

KAURIFINANCE OÜ PRIVACY POLICY

KAURIFINANCE OÜ

Registration code: 14559136

Address: Harju maakond, Tallinn,

Kesklinna linnaosa, Jõe tn 2a

Email: kyc@kauri.finance

Effective from:

06.08.2025

1. INTRODUCTION.....	1
2. DEFINITIONS.....	2
3. IMPORTANT INFORMATION.....	3
4. THE DATA WE MAY COLLECT ABOUT YOU.....	3
5. ORDERS.....	4
6. RETENTION OF PERSONAL DATA.....	5
7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES.....	6
8. INTERNATIONAL TRANSFERS.....	6
9. AUTOMATED DECISION-MAKING.....	6
10. YOUR RIGHTS REGARDING YOUR PERSONAL DATA.....	7

1. INTRODUCTION

1.1. At KAURIFINANCE OÜ, your privacy and trust are of utmost importance. This Privacy Policy explains how we collect, use, disclose, and protect your personal data when you interact with our website and services.

1.2. By accessing our website (<https://kauri.finance>) or using our services, you agree to the terms of this Policy.

1.3. We are committed to safeguarding your personal information, both online and offline. This Policy applies to all services provided through the KAURIFINANCE website (the Website) and any related platforms or tools we operate (collectively, the Platform).

1.4. Please read this Policy. If you have any questions about our data protection practices, you can reach out to us by email: kyc@kauri.finance

1.5. We may update this Policy from time to time. Any significant changes will be communicated via email or another way. This version of the Privacy Policy was last updated on the “Effective from” date mentioned above.

1.6. This Privacy Policy (“Policy”) describes how KAURIFINANCE OÜ collects, uses, processes, and protects personal data of clients, prospective clients, and website visitors (“you”), and outlines your rights under applicable data protection law.

1.7. KAURIFINANCE OÜ is a private limited company registered in Estonia (registry code: 14559136), with its registered address at Jõe tn 2a, 10151, Tallinn, Estonia. We hold a Virtual Asset Service Provider License No. FVT000328, issued on 17.11.2020.

1.8. If this Policy is published in different languages and any discrepancies arise, the English version shall prevail.

1.9. This Policy does not cover personal data processing on third-party websites or applications which may be linked from our website.

2. DEFINITIONS

Definitions are listed below in the order in which they appear in the text of the current Policy..

Term	Definition
AML	Anti-Money Laundering – legal frameworks used to prevent money laundering and terrorism financing.
Consent	A freely given, specific, informed, and unambiguous indication of a data subject’s agreement to process personal data.
Controller	The entity that determines the purposes and means of processing personal data.
Cookies	Small text files stored on a user’s browser to collect information about website usage.
Data Subject	The individual whose personal data is processed.
EEA	European Economic Area – includes EU countries and a few additional nations adhering to GDPR rules.

GDPR	The General Data Protection Regulation (EU) 2016/679.
Legitimate Interest	A lawful basis for processing data when it serves a clear and necessary business or legal purpose.
PEP	Politically Exposed Person – an individual with a prominent public function and their relatives/associates.
Personal Data	Any information relating to an identified or identifiable natural person.
Processing	Any operation or set of operations performed on personal data (e.g., collection, use, disclosure).
Processor	A third party that processes personal data on behalf of the controller.
User	This means a User of the Company who has registered and duly verified their identity on the Platform. The User can be either an individual or a corporate entity.

3. IMPORTANT INFORMATION

3.1. KAURIFINANCE OÜ acts as a data controller. We collect, use, disclose, transfer, and store your personal data where necessary to deliver our services and to support our operational and business activities, as outlined in this Policy. Our aim is to be transparent about how we handle your information so that you can make informed decisions about the use of your personal data.

3.2. If you do not provide certain information when requested, we may be unable to provide some services, such as identity verification or account registration.

3.3. You may contact our team with questions about your data or rights at kyc@kauri.finance.

3.4. If you are unsatisfied with our handling of your data, you may contact the Estonian Data Protection Inspectorate. The Estonian Data Protection Inspectorate can be contacted at: address: Tatari tn 39, 10134

Tallinn, Estonia; phone: (+372) 627 4135, +372 5620 2341 and Email: info@aki.ee. Further information is available on the Data Protection Inspectorate's website: www.aki.ee.

