Plain-English Overview (non-binding): This Agreement explains how you (the “Customer”) may use Corpus (the “Service”), how we protect your data, what we each promise, and what happens if things go wrong. The legal terms below control if anything in this overview conflicts with them.

Effective Date: [YYYY-MM-DD]

Provider: [Company Legal Name], a [jurisdiction] company with its principal place of business at [address] (”Provider,” “we,” “us”).

Customer: The entity or person agreeing to these terms (”Customer,” “you”).

Order Form(s): One or more ordering documents referencing this Agreement (each, an “Order”).

1) Definitions

- Affiliate: Entity controlling, controlled by, or under common control with a party.
- Authorized Users: Employees, contractors, or agents whom Customer authorizes to use the Service.
- Customer Data: Data submitted to or collected by the Service on behalf of Customer, including personal data.
- Documentation: User guides, help text, and specs for the Service.
- Service: Provider’s multi-tenant, web-based Corpus application and related hosted components, as further described in the Order and Documentation.
- Sensitive Data: Data needing special protections (e.g., special categories under GDPR, children’s data under 13/16, financial account numbers, precise geolocation, government IDs) unless expressly permitted in writing.
- SLA: The service level and support commitments in Annex C.

2) Service; Access & Use

2.1 Provision. During the Subscription Term set in the Order, Provider will make the Service available in accordance with this Agreement, the Documentation, and the SLA.

2.2 Accounts. Customer is responsible for configuring roles/permissions, keeping credentials confidential, and for all activities under its accounts.

2.3 Restrictions. Customer will not (and will not allow others to): (a) reverse engineer, decompile, or attempt to derive the Service's source; (b) circumvent security; (c) access the Service to build a competing product; (d) use the Service in violation of Annex A (AUP); (e) copy or modify non-open-source components of the Service except as permitted by law.

3) Service Description & Architecture

3.1 What Corpus Is. Corpus is a SaaS platform for literary agencies, publishers, and rights departments, covering submission tracking, rights/contract lifecycle, performance analytics, and notifications. It is hosted in a dedicated Linux/Ubuntu environment and designed as a multi-tenant service with data isolation between tenants.

3.2 Third-Party Services. The Service may interoperate with third-party services (e.g., email/SMS providers, storage, AI services). Customer's use of such third-party services is governed by their terms. Provider is not responsible for third-party services not controlled by Provider. Current subprocessors are listed in Annex B(4) and may change with notice as set forth therein.

4) Customer Responsibilities

4.1 Compliance. Customer will use the Service only in compliance with applicable laws (including privacy and export laws) and the AUP.

4.2 Content & Rights. Customer represents it has all rights to Customer Data and that use of Customer Data with the Service will not infringe third-party rights.

4.3 Security Configuration. Customer is responsible for secure configuration of its users, SSO, API keys, and data classification; Provider will provide reasonable guidance.

5) Intellectual Property; Feedback; Open Source

5.1 Ownership. Except for the rights expressly granted here, Provider retains all IP rights in the Service and Documentation; Customer retains all IP rights in Customer Data.

5.2 License to Use Service. Subject to payment and compliance, Provider grants Customer a non-exclusive, non-transferable right for Authorized Users to access and use the Service during the Subscription Term.

5.3 Feedback. Customer grants Provider a perpetual, irrevocable, royalty-free license to use ideas/feedback to improve the Service, without identifying Customer.

5.4 Open-Source Notices. The Service may include OSS components subject to their licenses. Notices and licenses are provided on request.

6) Data; Privacy; Security

6.1 Ownership & Control. As between the parties, Customer owns and controls Customer Data. Provider acts as a processor/service provider of Customer Data.

6.2 Data Processing Addendum. The DPA in Annex B is incorporated by reference and governs processing of personal data under GDPR, KVKK, CCPA/CPRA, and analogous laws. In case of conflict, Annex B controls regarding personal data.

6.3 Security Program. Provider will maintain administrative, physical, and technical safeguards as described in Annex D (Security Overview), including encryption in transit, role-based access, logging, backups, and vulnerability management.

6.4 Customer Responsibilities. Customer is responsible for lawful collection of personal data, providing notices, and obtaining consents

where required; and for not storing Sensitive Data in the Service unless expressly permitted in the Order.

6.5 Subprocessors. Provider may engage subprocessors per Annex B with appropriate data-protection commitments; Provider remains responsible for their performance.

6.6 Incident Response. Provider will notify Customer without undue delay after becoming aware of a confirmed personal-data breach affecting Customer Data, and will provide information and cooperation as described in Annex B.

