CoreSR Inc.
c/o LaBarge Weinstein LLP, 800-515 Legget Drive, Kanata, ON K2K 3G4, Canada
help@coresr.ai · coresr.ai

PUB-004 · Version 1.4
Effective: 2026-11-17
Public Procurement & Governance

Data Processing Addendum (PIPEDA & GDPR Article 28)

Public Endpoint: https://coresr.ai/api/public/dpa
Legal, Privacy & Security Contacts: legal@coresr.ai · security@coresr.ai

This Data Processing Addendum ("**DPA**"), including Annexes I, II, and III, forms part of the Master Subscription Agreement, Institutional Order Form, or Terms of Service ("**Principal Agreement**") between **CoreSR Inc.**, a corporation organized under the laws of Canada with registered corporate address at c/o LaBarge Weinstein LLP, 800-515 Legget Drive, Kanata, ON K2K 3G4, Canada ("**CoreSR**" or "**Processor**"), and the institutional, organizational, or commercial customer identified in the Principal Agreement or signature block below ("**Customer**" or "**Controller**").

This DPA is pre-drafted for execution without bespoke redlining and satisfies:

1. **Canadian Federal & Provincial Privacy Law:** The *Personal Information Protection and Electronic Documents Act* (**PIPEDA**, S.C. 2000, c. 5, Schedule 1, Principle 4.1.3 — Accountability for Third-Party Processing, and Principle 4.7 — Safeguards) and substantially similar provincial private-sector statutes; and
2. **European, UK & Swiss Data Protection Law: Article 28** of Regulation (EU) 2016/679 (**GDPR**), the UK GDPR, and the Swiss Federal Act on Data Protection (FADP), given that CoreSR's primary production infrastructure is hosted in **Helsinki, Finland (European Economic Area)**.

1. Definitions

1. **"Applicable Data Protection Law"** means, as applicable to the Processing of Customer Personal Data: (a) PIPEDA and applicable Canadian provincial privacy legislation; (b) the EU GDPR (Regulation (EU) 2016/679); (c) the UK GDPR and Data Protection Act 2018; and (d) the Swiss FADP.
2. **"Customer Content"** means all systematic-review protocols, PICO criteria, bibliographic collections, screening decisions, full-text research PDFs, structured extractions, Risk-of-Bias assessments, GRADE evidence profiles, meta-analytic datasets, and manuscript drafts uploaded or generated by Authorized Users in Customer's workspace(s).
3. **"Customer Personal Data"** means any Personal Data / Personal Information (as defined under Applicable Data Protection Law) contained within Customer account records or Customer Content for which Customer acts as Controller (or accountable organization under PIPEDA) and CoreSR acts as Processor (or service provider).
4. **"EU SCCs"** means the Standard Contractual Clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (**Module Two: Controller to Processor**), supplemented where applicable by the UK International Data Transfer Addendum (vB1.0).
5. **"Subprocessor"** means any third party engaged by CoreSR to Process Customer Personal Data on behalf of Customer, as listed in **Annex III** (https://coresr.ai/api/public/subprocessors).

2. Scope, Roles, and Prohibition on Regulated Patient Records (PHI)

2.1 **Roles of the Parties.** With respect to Customer Personal Data, Customer is the Controller (or accountable organization under PIPEDA) and CoreSR is the Processor (or service provider). CoreSR acts as an independent Controller solely for billing records, corporate accounting, and aggregate platform security telemetry necessary to protect the Service.

2.2 **Documented Instructions.** CoreSR shall Process Customer Personal Data **solely** on documented instructions from Customer — namely, to provide, secure, maintain, and support the Service in accordance with the Principal Agreement, this DPA, and Authorized Users' in-product actions — unless otherwise required by applicable Canadian or EU/Member State law, in which case CoreSR shall inform Customer of that legal requirement before Processing unless prohibited by law on important grounds of public interest (GDPR Art. 28(3)(a)).

