

PRIVACY POLICY

Trade Lumora Pty Ltd

ACN 690 260 390 | ABN 21 690 260 390

Effective Date: 23 March 2026

1. About This Privacy Policy

1.1 This Privacy Policy (**Policy**) sets out how Trade Lumora Pty Ltd (ACN 690 260 390; ABN 21 690 260 390) (**Trade Lumora, TL, we, us or our**) collects, holds, uses, and discloses personal information in connection with the operation of our digital currency exchange platform and related services (the **Platform**).

1.2 We are committed to protecting your privacy and handling your personal information in compliance with the Privacy Act 1988 (Cth) (Privacy Act), including the Australian Privacy Principles (APPs), and any other applicable privacy legislation.

1.3 We are also a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act). Certain obligations under the AML/CTF Act require us to collect, verify, and retain personal information, and these obligations operate in addition to (and in some cases override) the Privacy Act.

1.4 By accessing the Platform, creating an account, or using our services, you acknowledge that you have read and understood this Policy.

2. Information We Collect

2.1 Personal Information You Provide

We collect personal information that you provide to us directly, including when you register for an account, complete identity verification, place an order, or contact us. This may include:

- (a) full legal name;
- (b) date of birth;
- (c) residential address;
- (d) email address;
- (e) telephone number;
- (f) copies of government-issued identification documents (such as a passport, driver's licence, or photo ID card);
- (g) selfie or liveness verification images and video;
- (h) tax file number (TFN) or tax identification number (where required by law);
- (i) source of funds and source of wealth information;
- (j) bank account details, credit or debit card details, and other payment information;
- (k) Digital Currency wallet addresses;
- (l) for non-individual customers: company registration details (including ACN, ABN, and incorporation documents), trust deed details, names of directors, beneficial owners, trustees, and settlors; and
- (m) any other information you provide to us in the course of using the Platform or communicating with us.

2.2 Information Collected Automatically

When you access or use the Platform, we may automatically collect certain information, including:

- (a) device information (such as device type, operating system, and browser type);
- (b) IP address and geolocation data;
- (c) log data (such as access times, pages viewed, and referring URLs);
- (d) transaction data (such as the date, time, type, amount, and details of transactions);
- (e) cookie and tracking technology data (see section 10 below); and
- (f) telephone recordings of conversations with our trading desk (with your consent).

2.3 Information from Third Parties

We may collect personal information about you from third parties, including:

- (a) identity verification service providers (such as Sumsub), including the results of Document Verification Service (DVS) checks, PEP and sanctions screening, and liveness checks;
- (b) credit and financial information from credit reporting bodies or financial institutions;
- (c) publicly available information (including from company registries, court records, and open-source media); and
- (d) information from our liquidity providers, payment service providers, or other business partners.

2.4 Sensitive Information

We do not generally collect sensitive information (as defined in the Privacy Act). However, copies of government-issued identification documents may incidentally reveal information such as nationality, ethnicity, or place of birth. We will only collect such information where it is reasonably necessary for identity verification or compliance with the AML/CTF Laws, and with your consent.

3. How We Use Your Information

3.1 We collect and use your personal information for the following purposes:

- (a) to verify your identity and conduct customer due diligence in accordance with the AML/CTF Laws and our AML/CTF Program;
- (b) to create, administer, and maintain your account;
- (c) to process your transactions, including executing buy and sell orders and managing deposits and withdrawals;
- (d) to maintain and operate Hosted Wallets on your behalf;
- (e) to communicate with you regarding your account, transactions, and our services (including service-related notifications);
- (f) to detect, prevent, and investigate fraud, money laundering, terrorism financing, and other unlawful or suspicious activities;
- (g) to comply with our legal and regulatory obligations, including reporting obligations under the AML/CTF Laws, taxation laws, and any court orders, subpoenas, or regulatory directions;

- (h) to screen customers against sanctions lists, PEP databases, and adverse media sources;
- (i) to conduct transaction monitoring and ongoing customer due diligence;
- (j) to manage and resolve complaints and disputes;
- (k) to improve, develop, and enhance the Platform and our services;
- (l) to conduct data analytics and research (using aggregated or de-identified data where possible);
- (m) to send you marketing communications (with your consent and subject to your right to opt out — see section 11); and
- (n) for any other purpose disclosed to you at the time of collection or to which you have consented.

