EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT

European Center for Not-for-Profit Law

PILnet

PORTUGAL

Law firms participating in this research are not liable towards third parties for the accuracy of the information contained in this guide. The research cannot be considered as legal advice. It was carried out in 2022 and responds to the regulatory framework on organizational banking in this time period. If you have further queries please reach out to our clearinghouse for legal help.

European Center for Not-for-Profit Law Stichting (ECNL)

ECNL' s mission is to create legal and policy environments that enable individuals, movements and organizations to exercise and protect their civic freedoms and to put into action transformational ideas that address national and global challenges. We envision a space in which everyone can exercise their rights freely, work in solidarity and shape their societies.

PILnet

PILnet is a global non-governmental organization that creates opportunities for social change by unlocking law's full potential. With programs in Europe & Eurasia, Asia, and at the global level, PILnet aims to reclaim and reimagine the role of law so that it works for the benefit of all. PILnet builds networks and collaborations of public interest and private lawyers who understand how law works when it serves the interests of the privileged and then it uses that knowledge to strengthen civil society and the communities they serve. PILnet not only obtains high-quality, free legal assistance for civil society organizations when they urgently need it but also helps organizations to capitalize on the full range of specialized legal expertise that can be provided by corporate lawyers, including against ongoing, or even yet-to-be-determined, challenges.

© 2022 by the European Center for Not-for-Profit Law Stichting (ECNL), PILnet and Partnering Law Firms.

1. OPENING AN ORGANISATIONAL BANK ACCOUNT

a. What are the requirements to open an organisational bank account?

i. Do organisations have to be physically present in the country to open a bank account? I.e., can they operate in country X but have a bank account in country Y? Is the presence of a statutory representative required or can the presence be fulfilled through an authorization?

In principle, organizations do not have to be physically present in Portugal to open a bank account with national banks (i.e. they can operate in country X but have a bank account in Portugal).

We note, however, that in accordance with article 24 of the Anti-Money Laundering and Terrorist Financing Act (Law 83/2017 of 18 August, which transposes Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 and Council Directive 2016/2258/EU of 6 December 2016, hereinafter the "**AMLTF Law**"), legal persons must provide the bank with their Portuguese TIN (Tax Identification Number) – which can be obtained by appointing a tax representative resident in Portugal – or, if the legal person is established in an EU member state or Norway, Iceland and Liechtenstein, an equivalent number issued by the competent foreign authority. is sufficient. Foreign CSOs located outside of the EU (and the countries listed above) will need to appoint a tax representative in Portugal given that it is mandatory to have a tax representative to obtain a Portuguese TIN.

ii. Are there specific requirements for CSOs to open accounts by law or asked in practice by the banks (e.g, years of operations, annual turnover, to have director or member of governing body to be national of the country)

Although Portuguese law does not generally set special requirements for the opening of accounts by CSOs, national banks usually require customized documentation. The documentation may vary because banks have some margin to set out specific internal AML policies and procedures. Documents such as ID card, permanent certificate of companies and the

instrument granting powers to the representative of the client will always be required when the client is a legal person like CSOs. Additionally, to confirm certain information of the clients that is not featured in the legally required documents mentioned above, banks may require additional ad hoc documentation (e.g. utilities invoices to prove the address of the client, company charts executed by the representative of the client or specific statements).

The applicable requirements should be clarified with the bank opening the account. For additional information on the KYC (Know your Customer) process, please refer to point 3a.

iii. Who is authorized/required to open a bank account? Can this be done online, or that person needs to be present in the country?

Pursuant to the [AMLTF Law](), several documents necessary to open a bank account can be sent digitally, provided that the bank is able to confirm the relevant information by the means foreseen in article 25 of the AMLTF Law and in the relevant regulations. By way of example, the use of interoperability platforms between information systems issued by public services can be especially useful for foreign CSOs.

Additionally, according to article 25, no. 1 of the AMLTF Law, during the bank account opening process, the bank may verify the identity of the representative of the legal person through the use of videoconference given that the representative is a natural person and only natural persons can be identified by videoconference. The documentation required by the bank must fulfil the requirements set forth in article 25 no. 1 of AMLTF Law. As such, according to the latter article, banks will require the presentation of valid identification documents which fulfil the requirements explained in point 3 (a) below.

Legal persons are usually represented by their directors, in accordance with the requirements established in their bylaws. Attorneys empowered by proxy may also represent legal persons. We stress that, according to the AMLTF Law, banks must verify and collect a copy of the relevant powers of attorney.

