Codex Labs LLC Privacy Policy

Last Updated: January 30, 2026

Data protection is of a particularly high priority for Codex Labs LLC, a subsidiary of Integral Development Corp. and its affiliates Integral Ventures II LLC, PrimeOne Services LLC, Mint Digital, Inc. and Creditnet LLC (collectively "Codex Labs", "we", "us", or "our"). This Privacy Policy explains how we collect, use, process, and share personal data, and your rights regarding that data. This Privacy Policy embodies our commitment to you on protection of your data.

SCOPE AND APPLICABILITY

This Privacy Policy applies to:

- All personal data we collect, process, and transfer
- Personal data received from the EU, UK, and Switzerland in our capacity as a data controller
- Our subsidiaries and affiliates that handle personal data under the DPF
- All employees, contractors, and third parties acting on our behalf

The DPF Principles apply specifically to personal data we receive from the EU, UK, and Switzerland in reliance on the respective Data Privacy Frameworks.

1. WHO WE ARE AND HOW TO CONTACT US

Data Controller:

- Integral Development Corp.
- 380 Portage Ave, Palo Alto, CA 94306 USA
- Email: privacy@codexlabs.org
- Website: https://www.codexlabs.org/

Data Protection Officer:

- Email: dpo@codexlabs.org
- Address: 380 Portage Ave, Palo Alto, CA 94306 USA

DPF Contact:

- Email: dpf@codexlabs.org
- Phone: 650-424-4500

2. WHAT PERSONAL DATA WE COLLECT

2.1 Information You Provide Directly

- **Contact Information:** Name, email address, phone number, fax number, postal address
- **Professional Information:** Company/organization name, job title, business contact details
- **Account Information:** Username, password, account preferences
- **Identity Verification:** National ID, passport, driving license, tax ID (where required by law, such as MiFID II)
- **Employee Information:** For Integral employees - employment details, salary information, emergency contacts, photo, marital status, bank details, ethnicity (self-identified), employment history
- **Communications:** Content of messages, emails, and other communications with us

2.2 Information Collected Automatically

- **Device Information:** IP address, browser type and version, device identifiers
- **Usage Data:** Pages visited, time spent on pages, click-through rates, referral sources
- **Technical Data:** Operating system, time zone settings, browser plug-in types
- **Location Data:** General geographic location based on IP address

2.3 Information from Third Parties

- Information from our business partners and service providers
- Data from employees or agents of our institutional customers (where we act as processor)
- Publicly available information from legitimate sources

3. HOW WE USE YOUR PERSONAL DATA

3.1 Purposes and Legal Bases

We process your personal data for the following purposes with the corresponding legal bases:

Purpose	Legal Basis	Data Categories
Service Provision – Operating our platforms, applications and websites	Contract Performance (Article 6(1)(b))	Contact info, account data, usage data
Identity Verification – Compliance with financial regulations	Legal Obligation (Article 6(1)(c))	Identity documents, verification data
Customer Support – Responding to inquiries and providing assistance	Contract Performance / Legitimate Interest (Article 6(1)(f))	Contact info, communications, technical data

Marketing Communications – Sending promotional materials about related products/services	Consent (Article 6(1)(a)) OR Legitimate Interest (Article 6(1)(f))	Contact info, preferences
Analytics & Improvement – Analyzing usage to improve our services	Legitimate Interest (Article 6(1)(f))	Usage data, technical data
Security & Fraud Prevention – Protecting our systems and users	Legitimate Interest (Article 6(1)(f))	All categories as needed
Employment Management – HR processes for employees	Contract Performance / Legal Obligation	Employee information
Legal Compliance – Meeting regulatory and legal requirements	Legal Obligation (Article 6(1)(c))	All categories as required

3.2 Legitimate Interests

Where we rely on legitimate interests, these include:

- Network and information security
- Fraud prevention and detection
- Business development and improvement of services
- Internal group administration
- Compliance with non-EU legal obligations