4. THE DATA WE MAY COLLECT ABOUT YOU

4.1. We may collect the following types of personal data, as necessary for providing our services and complying with legal obligations:

Data Category	Description
Identity Information	Full name, date of birth, national ID/passport data, gender, TIN, etc.
Contact Information	Email, phone number, residential address.
Biometric Data	Facial image or video used for liveness and identity verification.
Financial Information	Wallet addresses, bank/payment card details, source of funds/wealth.
Economic Profile	Income level, employment information, occupation.
PEP Information	Status as a politically exposed or linked individual.
Transactional Information	Crypto and fiat transaction data, including recipient address, transaction ID.
Device Information	Device ID, OS, hardware model, IP address, browser data.
Location Information	IP-derived or GPS-based location.
Log Information	Timestamps, login data, and authentication history.
Other Information	Any data voluntarily submitted or collected for AML/sanctions compliance.

4.2. We do not intentionally collect sensitive data such as race, ethnicity, health information, or

religious beliefs, except where required by law.

4.3. We use your personal data for the following purposes:

4.3.1. To register your User Account on our Platform;

4.3.2. To provide services, including processing transactions, enabling access to the Platform, managing your account, and fulfilling our contractual obligations;

4.3.3. To communicate with you, for customer support, service-related updates, and responding to your enquiries;

4.3.4. To provide relevant information about the products and markets you interact with on the Platform;

4.3.5. To promote our services in accordance with our legitimate interests, we may use your information to market our products and services to users with similar profiles.

4.4. If we intend to use your personal data for any other purpose not covered in this Policy, we will provide a separate notice and, where necessary, request your consent in advance.

4.5. We use certain types of personal data, such as your location, trading history, and related activity, to deliver personalised content, including news updates, research materials, reports, and market information. This allows us to tailor your experience and ensure that the services we provide are relevant to your interests and trading behaviour.

4.6. In addition, we collect and process anonymised, non-personal data for statistical analysis and internal reporting. This helps us improve the performance, functionality, and quality of our services over time.

4.7. Cookies are small text files that are stored on your device and are commonly used across websites and online services. We use cookies on our Website and Platform to enhance user experience, analyse performance, and support essential platform features.

5. ORDERS

5.1. We process your personal data based on one or more of the legal bases outlined in the General Data Protection Regulation (GDPR). The table below describes the purposes for which we process your data and the corresponding legal grounds.

Purpose of Processing	Categories of Personal Data	Legal Basis
Identity verification, customer due diligence, and onboarding	Identity, contact, biometric, financial, economic profile, PEP information, location data	Legal obligation under AML laws and performance of contract
Processing payments and providing services	Identity, contact, financial, transactional, economic profile, log data	Performance of contract

Communication about services and account matters	Identity, contact, transactional	Performance of contract
Direct marketing (newsletters, offers, service updates)	Identity, contact, financial, and log data	Consent
Service improvement and customer analytics	Identity, contact, financial, PEP, log, location, device	Legitimate interest (ensuring service relevance and quality)
Location-based due diligence (e.g. IP-based geolocation)	Location, device, log	Consent
Legal and regulatory compliance (e.g. disclosures to authorities)	All categories of data	Legal obligation
Ongoing verification and monitoring (e.g. updating data)	Identity, contact, financial, PEP, location	Legal obligation, legitimate interest (fraud prevention)
Risk assessment and fraud prevention	Identity, economic profile, transaction, device, log	Legitimate interest (security and crime prevention)
Pricing strategy and internal business planning	Financial, economic profile	Legitimate interest
AML plausibility assessments (e.g. evaluating source of funds)	Economic profile, financial information	Consent
Use of third-party providers (e.g. legal, analytics, IT)	All relevant categories	Legitimate interest (business operations)

Any other purpose for which you explicitly instruct us	Any data provided by you	Consent
--	--------------------------	---------

5.2. Where applicable laws require us to rely on your consent as the lawful basis for certain types of processing (e.g. marketing or biometrics), you may withdraw your consent at any time by contacting us.

6. RETENTION OF PERSONAL DATA

6.1. We retain personal data only for as long as necessary to fulfil the purposes outlined above and to comply with our legal and regulatory obligations, including anti-money laundering requirements.

Data Category	Retention Period
Identity, contact, financial, economic profile, biometric, transactional, PEP, device, log, location information	5 years after termination of the business relationship
Personal data stored on blockchain	Permanently stored and immutable, though anonymised where possible

6.2. Some data may be retained in anonymised format for statistical or analytical purposes beyond the retention periods listed above.