3.2 If we propose to use your personal information for a purpose other than those set out above, we will seek your consent before doing so, unless the use is permitted or required by law.

4. Legal Basis for Collection and Use

4.1 Under the Privacy Act, we may collect and use personal information where it is reasonably necessary for one or more of our functions or activities. The primary legal bases on which we rely are:

- (a) your consent (for example, when you provide identification documents or opt in to marketing communications);
- (b) the performance of our contract with you (that is, the Terms and Conditions governing your use of the Platform);
- (c) compliance with a legal obligation (including obligations under the AML/CTF Laws, the Corporations Act 2001 (Cth), taxation legislation, and court or regulatory orders); and
- (d) our legitimate interests in operating the Platform, preventing fraud, and improving our services, provided that these interests are not overridden by your rights and interests.

5. Disclosure of Personal Information

5.1 We may disclose your personal information to the following categories of recipients:

- (a) **Regulatory and law enforcement bodies:** including AUSTRAC, the Australian Taxation Office (ATO), the Australian Securities and Investments Commission (ASIC), state and federal police, and other government agencies, where required or authorised by law;
- (b) **Identity verification providers:** such as Sumsub, for the purpose of verifying your identity, conducting DVS checks, and screening against PEP and sanctions databases;
- (c) **Payment service providers:** including fiat currency payment rail providers, for the purpose of processing deposits and withdrawals;

- (d) **Liquidity providers:** for the purpose of sourcing prices and executing transactions on your behalf;
- (e) **Cloud hosting and IT service providers:** including as an example, Amazon Web Services (AWS), for the purpose of hosting and maintaining the Platform and storing data securely;
- (f) **Professional advisers:** including lawyers, accountants, and auditors, for the purpose of obtaining professional advice or conducting audits;
- (g) **Related bodies corporate:** any related body corporate of Trade Lumora (as defined in the Corporations Act 2001 (Cth));
- (h) **Courts and tribunals:** in connection with legal proceedings or in response to a valid subpoena or court order; and
- (i) **Other third parties:** with your consent, or as otherwise permitted or required by law.

5.2 We require all third-party service providers to handle your personal information in accordance with applicable privacy laws and our contractual obligations. We do not sell your personal information to any third party.

6. Overseas Disclosure

6.1 Some of our third-party service providers may be located overseas or may store data overseas. In particular, as an example, any cloud hosting infrastructure may involve data being stored on servers located outside of Australia.

6.2 Before disclosing personal information to an overseas recipient, we will take reasonable steps to ensure that the overseas recipient complies with the APPs or is subject to a law or binding scheme that is at least substantially similar to the APPs, in accordance with APP 8.

6.3 By using the Platform and providing your personal information, you consent to the disclosure of your personal information to overseas recipients for the purposes described in this Policy.

7. Data Retention

7.1 We retain personal information for as long as it is reasonably necessary for the purposes for which it was collected, or as required by law.

7.2 Under the AML/CTF Laws, we are required to retain customer identification records and transaction records for a minimum of seven (7) years after the end of the business relationship or the date of the relevant transaction (whichever is later).

7.3 Where we no longer need your personal information for any purpose (including legal obligations), we will take reasonable steps to destroy or de-identify the information, in accordance with APP 11.2.

8. Data Security

8.1 We take reasonable steps to protect your personal information from misuse, interference, loss, unauthorised access, modification, and disclosure, in accordance with APP 11.1.

8.2 Our security measures include (without limitation):

- (a) encryption of data in transit and at rest;
- (b) access controls limiting access to personal information to authorised personnel on a need-to-know basis;
- (c) secure cloud hosting infrastructure with industry-standard security certifications;
- (d) regular security assessments and vulnerability testing; and
- (e) employee training on data security and privacy obligations.

8.3 Despite these measures, no method of electronic transmission or storage is completely secure. We cannot guarantee the absolute security of your personal information.

