

DAFRIGROUP AML/KYC Policy

Updated: 20 June 2021

This AML/KYC Policy encompasses all reasonable and appropriate procedures related to money laundering prevention, financing of terrorism and other illegal activities.

For purposes of this AML/KYC Policy, “us,” “we,” “our,” “**DAFRIGROUP PUBLIC LIMITED**” Sometimes referred to as **DAFRIBANK DIGITAL**, or “dafribank.com” refer to the website <https://dafribank.com/> and related services.

Our Anti-Money Laundering and Know Your Customer Policy (hereinafter referred to as “AML/KYC Policy”) is designated to prevent and mitigate possible risks of us being involved in any kind of illegal activity

DafriGroup provides secure payment solution, digital banking / fin-tech services, fiat-to-cryptocurrency, cryptocurrency-to-fiat and cryptocurrency-to-cryptocurrency services to all customers by identifying and eliminating potential risks of money laundering. The effectively implemented AML/KYC regulatory requirements are aimed at improving efficiency and stability in the crypto sphere and serve as a confidence-building measure for all parties.

Payment solution, digital banking, fin-tech, fiat-to-cryptocurrency, cryptocurrency-to-fiat and cryptocurrency-to-cryptocurrency services provider DafriGroup will not enter into a business arrangement with any individual or entity suspected of or directly involved in money laundering in order to conceal the source of illicit funds and make funds appear legitimate. Both international and local regulations require us to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity of our customers.

AML/KYC Policy covers the following matters:

- Compliance Officer
- Risk-Based Approach

- User Verification
- Monitoring Transactions
- Compliance Officer

The Compliance Officer is the person, duly authorized by DafriGroup, whose duty is to ensure the effective implementation and enforcement of AML/KYC Policy. In order to oversee internal AML/KYC Policy and remain compliant with all major international regulations, the Compliance Officer is responsible for maintaining and supervising all mandatory anti-money laundering and counter-terrorist financing requirements, including but not limited to:

- Implementing and managing an effective legal compliance program procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations.
- Regularly auditing company procedures, practices and documents to identify possible weaknesses or risk;
- Collecting customers' identification information
- Monitoring transactions and investigating any significant deviations from normal activity
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs.
- Updating risk assessment regularly, organizing regular training sessions for employees to communicate key regulatory changes.
- Providing law enforcement authorities with information as required under the applicable laws and regulations.

Risk-Based Approach:

DafriGroup adopts and maintains a Risk-Based Approach (“RBA”) in order to assess and prevent any money-laundering and terrorist financing risks. Successful implementation of the RBA will allow resources to be allocated in the most efficient ways. Prior to entering into any transaction or proposed transaction, mandatory checks shall be conducted in accordance with the RBA to ensure that the customer’s identity does not coincide with any person with known criminal background or with banned entities such as terrorist organizations. The main principle is that resources

should be directed in accordance with priorities so that the greatest risks receive the highest attention.

User Verification:

One of the international standards for detecting and preventing illegal activity is customer due diligence (“CDD”). In accordance with CDD, DafriGroup has established mandatory verification procedures within the standards of AML/KYC frameworks.

As a condition of verification and your use of the DafriGroup services, DafriGroup reserves the right to require you to provide us with such information, documentation, scans/photographs and/or "selfie" verification as applicable, as we may reasonably request from you to comply with our regulatory obligations:

Personal email address.

Personal phone number.

First name and last name.

Date of birth.

Gender.

Country.

City.

State/province/region/district.

ZIP/postal code.

Citizenship.

Identity document (ID) – this is a valid, reliable and independent source document issued by a federal, provincial, territorial or state government authority. It must include the following information: first name and last name; date of birth; gender; place of birth; date of birth; issuing country; customer's photo, ID serial number and

date of issue. ID should be valid due to the issue date. User is free to provide scanned copies (both front and back sides) of one of the following types of identity documents: national passport, international passport, driver license or national identity card. All legal methods for double-checking of the provided identification information will be used by DafriGroup. DafriGroup accepts scanned copies of your documents only if all the information contained therein is provided with Latin transliteration. DafriGroup reserves the right to verify the user's identity in an on-going basis, especially when provided identification information has been changed or the user's activity is deemed as suspicious or anomalous (unusual for the particular user). In addition, DafriGroup reserves the right to request up-to-date scanned copies of documents from any registered user, even if the user completed identity verification in the past.

