

Table of Contents

LINEUP PRIVACY POLICY1

1. Introduction and Scope.....1

2. Definitions2

3. The Personal Data We Collect.....2

4. How and Why We Use Your Personal Data4

5. Automated Decision-Making and Profiling5

6. Analytics, Cookies, and Tracking Technologies.....5

7. Marketing Communications.....6

8. How We Share Your Personal Data6

9. International Data Transfers.....7

10. Data Retention7

11. Data Security8

12. Your Rights.....8

13. Third-Party Services and Links9

14. Children.....9

15. Changes to This Policy9

16. Google Play Data Safety Disclosure9

17. Contact Us10

LINEUP PRIVACY POLICY

Effective Date: 15 July 2026 | **Last Updated:** 20 July 2026 | **Version:** 1.0 **Data Controller:** LineUp, established in the Emirate of Dubai, United Arab Emirates **Platform:** <https://lineup.trade/> | **Privacy contact:** Support@Lineup.trade

1. Introduction and Scope

1.1. This Privacy Policy (the “Policy”) explains how LineUp (“LineUp”, “we”, “us”, or “our”) collects, uses, shares, protects, and retains personal data when you access or use the LineUp platform, including our website at <https://lineup.trade/>, our mobile applications, and related services (together, the “Platform”). It also explains the rights available to you in respect of your personal data.

1.2. This Policy should be read together with the LineUp Terms & Conditions (<https://lineup.trade/terms>), the Cookie Policy (<https://lineup.trade/cookies>), and the AML/KYC Policy (<https://lineup.trade/aml-kyc>), each of which forms part of your relationship with LineUp. Capitalised terms not defined in this Policy have the meanings given in the Terms & Conditions.

1.3. **Data Controller.** LineUp is the data controller responsible for your personal data, meaning that LineUp determines the purposes and means by which your personal data is processed. The controller's full identity and contact details are set out in Section 17.

1.4. **Regulatory framework.** This Policy is designed principally around the requirements of the European Union General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), which we apply as our global baseline standard. Where you are located in the Dubai International Financial Centre (DIFC), the DIFC Data Protection Law also applies to the processing of your personal data. Where the data-protection laws of another jurisdiction in which we operate grant you additional rights, we honour those rights to the extent they apply to you.

1.5. **Plain language.** We have written this Policy to be clear and understandable while remaining legally precise. If anything is unclear, you may contact us at Support@Lineup.trade for an explanation before you decide whether to use the Platform.

1.6. By accessing or using the Platform, you acknowledge that you have read and understood this Policy. Where we rely on your consent to process personal data, we will request that consent separately, and you may withdraw it as described in Section 12.

2. Definitions

2.1. In this Policy: "personal data" means any information relating to an identified or identifiable natural person; "processing" means any operation performed on personal data, such as collection, use, storage, disclosure, or deletion; "data subject" means the individual to whom personal data relates; "processor" means a third party that processes personal data on our behalf and on our instructions; "special category data" means personal data revealing sensitive characteristics or, as used here, biometric data processed to uniquely identify a person; and "supervisory authority" means the data-protection regulator competent for you.

3. The Personal Data We Collect

We collect personal data in three ways: data you provide to us, data we collect automatically, and data we receive from third parties.

3.1. Data you provide to us.

- (a) **Account data:** your name, username, email address, telephone number, password (stored in hashed form), country of residence, and time zone.
- (b) **Identity and verification (KYC) data:** your full legal name, date of birth, nationality, residential address, government-issued identity documents (such as

passport, national identity card, or driving licence), a photograph or selfie, and, where applicable, a liveness check. A liveness check and any facial-matching step involve **biometric data**, which is special category data and is subject to the additional protections described in Section 4.4.

- (c) **Financial and transaction data:** your linked bank or UPI details as required by our payment partner, deposits, withdrawals, trading activity, positions, balances, fee records, and information about the source of your funds and wealth where we are required to collect it.
- (d) **Wallet data:** the public addresses of any self-custody cryptocurrency wallet you connect to your Account. We never collect, request, or have access to your private keys, seed phrases, or recovery phrases.
- (e) **Communications and preferences:** the content of your communications with us (including support tickets and correspondence), your marketing and notification preferences, and responses to any surveys.

