P A Y K I L L A

Anti-Money Laundering & Counter-Terrorist Financing Policy

For users of paykilla.com

Operator: Limited Liability Company "INGRASE"
Jurisdiction: Republic of Seychelles
IBC Registration Number: 245602
Registered Office: House of Francis, Room 303, Ile Du Port, Mahe, Seychelles
Director: Pareizs Normunds
Contact: info@paykilla.com

Effective date: 21 May 2026 · **Version:** 1.0

Last updated: 21 May 2026

PayKilla is committed to keeping the crypto economy clean. This page explains, in plain language, how we fight money laundering, terrorist financing, sanctions evasion, and other financial crime — and what we expect from you when you use our service.

The legal entity behind PayKilla is **Limited Liability Company "INGRASE"**, incorporated under the laws of the Republic of Seychelles on 5 March 2025 under IBC registration number **245602**, with registered office at **House of Francis, Room 303, Ile Du Port, Mahe, Seychelles**, represented by its director **Pareizs Normunds** ("we", "us", "PayKilla").

This Policy applies to everyone who uses or applies to use **paykilla.com** and the services we offer through it.

1. Our commitment

We follow the law and the global standards that apply to crypto payments, including:

- the Seychelles **Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020** and the guidance of the Seychelles **Financial Intelligence Unit (FIU)**;
- the **Recommendations of the Financial Action Task Force (FATF)**, including the Travel Rule;
- international sanctions issued by the **UN, EU, UK (OFSI), and OFAC**.

We have an internal AML/CFT framework, a designated Money Laundering Reporting Officer (MLRO), regular staff training, ongoing transaction monitoring, and independent reviews of how we comply.

2. Who we cannot serve

We do **not** provide our service to certain people and places. If any of the points below apply to you, please do not sign up — and if you have already signed up, your account will be closed.

2.1. No users from the United States

PayKilla does not accept users from the United States of America.

This means we do not onboard, serve, or process payments for:

- citizens or residents of the United States, wherever they currently live;
- companies, partnerships, LLCs, trusts, or other entities formed under U.S. federal or state law;
- branches or agencies of foreign entities located in the U.S.;
- anyone acting on behalf of any of the above;
- anyone whose access is routed from the United States, including U.S. territories and possessions (Puerto Rico, Guam, U.S. Virgin Islands, American Samoa, Northern Mariana Islands).

By using PayKilla you confirm that you are not a U.S. Person and that you are not using the service on behalf of one. If we discover otherwise, we reserve the right to suspend or close your account and to freeze or return funds.

2.2. No users from sanctioned or high-risk jurisdictions

We do not accept users located in, resident in, or operating from:

- comprehensively sanctioned countries and regions, including **North Korea (DPRK), Iran, Syria, Cuba**, and the non-government-controlled areas of Ukraine (**Crimea, Donetsk, Luhansk, Kherson, Zaporizhzhia**);
- countries identified by the **FATF** as subject to a call for action (so-called "black list");
- any other jurisdiction we identify as presenting an unacceptable financial-crime risk.

This list is updated as the world changes; we may add or remove jurisdictions without prior notice.

2.3. No prohibited businesses

We do not work with, and we do not process payments for, businesses involved in (among other things):

- illegal goods or services in the country where they are sold;
- narcotics and controlled substances;
- weapons, ammunition, explosives, and dual-use military goods;
- human trafficking, modern slavery, and any form of exploitation;
- child sexual abuse material;
- terrorism and the financing of designated terrorist groups;
- unlicensed gambling and illegal lotteries;
- Ponzi, pyramid, and "HYIP" schemes;
- darknet marketplaces, mixers, tumblers, and other anonymising services;
- ransomware, malware, hacking-as-a-service, and other cybercrime;
- counterfeit goods and IP infringement;
- unlicensed financial services (exchange, banking, securities, money transmission).

We may decline or end any relationship at our sole discretion if we believe an activity creates an unacceptable risk — even if it is not explicitly listed above.

3. Know Your Customer (KYC)

Before we open an account and during the relationship, we need to know who you are. This is called Customer Due Diligence ("CDD") or, for higher-risk cases, Enhanced Due Diligence ("EDD").

What we ask for

If you are an individual sole proprietor or an authorised representative of a company, we typically ask for:

- your full name, date of birth, nationality, and country of residence;
- a valid government-issued photo ID (passport, national ID, or driver's licence);
- proof of address (utility bill, bank statement, or equivalent issued within the last 3 months);
- a selfie or short liveness video to confirm it's really you;
- information about your role and authority to act for the business.