2.3 **No PHI / Clinical Medical Records.** The Service is engineered exclusively for **published or summary scientific research literature and methodological review work product**. Customer shall not upload identifiable patient health records or Protected Health Information ("PHI") governed by Ontario PHIPA, Alberta HIA, US HIPAA, or GDPR Article 9 special-category health data of identifiable patients. If Customer inadvertently uploads prohibited patient identifiers, Customer shall notify security@coresr.ai immediately and CoreSR shall assist in immediate purge.

3. Binding AI & Customer Content Commitments (Zero Training & Commercial LLM Egress)

3.1 **No Model Training on Customer Content.** For all **Team** and **Institution** workspaces, CoreSR contractually warrants and enforces in software that **Customer Content and Customer Personal Data are never used to train, fine-tune, distil, or evaluate CoreSR machine-learning or foundation models** (including TITAN-SR, GLASS, and ROB BERT). Any collaborative fine-tuning on an Institutional Customer's corpus requires a separate, mutually executed written research/co-development addendum.

3.2 **Third-Party Commercial LLM Egress.** For all **Team** and **Institution** workspaces, CoreSR warrants and enforces in software that, **apart from the single exception in clause 3.2.1, zero Customer Content or Customer Personal Data is transmitted to third-party commercial LLM API vendors** (such as OpenAI, Anthropic, Google Gemini, or DeepSeek). All AI screening (TITAN-SR) and generative extraction/GRADE/synthesis (GLASS and ROB BERT) execute exclusively on CoreSR-operated infrastructure (Helsinki, Finland and Ontario, Canada) or — only when CoreSR's private servers are down or unavailable — stateless, zero-persistence GPU containers executing CoreSR's own GLASS weights (RunPod, Inc., Annex III).

3.2.1 **Exception — Kaplan–Meier Figure Reading (KM Cor), effective November 17, 2026.** When a reviewer runs **KM Cor** on a Kaplan–Meier figure, the cropped image of that figure, its caption, and the review's subgroup names are sent to **Google's Gemini vision model** through a commercial model API, in Team and Institution workspaces as on every other plan. Nothing else is sent: not the PDF, not any other page, and no screening, extraction, risk-of-bias or GRADE data. KM Cor runs only when a reviewer starts it on a figure, and a figure can instead be traced by hand, which uses no AI. No Customer Personal Data is required for or included in that read.

3.3 **Human-in-the-Loop Governance.** AI outputs within CoreSR are methodological proposals stamped with model provenance metadata; final inclusion/exclusion decisions, extractions, and GRADE certainty ratings remain under human reviewer control.

4. Confidentiality and Security of Processing

4.1 **Confidentiality of Personnel (GDPR Art. 28(3)(b)).** CoreSR ensures that all persons authorized to Process Customer Personal Data have committed themselves to strict written confidentiality obligations surviving termination of engagement and have completed role-appropriate security training.

4.2 **Technical and Organisational Measures (GDPR Art. 32; PIPEDA Principle 4.7).** CoreSR implements and maintains the technical and organisational security controls set out in **Annex II**, including TLS 1.3 transport encryption, mutual TLS (mTLS) origin authentication, AES-256 volume encryption at rest, workspace-enforced TOTP multi-factor authentication, configurable

session lifetimes, append-only security audit logging with real-time anomaly alerting, and verified geo-redundant encrypted backups with Compliance-mode WORM Object Lock immutability. CoreSR may upgrade these controls provided overall security posture is never materially degraded.

5. Subprocessing (GDPR Art. 28(2) & (4); PIPEDA Principle 4.1.3)

5.1 **General Written Authorization.** Customer grants CoreSR general written authorization to engage the Subprocessors listed in **Annex III** (https://coresr.ai/api/public/subprocessors).

5.2 **Flow-Down Obligations.** CoreSR enters into a written agreement with each Subprocessor imposing data-protection and security obligations no less protective than those in this DPA, and CoreSR remains fully liable to Customer for the performance of each Subprocessor's data-protection obligations.

