

SWIVR PRIVACY POLICY

Swivr Trade Ltd

Effective Date: September 9, 2026

1. Introduction

This Privacy Policy (this "Policy") explains how Swivr Trade Ltd, a company incorporated in Panama (the "Company," "Swivr," "we," "us," or "our"), collects, uses, shares and protects information about you when you access or use the website at <https://swivr.trade> and the trading platform, applications, APIs and related services made available through it (together, the "Services").

This Policy forms part of, and should be read together with, our Terms of Use at <https://swivr.trade/terms> (the "Terms"). Capitalised terms used but not defined here have the meaning given in the Terms.

This Policy is a notice describing how we collect, use, share and protect personal information. Where we process personal information based on your consent for a particular purpose, we will identify that purpose and explain how you can withdraw consent. Your use of the Services remains subject to the Terms.

If you have questions about this Policy or about how we handle your information, contact us at legal@swivr.trade.

2. Scope

This Policy applies to information we collect through the Services. It does not apply to:

- **The Solana blockchain.** Swivr settles on a public blockchain. Anything recorded on-chain is public, permanent and outside our control. See Section 5.
- **Third-party services you choose to use**, including external wallet software (Phantom, Solflare, Backpack and similar), the wallet provider's own account services, and any site you reach from a link in the Services. Each has its own privacy policy, which governs what it does with your information.
- **Information collected offline** or through any other channel we or a third party operate.

Throughout this Policy, "personal information" means information that identifies, relates to or can reasonably be linked to you. Information that has been aggregated or de-identified so that it can no longer reasonably be linked to you is not personal information under this Policy.

3. Information We Collect

3a. Information you provide to us

- **Sign-in identity.** You sign in with an email address or a Google account. We receive the email address associated with that sign-in and an account identifier issued by our wallet and authentication provider.

- **Waitlist email.** If you join the beta waitlist, we collect the email address you submit.
- **Profile information.** A username you choose and, if you upload one, an avatar image.
- **User Content.** Comments, replies and other material you post through the Services, and any feedback you send us.
- **Support correspondence.** Messages you send through our in-app support messenger or by email, and our replies.
- **Referral information.** A referral code you were referred by, if you arrive through a referral link, and the referral code issued to you.

You are not obliged to provide any of this, but the Services will not work without a sign-in identity, and some features will not work without a username.

3b. Information generated by your use of the Services

- **Wallet addresses.** The public address of the wallet created for you when you first sign in, and the public address of any external wallet you link as a signer or funding source.
- **Trading activity.** Quotes you request, orders you place, limit orders you create, amend or cancel, positions you open, close or settle, deposits and withdrawals, transaction signatures, fees, and realised and unrealised profit and loss.
- **Account state.** Balances, portfolio history and leaderboard placement.
- **Security events.** Enrollment in, and use of, multi-factor authentication.

3c. Information collected automatically

When you use the Services we automatically collect:

- **Log and device information** — IP address, browser type and version, operating system, device type, language and time zone, referring and exit pages, and access times.
- **Product analytics.** We record events describing how you use the Services, tied to your account identifier once you sign in. These include page and market views, sign-in and sign-out, wallet connection, quote requests, order submissions, trade confirmations and failures, limit-order lifecycle events, deposits, withdrawals, settlements and redemptions, referral attribution, and beta-gate outcomes.
- **Session properties.** Your wallet address, wallet provider and whether the wallet is embedded or external are attached to your analytics profile.
- **Error reports.** When something goes wrong in the application, we capture the error and the technical context around it so we can diagnose it.
- **Automatically captured interactions.** Our analytics tool captures page views and certain interface interactions by default, in addition to the named events above.

