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

PUB-001 · Version 2.4
Effective: 2026-11-17
Public Procurement & Governance

Privacy Policy

This Privacy Policy explains what personal information **CoreSR Inc.** ("**CoreSR**", "we", "us", formerly operating under product brand Synthero) collects, why we collect it, where it is hosted, how AI features handle your data, who our subprocessors are, and how you exercise your privacy rights. It applies to https://coresr.ai (and legacy redirects from `synthero.ai`) and the CoreSR systematic-review, meta-analysis, and GRADE platform (the "**Service**").

> **Published Research & Review Work Product Only — No Patient Medical Records (PHI):** CoreSR is a research methodology platform for published scientific literature and analytical review work product. **Do not upload identifiable patient health records, medical record numbers, full dates of birth, or Protected Health Information (PHI) governed by PHIPA, HIPAA, or GDPR Article 9.** See Terms of Service §6.1 (https://coresr.ai/terms).

1. Who We Are & Data Protection Roles

CoreSR is operated by **CoreSR Inc.**, c/o LaBarge Weinstein LLP, 800-515 Legget Drive, Kanata, ON K2K 3G4, Canada.

- **General Support:** help@coresr.ai
- **Privacy, Data Subject Requests & Security Disclosures:** security@coresr.ai (https://coresr.ai/.well-known/security.txt)
- **Legal & Institutional DPAs:** legal@coresr.ai

Under Canadian federal privacy law (**PIPEDA**) and European data protection law (**GDPR** / **UK GDPR**):

- CoreSR acts as **Data Controller** for account registration, billing administration, and platform security telemetry.
- CoreSR acts as **Data Processor / Service Provider** for systematic-review project content uploaded or created by customers. Institutional and Team customers may download and counter-sign our pre-drafted PIPEDA & GDPR Article 28 Data Processing Addendum (PDF) at https://coresr.ai/api/public/dpa.

2. Information We Collect

2.1 Information You Provide

- **Account Profile:** Email address, display name, password (stored exclusively as a salted adaptive cryptographic hash — never plaintext), optional TOTP 2FA seed (encrypted at rest with AES-256-GCM), and optional institutional affiliation or country.
- **Billing Identifiers:** Subscription tier, billing contact email/address, and Stripe customer/subscription references. Payment card numbers are entered directly into **Stripe** (PCI-DSS Level 1) and never touch CoreSR servers.
- **Systematic Review Work Product:** PICO criteria, search strategies, imported citations, screening decisions, uploaded PDFs of published studies, structured extractions, Risk-of-Bias judgements, GRADE evidence tables, meta-analytic datasets, and

manuscript drafts.

- **Optional Customer Bibliographic API Keys:** Scopus or Web of Science API keys or institutional library resolver templates configured by you, stored encrypted at rest and masked across all API responses, used solely for searches you initiate.
- **Support Communications:** Emails or in-app feedback reports submitted to CoreSR.

2.2 Information Collected Automatically for Security & Operations

- **Security & Audit Logs:** Sign-in timestamps, source IP address, user-agent string, MFA enrollment/verification events, session revocations, privilege changes, and export/deletion events, used solely for security monitoring, brute-force protection, and auditability.
- **Strictly Necessary Cookies:** HttpOnly, `Secure`, `SameSite=Lax` session cookie (stored server-side solely as a one-way SHA-256 digest) and CSRF protection token. **CoreSR uses zero third-party advertising trackers or cross-site marketing cookies.**

---

3. AI & Your Data — Model Training and Third-Party Egress

CoreSR operates its own domain-specific biomedical models — **TITAN-SR** (literature screening), **GLASS** (structured extraction, Risk-of-Bias, GRADE rating, and synthesis), and **ROB BERT** — rather than acting as a thin wrapper around third-party consumer chatbots.

1. **Team & Institution Workspaces — Never Used for Model Training & No Commercial LLM Egress, With One Stated Exception:**
    - Project content in **Team** and **Institution** workspaces is **never** used to train, fine-tune, or evaluate CoreSR models, unless governed by a separate, bilaterally signed written research/co-development agreement.
    - **Third-party commercial LLM egress is blocked in server code, with the one exception below:** prompts and study excerpts from Team and Institution workspaces are processed on CoreSR-operated infrastructure (Helsinki, Finland and Ontario, Canada) and — only when CoreSR's private servers are down or unavailable — stateless, zero-persistence GPU containers running CoreSR's own GLASS models (RunPod, Inc.), and are blocked in code from calling commercial LLM vendor APIs.
    - **The 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.
2. **Individual / Free Accounts — Transparent Control & Opt-Out:**
    - Individual/Free accounts can toggle **"Exclude my reviews from model training"** at any time under **Account Settings → Privacy**, taking effect immediately and prospectively. Even when not opted out, manuscript drafts, private notes, and personal identifiers are never exported for training — only de-identified bibliographic title/abstract screening pairs.
    - CoreSR does **not** use DeepSeek or any China-domiciled AI provider.

