Privacy Policy

BroadcastWallet.com

Effective Date:

March 7, 2026

Last Updated: March 7, 2026

BroadcastWallet.com (the "Platform," "Broadcast Wallet," "we," "us," or "our") provides a decentralized, non-custodial cryptocurrency toolkit enabling users to connect self-hosted wallets, sign and broadcast transactions across supported blockchains, manage programmable treasuries and operations on-chain, participate in token sales/airdrops, settle movements using reserve-linked or field-intelligence assets, and access related web3 finance features (collectively, the "Services").

We are committed to protecting your privacy while complying fully with applicable privacy laws in the United States and Canada, including:

- **United States**: California Consumer Privacy Act of 2018 as amended (CCPA/CPRA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Virginia Consumer Data Protection Act (VCDPA), Utah Consumer Privacy Act (UCPA), and other state laws where applicable, plus federal Trade Commission Act standards.
- **Canada**: Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta Personal Information Protection Act (PIPA), British Columbia Personal Information Protection Act (PIPA), Quebec Act respecting the protection of personal information in the private sector (Law 25 / modernized PIPEDA-equivalent obligations).

This Privacy Policy describes how we collect, use, disclose, retain, protect, and let you control your **personal information** (also called "personal data"). "Personal information" means any information about an identifiable individual.

By accessing or using the Services, you consent to the collection, use, and disclosure practices described here. If you do **not** agree, do not use the Platform.

We may revise this Policy. Material changes will be posted here with an updated "Last Updated" date; we may also notify you via in-app notice, email (if we have your address), or prominent Website banner. Continued use after changes constitutes acceptance.

1. Personal Information We Collect

We collect information in these categories (with examples):

A. Information You Provide Directly

- Account & Identity: full name, email address, phone number (with country code), date of birth, username/handle, password credentials, recovery email/phone.

- Verification / KYC/AML (when required for token sales, high-value features, or regulatory compliance): government-issued ID (passport, driver's license, national ID), selfie or liveness check images, proof of address (utility bill, bank statement), tax ID/SSN/ITIN (U.S.), SIN (Canada), or equivalent.
- Financial/Transaction Intent: wallet addresses you connect, signed (but not broadcast) transaction payloads you submit for relay, memo/notes, intended recipient addresses.
- Communications: messages sent via support chat, email inquiries, community forms, or feedback.
- Token Sale/Participation: contribution amounts, wallet used, referral codes, KYC status.

B. Automatically Collected / Device & Usage Data

- Identifiers: IP address, device ID/advertising ID, browser fingerprint.
- Geolocation: approximate location derived from IP (city/region level); precise geolocation only if you expressly enable it (rare).
- Technical: browser type/version, OS, screen resolution, language, timezone, referring URL, pages viewed, time spent, clickstream, scroll depth.
- Blockchain Interaction: public wallet addresses connected, transaction hashes broadcast via our relay, smart contract interactions, gas settings chosen.
- Analytics & Inferences: session duration, feature usage frequency (e.g., treasury dashboard vs. broadcast tool), inferred interests/preferences from behavior.

C. Sensitive Personal Information (CCPA/CPRA definition – collected only when strictly necessary)

- Government identifiers (ID numbers, passport numbers).
- Precise geolocation (if enabled).
- Financial account information tied to KYC (limited scope).
- Racial/ethnic origin, religious beliefs, health data (never collected).

D. Blockchain & Public Data

- All data you broadcast (transactions, contract calls) becomes permanently public and immutable on the blockchain — we do not control or delete it.
- We observe public on-chain activity linked to wallets you connect (balances, history, labels from explorers).

E. Third-Party Sources

- KYC/AML providers (Sumsub, Persona, or similar – results only).
- Analytics (Google Analytics, Mixpanel, or on-chain analytics like Dune, Nansen – aggregated/pseudonymized).
- Wallet providers (MetaMask, WalletConnect) – public address & basic connection metadata.
- Chain nodes/explorers – confirmation status of broadcast transactions.

We **never** collect, request, or store your **private keys**, **seed phrases**, **mnemonic phrases**, or any non-public signing material. The Services are **non-custodial** — you retain full control of your assets and keys.

2. How We Collect Personal Information

- **Voluntarily provided** by you during registration, wallet connection, KYC flows, token participation, support tickets.
- **Automatically** via cookies, pixels, server logs, SDKs embedded in the dApp interface.
- **From blockchain nodes** when you broadcast or query via our relay.
- **From third-party service providers** under contract (with data processing agreements).

3. Purposes of Collection & Use (Business & Commercial Purposes)

We use personal information only for:

1. Providing, maintaining, and improving the Services (core functionality – broadcasting, treasury views, token interactions).
2. Account creation, authentication, session management, password reset.
3. KYC/AML/sanctions screening and ongoing monitoring (legal obligation under U.S. Bank Secrecy Act, Patriot Act, Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act, FINTRAC rules).
4. Fraud detection, risk scoring, security incident response.
5. Transaction relay, confirmation tracking, user support.
6. Analytics, debugging, product/feature development (aggregated or de-identified where possible).
7. Compliance with court orders, subpoenas, regulatory inquiries.
8. Direct marketing & promotional communications (only with opt-in consent in most jurisdictions).
9. Enforcing Terms of Service, preventing abuse.
10. Business planning, audits, corporate transactions (merger, acquisition).

We apply **data minimization** — collecting only what is necessary for each purpose.