7) Confidentiality

7.1 Definition. “Confidential Information” means information disclosed by a party that is marked confidential or should reasonably be considered confidential. Customer Data is Customer’s Confidential Information. The Service and technical information about it are Provider’s Confidential Information.

7.2 Obligations. Each party will: (a) use the other’s Confidential Information only to perform this Agreement; (b) protect it using at least reasonable care; and (c) disclose it only to those who need to know and are bound by similar duties.

7.3 Exclusions. Information that is public, already known, independently developed, or rightfully received without duty of confidentiality is excluded.

7.4 Compelled Disclosure. A party may disclose Confidential Information when legally compelled, after providing notice and cooperation where lawful.

8) Fees; Taxes; Billing; Late Payments

8.1 Fees. Fees are set in the Order and may be based on seats, usage, features, or tiers. Unless stated otherwise, subscriptions auto-renew for successive terms at then-current rates with at least [60] days’ prior notice of price changes.

8.2 Invoices & Payment. Unless otherwise stated, invoices are due within [30] days of invoice date. Late amounts may accrue [1.5%] monthly interest (or the maximum allowed by law, if lower).

8.3 Taxes. Fees are exclusive of taxes. Customer is responsible for all taxes, duties, and withholdings, except for taxes based on Provider's income.

8.4 Non-Payment; Suspension. Provider may suspend the Service for material non-payment after [10] days' notice. Suspension does not waive the obligation to pay.

9) Term; Termination; Suspension

9.1 Term. This Agreement begins on the Effective Date and continues until all Orders expire or are terminated.

9.2 Termination for Cause. Either party may terminate an Order or this Agreement for material breach not cured within [30] days after written notice.

9.3 Convenience. If expressly allowed in an Order, Customer may terminate for convenience as specified therein.

9.4 Suspension. Provider may suspend access immediately for (a) security risk, (b) suspected unlawful activity or AUP violation, or (c) urgent maintenance. Provider will reinstate when the issue is resolved.

10) Data Portability; Return & Deletion

10.1 Self-Service Export. During the Subscription Term and for 30 days after termination, Customer may export Customer Data in common formats (e.g., CSV/JSON/XML) via available tools at no additional cost.

10.2 Assisted Export. On request, Provider can provide commercially reasonable assistance (e.g., custom exports, SFTP packages). Such services are billed at then-current professional-services rates.

10.3 Deletion. Following the export window, Provider will delete or irreversibly anonymize Customer Data from active systems within 60 days and from backups within 90 days, unless longer retention is required by law.

10.4 Retention & Logs. Standard application logs are retained for [90] days unless otherwise stated in an Order.

11) Warranties; Disclaimers

11.1 Mutual. Each party represents that it is duly organized, validly existing, and has authority to enter this Agreement.

11.2 Service Warranty. Provider warrants that the Service will conform materially to the Documentation and that professional services (if any) will be performed in a professional and workmanlike manner.

11.3 Disclaimers. Except as expressly stated, the Service and all related materials are provided “AS IS” and “AS AVAILABLE.” Provider disclaims implied warranties (merchantability, fitness for a particular purpose, non-infringement) to the maximum extent permitted by law. Beta/preview features are provided without warranties.

12) Indemnification

12.1 By Provider (IP). Provider will defend and indemnify Customer against third-party claims alleging that the Service, as provided by Provider, infringes a third party’s IP right, and will pay any final damages and reasonable costs. Provider may (at its option) modify the Service, procure a license, or terminate the affected Order with a prorated refund. This does not apply to claims arising from Customer Data, third-party services, or unauthorized use.

12.2 By Customer. Customer will defend and indemnify Provider against claims arising from Customer Data, use in violation of the AUP/law, or combinations not authorized by Provider.

12.3 Procedure. The indemnified party must promptly notify the indemnifying party, allow control of the defense, and provide reasonable cooperation.

13) Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW: (a) NEITHER PARTY IS LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, LOSS OF PROFITS, REVENUE, OR DATA, EVEN IF ADVISED OF THE POSSIBILITY; AND (b) EACH PARTY'S TOTAL LIABILITY IN ANY 12-MONTH PERIOD IS CAPPED AT THE AMOUNTS PAID OR PAYABLE BY CUSTOMER FOR THE SERVICE UNDER THE APPLICABLE ORDER IN THAT PERIOD. THESE LIMITATIONS DO NOT APPLY TO FEES DUE, INFRINGEMENT OF IP RIGHTS, BREACH OF CONFIDENTIALITY, OR INDEMNITY OBLIGATIONS.