---

4. Where Your Data Is Hosted & Cross-Border Transfers

- **Primary Production Hosting (EU / EEA):** Application servers, relational databases, and customer uploads are hosted at **Hetzner Online GmbH in Helsinki, Finland**, encrypted at rest on AES-256 storage volumes.
- **Encrypted Disaster Recovery & Private GPU Infrastructure (Canada):** Daily asymmetrically pre-encrypted backups and primary GPU inference operate over an authenticated point-to-point encrypted tunnel on CoreSR-operated infrastructure in

Ontario, Canada (covered by EU Commission Canadian PIPEDA Adequacy Decision 2002/2/EC, reaffirmed 2024), with pre-encrypted backup ciphertext replicated to Google Cloud/Workspace and an **immutable Compliance-mode WORM Object Lock store on Backblaze B2** (neither cloud storage provider ever holds decryption keys).

- **Subprocessors & Transfer Safeguards:** Our complete Authorized Subprocessor Register — with 30-day advance change notification — is published at https://coresr.ai/api/public/subprocessors. Where transfers occur outside the EEA/UK/Canada (e.g., Cloudflare global edge, Stripe, RunPod stateless GPUs), CoreSR relies on the 2021 EU Standard Contractual Clauses (Module Two) and UK IDTA.

5. Legal Bases (GDPR / UK GDPR) & PIPEDA Purposes

Purpose	GDPR Legal Basis	PIPEDA Schedule 1 Basis
Authenticate accounts, host projects, execute analyses, and deliver exports	Contract performance — Art. 6(1)(b)	Identified service delivery purpose (Principle 4.2 / 4.3)
Subscription billing, tax invoicing, and statutory accounting	Contract & Legal obligation — Art. 6(1)(b), 6(1)(c)	Billing & statutory tax compliance
Brute-force protection, MFA enforcement, audit logging, and incident detection	Legitimate interests — Art. 6(1)(f)	Security safeguards (Principle 4.7)
De-identified screening classifier improvement (Individual/Free accounts unless opted out; never Team/Institution)	Legitimate interests with unconditional opt-out — Art. 6(1)(f)	Expressly disclosed purpose with one-click Account Settings opt-out

We **never** sell personal information or monetize research topics for advertising.

6. Data Retention, Self-Service Export & Account Deletion

Data Category	Retention & Disposal Schedule
Active Account & Review Projects	Retained while your account remains active. Downloadable at any time in one click via **Account Settings → Full Data Export** (CSV, Markdown, and lossless JSON ZIP archive).
Self-Service Account Deletion	Initiating **Delete Account** (`Account Settings → Delete Account`) schedules deletion with a **7-day revocable grace window** and immediately revokes other sessions. After 7 days, automated purge workflows permanently delete your account and owned project records from live production storage.
Encrypted Off-Site Backups	Pre-encrypted backup archives expire and age out automatically within **30 to 35 calendar days**, after which zero copies remain.
Security Audit Logs	Minimum 365 days for incident forensics; deleted accounts retain only an irreversible SHA-256 email digest in the deletion audit entry.
Stripe Tax & Billing Records	7 years as mandated by Canadian federal tax legislation (*Income Tax Act / Excise Tax Act*).

7. Security Safeguards & Breach Notification

CoreSR maintains an internal security programme modelled on **ISO/IEC 27001:2022**, continuously verified across seven security control domains:

- TLS 1.3 + HSTS preload, mutual-TLS origin authentication, and strict HTTP security headers;
- AES-256 volume encryption at rest and asymmetrically pre-encrypted off-site backups with Compliance-mode WORM Object Lock;
- Salted adaptive password hashing, AES-256-GCM TOTP MFA, organization-level mandatory 2FA enforcement, configurable session lifetimes (8h–7d), and admin session revocation;
- Automated daily OS security patching, blocking CI/CD SAST/SCA/secret-detection gates, and weekly dynamic security scans.

In the event of a confirmed Personal Data Breach posing a real risk of significant harm or affecting Customer Personal Data, CoreSR notifies affected customers **without undue delay and within 72 hours** (targeting 24 hours for Institutional customers) in accordance with GDPR Art. 33 and PIPEDA s. 10.1.

---

8. Your Privacy Rights (PIPEDA, GDPR, UK GDPR, State Privacy Laws)

You have the right to **access**, **correct**, **export (port)**, **delete**, **restrict**, or **object to** the processing of your personal information, and to withdraw consent where applicable.

- Use **Account Settings** for immediate self-service **Full Data Export**, **Training Opt-Out**, **Active Session Revocation**, and **Account Deletion**.
- Or email security@coresr.ai — we respond to all verified privacy requests within **30 calendar days** (and typically within 5 business days).
- You may lodge a complaint with the **Office of the Privacy Commissioner of Canada (OPC)** (`priv.gc.ca`) or your local EU/UK Data Protection Supervisory Authority (including the Office of the Data Protection Ombudsman of Finland).

---

9. Changes & Contact

Material updates to this Privacy Policy are announced at least **14 days** prior to taking effect (and **30 days** in advance for new Subprocessors).

- **Privacy Officer & Security Disclosures:** CoreSR Inc. — security@coresr.ai
- **Legal & Institutional Contracts:** legal@coresr.ai