4. WHO WE SHARE YOUR PERSONAL DATA WITH

4.1 Categories of Recipients

- **Integral Group Companies:** We may share data with our subsidiaries and affiliates for the purposes described in this policy
- **Service Providers:** Third-party processors who provide IT, payment, marketing, and other business services
- **Business Partners:** Organizations we work with to provide joint services (with your consent where required)
- **Professional Advisors:** Lawyers, accountants, auditors, and other advisors
- **Regulatory Authorities:** Financial regulators, tax authorities, and other government bodies where required by law
- **Law Enforcement:** Police, courts, and other authorities when legally required

4.2 International Transfers

We may transfer your personal data outside the European Economic Area (EEA) to:

United States: Under adequacy decisions or appropriate safeguards (Standard Contractual Clauses)

Other Countries: Only where adequate protection is ensured through:

- Adequacy decisions by the European Commission
- Standard Contractual Clauses approved by the European Commission
- Binding Corporate Rules (where applicable)
- Other appropriate safeguards under GDPR Article 46
- For copies of safeguards or further information about transfers, contact us at privacy@codexlabs.org.

4.3 ACCOUNTABILITY FOR ONWARD TRANSFER PRINCIPLE

In the context of an onward transfer, Integral Development Corp. has responsibility for the processing of personal information it receives under the DPF and subsequently transfers to a third party acting as an agent on its behalf. Integral Development Corp. remains liable under the DPF Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless Integral Development Corp. proves that it is not responsible for the event giving rise to the damage.

Before transferring personal data to third parties, we:

- Provide Notice and Choice as described above
- Enter into a contract with the third party that provides the same level of protection as required by the DPF Principles
- Take reasonable and appropriate steps to ensure the third party effectively processes personal data in a manner consistent with our DPF obligations

Onward Transfer Requirements:

- We remain liable if third-party agents process personal data inconsistently with the DPF Principles, unless we prove we are not responsible for the event giving rise to the damage
- We conduct due diligence on potential transfer recipients
- We provide stop transfer procedures when we have knowledge that a recipient is processing personal data in a way contrary to the DPF Principles

4.4 SECURITY PRINCIPLE

We take reasonable and appropriate measures to protect personal data from:

- Loss
- Misuse
- Unauthorized access, disclosure, alteration, and destruction

Security Measures Include:

- Encryption of data in transit and at rest using industry-standard protocols
- Role-based access controls with multi-factor authentication
- Network security including firewalls, intrusion detection systems, and security monitoring
- Regular employee training on security awareness and data protection
- Incident response procedures for detecting, investigating, and responding to breaches
- Regular security assessments and compliance reviews
- Secure data centers with physical access controls
- Regular security audits and penetration testing

4.5 DATA INTEGRITY AND PURPOSE LIMITATION PRINCIPLE

We ensure that personal data is:

- Reliable for its intended use
- Accurate, complete, and current as necessary for the purposes for which it is used
- Limited to what is relevant for the purposes of processing

Data Quality Measures:

- Regular data accuracy reviews and updates
- Automated data validation processes
- User access to review and correct their personal data
- Data minimization practices
- Regular purging of outdated or unnecessary data

4.6 ACCESS PRINCIPLE

We provide individuals with:

- Reasonable access to personal data about them that we hold
- The opportunity to correct, amend, or delete information that is inaccurate or has been processed in violation of the DPF Principles

Access Procedures:

- Submit requests to privacy@codexlabs.org
- Include sufficient information to identify yourself and specify the data requested
- We respond within 30 days of receiving a complete request
- We may charge a reasonable fee for access that covers our costs
- We provide data in a readily understandable format

Limitations on Access: We may limit or deny access where:

- The burden or expense of providing access would be disproportionate to the risks to privacy
- The rights of persons other than the individual would be violated
- It is commercially proprietary information
- Access is otherwise restricted by law or regulation

4.7 RECOURSE, ENFORCEMENT AND LIABILITY PRINCIPLE

We provide effective mechanisms for:

- Investigating and resolving individual complaints and disputes
- Verifying compliance with the DPF Principles
- Remedying problems arising out of failure to comply with the Principles

Internal Compliance:

- Annual DPF compliance reviews
- Employee training on DPF requirements
- Regular audits of data processing activities
- Documented procedures for handling complaints and breaches

5. HOW LONG WE KEEP YOUR PERSONAL DATA

We retain personal data for the longer of:

Business Need: As long as necessary for the purposes for which it was collected

Legal Requirements: 10 years or as required by applicable financial regulations

Specific Categories:

- Account data: Duration of relationship + 7 years
- Employee data: Employment period + 7 years
- Marketing data: Until consent withdrawn or legitimate interests cease
- Regulatory compliance data: As required by applicable law (typically 5-10 years)

Data is securely deleted or anonymized when retention periods expire.

6. YOUR RIGHTS (EU, UK, AND SWITZERLAND)

6.1 Individual Rights

Individuals in the European Union, United Kingdom, and Switzerland have the following rights regarding their personal data under the EU GDPR, UK GDPR, and the Swiss FADP respectively:

- **Right of Access:** Obtain confirmation of processing and access to your personal data
- **Right of Rectification:** Correct inaccurate or incomplete data
- **Right of Erasure:** Request deletion of personal data in certain circumstances
- **Right to Restrict Processing:** Limit how we use your data in specific situations
- **Right to Data Portability:** Receive your data in a structured, machine-readable format
- **Right to Object:** Object to processing based on legitimate interests or for direct marketing
- **Rights Related to Automated Decision-Making:** Not to be subject to solely automated decisions with legal effects
- **Right to Withdraw Consent:** Where processing is based on consent, withdraw it at any time

6.2 Right to Opt Out

- For personal data received from the European Union, United Kingdom, or Switzerland under the Data Privacy Framework, Integral offers individuals the opportunity to choose (opt out) whether their personal data is (i) to be disclosed to a third party (other than a service provider acting on our behalf), or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individual.
- For sensitive personal information, we will obtain affirmative express consent (opt in) from individuals before disclosing such information to a third party or using it for a purpose other than those for which it was originally collected or subsequently authorized through the exercise of opt-in choice.
- To exercise your choice or opt-out, please contact us at privacy@integral.com.

6.3 How to Exercise Your Rights

To exercise your rights:

- **Email:** privacy@codexlabs.org
- **Post:** Data Protection Officer, Integral Development Corp., 380 Portage Ave, Palo Alto, CA 94306 USA

- We will respond to valid requests within one month (extendable by two months for complex requests).

6.4 Right to Complain

Integral Development Corp. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). You have the right to lodge a complaint with any of the following supervisory authorities.

Supervisory Authorities:

United States

- Federal Trade Commission (FTC)
- **Address:** 600 Pennsylvania Avenue, NW, Washington, DC 20580
- **Phone:** (202) 326-2222
- **Consumer Complaint Line:** 1-877-FTC-HELP (1-877-382-4357)
- **Website:** https://www.ftc.gov
- **Online Complaints:** https://reportfraud.ftc.gov

United Kingdom

- Information Commissioner's Office (ICO)
- **Address:** Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
- **Phone:** 0303 123 1113 (UK) / +44 1625 545 745 (International)
- **Website:** https://ico.org.uk
- **Online Reporting:** https://ico.org.uk/make-a-complaint
- **Live Chat:** Available on website
- Postal Address for Complaints: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

European Union

- European Data Protection Board (EDPB)
- Address: Rue Wiertz 60, B-1047 Brussels, Belgium
- Website: https://edpb.europa.eu
- Email: edpb@edpb.europa.eu

6.5 Data Privacy Framework (DPF)

Integral Development Corp. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). Under certain conditions, an individual may invoke binding arbitration as set forth in Annex I of the DPF Principles. For more information, please visit https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction

Please be aware that Integral Development Corp. may be required to disclose an individual's personal information in response to lawful request by public authorities, including to meet national security and law enforcement requirements.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Integral Development Corp., Integral Ventures II LLC, PrimeOne Services LLC, Mint Digital, Inc., and Creditnet LLC commit to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to ICDR/AAA, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://go.adr.org/dpf_irm.html for more information or to file a complaint. The services of ICDR/AAA are provided at no cost to you.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Integral Development Corp., Integral Ventures II LLC, PrimeOne Services LLC, Mint Digital, Inc., and Creditnet LLC commit to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

7. COOKIES AND SIMILAR TECHNOLOGIES

7.1 What We Use

We use cookies, web beacons, and similar technologies for:

- **Strictly Necessary:** Essential for website functionality
- **Performance:** Analytics and site improvement
- **Functional:** Enhanced user experience and preferences
- **Marketing:** Targeted advertising and content

7.2 Managing Cookies

- **Cookie Settings:** Manage preferences via our Cookie Declaration at https://www.codexlabs.org/cookie-policy
- **Browser Settings:** Configure your browser to block or delete cookies
- **Opt-out Tools:** Industry opt-out mechanisms for advertising cookies
- For detailed cookie information, see our separate Cookie Policy.

8. SECURITY MEASURES

We implement appropriate technical and organizational measures including:

- **Encryption:** Data encryption in transit and at rest using industry-standard protocols
- **Access Controls:** Role-based access with multi-factor authentication
- **Network Security:** Firewalls, intrusion detection systems, and security monitoring
- **Employee Training:** Regular security awareness and data protection training
- **Incident Response:** Procedures for detecting, investigating, and responding to breaches
- **Regular Audits:** Security assessments and compliance reviews

9. SPECIAL CATEGORIES AND CHILDREN

9.1 Special Categories of Personal Data

We do not generally process special categories of personal data (sensitive data) except for employee ethnicity data (self-identified, with explicit consent) or where necessary for legal requirements.

9.2 Children's Data

Our services are not directed at children under 16. We do not knowingly collect personal data from children under 16 without appropriate parental consent.

10. CHANGES TO THIS POLICY

We may update this Privacy Policy to reflect changes in our practices or applicable law. We will:

- Post updates on our website with the new effective date
- Notify you directly of material changes where required by law
- Obtain fresh consent where necessary for new processing purposes

11. ADDITIONAL INFORMATION

11.1 Automated Decision-Making

We may use automated systems for:

- **Fraud Detection:** Automated screening for security purposes
- **Service Personalization:** Algorithm-based content recommendations
- **Risk Assessment:** Automated compliance checks
- You have the right to obtain human intervention and contest automated decisions that significantly affect you.

11.2 Profiling

We may create profiles based on your usage patterns to:

- Improve service delivery
- Provide personalized experiences
- Detect fraudulent activity

11.3 Third-Party Links

Our services may contain links to third-party websites. We are not responsible for their privacy practices. Please review their privacy policies separately.

12. CONTACT US

For any questions about this Privacy Policy or our data practices:

General Privacy Inquiries:

- **Email:** privacy@codexlabs.org
- **Post:** Data Protection Officer, Integral Development Corp., 380 Portage Ave, Palo Alto, CA 94306 USA
- **Phone:** 650-424-4500
- **Effective date:** Jan. 30, 2026

Legal Notices or Formal Inquiries

- **Contact:** Tim Mahota – General Counsel
- **Phone:** 650-424-4500
- **Email:** tim.mahota@integral.com

DPF-Specific Inquiries:

- **Email:** dpf@codexlabs.org
- **Phone:** 650-424-4500
- **Post:** DPF Compliance Officer, Integral Development Corp., 380 Portage Ave, Palo Alto, CA 94306 USA

13. COMMITMENT TO THE DATA PRIVACY FRAMEWORK

Codex Labs LLC affirms that all activities covered by this certification adhere to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), as well as the DPF principles. We have

certified to the U.S. Department of Commerce that we adhere to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF., and the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/