

# Privacy Policy

Last updated: April 15, 2026 | Effective date: April 15, 2026

---

## 1. Introduction

At RIPE Tech Corp. ("RIPE," "we," "us," or "our"), we value your privacy and are committed to protecting your personal data. This Privacy Policy describes how we collect, use, store, share, and otherwise process information relating to individuals ("Personal Data") when you use our platform, website, and services.

RIPE operates a digital investment platform that enables users to purchase tokenized securities representing fractional ownership interests in music royalty catalogs. Our platform utilizes blockchain technology (Arbitrum network) and account abstraction wallets.

We comply with the following data protection regulations:

- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial legislation
- EU General Data Protection Regulation (GDPR)
- Brazil's Lei Geral de Proteção de Dados (LGPD)
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Delaware Online Privacy and Protection Act

**Data Controller:** RIPE Tech Corp., 919 North Market Street, Suite 915, Wilmington, Delaware 19801, United States. Email: support@ripe.capital

## 2. Scope

This Policy applies when you:

- Visit ripe.capital or any RIPE-operated website or application
- Create an account and use our investment platform
- Purchase, hold, sell, or receive distributions from tokenized securities
- Interact with our blockchain-based smart contracts and wallet infrastructure
- Receive communications from us, including emails, notifications, and marketing

This Policy does not apply to third-party applications, websites, or services accessible through links on our platform. These are governed by their own privacy policies, and we are not responsible for their data practices.

## 3. Personal Data We Collect

### 3.1 Information you provide directly

- **Account registration:** name, email address, phone number, date of birth, country of residence
- **Identity verification (KYC/AML):** government-issued ID, proof of address, selfie/photo for identity matching, tax identification number (SSN/TIN for US persons)
- **Accredited investor verification** (if applicable): income documentation, net worth statements, or professional certifications
- **Financial information:** payment method details (processed by third-party payment processors; we do not store full card numbers), bank account information for withdrawals
- **Communications:** messages sent through our support channels, survey responses, feedback

### 3.2 Information collected automatically

- **Device and usage data:** IP address, browser type and version, operating system, device identifiers, screen resolution, referring URLs
- **Platform usage:** pages visited, features used, transaction history, time spent on pages, click patterns
- **Cookies and similar technologies:** as described in Section 7 below

### 3.3 Blockchain and wallet data

When you use our platform, certain data is recorded on the Arbitrum blockchain, which is a public, immutable distributed ledger. This includes:

- **Wallet addresses:** your account abstraction wallet address on Arbitrum
- **Transaction records:** purchases, sales, transfers, and distribution claims recorded on-chain
- **Token holdings:** your tokenized security balances, visible on the public blockchain

**Important:** Blockchain data is pseudonymous (identified by wallet address, not name) but is publicly accessible and cannot be modified or deleted by RIPE or any party. We do not control the Arbitrum blockchain. Your on-chain wallet address is not publicly linked to your identity by RIPE, but may be linked by third parties through blockchain analysis.

### **3.4 Information from third parties**

- **Identity verification providers:** KYC/AML screening results (e.g., Jumio, Onfido, or similar)
- **Payment processors:** transaction confirmation data (e.g., Transak, MoonPay, or similar)
- **Blockchain analytics providers:** wallet risk scoring and sanctions screening (e.g., Chainalysis, TRM Labs)
- **Embedded wallet providers:** authentication events and wallet creation data (e.g., Privy, Dynamic, or similar)

## **4. How We Use Your Personal Data**

### **4.1 To provide and operate our services**

- Create and manage your account and wallet
- Process investment transactions (purchases, sales, distributions)
- Calculate and distribute royalty earnings to token holders
- Provide customer support and respond to inquiries

### **4.2 Legal and regulatory compliance**

- Conduct KYC/AML identity verification as required by law
- Screen transactions and wallet addresses against sanctions lists
- File regulatory reports (e.g., tax reporting for US investors, suspicious activity reports)
- Comply with securities laws, including Regulation D, Regulation A+, Regulation S, and applicable SEC requirements