3.2. Data we collect automatically.

- (a) **Device and technical data:** your IP address, device and browser type, operating system, unique device identifiers, application version, language settings, and mobile network information.
- (b) **Usage and interaction data:** how you navigate and interact with the Platform, pages and screens viewed, features used, orders and actions taken, session duration, and referring pages.
- (c) **Approximate location data:** location inferred from your IP address and, where applicable, from your KYC and payment data, which we use to determine eligibility and to enforce the jurisdiction restrictions described in the Terms & Conditions.
- (d) **Diagnostic and crash data:** crash logs, error reports, and performance data used to maintain and improve the Platform.
- (e) **Cookies and similar technologies:** as described in Section 6 and in the Cookie Policy.
- (f) **Analytics data:** collected through Google Analytics and Google Firebase, as described in Section 6.

3.3. Data we receive from third parties.

- (a) our third-party identity-verification provider(s), which verify your identity documents and biometric data and return verification results;
- (b) our third-party blockchain-analytics provider(s), which screen connected wallet addresses against risk and sanctions indicators;

- (c) our payment partner (Razorpay) and other financial-service providers, which confirm and process transactions;
- (d) sanctions, politically-exposed-persons, and adverse-media screening providers; and
- (e) analytics and infrastructure providers, as described in this Policy.

3.4. We do not knowingly collect personal data from any person under the age of 18 (Section 14).

4. How and Why We Use Your Personal Data

4.1. We process personal data only where we have a lawful basis to do so under the GDPR. The following table sets out our principal processing purposes and the corresponding legal bases.

Purpose	Personal data used	Legal basis (GDPR Article 6)
Creating and operating your Account, executing orders, managing positions, and settling trades	Account, financial, transaction, and wallet data	Performance of a contract (Art. 6(1)(b))
Verifying your identity and age, and conducting anti-money-laundering, sanctions, and fraud checks	Identity and verification data, financial data, device data	Compliance with a legal obligation (Art. 6(1)(c))
Preventing, detecting, and investigating fraud, market abuse, and security incidents, and ensuring market integrity	Account, transaction, device, usage, and wallet data	Legitimate interests (Art. 6(1)(f)) and legal obligation (Art. 6(1)(c))
Calculating margin, risk, and exposure, and applying platform controls	Transaction and position data	Performance of a contract (Art. 6(1)(b)) and legitimate interests (Art. 6(1)(f))
Providing customer support and responding to your requests	Account and communications data	Performance of a contract (Art. 6(1)(b)) and legitimate interests (Art. 6(1)(f))
Sending service, transactional, risk, and security communications	Account and contact data	Performance of a contract (Art. 6(1)(b))
Sending marketing communications	Account, contact, and preference data	Consent (Art. 6(1)(a))
Analysing and improving the Platform through analytics and diagnostics	Device, usage, and diagnostic data	Consent (Art. 6(1)(a)) for non-essential analytics, and legitimate interests

Purpose	Personal data used	Legal basis (GDPR Article 6)
		(Art. 6(1)(f))
Complying with legal, regulatory, tax, and court obligations	Any relevant data	Compliance with a legal obligation (Art. 6(1)(c))
Establishing, exercising, or defending legal claims	Any relevant data	Legitimate interests (Art. 6(1)(f))

4.2. Legitimate interests. Where we rely on legitimate interests, those interests are operating a secure, lawful, and orderly trading platform, protecting our Users and the market from abuse and fraud, and developing and improving our services. We balance those interests against your rights and freedoms, and you may object as described in Section 12.

4.3. Consequences of not providing data. Providing identity and verification data is a legal and contractual requirement for using the Platform. If you do not provide it, we cannot verify you and you will not be able to open an Account, deposit, trade, or withdraw.

4.4. Special category (biometric) data. Where identity verification involves biometric data (for example, a liveness check or facial matching), we process that data on the basis of your **explicit consent** (GDPR Article 9(2)(a)) and, where applicable, because processing is necessary for reasons of substantial public interest in preventing financial crime and for compliance with our legal obligations. You may decline biometric verification, but we may then be unable to verify your identity and provide the Platform to you. Biometric data is subject to enhanced security measures and is retained only as long as necessary for verification and legal record-keeping.

5. Automated Decision-Making and Profiling

5.1. We use automated systems to price Synthetic Player Assets, to calculate margin, risk, and liquidation levels, to apply circuit breakers and market controls, to screen identity and wallet data, and to detect fraud and market abuse. These processes may involve automated processing of your personal data.

5.2. Where an automated decision produces legal effects concerning you or similarly significantly affects you (for example, a decision to decline verification, restrict, or close an Account on financial-crime or risk grounds), we take such decisions on the basis of legal obligation or contractual necessity, or with your explicit consent, and we implement suitable measures to safeguard your rights. You may request human review of, express your point of view on, or contest such a decision by contacting Support@Lineup.trade, subject to any legal restriction that prevents us from disclosing the details of financial-crime controls.