8.4 If we become aware of a data breach that is likely to result in serious harm to you, we will notify you and the Office of the Australian Information Commissioner (OAIC) in accordance with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act.

9. Your Rights Under the Australian Privacy Principles

9.1 Access

You have the right to request access to the personal information we hold about you (APP 12). We will respond to your request within a reasonable period (generally 30 days). We may charge a reasonable fee for providing access. In some circumstances, we may refuse access in accordance with the Privacy Act (for example, where providing access would prejudice law enforcement activities or an ongoing investigation).

9.2 Correction

You have the right to request that we correct personal information that is inaccurate, incomplete, out of date, irrelevant, or misleading (APP 13). If we correct information that has previously been disclosed to a third party, we will take reasonable steps to notify that third party of the correction, unless it is impracticable to do so.

9.3 Complaints

If you believe that we have breached the APPs or this Policy, you may lodge a complaint with us (see section 12 below). If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

9.4 Anonymity and Pseudonymity

Under APP 2, you have the right to deal with us anonymously or under a pseudonym. However, due to our obligations under the AML/CTF Laws, we are unable to provide our services to you without verifying your identity. Accordingly, this right does not apply to the extent that it is impracticable for us to deal with you on an anonymous or pseudonymous basis.

10. Cookies and Tracking Technologies

10.1 We may use cookies, web beacons, and similar tracking technologies on the Platform to collect information about your browsing activity and preferences.

10.2 Types of Cookies

We may use the following types of cookies:

- (a) **Essential cookies:** These are necessary for the operation of the Platform, such as session cookies that enable you to log in to your account.
- (b) **Analytics cookies:** These help us understand how visitors interact with the Platform, including which pages are visited most frequently. We may use third-party analytics tools such as Google Analytics for this purpose.
- (c) **Marketing cookies:** These may be used to deliver relevant advertisements and track the effectiveness of marketing campaigns. We may use marketing pixels or tags from third-party advertising platforms.

10.3 Managing Cookies

You can manage your cookie preferences through your browser settings. Most browsers allow you to refuse cookies or alert you when a cookie is being set. Please note that disabling certain cookies may affect the functionality of the Platform.

10.4 Google Analytics

If we use Google Analytics, information collected by Google Analytics will be transmitted to and stored by Google on servers that may be located outside Australia. For more information on how Google collects and processes data, please refer to Google's privacy policy at <https://policies.google.com/privacy>.

11. Marketing Communications

11.1 With your consent, we may send you marketing communications (by email, SMS, or other electronic means) about our products, services, promotions, and news.

11.2 You may opt out of receiving marketing communications at any time by:

- (a) clicking the "unsubscribe" link in any marketing email;
- (b) replying "STOP" to any marketing SMS; or
- (c) contacting us at service@tradelumora.com.

11.3 We will process your opt-out request as soon as practicable. Please note that even if you opt out of marketing communications, we may still send you service-related communications that are necessary for the operation of your account (such as transaction confirmations, security alerts, and regulatory notices).

11.4 Our marketing communications will comply with the Spam Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth), as applicable.

12. Privacy Complaints

12.1 If you have a complaint about how we have handled your personal information, please contact our Privacy Officer at:

Email: service@tradelumora.com

Subject Line: Privacy Complaint

12.2 We will acknowledge receipt of your complaint within 5 business days and will endeavour to investigate and respond to your complaint within 30 days.

12.3 If you are not satisfied with our response, you may escalate your complaint to the Office of the Australian Information Commissioner (OAIC):

Online: www.oaic.gov.au

Phone: 1300 363 992

Post: GPO Box 5218, Sydney NSW 2001

13. Changes to This Policy

13.1 We may update this Policy from time to time to reflect changes in our practices, legal requirements, or for other operational reasons. Where we make material changes, we will publish the updated Policy on the Platform and, where practicable, notify you by email.

13.2 The date of the most recent update will be indicated at the top of this Policy. We encourage you to review this Policy periodically.

14. Contact Us

If you have any questions about this Privacy Policy or our handling of your personal information, please contact us at:

Trade Lumora Pty Ltd

ACN 690 260 390

Email: service@tradelumora.com