7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

7.1. We may disclose your personal data to third parties where necessary for the performance of services, compliance with legal obligations, or to protect our legitimate interests. These parties include:

- Financial institutions, payment processors, and blockchain analytics providers
- Legal, audit, consulting, compliance, and regulatory professionals
- Hosting and IT service providers
- Identity verification partners such as **Sum and Substance Ltd** and **SumSub Tech Ltd**
- AML and sanctions compliance providers

7.2. Each third party is required to adhere to data protection agreements in line with Article 28(3) GDPR and to implement appropriate confidentiality and security measures.

8. INTERNATIONAL TRANSFERS

8.1. If we transfer personal data outside the European Economic Area (EEA) or the United Kingdom, we ensure such transfers are compliant with the GDPR. This includes:

- 8.1.1. Use of countries with adequacy decisions from the European Commission
- 8.1.2. Standard Contractual Clauses (SCCs) or other appropriate safeguards
- 8.1.3. Ongoing assessment of the legal framework in the receiving country

8.2. You may request a copy of the safeguards applied to your data by contacting us.

9. AUTOMATED DECISION-MAKING

9.1. We may use automated processes to assist in decision-making, particularly for identity verification. For example, biometric data collected via third-party tools may be automatically compared against your submitted ID to approve, reject, or flag a verification.

9.2. This is necessary for the performance of our contract with you and to comply with AML obligations. However, you maintain the right to:

- 9.2.1. Request human review
- 9.2.2. Express your point of view
- 9.2.3. Contest a decision made solely through automated means

9.3. These rights are available under Article 22(3) of the GDPR.

10. LEGAL AND REGULATORY OBLIGATIONS

10.1. We may retain and use your personal data as required to meet our internal compliance procedures, AML audit requirements, and data security standards. In certain circumstances, we are also legally obligated - or consider it necessary - to process personal data for the following purposes:

- 10.1.1. To comply with applicable laws and regulations, including those outside your country of residence;
- 10.1.2. To respond to lawful requests from courts, law enforcement authorities, regulatory bodies, or other governmental entities, whether domestic or foreign;
- 10.1.3. To monitor and enforce compliance with our Platform's terms and conditions;
- 10.1.4. To conduct anti-money laundering (AML), counter-terrorism financing (CTF), sanctions screening, and Know Your Customer (KYC) checks as required by law;
- 10.1.5. To protect our legal rights, safety, property, and the rights and safety of others.

10.2. We may also be required to retain certain personal data after you close your account with us, for legal or regulatory reasons. This includes, for example, the prevention, detection, or investigation of fraud, financial crime, or other unlawful activity.

10.3. We are committed to safeguarding your personal data and have implemented appropriate technical and organisational measures to ensure a level of security that is proportionate to the risk. These measures are designed to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access—whether the data is being transmitted, stored, or

otherwise processed.

10.4. We retain personal data only for as long as necessary to fulfil our legal, regulatory, and business obligations, subject to any minimum statutory or regulatory retention periods. When determining the appropriate retention period, we consider local legal requirements, contractual commitments, and the nature of the data involved. Once your data is no longer needed, we take appropriate steps to securely delete or destroy it.

11. YOUR RIGHTS REGARDING YOUR PERSONAL DATA

11.1. You have the following rights under GDPR, which you may exercise at any time by contacting us at kyc@kauri.finance:

11.1.1. Access – Request confirmation on whether we process your personal data and access to such data.

11.1.2. Rectification – Request correction of inaccurate or outdated personal data.

11.1.3. Erasure – Request deletion of your data where no lawful basis for retention remains.

11.1.4. Restriction of Processing – Ask us to pause processing where accuracy is contested or legal grounds are in question.

11.1.5. Data Portability – Request your data in a structured, machine-readable format, where applicable.

11.1.6. Objection – Object to processing where based on our legitimate interest, including for direct marketing.

11.2. The request for a data deletion is possible if the law does not oblige us as an entity under license to obtain data, for instance, AML-related data.

11.3. We may ask you to verify your identity before fulfilling any such request. If you believe we have not handled your data appropriately, you also have the right to lodge a complaint with the Estonian Data Protection Inspectorate.

THE COMPANY RESERVES THE RIGHT TO AMEND THIS PRIVACY POLICY AT ANY TIME, INFORMING THE EXISTING USERS ABOUT IT PRIOR TO 1 MONTH, AS WELL AS PROVIDING OTHER SERVICES ACCOMPANYING THE SERVICES MENTIONED HEREIN.

If there are any questions regarding this Policy, you may reach our Support Team at support@kauri.finance.