5.3 **30-Day Advance Notice & Right to Object.** CoreSR shall notify Customer in writing at least **thirty (30) calendar days** before adding any new Subprocessor or materially changing an existing Subprocessor's processing scope (save for immediate emergency security replacements, notified without undue delay). Customer may object in writing on reasonable data-protection grounds within fourteen (14) calendar days at security@coresr.ai. If CoreSR cannot reasonably accommodate Customer's objection, Customer may terminate the affected subscription effective prior to the change and receive a pro-rata refund of prepaid unused fees.

6. International Data Transfers

6.1 **Primary EEA Hosting & Canadian Adequacy.** Primary application compute, relational databases, and file storage reside in **Helsinki, Finland (EEA)**. CoreSR Inc. is incorporated in **Canada**, and verified pre-encrypted backups and private GPU inference operate in Ontario, Canada over an authenticated point-to-point encrypted tunnel. Transfers from the EEA/UK to CoreSR Inc. in Canada for commercial activities under PIPEDA rely on **European Commission Adequacy Decision 2002/2/EC** (reaffirmed January 15, 2024 under GDPR Art. 45) and UK adequacy regulations.

6.2 **Standard Contractual Clauses.** To the extent Processing involves a restricted transfer of EEA, UK, or Swiss Personal Data to a Subprocessor or jurisdiction not covered by an adequacy decision (such as United States cloud infrastructure), the **EU SCCs (Module Two: Controller to Processor)** are hereby incorporated by reference and apply as follows:

- **Clause 7 (Docking):** Included.
- **Clause 9(a) (Subprocessors):** Option 2 — General Written Authorization, 30 days' advance notice.
- **Clause 11 (Redress):** Optional language excluded.
- **Clause 17 (Governing Law):** Laws of **Ireland** (or Finland where required by host Member State).
- **Clause 18(b) (Forum):** Courts of **Ireland** (and for UK transfers, the UK IDTA Table 1–4 parameters apply under the laws and courts of England and Wales).
- **Annexes I, II, and III of the EU SCCs** are populated by **Annexes I, II, and III** of this DPA.

7. Data Subject Rights & Regulatory Cooperation (GDPR Art. 28(3)(e)–(f))

7.1 **Self-Service Tools.** The Service provides built-in self-service portability and erasure capabilities: (a) **One-Click Full Account & Project Export** (streaming CSV, Markdown, and lossless JSON archives); and (b) **Self-Service Account Deletion** (`Account Settings → Delete Account`).

7.2 **Processor Assistance.** If CoreSR receives a request directly from a Data Subject (or individual under PIPEDA Principle 4.9) regarding Customer Personal Data, CoreSR shall promptly redirect the requester to Customer (unless legally prohibited) and shall reasonably assist Customer in fulfilling access, rectification, portability, restriction, or erasure requests within statutory timelines, and in conducting Data Protection Impact Assessments (DPIAs) where required under GDPR Articles 35–36.

8. Personal Data Breach Notification (GDPR Art. 33; PIPEDA s. 10.1)

8.1 **Notification SLA.** CoreSR shall notify Customer **without undue delay, and in any event within seventy-two (72) hours** (targeting within **twenty-four (24) hours** for Institution-tier customers), after becoming aware of a confirmed Personal Data Breach ("real risk of significant harm" under PIPEDA s. 10.1 or accidental/unlawful destruction, loss, alteration, or unauthorized disclosure/access under GDPR Art. 4(12)) affecting Customer Personal Data.

8.2 **Breach Notice Contents.** Notification shall be sent to Customer's designated administrative/security email and shall describe: (a) the nature and timeline of the breach; (b) categories and approximate number of affected users and records; (c) likely consequences; (d) containment, remediation, and forensic preservation steps taken; and (e) CoreSR's Incident Commander contact (security@coresr.ai). Notification of a breach is not an acknowledgement of fault or liability.

9. Return and Deletion of Customer Data (GDPR Art. 28(3)(g))

9.1 **Export Prior to Termination.** At any time during the subscription term and prior to account deletion, Customer may export all Customer Content (references, screening decisions, extractions, GRADE tables, manuscripts, and full project JSON snapshots) via the One-Click Full Export tool without additional charge.