3d. Geolocation Information

Geolocation Information. We collect information that identifies your location at a country level and, in certain countries, at a state, province or regional level, derived from your IP address and other information available to us about the connection through which you access the Services, together with an assessment of whether that connection is made through a virtual private network, proxy, Tor or other anonymising network, or cannot be resolved (collectively, "Geolocation Information"). We collect and use this data to determine and enforce the availability of the Services in your jurisdiction under the Terms, and for regulatory compliance, fraud prevention and risk management purposes, among other

reasons. If you do not agree to our collection of this information, you may not be able to use the Services.

We make this determination on each request, and it is enforced by our servers on every trading and funding request. It is also read by the application so that controls unavailable to you can be disabled and the reason shown. Being located in a Restricted Jurisdiction or a Close-Only Jurisdiction does not prevent you from browsing the Services, and we collect the information described in Section 3c from you in either case.

3e. Information we receive from third parties

- **From our wallet and authentication provider** — your account identifier, the email address or Google account you signed in with, the public addresses of your embedded and linked wallets, and which multi-factor methods you have enrolled.
- **From the public blockchain** — the transaction history and balances associated with your wallet addresses, which we read to display your portfolio.
- **From our support provider** — the contents of support conversations you start.

3f. Information we do not collect

For the avoidance of doubt, and in contrast to platforms that take fiat payments:

- We do not collect or store **credit or debit card numbers, bank account numbers or routing numbers**. Swivr does not take fiat payments.
- We do not hold your **private keys, recovery phrase or passwords**. We will not and cannot access them, or any cryptoassets held within your Wallet. You may export the private key to your Wallet at any time.
- We do not currently collect **government identity documents**.

4. Minors

The Services are not directed to anyone under 18, and you must be at least 18 to use them. We do not knowingly collect personal information from anyone under 18. If we learn that we have, we will delete it promptly unless we are legally required to retain it. If you believe we hold information about someone under 18, contact us at legal@swivr.trade

5. Public and On-Chain Information

This section describes information that is public by design. Read it carefully — it is the most consequential part of this Policy.

Some of the information described above is visible to anyone, whether or not they use Swivr:

- **On the blockchain.** Deposits, withdrawals, trades and settlements are recorded on the Solana blockchain. Blockchain records are **public, permanent and cannot be altered or deleted by us or by you**. Anyone can view the full transaction history of any wallet address, and anyone who learns that an address is yours can link that history to you. Blockchain records are generally immutable and are not controlled by Swivr.
- **In the Services.** Your username, avatar, wallet address, positions, trading activity, profit and loss, leaderboard placement, account creation date and any comments you post are displayed publicly in the Services and are available through our public API.

Public information may be viewed, copied, indexed, re-shared or downloaded by anyone, including through APIs and third-party services, and may persist in their systems after you delete your Swivr account.

6. How We Use Information

We use the information described above to:

- **Operate the Services** — create and maintain your account and embedded wallet, quote and execute trades, settle contracts, process deposits and withdrawals, display your portfolio, and run comments, notifications, profiles and leaderboards.
- **Authenticate you and secure your account** — including multi-factor authentication on withdrawals and key exports.
- **Enforce eligibility** — determine whether you are in a restricted jurisdiction, administer the beta waitlist, and enforce the Terms.
- **Prevent fraud, abuse and prohibited conduct** — detect market manipulation, self-dealing, referral abuse, multiple accounts and other conduct prohibited by the Terms, and investigate suspected illegal activity.
- **Provide support** — respond to your questions and resolve disputes.
- **Understand and improve the Services** — measure how features are used, diagnose errors and outages, and inform what we build next.
- **Administer Programs** — referrals, rewards, competitions and promotions under Terms § 8.
- **Communicate with you** — send transactional and administrative messages about your account, trades and security. If we send marketing messages, we will do so only where permitted by applicable law, and you can opt out at any time; you cannot opt out of transactional and security messages while you have an account.
- **Comply with law** — meet our legal, regulatory, sanctions and record-keeping obligations, and respond to lawful requests from authorities.
- **Marketing communications** — if we send you marketing communications, use your contact information to send them in accordance with Section 13 and applicable law. We do not currently use personal information for targeted advertising or cross-context behavioural advertising.

