

BlocPay - AML/KYC

AML/KYC

The objective of the Anti-Money Laundering (AML) Policy at BlocPay Ltd

is to comply with the requirements set forth by the Money Laundering and Terrorist Financing Prevention Act 2017, which obligates companies providing financial services, including virtual asset exchange, to perform appropriate due diligence on their customers. Our staff are dedicated to upholding the highest standards of AML and Know Your Customer (KYC) compliance to prevent our services from being used for illicit financial activities. To achieve this goal, we will verify the identities of all new and existing customers to a reasonable level of certainty and report any suspicious activities. Our AML Policy framework ensures that all necessary measures are taken to safeguard our services against being used as intermediaries for money laundering, terrorism financing, and other criminal activities. We commit to following the provisions outlined in Polish AML laws, as well as EU and international AML guidelines, and will maintain records of all identity checks for up to 10 years.

The AML Policy at BlocPay Ltd

is a set of procedures designed to prevent our services from being used for criminal activities such as money laundering or terrorist financing. Know Your Customer (KYC) measures are a key component of the AML Policy and are intended to enhance our understanding of our customers and help us manage risks associated with their activities. We may update our AML Policy in the future to ensure compliance with applicable laws and best practices. To address any potentially suspicious or unusual transactions or customer behaviour, our compliance officers are authorized to request additional documents, such as proof of source of funds, as deemed necessary. Our AML Policy includes identification and verification of each customer before entering into a financial business relationship, regular AML training for our staff, monitoring of customer financial behaviour based on risk-based analysis, procedures for reporting suspicious activity internally and to relevant law enforcement authorities, and the establishment and maintenance of risk-based customer due diligence, including enhanced due diligence for customers presenting higher risks. We are committed to

rejecting customer documents and terminating business relationships if we identify any suspicious activity, false documents, or non-cooperation during the customer due diligence process.