DECODR, INC.

PRIVACY POLICY

Effective Date: April 30, 2026

This Privacy Policy is incorporated by reference into the DECODR Terms of Service.

In the event of a conflict between this Policy and the Terms of Service on data privacy matters, this Policy governs.

1. SCOPE & APPLICABILITY

- This Privacy Policy applies to all Users of the DECODR platform, including Basic (free) and Paid (Plus, Pro and Power) accounts.
- It governs the collection, processing, storage, transfer, and deletion of personal data and usage data in connection with the Service.
- Enhanced obligations under Sections 3–6 apply where User is established in, or submits personal data relating to individuals located in:
  - European Economic Area (EEA)
  - Switzerland
  - United Kingdom (UK)
  - California, United States

2. DEFINITIONS — APPLICABLE DATA PROTECTION LAWS

- 'Applicable Data Protection Laws' means all privacy, data protection, and security laws applicable to a party's processing of personal data in connection with the Service, including:
  - GDPR — General Data Protection Regulation (EU) 2016/679
  - UK GDPR — as retained under the European Union (Withdrawal) Act 2018
  - Swiss revFADP — Federal Act on Data Protection, as amended (effective September 1, 2023)
  - CCPA/CPRA — California Consumer Privacy Act (Cal. Civ. Code §1798.100 et seq.), as amended
  - HIPAA — Health Insurance Portability and Accountability Act, including HITECH
  - GINA — Genetic Information Nondiscrimination Act
  - Any other applicable national, federal, state, or provincial data protection or genetic privacy laws
- 'Personal Data' has the meaning given in the applicable law for each jurisdiction.
- 'Genomic Data' means DNA, RNA, or other biological sequence data submitted to the Service for analysis. Genomic data is treated as special category / sensitive personal information under all applicable laws.

3. PROHIBITED DATA SUBMISSIONS

- **NOTICE:** STRICT PROHIBITION — The following categories of data are expressly prohibited from being uploaded, submitted, or transmitted to the DECODR Service by any User, under any account, for any purpose:
  - Protected Health Information (PHI) as defined under HIPAA (45 CFR §160.103), including any individually identifiable health information in any form or medium;
  - Any personal data subject to GDPR, UK GDPR, Swiss revFADP, or CCPA/CPRA that has not been fully anonymized or de-identified in accordance with Section 5 of this Policy;

- Genetic data, biometric data, or health data that identifies or is reasonably capable of identifying any living individual;
- Any data originating from a HIPAA-covered entity or business associate relationship.

- This prohibition applies to ALL Users regardless of Account type.
- DECODR does not operate as a HIPAA-covered entity or HIPAA business associate under any account. No Business Associate Agreement (BAA) is offered or available. Submission of PHI is prohibited under any circumstances.
- Submission of prohibited data constitutes a material breach of this Policy and the Terms of Service and may result in:
  - Immediate account suspension or termination
  - Reporting to applicable regulatory authorities
  - User liability for all resulting damages, penalties, fines, and costs
- Users bear sole and exclusive responsibility for ensuring all submitted data has been properly anonymized prior to upload. See Section 5.

4. MUTUAL COMPLIANCE & CONTROLLER / PROCESSOR ROLES

- Each party shall comply with its respective obligations under all Applicable Data Protection Laws.
- The following applies where User is established in, or provides DECODR with personal data relating to individuals located in, the EEA, Switzerland, the UK, or California:
  - DECODR acts as Data Processor (or Service Provider under CCPA/CPRA) with respect to anonymized usage and account data only.
  - User acts as Data Controller (or Business under CCPA/CPRA).
  - Processing occurs only on documented instructions from User.
  - A Data Processing Addendum (DPA) governs the parties' obligations and, where applicable, incorporates Standard Contractual Clauses (SCCs) or the UK International Data Transfer Addendum (IDTA).
- For DPA execution or data privacy inquiries, contact: legal@decodrinc.com.

5. ANONYMIZATION REQUIREMENTS

- **REQUIRED:** ALL data submitted to the Service must be fully anonymized prior to upload. This requirement applies to all Users and all accounts without exception.
- No direct or indirect identifiers are permitted in any submitted file. Anonymization must meet the applicable regulatory standard for User's jurisdiction:
  - HIPAA: Safe Harbor method (45 CFR §164.514(b)) — removal of all 18 enumerated identifiers — or Expert Determination by a qualified statistician
  - GDPR / UK GDPR / revFADP: Irreversible anonymization per Art. 4(1) such that re-identification is not reasonably possible by any means likely to be used
  - CCPA/CPRA: De-identification per Cal. Civ. Code §1798.140(m), with technical safeguards prohibiting re-identification
- User acknowledges that genomic data presents unique re-identification risks even after standard de-identification, and that removing standard identifiers alone may be insufficient. User bears sole responsibility for compliance.
- DECODR reserves the right to reject, quarantine, or delete any submission it has reasonable grounds to believe contains non-anonymized or identifiable data, without liability to User.

