Terms & Policies
Privacy Policy
Last updated September 7, 2026 | Version 2026-09-07

This document is a product and legal review draft. It is not final legal advice and should not be published until reviewed by counsel. Before publication, confirm the operator legal name, notice address, privacy email, support email, state privacy coverage, international transfer posture, cookie tooling, vendor list, and retention schedule.

Overview

This Privacy Policy explains how Pocket collects, uses, discloses, retains, and protects information when a user visits Pocket websites, uses Pocket apps, connects a wallet, views markets, funds a wallet, prepares or submits a trade, uses social features, uses Mimic Trade, contacts support, or otherwise uses Pocket services.

Pocket is a non-custodial trading terminal. Pocket does not ask for or store wallet seed phrases, wallet private keys, card numbers, or bank credentials. Third-party wallet, onramp, offramp, payment, venue, chain, and identity providers may collect information under their own policies.

Information Pocket Collects

Pocket may collect the following categories of information:

- Account information, such as user identifiers, email address, phone number, username, display name, avatar, connected login methods, account settings, preferences, and policy acknowledgement receipts.
- Wallet and venue information, such as wallet addresses, smart account addresses, venue account references, delegated key metadata, balances, collateral snapshots, positions, orders, fills, transfers, approvals, transaction hashes, account status, and venue capability state.
- Trading and funding information, such as market selections, quotes, order drafts, submitted user-authorized payloads, trade gateway submissions, funding intents, funding quotes, route estimates, provider status, gas and fee estimates, errors, retries, and support context.
- Social information, such as profile details, follows, posts, comments, reactions, shared trade snapshots, PnL cards, win-rate displays, visibility settings, mimic intents, reports, moderation actions, and content metadata.
- Device, usage, and log information, such as IP address, browser, device, operating system, app version, language, time zone, referrer, pages viewed, actions taken, session timing, diagnostics, crash logs, analytics events, security signals, and network information.
- Communications, such as support requests, feedback, survey responses, emails,

chat messages, issue reports, and administrative messages.
- Compliance information, such as country or region, sanctions screening signals, geolocation signals, wallet-risk signals, provider KYC status, source-of-funds information where required by a provider, and records needed to enforce eligibility or respond to legal requests.

Pocket may receive information directly from the user, from the user's device, from wallet and authentication providers, from onramp or payment providers, from venues, from blockchains, from RPC and indexing providers, from analytics and security providers, from support tools, from other users, and from public or commercially available sources.

Public Blockchain And Venue Records

Blockchain networks and some venues create records that can be public, permanent, copied by others, indexed by third parties, and difficult or impossible to delete or correct. These records can include wallet addresses, token balances, transaction hashes, approvals, transfers, bridge activity, orders, fills, and other transaction metadata.

Pocket may hide or delete information from Pocket-controlled interfaces where appropriate, but Pocket cannot delete or change records controlled by blockchains, venues, wallets, bridges, RPC providers, indexers, onramps, offramps, payment processors, or other third parties.

How Pocket Uses Information

Pocket uses information to:

- Provide, secure, maintain, troubleshoot, and improve the services.
- Authenticate users, connect wallets, display balances, display market data, prepare transaction drafts, transmit user-authorized payloads, observe venue status, and show portfolio context.
- Provide funding, transfer, onramp, offramp, bridge, quote, and route interfaces through third-party providers.
- Operate social features, trade-share posts, PnL cards, mimic-trade drafts, follows, rankings, reports, moderation, and abuse prevention.
- Maintain policy versions, acknowledgements, consent records, preferences, feature gates, and audit trails.
- Detect, prevent, investigate, and respond to fraud, spam, account compromise, market manipulation, sanctions risk, security incidents, unauthorized access, and violations of Pocket rules or provider rules.
- Communicate about account activity, service updates, policies, security, support, product changes, and marketing where allowed.
- Analyze usage, measure performance, test features, debug issues, and make business and product decisions.

- Comply with law, legal process, sanctions programs, regulatory requests, accounting obligations, tax obligations, dispute resolution, and enforcement of agreements.

How Pocket Discloses Information

Pocket may disclose information to:

- Wallet, authentication, custody-technology, or account-abstraction providers used to provide user-controlled signing and account access.
- Trading venues, perps venues, protocols, blockchains, bridges, RPC providers, market-data providers, indexers, and other infrastructure needed to prepare, submit, observe, or display user-authorized activity.
- Onramp, offramp, payment, KYC, compliance, sanctions, fraud-prevention, and banking providers needed for funding and identity workflows.
- Cloud hosting, analytics, logging, observability, database, email, support, security, and communications providers.
- Affiliates, contractors, advisors, auditors, lawyers, accountants, insurers, and prospective transaction parties in connection with business operations or a corporate transaction.
- Government authorities, regulators, courts, law enforcement, third parties, or other users where Pocket believes disclosure is required or appropriate to comply with law, protect users, prevent fraud, enforce agreements, respond to legal process, or defend rights.