7. Legal Bases for Processing

Where the GDPR or UK GDPR applies, we rely on:

- **Performance of a contract** — to provide the Services you have asked for under the Terms.
- **Legal obligation** — for sanctions screening, record-keeping and responses to lawful requests.
- **Legitimate interests** — to secure the Services, prevent fraud and abuse, understand how the Services are used, and improve them. We have considered these interests against your rights and freedoms.

- **Consent** — where you have provided it for a specified purpose, including marketing communications and any non-essential cookies or analytics for which applicable law requires consent. You may withdraw consent at any time; withdrawal does not affect processing carried out before withdrawal.

8. Cookies and Similar Technologies

We and our providers use cookies, browser local storage and similar technologies. Some are necessary to provide core functionality; others help us understand how the Services are used and diagnose errors. We use them to:

- keep you signed in and maintain your session;
- remember your display preferences (such as odds format and fee display) and interface state;
- remember a referral code across your sign-up; and
- measure how the Services are used, and diagnose errors.

Do Not Track. We do not currently respond to browser "Do Not Track" signals.

9. How We Share Information

We share personal information only as described below.

9a. Service providers

We may employ other companies and individuals to perform functions on our behalf. Examples include providing authentication and wallet infrastructure, product analytics and error reporting, customer support, website hosting and content delivery, edge network and traffic classification services, backend hosting and database services, and blockchain infrastructure. In particular, we use third-party cloud hosting providers to store user information and configurations, a third-party provider to create and secure the wallet associated with your account and to administer multi-factor authentication, and a third-party provider to operate our support messenger.

These providers have access to your personal information only to perform these tasks on our behalf, and are contractually obliged not to disclose it or to use it for any other purpose.

9b. Legal and safety

We may disclose information where we believe in good faith that it is necessary to: comply with applicable law, regulation, sanctions obligations, subpoena, court order or other lawful request from a public authority; enforce the Terms; investigate suspected fraud, market abuse or illegal activity; or protect the rights, property or safety of you, us or others.

9c. Corporate transactions

If we are involved in a merger, acquisition, financing, reorganisation, insolvency or sale of assets, information we hold may be transferred as part of that transaction. We will require the recipient to honour this Policy or give you notice before your information becomes subject to a materially different policy.

9d. Affiliates

We may share information with our parent, subsidiaries and companies under common control, for the purposes described in this Policy.

9e. Aggregated and de-identified information

We may create and share aggregated or de-identified information — such as platform volume, market statistics or usage trends — that cannot reasonably be used to identify you. We will not attempt to re-identify it.

9f. With your direction

We share information with a third party where you ask us to, or where you connect a third-party account or wallet to your Swivr account. What that third party does with your information is governed by its own privacy policy, which you should read before connecting.

9g. Third-party analytics

We use a third-party analytics provider to understand how the Services are used, compile reports on activity and events, analyse performance and usage, and diagnose errors. The provider receives the analytics information described in Section 3c, which is tied to your account identifier once you sign in, and may use cookies, browser local storage or similar technologies to provide these services.

We do not currently use third-party analytics for targeted advertising or retargeting, and we do not currently share personal information with third-party advertising networks. If that changes, we will update this Policy and obtain any consent required by applicable law before doing so. Where a provider makes an opt-out available, we will identify the provider and its opt-out in this section.

9h. Marketing partners

We do not currently share personal information with third-party marketing partners for their own marketing purposes. If that changes, we will update this Policy and provide any notice and obtain any consent required by applicable law before doing so.

We will not disclose your bank account details or payment card details to any third party for marketing purposes. As set out in Section 3f, we do not collect them.

10. Security

We use administrative, technical and physical safeguards designed to protect your information, including encryption in transit, access controls limiting staff access to what their role requires, and multi-factor authentication on sensitive wallet operations such as withdrawals and key export.