Proof of address — this is an official document which confirms the user's residential address and includes the user's first name and last name, residential address and issued within the last 3 months. User is free to provide scanned copies of any of the following types of documents: utility bill; electricity bill; bank statement; tax return; council tax; other official document with current residential address, first name and last name and issued within the last 3 months. DafriGroup accepts scanned copies of your address documents only if all the information contained therein is provided with Latin transliteration.

Important! The proof of address document must be issued to your name and contain the date of issuance.

Payment card this is a card issued by a financial institution for cashless payments at retailers, internet stores or for cash withdrawals at ATMs. It must contain the following information: issuer, cardholder's name, cardholder's signature, card number, date of issue and expiration date. Copies of front and back sides are required for user verification.

Important! Before making the scans of your payment card (front and back sides), please hide the CVV code (you can use a piece of paper, for example) and a part of the card number. Only the first 6 and the last 4 digits of the card number are required for verification. It is aimed at preventing misuse of your payment card and for safety reasons.

“Selfie” verification — it is validation of a one-time selfie photo of a user to ensure the legitimacy and enhanced security of user sensitive data. There are 2 (two) types of

“selfie” verification at dafribank.com, a “selfie” with user’s login information (a user holds a white piece of paper with the text “dafribank.com,” the current date (DD//MM//YY) and valid login information for accessing the dafribank.com website) and a “selfie” with a valid payment card (a user holds a white piece of paper with the text “DafriBank” and the current date (DD//MM//YY) in one hand and a valid payment card (front side) in the other hand.

All required scanned/copied documents should be provided in good quality, all texts should be readable, there should not be any modifications or edits of the document scans/photos, otherwise we would have to reject them and request new copies without modification or in better quality.

Proof of income — it is an official document or set of documents necessary for establishing the origins of the particular funds or assets, which are the subjects of the business relationship between DafriGroup and the user and the transactions DafriGroup needs to execute on the behalf of the user. This verification measure is required for the purpose of enhanced due diligence and a transaction execution of particularly large sums of money. User is required to provide scanned copies of an official bank statement (personal or business) or pay stubs or tax returns.

Once the spending limit for your verification tier has been reached, it is mandatory to complete one or more verification tiers to continue using the exchange services rendered by the DafriGroup /[Dafribank.com](https://dafribank.com) website in accordance with cumulative spending limit system.

We reserve the right to reject any person on registering on <https://dafribank.com/> and using related services if we are unable to verify any information due to non cooperation of the customer, or if customer's actions are likely to have a material adverse effect on us for being in violation of any applicable laws or industry best-practice guidelines. We will also reject and terminate any relationship with any person who is a subject of sanctions (financial and others) of any country of the world as well as any international respected organization.

We may from time to time temporarily reject customers from some countries/territories according to FATF “High-Risk and Other Monitored Jurisdictions” recommendations and our RBA. This applies to both new customers at the registration stage and existing users of our services. In the latter case, we will notify the customer of the refusal to provide services in advance, and provide reasonable time for the termination of the use of our services.

Monitoring Transactions:

DafriGroup diligently monitors transactions for suspicious activity. Therefore, we rely on data analysis as a risk-assessment and suspicion detection tool. We perform a variety of compliance-related tasks, including capturing data, filtering, record keeping, investigation management and reporting. System functionalities include:

- a) A daily check of customers against recognized “black lists” (e.g. OFAC), aggregating transfers by multiple data points, placing customers on watch and service denial lists, opening cases for investigation if it is essential, sending internal communications and filling out statutory reports, if applicable;
- b) Case and document management with regard to AML/KYC Policy, we will analyze all provided customers' data and monitor all transactions and it reserves the right to: ensure that transactions of suspicious nature are reported to the proper law enforcement authority through the Compliance Officer; request the customer to provide any additional information and documents in case of suspicious transactions; temporary suspend (block) or terminate customer's account when we have reasonable suspicion that such customer is engaged in illegal activity.

The above list is not exhaustive and the Compliance Officer will monitor users' transactions on a day-to-day basis to establish whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide. We reserve the right to refuse to process a transaction at any stage. Especially, when we believe that a transaction is connected in any way to money laundering or any other type of criminal activity.

AML/KYC Policy is revisited periodically and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity, inclusive of money laundering and terrorist financing. We recommend that you regularly check for changes and that you review our AML/KYC Policy when visiting our website. If you do not agree with any aspect of the updated AML/KYC Policy, you must notify us promptly and cease using our services.

By registering as a user of dafribank.com, you consent to the terms of AML/KYC Policy without any exclusions or reservations. AML/KYC Policy is an integral part of Terms of Use you are to agree when registering on <https://dafribank.com/>

© DAFRIGROUP LIMITED. All Rights Reserved.