PRIVACY POLICY

Last updated: 8 September, 2025

*At Avelot Limited, a company registered in Hong Kong ("**Purefi**", "**we**," "**us**," or "**our**"), we process your personal data in accordance with applicable privacy laws. This Privacy Policy explains how we collect, use, store, share, and protect personal information in connection with our KYC/KYT services provided through our website https://purefi.io/ and related API platforms (collectively, the "**Service**"). We operate in compliance with the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") and, where applicable, the European Union General Data Protection Regulation ("**GDPR**") for residents of the European Economic Area (**EEA**).*

*This policy applies to all users of our Service, including individuals and businesses ("**you**" or "**your**"). By using our Service, you agree to the collection and use of information as described in this Privacy Policy. For EEA residents, please refer to the **Annex for EEA Residents** for additional GDPR-specific provisions.*

To provide Services, Purefi processes Personal data according to our Clients instructions. Clients are Controllers that determine purposes of data processing, exercise control over Users' Personal data, and stipulate retention periods of Users' data according to their purposes. Purefi, in turn, is a Processor that conducts only those data processing activities that Clients request. Before passing such procedures, Users should be properly notified by Clients in line with their privacy policies and, depending on Clients' legal basis for data processing, may be asked to consent to such processing.

When developing and improving Services and in other cases specified in this Privacy Policy, Purefi is the Controller of Users' Personal data.

1. DEFINITIONS

Personal Data: Information relating to an identified or identifiable individual, including but not limited to name, identification numbers, location data, or other identifiers.

Service: The KYC/KYT and other compliance solutions provided through https://purefi.io/, including KYC (Know-Your-Customer), AML (Anti-Money Laundering) screening, and KYB (Know Your Business) checks.

Data Controller: The entity that determines the purposes and means of processing personal data.

Data Processor: An entity that processes personal data on behalf of a data controller.

2. INFORMATION WE COLLECT

We collect the following types of information in connection with our Service:

2.1 Personal Data You Provide

- **Identity Information**: Name, date of birth, government-issued identification numbers (e.g., passport, ID card, driver's license), photographs, or biometric data (e.g., facial recognition data for liveness detection).
- **Contact Information**: Email address, phone number, or address.
- **Business Information**: For KYB services, we may collect business registration details, incorporation documents, tax information, or beneficial ownership data.
- **Verification Data**: Proof of address, source of funds, or other documents submitted for KYC/AML compliance.

2.2 Information Collected Automatically

- **Usage Data**: IP address and browsing behavior on our website.
- **Cookies and Tracking Technologies**: We use cookies to enhance user experience, analyze usage, and improve our Service. You can manage cookie preferences through your browser settings.
- **Transaction data**: We may collect the crypto addresses associated with you for KYT check. KYT check is a check that analyses transaction data relating to senders and recipients. It enables clients to detect and report unusual/uncharacteristic behaviour and patterns that are characteristic of money laundering, terrorist financing, fraud, or other illicit activity.

2.3 Information from Third Parties

We may obtain data from government registries, public authorities, third-party compliance service providers or databases (e.g., sanctions lists, PEP lists) to perform KYC/AML checks.

3. HOW WE USE YOUR INFORMATION

We use your personal data for the following purposes, in compliance with the PDPO and, where applicable, GDPR:

- To Provide and Maintain the Service: Verify identities, conduct KYC/KYB/AML checks, and ensure compliance with regulatory requirements.
- Customer Support: Respond to inquiries, provide technical assistance, and resolve issues.
- Compliance with Legal Obligations: Fulfill obligations under anti-money laundering, counter-terrorist financing, and other applicable regulations.
- Service Improvement: Analyze usage data to enhance the functionality and performance of our Service.
- Notifications: Inform you about updates to our Service, account status, or subscription renewals.
- Marketing: With your consent, provide news, offers, or information about related services, unless you opt out.
- Fraud Prevention: Detect, prevent, and address fraudulent activities or security threats.

4. PURPOSE AND LEGAL BASIS OF PROCESSING

4.1. Performance of the Agreement

While serving Clients, We primarily act as a Processor, handling your data for the benefit of our Clients. We process Personal data to fulfill Agreements, including the provision of specified Services, obligations arising from Agreements, and associated rights, as well as to execute rights and obligations under applicable legal acts and to address Users' requests. Purefi collects and processes Users' data on behalf of Clients, which may involve compliance with applicable AML/CFT and other laws, regulations, and/or Clients' internal customer due diligence procedures. Once Personal data is no longer needed for the relevant purpose, and upon the Client's written instructions, We transfer the data to Clients and delete it from our servers without retaining any backup copies.

4.2. Other Purposes

We may process your data for purposes that serve our legitimate interests, including the following:

- Where permitted by applicable laws and with our Clients' consent, We may process certain Personal data to develop and enhance our Services, including preventing and detecting fraud and other illicit activities using artificial intelligence;
- Given the nature of our Services, We aim to detect and prevent criminal activity, fraud, and money laundering by cross-referencing User data with records of confirmed or suspected illegal activities, fraud, or money laundering. If such issues are identified, We will notify our Clients;
- In connection with the above, We may conduct profiling, statistical analysis, and analytics to identify AML/CFT trends, fraud detection, and prevention. Our system may aggregate Users' data to generate reports and charts that Clients can use to assess risk likelihood associated with specific characteristics;
- We may process Personal data, including biometric data, to identify a User or a Client's representative for identity verification purposes, enabling us to process data subject access requests or Client requests accordingly;
- We may be required to process or retain certain Personal data for the establishment, exercise, or defense of legal claims;
- For crypto-related services, We may process Users' Personal data to establish and maintain a wallet address book.