6. Analytics, Cookies, and Tracking Technologies

6.1. Analytics providers. We use **Google Analytics** and **Google Firebase** (including its analytics, crash-reporting, and push-notification services) to understand how the Platform

is used, to diagnose problems, and to improve our services. These tools may collect device identifiers, IP address, usage and interaction data, and diagnostic and crash data, and process that data as our processor. Information collected by these tools may be processed by Google as described in its own privacy documentation.

6.2. We do not use Google Analytics or Firebase to sell your personal data or to conduct cross-context behavioural advertising.

6.3. **Cookies and similar technologies.** We and our providers use cookies and similar technologies for essential functions (such as authentication and security), for functional preferences, and, where you consent, for analytics. Non-essential analytics and functional technologies are used only where required consent has been given. You can manage your preferences through our cookie controls and your device or browser settings. Full details are in the Cookie Policy (<https://lineup.trade/cookies>).

7. Marketing Communications

7.1. We send service, transactional, risk, and security communications (such as order confirmations, margin and liquidation notices, and legal notices) as a necessary part of providing the Platform. You cannot opt out of these while your Account is active.

7.2. We send **marketing communications** only where you have consented or where otherwise permitted by applicable law. You may withdraw your consent and unsubscribe at any time using the unsubscribe mechanism in the communication or in your Account settings, without affecting service communications.

8. How We Share Your Personal Data

8.1. We share personal data only as described in this Policy, with the following categories of recipient, and only to the extent necessary:

- (a) **Processors and service providers**, including: our third-party identity-verification provider(s); our third-party blockchain-analytics provider(s); our payment partner (Razorpay) and other financial-service providers; sanctions, politically-exposed-persons, and adverse-media screening providers; cloud hosting and infrastructure providers; analytics providers (Google Analytics and Firebase); communications and customer-support providers; and professional advisers. These processors act on our documented instructions under contracts that impose confidentiality and security obligations.
- (b) **Regulators, authorities, and courts**, including data-protection authorities, financial regulators, tax authorities, law-enforcement agencies, and, in matters of sports integrity, relevant sporting bodies and integrity units, where we are required or permitted by law to disclose. We may be prohibited by law from informing you of certain disclosures made for financial-crime reasons.
- (c) **Corporate transactions**, where we are involved in a merger, acquisition, reorganisation, or sale of assets, in which case personal data may be disclosed to

advisers and prospective counterparties under confidentiality obligations, and any successor will be bound by this Policy or a materially equivalent policy.

8.2. We do not sell your personal data. We do not sell, rent, or trade your personal data to any third party, and we do not share it for third-party advertising or cross-context behavioural advertising.

8.3. Independent controllers. Our payment partner and any wallet provider you choose are independent controllers of the personal data they process under their own terms and privacy notices. Their processing is governed by their own policies, which we encourage you to review.

8.4. A current list of our principal sub-processors is available at <https://lineup.trade/sub-processors>.

9. International Data Transfers

9.1. LineUp operates internationally, and your personal data may be processed in, or accessed from, countries outside your own, including countries that may not provide the same level of data protection as your home jurisdiction.

9.2. Where we transfer personal data outside the European Economic Area, the United Kingdom, or the DIFC to a country that has not received an adequacy decision, we rely on appropriate safeguards, such as the European Commission's Standard Contractual Clauses (and the UK International Data Transfer Agreement or Addendum where applicable), together with any supplementary measures required. Where the DIFC Data Protection Law applies, we transfer personal data in accordance with its permitted transfer mechanisms.

9.3. You may request further information about the safeguards we apply, and a copy where available, by contacting Support@Lineup.trade.

10. Data Retention

10.1. We retain personal data only for as long as necessary for the purposes for which it was collected, including to provide the Platform, to comply with our legal, regulatory, tax, and accounting obligations, to resolve disputes, and to enforce our agreements.

10.2. Anti-money-laundering records. Identity, verification, and transaction records are retained for at least **five years** after the end of your relationship with LineUp, or longer where a longer period is required by applicable law.

10.3. Retention criteria. Where no fixed statutory period applies, we determine the retention period by reference to the nature and sensitivity of the data, the purposes of processing, the potential for harm from unauthorised use or disclosure, applicable limitation periods for legal claims, and applicable legal requirements.

10.4. When personal data is no longer required, we delete it or irreversibly anonymise it. Personal data that we are legally required to retain is securely stored and access-restricted until the retention period expires.

11. Data Security

11.1. We implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These measures include encryption of personal data in transit and at rest, access controls and role-based permissions, network and application security controls, monitoring and logging, and staff confidentiality obligations. Biometric data is subject to enhanced protection.