Nonetheless, we advise inquiring with the bank in question.

iv. What is the process of setting up a bank account? E.g., how long it takes, is there a practice to have an interview in the bank?

The process of setting up a bank account typically begins with an application, which must be completed by the organization, and the submission of the documents requested by the bank. After this, the bank will analyze the application, which may likely take, in case the CSOs are Portuguese entities or EU entities, a couple of weeks. The process can be quicker if the entity has another account open in an EU system. Foreign CSOs without relationships established with EU banks may take more time to complete the onboarding procedures. We would estimate a couple of weeks in the first case and up to a month in the second case. Please note these are general estimations depending on the entity.

In Portugal, banks often tend to request from non-profit organizations documents which are, in practice, non-applicable. For example, when trying to open a bank account for the initial funding deposit, banks commonly ask for a foundation's proof of registry which is in fact only due after its recognition by the government, which in turn implies the opening of a bank account. In conclusion, CSOs may face additional hurdles in comparison with other legal persons or individuals, potentially making the bank account opening process more lengthy.

© 2022 by ECNL, PILnet and Partnering Law Firms

2. BANKING ACTIVITIES

a. What customer due diligence requirements are in place and what is their impact on civil society organisations' banking activities?

The AMLTF Law establishes a set of measures to combat money laundering and the financing of terrorism. National banks must abide by preventive duties, including the duty to carry out due diligence when establishing business relationships (such as the opening of a bank account).

To fulfill such duty, national banks must comply with the KYC requirements provided for in article 24 of the AMLTF Law, in accordance with which legal entities are always required to present their certificate of incorporation or, in case of an entity with its head office located outside Portugal, an equivalent document issued by the competent authority, which provides and proves the following information details:

1. Legal denomination;
2. Corporate scope;
3. Full address of the head office and, whenever applicable, of the branch or permanent establishment, as well as any other address where it carries out its activities (if different);
4. Portuguese TIN (Tax Identification Number) or, if the legal person is established in an EU member state, an equivalent number issued by the competent foreign authority;
5. Legal person number or, when the person has none, an equivalent number issued by the competent foreign authority;
6. Country of incorporation;
7. Economic activity code, sectoral code or other code of similar nature (NACE code), when available.

Additionally, banks ask for:

1. Identification of the holders of shareholdings and voting rights equal to or greater than 5%, including the following details:
    - Individuals:

    a. Full name;

b. Date of birth;
c. Nationality referred in the ID;
d. Type, number, date of validity and issuer of the ID; and
e. Taxpayer number or, when the person has none, an equivalent number issued by the competent foreign authority.

- Legal persons:

a. Corporate scope;
b. Address of the head office;
c. Legal person number or, when the person has none, an equivalent number issued by the competent foreign authority.

2. Identification of the members of the management body or equivalent body, as well as key persons (senior directors) with management powers, including the following details:
    - Full name;
    - Date of birth;
    - Nationality referred in the ID;
    - Type, number, date of validity and issuer of the ID; and
    - Taxpayer number or, when the person has none, an equivalent number issued by the competent foreign authority.

Banks must also obtain information on the purpose and intended nature of the business relationship and, when applicable considering the customer's risk profile or the characteristics of the transaction, the origin and destination of the funds moved in the context of the business relationship or when carrying out an occasional transaction.

Once the business relationship is established, banks will continue to monitor their clients to ensure that the transactions performed in the course of the established relationship are consistent with the obliged entity's knowledge of the client's activities and risk profile and, where necessary, of the origin and destination of the moved funds.

b. Which internal principles or official (central bank) "suspicious transaction" monitoring criteria are in place affecting the civil society organisations? Is it publicly available?

The AMLTF Law does not foresee specific rules concerning the monitoring of "suspicious transactions" pertaining to CSOs in particular.

Pursuant to the regime set forth in the AMLTF Law, national banks are obliged to comply with the duty of due diligence whenever, in the context of a business relationship or any occasional transaction, regardless of the amount involved, suspicions arise of a possible link with money laundering or terrorist financing.

We additionally note that pursuant to article 43 of the AMLTF Law, banks are obliged to report to the competent authorities any attempted, ongoing or executed transaction, regardless of the amount involved, linked to criminal activities or the financing of terrorism.