We process certain Personal data in adherence to principles of lawfulness and accountability, ensuring a legal basis for processing specific Personal data concerning certain Users, as required by applicable laws.

5. SHARING AND DISCLOSURE

We may share your personal data in the following circumstances:

1. With Service Providers: We engage third-party processors (e.g., cloud hosting, analytics providers, or compliance providers and databases, etc) to support our Service. These providers are bound by data protection agreements to ensure confidentiality and security.

2. With Clients: If we act as a data processor on behalf of a Client, we share verification results with the Client.

3. For Legal Compliance: We may disclose data to public authorities or law enforcement if required by law or in response to valid requests.

4. Business Transfers: In the event of a merger, acquisition, or asset sale, personal data may be transferred to the acquiring entity.

5. With Affiliates: We may share data with our subsidiaries or affiliates for internal business purposes, subject to this Privacy Policy.

We do not sell or lease your personal data to third parties for marketing purposes without your explicit consent.

6. DATA SECURITY

We implement appropriate technical and organizational measures to protect your personal data, including:

- Encryption of data in transit and at rest.

- Access controls to limit data access to authorized personnel.

- Regular security audits and vulnerability assessments.

Despite these measures, no online system is completely secure. If a data breach occurs, we will notify affected individuals and relevant authorities as required by law.

7. DATA RETENTION

We retain personal data only for as long as necessary to fulfill the purposes outlined in this Privacy Policy or as required by law. After the retention period, we securely delete or anonymize your data.

Please note that if you, as a User, would like to make a request to delete the personal data that you have provided for the purpose of a particular Client, please make that request directly to the Client that controls your verification process.

8. YOUR RIGHTS UNDER THE PDPO

Under the PDPO, you have the following rights:

- Access: Request access to the personal data we hold about you.

- Correction: Request correction of inaccurate or incomplete data.

- Objection: Object to the use of your data for certain purposes, such as direct marketing.

To exercise these rights, contact us at support@purefi.io.

For EEA residents, additional rights under GDPR are outlined in the **Annex for EEA Residents**.

9. INTERNATIONAL DATA TRANSFERS

As a Hong Kong-based company, we may transfer personal data to jurisdictions outside Hong Kong, including for processing by third-party service providers. We ensure that such transfers comply with the applicable laws and include appropriate safeguards, such as contractual clauses or encryption.

10. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices or legal requirements. In case of any change, we will amend the date of the last update at the beginning of these Privacy Policy. By continuing using our Services, or other method of legal consent, you are agreeing to the changes/updated terms and will be legally bound by them. Please check this page regularly for updates.

11. CONTACT US

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Email: support@purefi.io

ANNEX FOR EEA RESIDENTS (GDPR COMPLIANCE)

This Annex applies to individuals residing in the European Economic Area (EEA) and supplements the main Privacy Policy to ensure compliance with the General Data Protection Regulation (GDPR).

1. Legal Bases for Processing

We process your personal data under the following GDPR legal bases:

Consent – freely given, informed, and unambiguous indication of your wishes to the processing of your personal data for a specific purpose which signifies agreement to the processing of personal data.

Contract – a legal ground for the processing of the personal data necessary for us to perform a contract or the terms of service to which you are a party or in order to take steps at your request prior to entering into the contract or the terms of service.

Legal obligations – a legal ground for the processing of the personal data when there is an obligation to comply with a legal obligation to which we are subject.

Legitimate Interests – a legal ground for the processing of the personal data when it is based on our legitimate interests or the legitimate interests of a third party, provided that those interests are not outweighed by your rights and interests and those interests have a specific purpose, they are necessary, and they are balanced.

Applicable laws have other legal grounds for the processing and when they are applicable we will use such grounds to process the personal data.

2. Your GDPR Rights

You can exercise the following rights by contacting us.

You have the right to access information about you, especially:

- the categories of data;
- the purposes of data processing;
- third parties to whom the data disclosed;
- how long the data will be retained and the criteria used to determine that period;
- other rights regarding the use of your data.

The right to access information may be performed only by you or your legal representative. In case if you request the right to access information via a legal representative, you have to provide proof of whether such a person may represent you.

You have the right to make us correct any inaccurate personal data about you.

You can object to using your personal data for profiling you or making automated decisions about you. We may use your data to determine whether we should let you know the information that might be relevant to you.

You have the right to restrict processing – You have the right to ask us to restrict the processing of your personal data in certain circumstances.

You have the right to the data portability of your data to another service or website. We will give you a copy of your data in a readable format so that you can provide it to another service. If you ask us and it is technically possible, we will directly transfer the data to the other service for you.

You have the right to be "forgotten". You may ask to erase any personal data about you if it is no longer necessary for us to store the data or in other certain circumstances. We will also deactivate your account. Please, note, that we cannot restore permanently deleted accounts or personal data.

You have the right to lodge a complaint regarding the use of your data by us.

Once we receive any of your requests we will consider and decide on it within one month unless there is a justified requirement to provide such information faster. This term may be extended according to the applicable law.

We may request specific information from you to confirm your identity when necessary and reasonable. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

You do not need to pay a fee to access information or other rights but we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive or refuse to comply with your request in these circumstances.