9.2 **Deletion & Backup Age-Out.** Upon Customer-initiated account deletion or written deletion instruction at termination:

1. Live accounts enter a **seven (7)-day soft-delete grace window** (revocable by the account holder in case of accidental trigger), during which active sessions are revoked;
2. Upon expiry of the 7-day grace window (or immediately upon verified written instruction from an Institution administrator), Customer Content and Customer Personal Data are **permanently deleted from live databases and encrypted production storage**, leaving only a non-reversible SHA-256 hash audit entry; and
3. Pre-encrypted off-site disaster-recovery backup archives **automatically expire and age out within 30 to 35 calendar days**, except to the limited extent statutory tax/billing records must be retained under Canadian law.

10. Audits and Verification (GDPR Art. 28(3)(h))

10.1 **Documentation & Automated Posture Evidence.** Upon written request (up to once annually, or following a confirmed Personal Data Breach), CoreSR shall make available to Customer under confidentiality: (a) CoreSR's complete ISO/IEC 27001:2022-aligned policy suite, Statement of Applicability, Privileged Access Register, and Vulnerability SLA logs; (b) CoreSR's automated production security posture assessment summary and CI/DAST scan attestations; and (c) once completed, CoreSR's third-party penetration test executive summary and SOC 2 Type II report.

10.2 **Remote or On-Site Inspection.** Where Applicable Data Protection Law grants audit rights not satisfied by §10.1, Customer (or an independent, accredited third-party auditor bound by written confidentiality and not a competitor of CoreSR) may conduct a scoped remote audit upon thirty (30) days' prior written notice during normal business hours in a manner that avoids disrupting clinical/research users or exposing other customers' data. Each party bears its own costs of routine annual audits.

11. Liability, Precedence, and Governing Law

11.1 **Liability.** Each party's liability under this DPA is subject to the exclusions and aggregate limitations of liability set forth in the Principal Agreement, except where Applicable Data Protection Law or the EU SCCs prohibit limitation of Data Subject claims.

11.2 **Order of Precedence.** In the event of conflict regarding data protection: (1) the EU SCCs (where applicable) prevail over this DPA; and (2) this DPA prevails over the Principal Agreement.

11.3 **Governing Law.** Except as otherwise mandated by §6.2 (EU SCCs), this DPA is governed by the laws of the **Province of Ontario and the federal laws of Canada applicable therein**.

Execution Block

This DPA becomes legally binding upon the earlier of: (a) execution of an Institutional Order Form or Principal Agreement incorporating this DPA by reference; or (b) counter-signature of the signature block below and delivery to legal@coresr.ai.

On behalf of Customer (Controller)	On behalf of CoreSR Inc. (Processor)
Legal Entity Name: _____	Legal Entity Name: **CoreSR Inc.**
Authorized Signatory: _____	Authorized Signatory: **Tyler Pitre, MD PhD FRCPC**
Title: _____	Title: **Founder and Chief Executive Officer**
Security / Privacy Notice Email: _____	Security & Privacy Contact: `security@coresr.ai`
Signature: _____	Signature: _____
Date: _____	Date: _____

Annex I — Description of Processing

- **Data Exporter (Controller):** Customer and its Authorized Users using CoreSR for systematic literature review, meta-analysis, and clinical practice guideline methodology.
- **Data Importer (Processor):** CoreSR Inc., c/o LaBarge Weinstein LLP, 800-515 Legget Drive, Kanata, ON K2K 3G4, Canada (primary production servers in Helsinki, Finland).
- **Categories of Data Subjects:** (1) Customer's Authorized Users (researchers, methodologists, clinicians, librarians, students, workspace administrators); and (2) authors of published scientific studies cited in public bibliographic metadata. **Identifiable patients / clinical subjects are strictly excluded.**
- **Categories of Personal Data:** Account email address, display name, institutional affiliation, role, hashed password / encrypted TOTP seed, session IP address and user-agent security audit logs, billing contact details, and attribution of review screening/extraction decisions to Authorized Users.
- **Special Categories of Data (GDPR Art. 9): None permitted.** Prohibited under Section 2.3 and Terms of Service §6.1.
- **Frequency & Duration:** Continuous throughout the subscription term plus the 7-day deletion grace window and 30–35 day rolling encrypted backup age-out window.
- **Nature & Purpose:** Hosting, authenticating, collaborating on, and executing AI-assisted literature screening, structured data extraction, GRADE assessment, and export of systematic reviews.

