PRIVACY · OVERVIEW

Privacy at Jump.

Jump is the AI meeting platform built for financial professionals. We are committed to protecting our customers' data by aligning our privacy program with GDPR, PIPEDA, CCPA and other relevant privacy laws and regulations.

PRIVACY PROGRAM

Governance

Jump's alignment to GDPR and PIPEDA objectives is tracked continuously through our privacy program, with controls mapped across **data subject rights, breach notification and response, data retention and disposal, and cross-border transfer safeguards.**

Personnel complete privacy training upon hire and annually thereafter, and acknowledge Jump's internal privacy policy governing the handling of personal information.

Privacy by Design

Privacy is built into Jump's systems from the design stage. We conduct privacy impact assessments for new processing activities that carry elevated risk to data subjects, apply data minimization and access controls by default, and encrypt personal data at rest and in transit.

DATA HANDLING

Data Processing & Training

Jump processes customer data only to provide the contracted service and only in accordance with the customer's documented instructions. **We do not use customer data for any other purpose, including training AI models.**

Data Hosting

Jump supports US, Canada, and EU hosting regions. Customer data, including backups, is stored in the region designated.

Sub-processors

Jump partners with select third parties to help provide our services, performing due diligence prior to onboarding and on an ongoing basis.

Our sub-processor list is published in our Trust Center, where we publish changes in Updates. Customers may opt in to receive email notifications for Updates. We provide **30 days written notice** before adding or replacing a sub-processor.

PRIVACY INCIDENTS

Breach Notification

Jump notifies affected customers of a security incident, including incidents involving personal data, **no later than 72 hours** after confirmation. We cooperate with affected customers and, where necessary, supervisory authorities and regulators to support their own notification obligations.

DATA SUBJECT RIGHTS

Supporting Requests

Jump supports data subject rights requests and assist customers in fulfilling their own obligations. We do not respond directly to a data subject request without the customer's prior written authorization, unless required by law. Data subjects may submit requests via the method outlined in Jump's Privacy Policy.

Workspace Deletion

Admin users may request workspace deletion by submitting a help request within the application or via help@jumpapp.com. After **30 days**, the content is permanently deleted and can no longer be recovered.

PREFERENCES & AGREEMENTS

Cookie & Consent Management

Visitors of our marketing site and users of the Jump application may manage cookie and tracking preferences at any time — via **Manage Cookies** in the website footer and User Preferences in the application, respectively.

Jump also honors the Global Privacy Control (GPC) "do not track" signal.

Data Processing Agreement

Jump relies on **Standard Contractual Clauses (SCCs)** to safeguard personal data transfers from the EU to countries outside the EU. Our SCCs are included in our standard Data Processing Agreement (DPA), which governs how we process personal data as a processor.

PRIVACY & LEGAL RESOURCES

Transparency

We are committed to being transparent about how we collect, process, store, and use personal data:

- Jump's Privacy Policy
- Jump's MSA
- Jump's DPA

Please send any privacy-related questions, requests, or concerns to privacy@jumpapp.com.