Privacy & Data Protection Overview

Version: 2.0
Last Updated: 1st September 2026
Classification: Public

Privacy & Data Protection Overview

This document describes Concord's privacy governance framework, data processing practices, and privacy controls. Read together with our Privacy Policy, Master Services Agreement, and Data Processing Addendum (DPA).

Our Privacy Commitment

Concord processes personal information responsibly, transparently, and in accordance with applicable privacy laws and contractual obligations, guided by lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

Roles and Responsibilities

Depending on the services provided, the customer generally acts as Data Controller (or equivalent), determining the purposes and means of processing; Concord generally acts as Data Processor (or equivalent), processing personal information only on the customer's documented instructions except where required by law. Specific responsibilities are set out in the applicable DPA.

Categories of Data We Process

Depending on how a customer uses the platform: user account information, business contact information, authentication and access logs, AI governance records, workflow and approval records, uploaded documents, customer-generated prompts and AI outputs, and technical diagnostics. Customers determine what information they submit to the Services.

Purpose of Processing

Personal information is processed only as reasonably necessary to provide and maintain the Services, authenticate users, process customer requests, deliver AI-enabled functionality, support governance workflows, secure the platform, monitor performance, respond to support requests, comply with legal obligations, and improve service quality using aggregated or de-identified information where appropriate.

Data Minimization

Concord collects and processes only the information reasonably necessary to provide the Services. Customers are encouraged to avoid submitting unnecessary personal information and to configure workflows consistent with their own data governance policies.

Data Retention and Deletion

Customer data is retained only as long as necessary to provide the Services, fulfil contractual obligations, meet legal or regulatory requirements, or support legitimate operational needs such as backup and security investigation. On termination, customer data is returned or deleted per the applicable contract and DPA. Customers may request deletion consistent with the MSA and applicable terms; certain information may be retained where required by law or for legitimate business purposes.

International Data Transfers

Concord's application infrastructure runs on Google Cloud Platform, primarily in the Canada (Toronto) region. Where cross-border transfer occurs, whether through subprocessor use or a customer's own configuration, Concord applies contractual, technical, and organizational safeguards appropriate to applicable privacy law. Customers with specific data-residency requirements should discuss them with us during procurement.

Subprocessors

Concord uses a small set of carefully selected subprocessors:

Subprocessor	Function
Google Cloud Platform	Application hosting, compute, managed database, and object storage
Google Gemini (via Vertex AI, Canada)	Primary AI/LLM processing
Azure OpenAI Service (Canada)	Fallback AI/LLM processing, invoked only if the primary provider is unavailable
SendGrid	Transactional email delivery

An up-to-date subprocessor list is available on request or through the Subprocessor & Data Residency Schedule. All subprocessors are subject to contractual security and privacy obligations

---

Security Safeguards

Encryption in transit and at rest, role-based access control, multi-factor authentication for privileged access, secure development practices, security monitoring, vulnerability management, incident response, and audit logging. See the Security Overview.

Privacy by Design

Data minimization, access controls, secure defaults, role-based permissions, audit logging, encryption, and data lifecycle management are built into the platform's design and operation, not addressed only after implementation.

Data Subject Rights

Where applicable law provides individuals with privacy rights — access, correction, deletion, restriction, portability, objection — requests should ordinarily be directed to the

customer as Data Controller. Concord provides reasonable assistance where required by contract or law.

AI and Personal Information

Customer prompts are processed only as necessary to provide the Services, under the same contractual and technical safeguards as other customer information. Concord does not knowingly use identifiable customer data or prompts to train publicly available foundation AI models without the customer's prior authorization.

Incident Response

Concord's privacy and security incident procedures cover identification, assessment, containment, investigation, remediation, customer notification where contractually required, and post-incident review.

Compliance Alignment

Concord's privacy program is designed with reference to PIPEDA (Canada), GDPR (EU), UK GDPR, CCPA/ CPRA (California), and ISO/IEC 27701. References to these frameworks indicate alignment objectives, not claims of certification or regulatory approval, unless expressly stated.

Shared Responsibility

Concord is responsible for: processing data per customer instructions, security safeguards, subprocessor management, and privacy governance processes.

Customers are responsible for: the lawful basis for processing, notices to individuals, consent where applicable, platform configuration, user access management, and responding to data subject requests.

Additional Information

Available on request, subject to confidentiality obligations: Privacy Policy, DPA, Subprocessor & Data Residency Schedule, Security Overview, and AI Governance & Responsible AI Overview.
