



Sécurité et confidentialité des dossiers clients

Ce que deviennent les données de vos clients, qui peut les voir, et ce que vous pouvez régler. Chaque chiffre de cette page est celui que l'application applique.

France	10 min	365 jours	48 h
Hébergement chez OVHcloud, à Gravelines	Code à usage unique sur chaque nouvel appareil	Journal d'accès conservé pour chaque dossier	Pour vous prévenir d'une violation de données

Hébergement

- L'application et sa base de données sont hébergées en France, chez OVHcloud (centre de données de Gravelines).
- Les documents des dossiers sont stockés chez Cloudflare R2, dans un espace réservé à l'Union européenne.
- La base de données est sauvegardée chaque jour ; chaque sauvegarde est conservée 7 jours, dans l'Union européenne (Cloudflare R2).
- Cloudflare est une société américaine : son accord de traitement repose sur les clauses contractuelles types de la Commission européenne et sur le Data Privacy Framework. La liste complète de nos sous-traitants figure dans la politique de confidentialité.

Chiffrement

- Toutes les connexions sont chiffrées (HTTPS), et le navigateur est tenu de ne jamais se connecter autrement (HSTS).
- Les documents et les sauvegardes sont chiffrés au repos par Cloudflare R2, l'hébergeur de stockage.
- Un document d'un dossier ne s'ouvre qu'après identification, et l'application vérifie à chaque ouverture que la personne a le droit de le lire. Un lien d'export est propre à une demande et expire après 7 jours.

Accès de vos intervenants

- Vos intervenants n'ont aucun mot de passe à retenir, et leur lien personnel ne suffit pas : un code à usage unique, valable 10 minutes, leur est envoyé par e-mail sur chaque nouvel appareil.
- La durée pendant laquelle un appareil reste reconnu se règle espace par espace.
- Votre équipe peut activer la double authentification (application ou clé d'accès), et un espace peut l'exiger de tous ses membres.
- Retirer quelqu'un d'un dossier, ou supprimer son contact, révoque immédiatement son accès.



Qui voit quoi

- Chaque publication a ses lecteurs : ce que voit une personne se décide publication par publication.
- Les notes internes restent invisibles des intervenants, exports compris.
- Une publication confidentielle (offre de prêt, pièce d'identité, avis d'imposition...) n'est lue que par l'équipe et par les intervenants qu'elle nomme ou mentionne : jamais via « Tous les intervenants », ni par un accès complet, ni par une mention en commentaire.
- Un intervenant à accès limité ne voit que ce qui le nomme ou le mentionne, et les jalons. L'espace peut lui retirer l'export, et couper son accès à la clôture du dossier.

Traçabilité

- Chaque dossier a son journal d'accès : qui l'a ouvert, quel document a été consulté ou téléchargé, quand et depuis quel appareil. Il est conservé 365 jours et s'exporte en CSV.
- Tant que l'option « Vu par » est active, vous savez qui a lu chaque publication ; le journal d'accès dit qui a consulté chaque document.

Export et suppression

- Chaque participant télécharge une archive de son dossier (PDF et documents), telle qu'il le voit. L'espace peut retirer l'export aux intervenants à accès limité, jamais aux autres.
- Si vous supprimez votre espace, vos intervenants en sont prévenus 30 jours à l'avance pour récupérer leurs dossiers ; les données et les documents sont ensuite effacés, et les sauvegardes les conservent encore 7 jours au plus.
- Aucun traceur publicitaire. La mesure d'audience est hébergée dans l'Union européenne, sans cookie.

Incidents et engagements

- Si une violation de données vous concerne, vous en êtes informé dans les 48 heures qui suivent sa découverte.
- Notre accord de traitement des données (article 28 du RGPD) fait partie de nos conditions générales d'utilisation.
- Une question sur la sécurité ou sur vos données : dpo@oxpeo.com.

Document généré le 7 octobre 2026 — <https://kolinea.com/fr/security>