We strongly recommend you enrol a multi-factor method, keep your sign-in email secure, and never share your recovery phrase or private keys with anyone — including with anyone claiming to be Swivr support. **We will never ask you for your private keys or recovery phrase.**

No system is completely secure. We cannot guarantee that your information will not be accessed, disclosed, altered or destroyed, and you use the Services at your own risk.

11. Retention

We keep personal information for as long as we need it for the purposes set out in this Policy, and then for as long as required by law.

- **Account and transaction records** — for the life of your account and for 5 years afterwards, or longer where required by applicable law, to meet record-keeping, anti-fraud, compliance and legal obligations.
- **Server and analytics logs** — generally for 12 months, unless a longer period is reasonably necessary for security, fraud prevention, dispute resolution or legal compliance.
- **Support correspondence** — for as long as required by law.
- **On-chain records** — permanently, by the nature of the blockchain, and outside our control (see Section 5).

12. Your Rights

Depending on where you live, you may have some or all of the following rights in respect of your personal information:

- **Access** — to obtain a copy of the information we hold about you.
- **Correction** — to have inaccurate or incomplete information corrected.
- **Deletion** — to have your information deleted, subject to the limits below.
- **Portability** — to receive your information in a structured, commonly used, machine-readable format.
- **Objection and restriction** — to object to, or ask us to restrict, processing based on our legitimate interests.
- **Withdrawal of consent** — where we rely on consent, at any time.
- **Non-discrimination** — we will not deny you the Services, or offer you worse terms, because you exercised a privacy right.
- **Opt out of sale or sharing** — where we sell personal information, or share it for cross-context behavioural advertising, you have the right to direct us not to. We do not currently sell personal information or share it for cross-context behavioural advertising. Should we begin, we will publish the opt-out mechanism required by applicable law here and at the point of collection, and you may in any event exercise this right at any time by emailing legal@swivr.trade
- **Opt out of marketing sharing** — if we begin sharing personal information with marketing partners, you may ask us not to do so as described in Section 9h.

How to exercise them. Email legal@swivr.trade from the email address associated with your account, and tell us which right you are exercising. We may need to verify your identity before we act, and we will respond within the time required by applicable law. You may use an authorised agent where the law allows.

Limits. Two limits matter on Swivr specifically:

1. **We cannot delete on-chain data.** Blockchain records are outside our control and cannot be altered or erased by anyone. Deleting your account removes your Swivr profile; it

does not remove your trading history from the blockchain, and does not make past public activity private.

2. **We may have to retain some information** despite a deletion request, where law requires us to keep it or where retention is otherwise permitted by applicable law, such as for anti-fraud, sanctions, and financial record-keeping obligations.

13. Marketing Communications

If we send you a marketing email, every message will carry an unsubscribe link, and you can also opt out by emailing legal@swivr.trade. You cannot opt out of transactional, administrative and security messages relating to your account while your account is open.

14. Third-Party Links

The Services may link to sites, applications and services we do not operate — including block explorers, wallet software and external market data. We do not control what they collect or how they use it, and this Policy does not apply to them. Read their privacy policies before providing information to them.

15. Changes to This Policy

We may update this Policy from time to time. When we do, we will change the effective date at the top and post the updated Policy in the Services. If a change materially affects how we process personal information, we will provide any notice or obtain any consent required by applicable law. Your continued use of the Services does not by itself create consent where consent is required.

16. Jurisdiction

The Services are made available from Panama. This Policy and any privacy-related matters arising from it are intended to be governed by the laws or jurisdiction of Panama, except to the extent applicable data protection law provides otherwise.

17. Contact Us

Questions, concerns or privacy requests:

- **Privacy and rights requests:** legal@swivr.trade
- **General support:** support@swivr.trade

Last updated: September 9th, 2026