



Data processing agreement

Annex to the terms of use — GDPR article 28

Last revised on September 29, 2026 8:00 AM

1. Purpose

This agreement is part of the [terms of use](#) of Kolinea. It sets out how OXPEO ("the processor") processes, on behalf of the customer who opened a workspace on Kolinea ("the controller"), the personal data that customer entrusts to it.

The parties undertake to comply with Regulation (EU) 2016/679 of 27 April 2016 ("GDPR") and the amended French law no. 78-17 of 6 January 1978. Where the terms of use and this agreement disagree on the protection of personal data, this agreement prevails.

2. Parties

- **Processor:** OXPEO, with a share capital of €1,000, *registration in progress*, publisher of Kolinea. Data protection contact: dpo@oxpeo.com.
- **Controller:** the professional, legal person or association that accepted the terms of use and opened a workspace on Kolinea.

3. Description of the processing

- **Purpose:** providing the Kolinea service — folders shared between the controller, its team, its clients and the contributors it invites.
- **Nature of the operations:** hosting, storage, consultation, transmission to the people the controller designates, sending notification and reminder e-mails, generating exports, logging accesses, erasure.
- **Data subjects:** the controller's clients, the contributors it invites (subcontractors, partners, advisers), the contacts in its address book and the members of its team.
- **Data processed:** identity and contact details (name, e-mail address, and whatever the controller adds to a contact's record); folder content (messages, documents shared, answers to requests); connection data and access log (IP address, browser, date and subject of the access).
- **Duration:** that of the contract. When the workspace is deleted, the people on its folders are told 30 days ahead, then the data and documents are erased. The access log is kept 365 days; backups are kept 7 days.

The controller alone chooses what it puts in its folders. It is up to the controller not to store data whose processing would require safeguards this agreement does not provide, health data in particular.

4. Obligations of the processor

The processor undertakes to:

- **Instructions:** process the data only for the purpose above and on the controller's documented instructions — the terms of use, this agreement and the settings the controller chooses in its workspace are instructions. If it considers an instruction infringes the law, it informs the controller immediately.
- **Confidentiality:** ensure that the people authorised to process the data are bound to confidentiality and receive the necessary data protection training.
- **Security:** implement the technical and organisational measures described on the [Security and privacy](#) page, including encrypted connections, access control on every document, a code confirming every new device, two-factor authentication and the access log.
- **Sub-processors:** use only the sub-processors listed in the [privacy policy](#), impose the same data protection obligations on them, and inform the controller beforehand of any addition or replacement, giving it the opportunity to object.
- **Data subjects' rights:** help the controller answer requests to exercise rights — the service lets it export a folder, remove a participant, edit, merge or delete a contact — and forward without delay any request received directly.
- **Personal data breaches:** notify the controller of any personal data breach that concerns it within at most 48 hours of becoming aware of it, with all the information the controller needs to notify the supervisory authority and inform the data subjects where required.
- **Assistance:** help the controller carry out a data protection impact assessment and, where needed, the prior consultation of the supervisory authority.
- **End of processing:** at the end of the contract, allow the folders to be exported during the notice period, then erase the data and documents; copies held in backups disappear as the backups rotate, at the latest 7 days later.
- **Documentation and audits:** make available to the controller the documentation needed to demonstrate compliance with these obligations, and allow for and contribute to audits, including inspections, conducted by the controller or another auditor it mandates.
- **Record:** keep a record of the categories of processing activities carried out on the controller's behalf.

5. Location and transfers

The data is hosted in the European Union. Among the sub-processors, Cloudflare is a company incorporated in the United States: its involvement is governed by the European Commission's standard contractual clauses and by the Data Privacy Framework. The privacy policy gives the role and location of each sub-processor.



6. Obligations of the controller

- Have a legal basis for every piece of data it entrusts to the service and inform the data subjects of the processing.
- Document in writing any instruction that does not follow from the terms of use, this agreement or its workspace settings.
- Ensure, beforehand and throughout the processing, that the processor complies with its GDPR obligations.

7. Term

This agreement applies for as long as the processor processes data on the controller's behalf, and ends when that data is erased.

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