### **4.3 Platform security and integrity**

- Detect and prevent fraud, unauthorized access, and market manipulation
- Monitor for MEV (Maximal Extractable Value) attacks and front-running
- Maintain platform security, including cybersecurity monitoring and incident response
- Enforce our Terms of Use

### **4.4 Communications and marketing**

- Send transactional notifications (e.g., payout confirmations, account alerts)
- Send marketing communications about new catalogs and platform updates (with your consent, where required)

- You may opt out of marketing communications at any time by clicking 'unsubscribe' or contacting us

## 4.5 Analytics and improvement

- Analyze platform usage to improve our services and user experience
- Conduct research and development for new features
- Generate aggregated, anonymized statistics about platform performance

## 5. Legal Basis for Processing (GDPR)

If you are in the European Economic Area (EEA), United Kingdom, or another jurisdiction that requires a legal basis for processing, we rely on the following:

- **Contract performance:** processing necessary to provide our services to you (account management, transactions, distributions)
- **Legal obligation:** processing required by law (KYC/AML, tax reporting, securities regulation compliance)
- **Legitimate interest:** fraud prevention, platform security, analytics, and improving our services, where these interests are not overridden by your rights
- **Consent:** marketing communications and non-essential cookies (you may withdraw consent at any time)

## 6. Who We Share Your Data With

We do not sell your Personal Data. We share your data only as described below:

### 6.1 Service providers

- **Identity verification:** KYC/AML providers for regulatory compliance
- **Payment processing:** fiat on-ramp providers for card and bank transactions
- **Blockchain infrastructure:** RPC providers, bundlers, and wallet infrastructure providers
- **Cloud hosting:** data storage and computing providers
- **Analytics:** usage analytics providers (e.g., Google Analytics, Mixpanel)
- **Customer support:** helpdesk and communication platforms

### 6.2 Legal and regulatory

- Law enforcement or regulatory authorities when required by law, court order, or subpoena
- Tax authorities for required reporting (e.g., IRS Form 1099 for US investors)
- SEC, FINRA, or other securities regulators upon lawful request

### 6.3 Business transfers

In connection with a merger, acquisition, reorganization, or sale of assets, your data may be transferred to the acquiring entity. We will notify you of any such transfer and any choices you may have.

### 6.4 Blockchain (public)

Transaction data recorded on the Arbitrum blockchain is publicly accessible. This includes wallet addresses, transaction amounts, and token balances. This data is pseudonymous and is not directly linked to your identity on-chain, but we cannot prevent third parties from attempting to link wallet addresses to identities through blockchain analysis.

## 7. Cookies and Tracking Technologies

We use cookies and similar technologies on our website and application:

- **Strictly necessary cookies:** required for the platform to function (authentication, security). Cannot be disabled.
- **Preference cookies:** remember your settings and preferences (language, display options).
- **Analytics cookies:** help us understand how visitors use our platform (e.g., Google Analytics). These collect anonymized usage data.
- **Marketing cookies:** used by third-party advertising partners to deliver relevant ads. Shared with advertising networks with your consent.

You can manage your cookie preferences through our cookie banner or your browser settings. Note that disabling strictly necessary cookies may prevent the platform from functioning properly.

## 8. Trading Information and Transaction Data

In accordance with SEC guidance on Covered User Interface Providers, we disclose the following about your trading information:

- We store records of your transactions (purchases, sales, distributions) for regulatory compliance, tax reporting, and customer support purposes.
- We do not share your individual trading data with third parties for their proprietary trading purposes.

- We do not engage in payment for order flow or receive compensation based on routing your transactions to specific venues.
- We may use aggregated, anonymized transaction data for platform analytics and research.
- Transactions on Arbitrum are subject to sequencer ordering. We employ measures to mitigate MEV (front-running) risks, but cannot eliminate them entirely. See our MEV Protection Disclosure at [ripe.capital/disclosures](https://ripe.capital/disclosures) for details.

## 9. International Data Transfers

RIPE Tech Corp. is based in the United States. If you access our platform from outside the US, your data will be transferred to and processed in the United States, which may have different data protection standards than your jurisdiction.

For EEA/UK users: we rely on Standard Contractual Clauses (SCCs) approved by the European Commission, or other lawful transfer mechanisms, to ensure adequate protection of your data when transferred outside the EEA/UK.

