveau de sécurité aux risques identifiés.

6. Sous-traitants

Worknest peut faire appel à des sous-traitants pour certains traitements, notamment :

- **Stripe** pour la gestion des paiements (tokenisation des données bancaires).

Les sous-traitants n'agissent que sur instruction de Worknest et dans le respect du RGPD.

7. Conservation des données

Les données personnelles sont conservées uniquement pour la durée nécessaire aux finalités poursuivies :

- données de compte : durée de vie du compte,
- données de facturation : durée légale applicable,
- données techniques : durée limitée à des fins de sécurité et d'analyse.

8. Droits des utilisateurs

Conformément au RGPD, les utilisateurs disposent des droits suivants :

- droit d'accès,
- droit de rectification,
- droit à l'effacement,
- droit à la limitation,
- droit d'opposition,
- droit à la portabilité des données,
- droit de retirer leur consentement à tout moment.

Toute demande peut être adressée à : **support@worknest.fr**

9. Modification de la politique

La présente politique de confidentialité peut être amenée à évoluer. Toute modification sera publiée sur cette page avec mise à jour de la date d'entrée en vigueur.

Cartographie des données (usuelles / sensibles)

	Responsable du traitement ?	Quoi ?	Pourquoi ?	Où ?	Jusqu'a quand ?	Comment ?
Page de connexion	Worknest	- email - mot de passe	Identification de l'utilisateur	Stockées dans la base de données	Jusqu'à 1 mois après la suppression du compte, en accord avec l'**article 12 §2 RGPD**	hashage et cryptage
Page d'inscription		- email - nom - prenom - adresse postale - organisation - mot de passe	Enregistrement du nouveau prospect			
Planning d'un espace		- email - mot de passe	Identification de l'utilisateur			
Page pour confirmer la réservation		- email - mot de passe	Identification de l'utilisateur			
Page pour le paiement de la réservation	Worknest + Stripe	- informations bancaires	Procéder au paiement	Chaque continent (voir plus)		Tokenisation **Chiffrement de bout en bout (E2EE)**
Page de gestion du profil	Worknest	- email - nom - prenom - adresse postale - organisation - mot de passe	Maintenir les informations du clients	Stockées dans la base de données		hashage et cryptage
Page de l'historique du profil		- informations bancaires - email - nom - prenom - adresse postale - organisation - mot de passe	Pouvoir accéder aux précédentes réservations et aux factures			

Méthodes de sécurité

Worknest étant actuellement en phase de développement, l'effort de sécurisation des données se concentre, dans un premier temps, sur la mise en œuvre des exigences minimales nécessaires à la protection des données personnelles.

Les données collectées sont stockées en base de données après application de mécanismes de sécurité adaptés à leur usage :
– les données destinées à être réutilisées dans la logique métier font l'objet d'un **chiffrement**,
– les données sensibles ne nécessitant aucune restitution, telles que les mots de passe, sont **hachées de manière irréversible**.

Par ailleurs, le système de gestion de base de données utilisé (MySQL) permet la **traçabilité des accès** grâce à des **journaux de connexion**, contribuant ainsi à la détection d'accès non autorisés et au suivi des opérations effectuées sur la base de données.

À mesure que le projet évoluera vers une phase de mise en production et de montée en charge, des **audits de sécurité** ainsi que des **réévaluations régulières des mesures de protection** seront mis en place afin de garantir un niveau de sécurité adapté aux risques, conformément au principe d'amélioration continue de la sécurité des données.