Annex II — Technical and Organisational Security Measures (TOMs)

Control Domain	Implemented Production Control
Encryption in Transit	TLS 1.3 (minimum TLS 1.2 AEAD) enforced across all public endpoints; HTTP Strict Transport Security preload; mutual TLS (mTLS) origin authentication between edge and origin; authenticated point-to-point encrypted tunnel for private GPU and backup links.
Encryption at Rest	AES-256 volume encryption across relational databases, full-text storage, customer uploads, and staging archives with hardware-isolated keys; TOTP MFA secrets encrypted with AES-256-GCM; salted adaptive password hashing; session tokens stored solely as SHA-256 digests; off-site backups asymmetrically pre-encrypted prior to cloud transfer.
Network & Edge Isolation	Global Anycast WAF/DDoS protection; default-deny host ingress restricted exclusively to authenticated edge origins; non-public internal isolation of database and application workers; strict Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy headers.
Identity, Org MFA & Session Control	Least-privilege RBAC and workspace isolation; 100% hardware/TOTP MFA across administrative consoles; public-key-only infrastructure access (password sign-in disabled); **workspace-level mandatory TOTP 2FA**, **configurable session lifetimes** (8 hours to 7 days), and **admin-initiated immediate session revocation**.
Vulnerability & Patch SLAs	Automated daily enterprise Linux security errata patching; blocking CI/CD SAST, SCA, and secret-detection gates; weekly automated DAST scans against production; written remediation SLAs: **Critical ≤ 7 days, High ≤ 30 days, Medium ≤ 90 days**.
Resilience & Immutable Backups	Daily asymmetrically encrypted database and file backups verified continuously via automated restore checks, replicated to Google Cloud/Workspace and **Backblaze B2 with Compliance-mode WORM Object Lock** (write-only credentials incapable of deletion); RPO ≤ 24h, RTO ≤ 24h; quarterly clean-room restore drills.
Audit Logging & Real-Time Alerting	Append-only security audit trail with sensitive-field redaction; real-time anomaly alerts on authentication spikes, privilege/MFA changes, and bulk exports; weekly security governance review.
AI & Data Loss Controls	Self-hosted TITAN-SR, GLASS, and ROB BERT models; **zero customer-data training** and **commercial LLM vendor egress blocked** in code for Team & Institution workspaces, except the Kaplan–Meier figure read of clause 3.2.1; One-Click Full Account ZIP Export; 7-day revocable soft-delete + automated permanent purge.

Annex III — Authorized Subprocessors

Incorporates the Authorized Subprocessor Register (https://coresr.ai/api/public/subprocessors) as updated in accordance with Section 5.3:

1. **Hetzner Online GmbH** — Helsinki, Finland (EEA) — Primary application, database, and AES-256 encrypted storage hosting (ISO/IEC 27001).
2. **Cloudflare, Inc.** — Global edge — DNS, CDN, WAF, TLS 1.3, mTLS origin authentication (SOC 2 Type II, ISO/IEC 27001).
3. **RunPod, Inc.** — US / EU — Stateless zero-persistence GPU containers executing CoreSR's own GLASS model weights, as a standby only when CoreSR's private servers are down or unavailable (SOC 2 Type II).
4. **Backblaze, Inc.** — US / Canada / EU — Immutable Compliance-mode WORM Object Lock storage of pre-encrypted backup ciphertext only (SOC 2 Type II).
5. **Google LLC** — Global — Secondary storage of pre-encrypted backup ciphertext, transactional email (Workspace), and optional user-selected Google OAuth 2.0 (SOC 2 Type II, ISO/IEC 27001).

6. **Stripe, Inc.** — US & Ireland (EU) — Subscription payment processing and PCI-DSS Level 1 card handling (PCI-DSS Level 1, SOC 2 Type II).