14) Publicity

Provider may use Customer's name and logo to identify Customer as a customer of Corpus on websites and marketing materials, subject to Customer's reasonable brand guidelines. Any public case study or press release requires Customer's prior written consent.

15) Compliance; Export; Sanctions; Anti-Bribery

Each party will comply with applicable anti-corruption, export control, and sanctions laws (including U.S., U.K., and EU regimes). Customer represents that it is not a sanctioned person and will not use the Service in prohibited jurisdictions. Each party will maintain policies prohibiting bribery and improper payments.

16) Changes to Service and Terms

Provider may improve or modify the Service provided such changes do not materially reduce core functionality during a Subscription Term. Provider may update these terms from time to time; material adverse changes will be notified at least 30 days in advance and will not apply retroactively to a current Subscription Term unless required by law.

17) Force Majeure

Neither party is liable for failures beyond its reasonable control (e.g., acts of God, labor disputes, internet failures, outages of third-party hosting providers, government actions), provided it uses reasonable efforts to mitigate and resume performance.

18) Notices

Legal notices must be in writing and sent to the addresses in the Order (and legal@ [Provider Domain] for Provider) and are deemed given upon receipt. Routine Service communications may be by dashboard or email.

19) Governing Law; Venue

This Agreement is governed by the laws of Türkiye (excluding conflict-of-laws rules). Courts of İstanbul, Türkiye shall have exclusive jurisdiction. The U.N. Convention on Contracts for the International Sale of Goods does not apply. (If arbitration is preferred, replace with an ICC/ ISTAC arbitration clause.)

20) Assignment; Subcontracting

Neither party may assign this Agreement without the other's consent, except to an Affiliate or in connection with a merger, acquisition, or sale of substantially all assets, provided the assignee assumes all obligations. Provider may subcontract obligations but remains responsible for performance.

21) Entire Agreement; Order of Precedence

This Agreement, the Order(s), and Annexes are the entire agreement. In case of conflict, the following order of precedence applies: (1) Order, (2) Annex B (for personal data matters), (3) this Agreement, (4) Annexes A/C/D, (5) Documentation.

22) Severability; Waiver; Independent Contractors

If a provision is unenforceable, it will be modified to the minimum extent necessary; the remainder remains in effect. Failure to enforce is not a waiver. The parties are independent contractors.

ANNEX A — ACCEPTABLE USE POLICY (AUP)

1. No Illegal/Abusive Use. Do not use the Service for unlawful, infringing, defamatory, harassing, or fraudulent activity.
2. Security. Do not probe, scan, or test vulnerability of the Service or bypass security controls. Do not introduce malware or use the Service to propagate it.
3. Email/Messaging. No spam, unsolicited bulk messages, or content that violates messaging laws (e.g., CAN-SPAM, e-Privacy, KVKK marketing rules).
4. Sensitive Data. Do not upload Sensitive Data without a written exception in the Order.

5. Resource Abuse. Do not use automated means to overload or materially degrade the Service.
6. IP Rights. Do not upload content that infringes third-party IP rights; promptly respond to takedown notices.
7. Interference. Do not access the Service via any interface other than the intended UI/API.

Provider may investigate suspected violations and suspend or terminate access for violations per Section 9.

ANNEX B — DATA PROCESSING ADDENDUM (DPA)

(Processor/Service Provider Terms under GDPR, KVKK, CCPA/CPRA, and analogous laws)

B1. Roles. Customer is Controller/Business; Provider is Processor/Service Provider.

B2. Scope & Instructions. Provider processes Customer personal data solely per Customer's documented instructions (this Agreement, Orders, and Customer's configuration) for providing the Service and related support.

B3. Nature & Purpose. Hosting, storage, indexing, analytics on operational metadata, and communications necessary to deliver the Service. Categories of data subjects typically include Customer's staff, contractors, authors, publishers, and business contacts; categories of data typically include identifiers, professional details, contact information, usage metadata.

B4. Subprocessors. Provider maintains a list of subprocessors (e.g., hosting, email delivery, monitoring, AI services). Provider will provide notice of changes and allow Customer to object on reasonable data-protection grounds. If unresolved, Customer may terminate the affected Order for convenience with a prorated refund.

B5. Security Measures. See Annex D. Provider will implement appropriate technical and organizational measures (TOMs) including encryption in transit, access controls, least-privilege, audit logging, backups, and business continuity.

