AML/KYC Policy

Last Updated: 16 November 2020

1. Introduction

1.1. NOWPayments NOWPayments Ltd., a company duly organized under the laws of Seychelles (**"the Company"**), is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Anti-Terrorist Financing, requires its management and employees to follow the named standards and actively prevents any actions that aim or facilitate the process of legalizing of illegally gained funds.
1.2. This AML/KYC Policy ("**the Policy"**) means preventing the use of the Company's services by the customers with the aim of money laundering, terrorist financing or other criminal activity.
1.3. The Company may change the Policy from time to time based on the industry standards and applicable legislation. Please review the "Last Updated" legend at the top of this page to determine when this Policy was last amended. Any changes to this Policy will become effective on the "Last Updated" date indicated above.

2. KYC and Customer Due Diligence

2.1. Company must identify all customers who wants to use the Company's services (regardless of whether the customer is a regular customer or not), and each customer of the Company has to finish a verification procedure.
2.2. *Individual customers*
For using the Company's services, each customer shall provide personal information, specifically:

Information collected	Purpose of collection of data
full name of the customer	● to provide the Company's services; ● to resolve the customer's claims; ● to communicate with the customer.
date of birth of the customer	
customer's e-mail	
origin of the customer (customer's place of residence)	
address of the customer's payment wallet	

The customer shall provide the Company with following valid documents serve as basis for identification:

- proof of identification (high-resolution copy of an identity card, passport or driving license - if the document shows the full name, photo or face image, signature of its holder);
- proof of residence (high-resolution copy of an utility bill of the customer, tax document or bank reference - these documents should not be older than three (3) months from the date of filing).

The Company does not transact with individuals who are Politically Exposed Persons (PEPs) or their family members.
2.3. *Corporate customers*

Information collected	Purpose of collection of data
legal name of the customer	● to provide the Company's services; ● to resolve the customer's claims; ● to communicate with the customer.
date of incorporation of the customer	
customer's e-mail	

customer's place of incorporation	
description and nature of the customer's business	
address of the customer's payment wallet	

The customer shall provide the Company with following valid documents serve as basis for identification:

- a high-resolution copy of the certificate of incorporation (an extract from the Commercial Register or equivalent document, evidencing the registration of the corporate customer);
- names and addresses of all directors and beneficial owners of the corporate entity.

The Company must identify the beneficial owners (UBOs) and, for the purpose of verifying their identities, taking measures to the extent that allows the Company to make certain that it knows who the beneficial owners are, and understands the ownership and control structure of the corporate customer, or of the person participating in the transaction.

A representative of the corporate customer must submit a document certifying his/her powers (a power of attorney), which has been authenticated by a public notary and/or legalized and/or certified with an apostille, unless otherwise provided for in an international agreement.

2.4. All the information and documents provided by the customer shall be completely clear and readable.

2.5. The Company verifies the correctness of the information of the customer using the information originating from a credible and independent source for that purpose.

2.6. The Company may ask additional information about the customer in case of any suspicion about the customer's identity information or the customer's behavior.

2.7. The Company may cross-check the customer through the internal and external databases.

2.8. The Company reserves the right to impose additional due diligence requirements to accept the customers residing in certain countries.

2.9. The Company reserves the right to suspend any customer's transactions if the customer does not provide the Company with necessary information.

2.910. The Company does not render services to the customers that are on the sanction lists.

3. Enhanced Due Diligence Procedure

3.1. The Company shall undertake enhanced due diligence (EDD) if there is a higher risk of money laundering or terrorist financing such as:

- there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
- the customer is from a high-risk third country or its place of residence is in a high-risk third country;
- the customer is from a territory that is considered a low tax rate territory (territory from the "black lists");
- when there are unusual factors in the customer onboarding, or when there are unusual transactions patterns without clear economic or lawful purpose;
- the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares.

3.2. The Company must identify what the risks are in every particular case and undertake all appropriate measures to mitigate those risks, such as gathering additional information about the customer and its business.

4. Record-keeping

4.1. The Company is obliged to keep all records about the customer and its behaviour in such a way that it can always be presented to inspectors checking the recorded transactions.
4.2. The Company is responsible for keeping all relevant data.
4.3. The information about the customer, including the customer's transactions, must be stored for no less than one (1) year after termination of the business relationship between the Company and such customer.
4.4. If a customer fails to submit all necessary documents and relevant information, or, if based on the documents provided, the Company has a suspicion that money laundering or terrorist financing might be involved, the Company shall not make any transactions with that customer and shall record as many customer's details as possible that will later help to identify the customer.

5. Monitoring

5.1. In addition to gathering information from the customers, the Company continues to monitor the activity of every customer to identify and prevent any suspicious transactions. The Company must investigate every initiated case.
5.2. The Company has implemented the system of monitoring the customer's transactions (both automatic and, if needed, manual) to prevent using the Company's services for criminal activity.
5.3. The Company reserves the right to suspend any customer's transactions, which can be regarded as illegal or, may be related to money laundering or terrorist financing in the opinion of the Company's staff.
5.4. The Company implements and maintains internal controls for the purposes of ensuring that all of its operations comply with AML legislation.

6. Reporting Procedure of Suspicious and Unusual Transactions

6.1. Upon the request of a supervision officer of the government authorities all necessary documents and information shall be provided to such officer immediately.
6.2. If the Company has a suspicion that money laundering or terrorist financing might be involved, the Company can provide such information and the customer's data to the relevant government authorities.
6.3. The Company is not on duty to notify the customer is suspected.

7. Employees and Training

7.1. All the Company's employees, managers and directors must be aware of this Policy.
7.2. The Company provides AML training to employees who will be dealing with the customers or will be involved in any AML checking, verification or monitoring processes. The Company may conduct its training internally or hire external third party consultants.
7.3. Proposals and claims to the Company related to this Policy may be sent to the email address: support@nowpayments.io.