Pocket may disclose aggregated or de-identified information that does not reasonably identify a user.

Third-Party Providers

Third-party services have their own privacy practices. Pocket may link to, embed, or route users through providers such as wallet infrastructure providers, onramp and payment providers, venues, blockchains, bridge providers, market-data providers, identity providers, analytics providers, hosting providers, and support tools.

When a user uses a third-party service, that provider may collect, process, retain, transfer, freeze, reject, or disclose information under its own policy and legal obligations. Pocket does not control those providers’ privacy practices.

Social And Shared Trade Data

Pocket social features can make profile information, posts, trade snapshots, PnL cards, market symbols, direction, leverage, entry or snapshot price, timing, performance, visibility settings, and selected statistics visible to other users or the public, depending on user settings and product design.

Social information can also include follows, followers, reactions, comments, direct messages, portfolio displays, trade results, hold time, linked social profiles, creator badges, reward participation, referral activity, and other interactions. Public or semi-public content may be visible to anyone, including people who are not logged in.

Users should not publish content, enable open-trade sharing, or use public profile features if they do not want others to view, copy, quote, index, infer, or preserve the shared information. Pocket may retain copies of social content, trade-share results, account associations, moderation records, and audit records for safety, moderation, compliance, dispute resolution, integrity of performance statistics, and abuse prevention.

Cookies, Analytics, And Similar Technologies

Pocket and its providers may use cookies, local storage, SDKs, pixels, device identifiers, and similar technologies to keep users signed in, remember settings, secure sessions, measure usage, detect abuse, debug errors, improve performance, support marketing, and understand product activity.

Some browser or device settings may limit these technologies. Disabling them can affect sign-in, wallet connectivity, security, preferences, analytics, or other features.

Retention

Pocket keeps information for as long as reasonably necessary to provide the services, maintain security, resolve disputes, enforce agreements, support tax and accounting records, comply with legal obligations, operate audit trails, and protect users.

Different categories may have different retention periods. Policy acknowledgements, trade records, funding records, security logs, moderation records, and legal records may be retained longer than general analytics or support data. Pocket may retain de-identified or aggregated information indefinitely.

Pocket cannot delete records maintained by blockchains, venues, wallet providers, payment providers, onramp providers, compliance vendors, or other third parties.

Security

Pocket uses administrative, technical, and organizational safeguards designed to protect information. No system can be guaranteed secure. The user is responsible for protecting devices, passwords, recovery methods, wallets, private keys, signing approvals, and connected accounts.

Pocket will never ask for a seed phrase or private key. Users should report suspected unauthorized access or suspicious requests.

User Choices And Rights

Depending on the user's location and applicable law, the user may have rights to request access, correction, deletion, portability, restriction, objection, withdrawal of consent, opt-out of certain sharing or targeted advertising, or appeal of a privacy decision.

Users can also control some information through account settings, wallet connections, social visibility settings, marketing unsubscribe links, cookie or browser controls, and provider dashboards.

Deleting or hiding content in Pocket may not remove copies, screenshots, quotes, blockchain records, venue records, search engine caches, third-party archives, provider records, or content already viewed or saved by others.

Pocket may need to verify a request before responding. Pocket may deny or limit a request where permitted by law, including when information is needed for security, fraud prevention, legal compliance, dispute resolution, or where the information is outside Pocket's control.

California And State Privacy Notice

If state privacy laws apply, users may have the right to know categories of personal information collected, sources, purposes, categories of recipients, retention criteria, and whether information is sold, shared, or used for targeted advertising. Users may also have rights to delete, correct, access, port, opt out, limit use of sensitive information, and avoid discrimination for exercising rights.

Pocket should finalize this section after confirming whether it meets statutory thresholds or elects to provide state rights voluntarily.

Children

Pocket is not intended for individuals under 18. Pocket does not knowingly collect personal information from individuals under 18. If Pocket learns that it collected information from an individual under 18, it will take appropriate steps to delete or restrict the information where possible.

International Use

Pocket may process information in the United States and other countries where Pocket or its providers operate. Those countries may have privacy laws different from the user’s country. Some features may be unavailable in certain locations.

Changes

Pocket may update this Privacy Policy. Pocket will post the updated version and may require renewed acknowledgement where required or appropriate.

Contact

Privacy questions and requests should be directed to:

- Privacy: privacy@usepocket.trade
- Support: support@usepocket.trade