CORPUS DATA POLICY & PRIVACY POLICY

Last Updated: January 2026

———

INTRODUCTION

Corpus is a web-based literary agency and publishing operations management platform designed to handle sensitive intellectual property, contractual data, financial information, and personal data across global jurisdictions. This Data Policy and Privacy Policy (together, the "Policies") are drafted to reflect maximum global data-protection standards, prioritizing data sovereignty, confidentiality, integrity, and lawful processing.

These Policies apply to all users, clients, partners, publishers, agencies, authors, contractors, and visitors ("Data Subjects") who interact with Corpus ("the Platform", "we", "our", "us").

Corpus is architected under a privacy-first, zero-exploitation, non-commercial data model.

———

CORE DATA PROTECTION PRINCIPLES

Corpus adheres to the following foundational principles:

1. Data Ownership by the Client – All uploaded or generated data remains the exclusive property of the client.
2. Purpose Limitation – Data is processed strictly for explicitly defined operational purposes.
3. Data Minimization – Only the minimum data necessary is collected or processed.
4. No Data Brokerage – Data is never sold, leased, shared, or monetized.
5. Confidentiality by Design – Security is embedded at architectural, procedural, and contractual levels.
6. Geographic Neutrality – Data protections apply regardless of the user's country.
7. Auditability & Transparency – All data actions are traceable and reviewable.

———

DATA CATEGORIES PROCESSED

Corpus may process the following categories of data:

1. Identity & Account Data
   - Names, email addresses, roles
   - Organizational affiliation
   - Authentication credentials (hashed)

2. Intellectual Property & Content Data
   - Manuscripts, proposals, synopses
   - Contracts, amendments, rights tables
   - Metadata related to literary works

3. Financial & Contractual Data
   - Royalties, advances, currency records
   - Payment schedules (no card storage)
   - Commission calculations

4. Operational & Analytical Data
   - Workflow timestamps
   - Performance metrics
   - Internal notes and system logs

5. Technical Data
- IP addresses (anonymized where possible)
- Device and browser metadata
- Error and security logs

Corpus does not intentionally process special-category personal data unless explicitly required and contractually authorized.

———

LEGAL BASES FOR PROCESSING

Data is processed under one or more of the following lawful bases:
- Performance of a contract
- Legitimate interest (strictly operational)
- Legal obligation
- Explicit user consent (where required)

Corpus does not rely on behavioral profiling, advertising consent, or data resale mechanisms.

———

DATA STORAGE & INFRASTRUCTURE
- Data is stored on dedicated, non-shared infrastructure.
- Logical and physical isolation is enforced between clients.
- Encryption at rest and in transit (industry-grade standards).
- No third-party analytics with data access privileges.

Corpus avoids unnecessary geographic replication and does not relocate data without legal and contractual justification.

———

ACCESS CONTROL & INTERNAL GOVERNANCE
- Role-based access control (RBAC)
- Principle of least privilege
- Multi-factor authentication for administrators
- All access is logged and auditable

No Corpus personnel may access client data without explicit operational necessity and authorization.

———

THIRD-PARTY PROCESSORS

Corpus works only with processors that:
- Comply with GDPR, KVKK, CCPA, and equivalent frameworks
- Are contractually bound by strict confidentiality clauses
- Are prohibited from secondary data usage

A current list of subprocessors may be provided upon request.

———

DATA SHARING POLICY

Corpus:

- ❌ Does NOT sell or rent data
- ❌ Does NOT share data for advertising or AI training
- ❌ Does NOT allow third-party indexing of private content

Data is shared only:

- With explicit user instruction
- Under legal obligation
- To fulfill contracted services

———

AI & AUTOMATION SAFEGUARDS

Where AI-assisted features are used:

- Processing occurs in controlled environments
- No client data is used to train public or third-party models
- Outputs remain client-owned
- Human override is always available

Corpus does not deploy autonomous decision-making with legal or financial consequences without human validation.

———

DATA RETENTION & DELETION

- Data is retained only for the duration of the service relationship
- Clients may request full deletion at any time
- Secure deletion protocols (cryptographic erasure)
- Backups are purged within defined cycles

Post-termination retention is limited to legally required obligations only.

———

DATA SUBJECT RIGHTS (GLOBAL)

All users are granted, regardless of jurisdiction:

- Right to access
- Right to rectification
- Right to erasure (“right to be forgotten”)
- Right to restriction of processing
- Right to portability
- Right to object

Requests are processed within a maximum of 30 days.

———

BREACH RESPONSE & INCIDENT MANAGEMENT

In the event of a data breach:

- Immediate containment and assessment
- Client notification without undue delay
- Regulatory notification where required
- Full incident report and remediation plan

Corpus maintains an internal incident response protocol aligned with ISO 27001 practices.

———

INTERNATIONAL TRANSFERS

Where cross-border data transfers are unavoidable:

- Standard Contractual Clauses (SCCs)
- Equivalent safeguard mechanisms
- No transfer to jurisdictions lacking adequate protection without consent

———

CHILDREN'S DATA

Corpus services are not directed at individuals under 18. No knowing collection of children's data occurs.

———

POLICY GOVERNANCE & UPDATES

- Policies are reviewed periodically
- Material changes are communicated in advance
- Continued use constitutes acknowledgment

———

CONTACT & DATA PROTECTION OFFICER

Privacy inquiries, data requests, and compliance issues may be directed to:

Data Protection Office
Email: info@corpus4agency.com

———

GOVERNING LAW

These Policies are governed by internationally recognized data protection principles and, where applicable, the laws of the user's jurisdiction.

———

FINAL STATEMENT

Corpus is built on the principle that data is not fuel — it is trust. The platform exists to protect intellectual labor, contractual integrity, and institutional memory at a global standard without compromise.