B6. Confidentiality. Provider ensures personnel are bound by confidentiality and trained on data protection.

B7. Personal-Data Breach. Provider will notify without undue delay after confirming a breach impacting Customer Data and will provide necessary information for Customer's legal obligations.

B8. Assistance. Provider will assist with data-subject requests (access, correction, deletion, portability, objection) and with DPIAs and consultations as reasonably necessary.

B9. International Transfers. If personal data is transferred outside the EEA/UK/Türkiye to a country without adequate protection, Provider will implement appropriate safeguards, such as EU Standard Contractual Clauses, UK Addendum, or KVKK-compliant mechanisms.

B10. Audits. Upon reasonable notice, Customer may review available security documentation and audit reports (e.g., penetration tests, policies). For on-site audits, Customer must provide 30 days' notice and conduct during business hours without unreasonably disrupting operations; limits and NDAs apply.

B11. Deletion/Return. Upon termination, Provider will return or delete personal data per Section 10.

B12. CCPA/CPRA. Provider will not: sell or share personal information; retain, use, or disclose it for purposes beyond those specified; or combine it with other data except as permitted for the Service.

ANNEX C — SERVICE LEVEL AGREEMENT & SUPPORT POLICY

C1. Availability. Target monthly uptime: 99.5% (excluding Maintenance Windows and Exclusions below).

C2. Maintenance Windows. Planned maintenance typically occurs Sundays 02:00–04:00 Europe/Istanbul with at least 72 hours notice for

non-urgent changes; urgent security patches may occur with shorter notice.

C3. Exclusions. SLA does not apply to outages caused by: Customer systems, third-party services outside Provider's control, force majeure, AUP violations, or scheduled maintenance within the window.

C4. Credits. If monthly uptime falls below target, Customer may request service credits within 30 days of month-end:

- 99.0–99.5%: 5% of monthly fee
- 98.0–98.99%: 10%
- 95.0–97.99%: 20%
- <95.0%: 30%

Credits apply to future invoices and are the sole remedy for SLA breaches.

C5. Support Hours & Channels. Business-hours email/ticket support [09:00–18:00 Europe/Istanbul, Mon–Fri, excluding local holidays].

C6. Response Targets. P1 (Service down): 1 business hour; P2 (major function impaired): 4 business hours; P3 (minor): 1 business day; P4 (how-to): 2 business days. Targets are not guarantees.

C7. Backups & DR. Daily encrypted backups retained 7 days rolling; disaster-recovery objective: RPO 24h, RTO 24–48h (targets).

C8. Pen-Testing. Annual penetration testing and remediation tracking. Summary reports available under NDA.

ANNEX D — SECURITY OVERVIEW (TOMs)

- Access Control: SSO/2FA support (where available), RBAC, least privilege, quarterly access reviews.
- Encryption: TLS in transit; at-rest encryption for databases and backups using industry-standard ciphers.
- Segregation: Logical tenant isolation; separate production and staging; secrets managed via secure vaulting.
- Monitoring & Logging: Centralized logs, alerting, anomaly detection, time-synced systems.
- Vulnerability & Patch Management: Regular scanning, prioritized patching for critical issues, emergency patch process.

- Secure SDLC: Code reviews, dependency checks, environment hardening, change control with approvals.
- Physical Security: Data centers with controlled access, surveillance, and environmental safeguards (via hosting provider).
- Employee Practices: Confidentiality agreements, security awareness training, device management.
- Incident Response: Documented playbooks, designation of incident commander, post-mortems for significant incidents.
- Data Lifecycle: Classification guidance, retention schedules, secure deletion, and export tools as in Section 10.

OPTIONAL ADDENDA (Attach if desired)

- Order Form Template (pricing, term, seats, features).
- Professional Services SOW (if any).
- Beta Program Terms.
- AI Features Disclosure (model providers, prompts/outputs handling, opt-in/opt-out).

Implementation Notes (to customize before use)

- Replace bracketed placeholders (e.g., [30], [Company Legal Name]).
- Confirm governing law/venue; consider arbitration if preferred.
- Align SLA numbers to your actual ops; ensure support hours/DR targets match reality.
- Attach subprocessor list and update procedure.
- Review DPA terms with counsel for GDPR/KVKK/CCPA specifics, including legal bases, SCCs, and any local registrations if applicable.
- Ensure your product UI exposes export and deletion controls as promised.

Disclaimer: This is a comprehensive template intended to protect both parties, but it is not legal advice. Have qualified counsel review and adapt it to your business, jurisdictions, and actual operating practices before publishing.