For Canadian users: we ensure compliance with PIPEDA requirements for cross-border transfers, including that your data receives a comparable level of protection.

## 10. Data Retention

We retain your Personal Data only as long as necessary for the purposes described in this Policy, or as required by law:

- **Account data:** retained for the duration of your account plus 5 years after closure (for regulatory compliance)
- **KYC/AML records:** retained for 5 years after the end of the business relationship (as required by anti-money laundering regulations)
- **Transaction records:** retained for 7 years (for tax and securities regulation compliance)
- **Marketing preferences:** retained until you withdraw consent or unsubscribe
- **Analytics data:** aggregated data retained indefinitely; individual-level data retained for up to 26 months
- **Blockchain data:** on-chain transaction records are permanent and immutable; we cannot delete them

When we no longer need your Personal Data, we will securely delete or anonymize it.

## 11. Children's Privacy

Our platform is not intended for individuals under the age of 18. We do not knowingly collect Personal Data from children under 18. If we become aware that we have collected data from a child under 18, we will take steps to delete it promptly. If you believe a child has provided us with Personal Data, please contact us at support@ripe.capital.

## 12. Your Rights

Depending on your jurisdiction, you have the following rights regarding your Personal Data:

### All users

- **Access:** request a copy of the Personal Data we hold about you
- **Rectification:** request correction of inaccurate or incomplete data
- **Deletion:** request deletion of your Personal Data (subject to legal retention requirements and blockchain immutability)
- **Data portability:** receive your data in a structured, machine-readable format
- **Withdraw consent:** withdraw consent for marketing communications at any time

### EEA/UK users (GDPR)

- **Restriction of processing:** request that we restrict processing of your data in certain circumstances
- **Object to processing:** object to processing based on legitimate interests
- **Lodge a complaint:** with your local data protection authority

### California residents (CCPA/CPRA)

- **Right to know:** what Personal Data we collect, use, disclose, and sell
- **Right to delete:** request deletion of Personal Data
- **Right to opt-out of sale:** we do not sell your Personal Data
- **Right to non-discrimination:** we will not discriminate against you for exercising your rights
- **Right to limit use of sensitive Personal Data:** request that we limit the use of sensitive information

### Brazilian users (LGPD)

- **Confirmation and access:** confirm whether your data is processed and access it
- **Anonymization, blocking, or deletion:** of unnecessary or excessive data
- **Information about sharing:** know which entities your data has been shared with

**Important limitation:** Data recorded on the Arbitrum blockchain (wallet addresses, transaction records, token balances) is publicly accessible and immutable. We cannot modify or delete on-chain data. Deletion requests apply only to off-chain data stored in our systems.

To exercise any of these rights, contact us at [support@ripe.capital](mailto:support@ripe.capital) or write to the address in Section 14.

## 13. Data Security

We implement appropriate technical and organizational measures to protect your Personal Data, including:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Access controls and authentication for internal systems
- Regular security assessments and penetration testing
- Smart contract security audits by independent auditors
- Incident response procedures for data breaches
- Employee training on data protection and security

No method of transmission or storage is 100% secure. While we strive to protect your data, we cannot guarantee absolute security. If you become aware of any security incident, please contact us immediately at [support@ripe.capital](mailto:support@ripe.capital).

## 14. Contact Us

For privacy-related inquiries, data subject requests, or complaints:

**RIPE Tech Corp.**

Attn: Data Privacy Officer

919 North Market Street, Suite 915

Wilmington, Delaware 19801, United States

Email: [support@ripe.capital](mailto:support@ripe.capital)

For EEA/UK users: if you are not satisfied with our response, you have the right to lodge a complaint with your local data protection authority. A list of EU DPAs is available at <https://edpb.europa.eu>.

## 15. Changes to This Policy

We may update this Privacy Policy from time to time. When we make material changes, we will notify you by email, in-app notification, or by posting a prominent notice on our platform. The 'Last updated' date at the top of this Policy indicates the most recent revision.

Your continued use of our platform after changes become effective constitutes your acceptance of the updated Policy. If you do not agree with the changes, you should discontinue use of the platform and contact us to close your account.