4. Sharing & Disclosure of Personal Information

We disclose personal information only in these limited cases (no "sale" of personal information under CCPA/CPRA definition):

Category	Recipients	Purpose	Categories Shared
Service Providers & Processors	Cloud hosting (AWS/GCP), KYC vendors, analytics tools, email/SMS providers, customer support platforms	Operational support, verification, analytics	All categories as needed
Affiliates	Entities under common control	Internal group operations	Limited – mostly identifiers & usage
Legal & Regulatory	Courts, regulators, law enforcement, FINTRAC, OFAC	Compliance, investigations	As required by law
Business Transfers	Successor in merger, acquisition, bankruptcy	Due diligence, continuity	All (under strict confidentiality)

Category	Recipients	Purpose	Categories Shared
With Your Consent	Third parties you explicitly authorize	e.g., sharing proof to partner protocol	Only what you approve
Public Blockchain	Anyone (decentralized network)	On-chain data is public by design	Transaction data, wallet addresses

We do **not** engage in cross-context behavioral advertising or targeted advertising based on sensitive data. We do **not** "sell" or "share" personal information for monetary or other valuable consideration under CCPA/CPRA.

5. Cookies, Tracking Technologies & Do-Not-Track / GPC

- **Essential cookies**: required for core functionality (wallet connection, session).
- **Analytics/performance cookies**: usage metrics (Google Analytics – IP-anonymized where possible).
- **Functional cookies**: remember preferences.

You can manage preferences via our cookie consent banner. We respect **Global Privacy Control (GPC)** signals (treated as opt-out of any sharing/sale under CCPA/CPRA). Most browsers offer Do-Not-Track settings; we do not currently alter behavior based on DNT signals alone.

6. Data Security

We use industry-standard safeguards:

- Encryption in transit (TLS 1.3) and at rest (AES-256 where applicable).
- Access controls, least-privilege principle, regular penetration testing.
- KYC data stored with encrypted, access-logged third-party processors.
- Incident response plan with 72-hour breach notification where required (CCPA, PIPEDA, Quebec Law 25).

Despite these measures, no internet or blockchain-based system is 100% secure. On-chain data cannot be secured or retracted once broadcast.

7. Data Retention Periods

- Account/KYC data: retained for 5–7 years after account closure to meet AML/CTF record-keeping obligations (U.S. & Canada).
- Usage logs: 12–24 months for security & analytics.
- Broadcast transaction metadata: indefinite (public blockchain).
- Marketing consent records: until withdrawal + reasonable period.

We delete or anonymize data when no longer needed, except where law requires retention.

8. Your Privacy Rights (U.S. & Canada)

General Rights (All Users)

- Access, correct, or delete your personal information.
- Withdraw consent (may restrict Services).
- Portability (machine-readable copy where technically feasible).
- Object to or restrict certain processing.

California Residents (CCPA/CPRA – including Limit Use of Sensitive Information) In the preceding 12 months we have:

- Collected: Identifiers, commercial info, internet/electronic activity, geolocation (approx.), financial info, professional/employment (if provided), inferences, sensitive personal info (gov't ID for KYC).
- Disclosed for business purposes: to service providers & legal authorities (no sales).
- Sold/Shared: None.

Rights: Know, Delete, Correct, Opt-out of sale/sharing (none to opt out of), Limit sensitive data use, Non-discrimination.

Other U.S. States (CPA, CTDPA, VCDPA, UCPA): Similar access, correction, deletion, opt-out, and non-discrimination rights.

Canadian Residents

- Access & correction (PIPEDA & provincial laws).
- Withdraw consent.
- Challenge compliance / file complaint with OPC or provincial commissioner.
- Quebec (Law 25): Additional rights re automated decision-making (explanation if used), right to be forgotten in certain cases, privacy impact assessments transparency.

How to Exercise Rights Submit a verifiable consumer request: Email → privacy@broadcastwallet.com Subject: "Privacy Rights Request – [Your Email/Username]" Include sufficient detail for verification (we may request ID). Authorized agents accepted with proof of authority. Response time: 45 days (extendable 45 days); free of charge (except excessive/frivolous requests).

9. International Data Transfers

The Platform is operated from the United States. Data may be transferred to/stored/processed in the U.S. and other countries where our providers operate. We use appropriate safeguards (e.g., Standard Contractual Clauses, adequacy decisions, or PIPEDA-equivalent protections) for transfers from Canada/EU/Quebec.

10. Children's Privacy & Age Restrictions

Services are **not** directed to anyone under 13 (U.S. COPPA) or 16/18 in certain Canadian provinces. We do **not** knowingly collect data from children. If discovered, we delete it immediately. Parents/guardians: contact us if you believe we hold child data.

11. Automated Decision-Making & Profiling

We do **not** currently use automated decisions that produce legal or similarly significant effects (e.g., denial of service based solely on algorithm). KYC risk scoring may involve automated elements but includes human review where material.

12. Third-Party Links & Integrations

Links to external wallets, DEXs, or protocols are not covered by this Policy. Review their privacy notices.

13. Contact Information

Data Protection Officer / Privacy Inquiries:

Email: privacy@broadcastwallet.com Mailing: [Insert Legal Entity Name & Address – e.g., Broadcast Wallet Inc., [Street], [City], [State/Province], [Postal Code],

By using BroadcastWallet, you acknowledge that blockchain data is public and irreversible, and that this Policy governs off-chain personal information only.