6. JURISDICTION-SPECIFIC USER OBLIGATIONS

6.1 EEA / GDPR

- Establish a lawful basis for processing (Art. 6); obtain explicit consent for special category of genetic data (Art. 9).
- Apply data minimization, purpose limitation, and storage limitation principles (Art. 5).
- Honor data subject rights: access, rectification, erasure, restriction, portability, and objection (Arts. 15–21).
- Conduct a Data Protection Impact Assessment (DPIA) where processing is high risk (Art. 35).
- Notify DECODR promptly of any data subject request or supervisory authority inquiry relating to DECODR-processed data.

6.2 Switzerland (revFADP)

- Comply with the revised Swiss Federal Act on Data Protection (effective September 1, 2023).
- Ensure cross-border transfers to DECODR are covered by adequate safeguards under revFADP Art. 16.
- Treat genetic data as particularly sensitive data requiring heightened protection.

6.3 United Kingdom (UK GDPR)

- Comply with UK GDPR and the Data Protection Act 2018.
- Ensure transfers from the UK to DECODR systems outside the UK use UK adequacy regulations or the UK IDTA.
- Maintain a Record of Processing Activities (ROPA) as required under UK GDPR Art. 30.

6.4 California (CCPA / CPRA)

- Do not direct DECODR to process California consumers' personal information inconsistently with CCPA/CPRA.
- Ensure DECODR's role as a Service Provider (not a Third Party) is documented; DECODR processes data only for specified Business Purposes.
- Honor opt-out rights and deletion requests for California consumers whose data is submitted to the Service.
- Recognize that genetic data is Sensitive Personal Information under CPRA, requiring heightened notice and opt-out rights (Cal. Civ. Code §1798.121).

7. CROSS-BORDER DATA TRANSFERS

- DECODR's Service infrastructure is operated in the United States. Use of the Service involves transfer of data to the United States.
- Required transfer mechanisms by jurisdiction:
  - EEA → US: EU Standard Contractual Clauses (Module 2: Controller to Processor), per Commission Decision 2021/914
  - UK → US: UK International Data Transfer Addendum (IDTA) to the EU SCCs, per ICO guidance
  - Switzerland → US: Swiss SCCs as approved by the Federal Data Protection and Information Commissioner (FDPIC)
  - California: No cross-border transfer restriction under CCPA/CPRA; Service Provider agreement governs
- DECODR will maintain and provide applicable transfer mechanism documentation upon request.

8. USER DATA SUBMISSION WARRANTIES

- User represents and warrants that all data submitted to the Service:
  - Has been fully anonymized in compliance with Section 5 of this Policy
  - Contains no PHI, PII, or individually identifiable information of any kind

- Was collected with all required notices, consents, and IRB / ethics board approvals
- Complies with applicable export controls (EAR, ITAR) where relevant
- Does not infringe any third-party intellectual property rights, including proprietary biological sequences subject to licensing restrictions

9. DECODR'S DATA PROCESSING COMMITMENTS

- DECODR processes User-submitted data solely as instructed and as described in this Privacy Policy and the Terms of Service.
- DECODR will not sell, lease, or share User data with third parties without explicit written consent or legal requirement.
- DECODR will not use submitted genomic data to train algorithms or models without explicit written User consent.
- DECODR will provide reasonable cooperation to assist User in fulfilling data subject rights requests under Applicable Data Protection Laws.
- DECODR implements appropriate technical and organizational measures (TOMs) including encryption at rest and in transit, access controls, and audit logging.

10. DATA RETENTION & DELETION

- Paid account: Account and usage data is retained for the duration of the active account and as required by applicable law thereafter.
- Basic account: No persistent data is stored. See Terms of Service Section 3.
- Upon account termination, data deletion timelines are governed by Terms of Service Section 10.
- DECODR will delete User data upon termination as directed and as required by Applicable Data Protection Laws.

11. DATA SUBJECT RIGHTS & CONTACT

- Data subjects may submit requests for access, rectification, erasure, restriction, or portability to: legal@decodrinc.com.
- DECODR will respond to verified data subject requests within the timeframe required by applicable law (e.g., 30 days under GDPR; 45 days under CCPA).
- DECODR will notify User of any data subject request relating to User-submitted data so that User, as Data Controller, may respond.
- For DPA execution, privacy incidents, or regulatory inquiries: legal@decodrinc.com.

12. MODIFICATIONS TO THIS POLICY

- DECODR may update this Privacy Policy with at least 30 days' advance written notice.
- Notice via email and/or in-platform notification.
- Continued use of the Service after the effective date constitutes acceptance of the updated Policy.