11.2. **Non-custodial architecture.** LineUp does not custody User funds. Fiat balances are held by our payment partner, and cryptocurrency remains in your self-custody wallet. **You are solely responsible for the security of your wallet, private keys, seed phrases, and recovery phrases, which we never hold and cannot recover.** You are also responsible for safeguarding your Account credentials and for enabling available security features such as two-factor authentication.

11.3. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. In the event of a personal-data breach that is likely to result in a risk to your rights and freedoms, we will notify the competent supervisory authority and, where required, affected individuals, in accordance with applicable law.

12. Your Rights

12.1. Subject to applicable law and to the conditions and exceptions it provides, you have the following rights in respect of your personal data:

- (a) **Access:** to obtain confirmation of whether we process your personal data and a copy of that data;
- (b) **Rectification:** to have inaccurate personal data corrected and incomplete data completed;
- (c) **Erasure:** to have your personal data deleted in certain circumstances (the “right to be forgotten”);
- (d) **Restriction:** to restrict our processing of your personal data in certain circumstances;
- (e) **Portability:** to receive certain personal data in a structured, commonly used, machine-readable format and to have it transmitted to another controller where technically feasible;
- (f) **Objection:** to object to processing based on legitimate interests, and to object to direct marketing at any time;
- (g) **Withdrawal of consent:** to withdraw your consent at any time where we rely on consent, without affecting the lawfulness of processing before withdrawal; and
- (h) **Rights relating to automated decision-making:** as described in Section 5.

12.2. How to exercise your rights. You may exercise your rights by contacting Support@Lineup.trade. We may need to verify your identity before responding. We will respond within the period required by applicable law (under the GDPR, generally within one month, extendable where permitted).

12.3. Limits on your rights. Certain rights are limited where we are legally required to retain or process personal data, in particular for anti-money-laundering, financial-crime, tax, and record-keeping purposes. In such cases we may be unable to erase or stop processing certain data, and we will explain the applicable limitation to the extent we are permitted.

12.4. Complaints. You have the right to lodge a complaint with a supervisory authority. Users in the European Economic Area may complain to the supervisory authority of their country; Users in the United Kingdom may complain to the Information Commissioner's Office; and matters governed by the DIFC Data Protection Law may be raised with the DIFC Commissioner of Data Protection. We ask that you first contact us so that we can try to resolve your concern.

13. Third-Party Services and Links

13.1. The Platform may interact with, or link to, third-party services, including our payment partner, wallet providers, and identity-verification providers. This Policy does not cover the practices of those third parties, which act under their own terms and privacy notices. We encourage you to review their policies before using their services.

14. Children

14.1. The Platform is intended solely for persons aged **18 years or older**, and is **not directed to children**. We do not knowingly collect personal data from anyone under 18.

14.2. If we become aware that we have collected personal data from a person under 18, we will delete that data promptly and close any associated Account. If you believe that a person under 18 has provided us with personal data, please contact Support@Lineup.trade.

15. Changes to This Policy

15.1. We may update this Policy from time to time. When we do, we will revise the "Last Updated" date and, where the changes are material, provide additional notice through the Platform or by email before the changes take effect.

15.2. Your continued use of the Platform after the effective date of an updated Policy constitutes acknowledgement of the updated Policy, except where your consent is required for a specific processing activity, in which case we will obtain that consent separately.

16. Google Play Data Safety Disclosure

16.1. This Section summarises our data practices for the purpose of transparency and consistency with the Google Play Data Safety declaration. In the event of any inconsistency

between this summary and the detailed provisions of this Policy, the detailed provisions govern.

16.2. Data collected and shared. We collect the categories of personal data described in Section 3, including personal identifiers, financial and transaction information, identity and biometric verification data, wallet addresses, device and usage data, approximate location, and diagnostic data. We share data with processors and authorities as described in Section 8. **We do not sell your personal data, and we do not share it for third-party advertising.**

16.3. Purposes. Data is collected and used for account management, identity verification and fraud prevention, financial-crime and legal compliance, providing and securing the Platform, analytics and app performance, customer support, and (with consent) marketing.

16.4. Security and choices. Personal data is encrypted in transit. Users can request access to and deletion of their data as described in Section 12, subject to legal retention requirements. Identity verification is required to use the Platform.

17. Contact Us

Data Controller: LineUp, established in the Emirate of Dubai, United Arab Emirates. Registered office: Dubai, United Arab Emirates (*insert full registered address and trade-licence number before publication*). Website: <https://lineup.trade/>

For any privacy question, to exercise your rights, or to contact our privacy function, email **Support@Lineup.trade**. We will route your request to the appropriate team and respond within the period required by applicable law.