If you are a company, we additionally ask for:

- certificate of incorporation and constitutional documents;
- recent extract from the commercial register (not older than 3 months);
- the full ownership and control structure, down to every **Ultimate Beneficial Owner (UBO)** holding 25% or more, or otherwise exercising control;
- ID verification for directors, officers, and UBOs;
- a description of your business, products, target markets, and expected payment volumes;
- your website(s) and any licences you hold;
- information on the source of funds and the source of wealth where relevant.

When we ask for more

In higher-risk situations we may request additional information and documents, ask for senior management approval before opening or continuing the account, set transaction limits, or apply closer monitoring. Higher risk may arise from, for example, a politically exposed person ("PEP") being involved, a complex ownership structure, exposure to high-risk industries or countries, or unusual transaction patterns.

Keeping information current

You agree to keep your information up to date and to inform us promptly of any material change — for example a change of ownership, business model, contact details, or licensing status. We may also ask for refreshed documents periodically.

4. Sanctions and wallet screening

We check our users, their representatives, their beneficial owners, and — where technically possible — the counterparties of on-chain transactions against international sanctions lists (**UN, EU, UK/OFSI, OFAC**) and reputable PEP and adverse-media databases.

For crypto specifically, we use **blockchain analytics** to assess wallet addresses involved in transactions for direct or indirect exposure to:

- sanctioned addresses,
- mixers and tumblers,
- darknet markets,
- ransomware and scam-related addresses,
- stolen funds, and
- other illicit categories.

If we identify a match or a serious risk, we may freeze funds, refuse the transaction, terminate the relationship, and report the matter to the competent authorities — as required by law.

5. Ongoing transaction monitoring

Once you start using PayKilla, our systems continuously monitor the payments processed through your account. We look for patterns that don't match your declared profile, including (but not limited to):

- unusual volumes, frequency, or velocity;
- structuring (splitting payments to stay below thresholds);
- rapid pass-through activity;
- exposure to high-risk wallets, services, or jurisdictions;
- attempts to use the service from a restricted location or by a U.S. Person.

Our compliance team reviews the alerts these systems generate. We may contact you to ask for additional information or supporting documents — and you agree to respond honestly and promptly.

6. Travel Rule

Where required, we comply with the **FATF Travel Rule (Recommendation 16)** and exchange required originator and beneficiary information with counterparty crypto service providers for qualifying transactions. We may refuse a transaction if the required information cannot be obtained or if the counterparty cannot meet the Travel Rule.

7. Suspicious activity reporting

If we suspect, or have reasonable grounds to suspect, that a transaction or attempted transaction relates to money laundering, terrorist financing, sanctions evasion, fraud, or any other crime, we will report it to the **Financial Intelligence Unit of Seychelles** in line with applicable law.

We are legally prohibited from telling you, or anyone else, that such a report has been made or is being considered. This is called the "no tipping-off" rule.

8. Record keeping

We keep your KYC information, transaction records, and AML-related documentation for at least **seven (7) years** after the end of our relationship or after the transaction, or longer where the law or a competent authority requires. Records are stored securely and accessed only by authorised personnel, in line with our **Privacy Policy**.

9. What we expect from you

By using PayKilla you commit to the following:

1. You will provide accurate, complete, and up-to-date information and documents whenever we ask.
2. You will not use PayKilla, directly or indirectly, for any illegal or prohibited purpose (see Section 2.3).
3. You will not let any **U.S. Person**, any user from a sanctioned or restricted jurisdiction, or any sanctioned person access PayKilla through your integration.
4. You will run your own AML/KYC/sanctions/fraud controls on your customers, appropriate to your business and the laws that apply to you.
5. You will cooperate in good faith with reasonable requests from our compliance team.

If you don't, we may restrict, suspend, or close your account, hold or return funds, and report the matter to the authorities — all in accordance with applicable law and our Terms and Conditions.

10. Cooperation with authorities

We cooperate fully with financial intelligence units, regulators, law enforcement, courts, and other competent authorities in connection with investigations into money laundering, terrorist financing, sanctions, and related offences — within the limits set by applicable law and respecting your rights.

11. Changes to this Policy

We review this Policy at least once a year and update it whenever the law, our business, or our risk profile changes. The current version is always available at **paykilla.com**, and the "Last updated" date at the top of the page tells you when the latest version took effect.

12. Contact

If you have any questions about this Policy, or you need to send a message to our Money Laundering Reporting Officer (MLRO), please contact us at:

> **Limited Liability Company "INGRASE"**
> House of Francis, Room 303, Ile Du Port, Mahe, Seychelles
> IBC Registration Number: 245602
> Email: **info@paykilla.com**

If anything in this Policy is inconsistent with mandatory applicable law, the law prevails.