



Security and privacy of client folders

What happens to your clients' data, who can see it, and what you can set. Every figure on this page is the one the application enforces.

France	10 min	365 days	48 h
Hosted by OVHcloud, in Gravelines	One-time code on every new device	Access log kept for every folder	To tell you about a data breach

Hosting

- The application and its database are hosted in France, by OVHcloud (Gravelines data centre).
- Folder documents are stored by Cloudflare R2, in storage restricted to the European Union.
- The database is backed up every day; each backup is kept 7 days, in the European Union (Cloudflare R2).
- Cloudflare is an American company: its data processing agreement relies on the European Commission's standard contractual clauses and on the Data Privacy Framework. The full list of our sub-processors is in the privacy policy.

Encryption

- Every connection is encrypted (HTTPS), and browsers are required never to connect otherwise (HSTS).
- Documents and backups are encrypted at rest by Cloudflare R2, the storage provider.
- A folder document only opens after identification, and the application checks each time that the person may read it. An export link belongs to one request and expires after 7 days.

Access for your contacts

- Your contacts have no password to remember, and their personal link is not enough: a one-time code, valid 10 minutes, is e-mailed to them on every new device.
- How long a device stays recognised is set workspace by workspace.
- Your team can turn on two-factor authentication (app or passkey), and a workspace can require it of all its members.
- Removing someone from a folder, or deleting their contact, revokes their access at once.

Who sees what

- Every publication has its readers: what a person sees is decided publication by publication.
- Internal notes stay hidden from contacts, exports included.



- A confidential publication (loan offer, ID, tax notice...) is only read by the team and the contacts it names or mentions: never through "Every contact", never through full access, never through a mention in a comment.
- A contact with limited access only sees what names or mentions them, and the milestones. The workspace can withdraw their export, and cut their access when the folder is closed.

Traceability

- Every folder has its access log: who opened it, which document was viewed or downloaded, when and from which device. It is kept 365 days and exports to CSV.
- While the "Seen by" option is on, you know who read each publication; the access log shows who viewed each document.

Export and deletion

- Every participant downloads an archive of their folder (PDF and documents), as they see it. The workspace can withdraw the export from contacts with limited access, never from the others.
- If you delete your workspace, your contacts are told 30 days ahead so they can take their folders; the data and documents are then erased, and backups still hold them for 7 days at most.
- No advertising tracker. Audience measurement is hosted in the European Union, without cookies.

Incidents and commitments

- If a data breach concerns you, you are told within 48 hours of its discovery.
- Our data processing agreement (GDPR article 28) is part of our terms of use.
- A question about security or your data: dpo@oxpeo.com.

Document generated on October 7, 2026 — <https://kolinea.com/en/security>