Generally, monitoring should include, in addition to the duty of identification, the obtaining of information on the purpose and intended nature of the business relationship and on the origin and destination of the funds moved in the context of a business relationship or occasional transaction, when justified by the client's risk profile or the characteristics of the transaction. The business relationship must then be continuously monitored to ensure that the transactions carried out in the course of that relationship are consistent with the bank's knowledge of the customer's activities and risk profile and, where necessary, of the origin and destination of the funds handled.

There may also be an obligation to apply enhanced measures in the following cases: high risk third countries, remote contracting, politically exposed persons, life insurance agreements and correspondent links.

In these cases, the mandatory measures are:

- Obtaining additional information on clients, their representatives and their effective beneficiaries, as well as information on any planned or executed transactions;
- Carrying out additional measures to confirm the information obtained;
- Intervention at the highest level of hierarchy for authorization of the establishment of business

relationships, execution of occasional transactions or the carrying out of operations in general;

- Intensification of the depth or frequency of monitoring procedures with respect to the relationship in general or certain operations or sets of operations, with a view to detecting any possible indicators of suspicion and subsequently fulfilling the duty to report;
- Reduction of time periods for the update of information and all other elements collected during the exercise of the duty of identification and due diligence;
- Follow-up of the business relationship by the person responsible for compliance or any other employee who did not participate in the business relationship.

The following measure is also applicable if the risk level identified justifies it: the requirement to make the first payment of a transaction through a traceable medium from a payment account opened by the customer with a financial institution or other legally authorized entity, which, not being located in a high-risk third country, demonstrably applies equivalent identification and due diligence measures.

Please note that banks may adapt their procedures according to the nature and type of transaction, therefore, we advise to check with the bank to determine what procedures it has in place.

c. Do the banks in the country of operations have any restrictions/limitations to bank transactions and transfers to certain jurisdictions (such as high-risk ones).

Yes.

i. If yes, is the list of jurisdictions publicly available?

Yes. National banks must take into consideration the list of third country jurisdictions which are deemed to represent a threat to the financial system due to strategic deficiencies in their anti-money laundering and counter-terrorist financing legal frameworks, approved by Directive (EU) 2015/849 and Commission Delegated Regulation (EU) 2016/1675 of the European Parliament and of the Council, as well as the blacklist prepared by the Financial Action Task Force (FATF).

ii. What would be the procedures the bank would follow in this case for their CSO clients?

National banks have the duty to adopt effective and proportionate enhanced measures, being obliged to at least:

a. Obtain additional information about a client, its representatives or effective beneficiaries, as well as information regarding other planned or executed transactions;

b. Obtain approval from senior management before establishing new correspondent relationships;

c. Reduction of time periods for updating the information and data received during the exercise of the duty of due diligence;

d. Intensification of the bank's monitoring procedures relating to the business relationship or specific transactions, taking into account certain indicators of suspicious activities and fulfilling the duty to report to the relevant authorities.

3. OBLIGATIONS AND REPORTING REQUIREMENTS

a. Are banks required to provide CSO clients' financial information to CSO regulatory authorities or public officials? If yes, under what circumstances must banks do so, and what types of information must they provide?

With respect to notifications of suspicious transactions, in order to comply with the AMLTF Law, sectoral authorities are responsible for the supervision of CSO clients. National banks are expected to immediately report to the authorities any suspicious activities that may be linked to money laundering or other crimes. In Portugal, the competent authority to receive such reports is the Central Bureau of Investigation and Criminal Action (hereinafter the "**DCIAP**") and the Financial Information Unit.

Banks also have the obligation to report any transactions or funds of suspicious origin directly to the DCIAP and to the Financial Information Unit.

The abovementioned reporting duty includes, according to article 44, no. 1, c) of the AMLFT Law, the identification of the person (natural or legal person) directly or indirectly involved in the suspicious transaction, as well as any known information about their activities. Furthermore, all information related to the bank's investigation and evaluation of the suspicious transaction should be provided to the relevant authorities, including all characterizing and descriptive elements, factors of suspicion concretely identified and copies of all supporting documentation.

b. What obligations do banks have to protect the privacy of clients' information?

Banks are bound to the duty of secrecy and discretion and are subject to the obligation of non-disclosure, therefore being contractually required to maintain the confidentiality of customer information.

This means that banks must not disclose their clients' private details; the amount of money on deposit in an account; or the existence of transactions under criminal investigation or enquiry.

The exceptions to this rule are foreseen in article 79 of Decree-Law no. 298/92, of 31 December, and include:

- Disclosure, with the customer's prior consent, of facts or elements of the customer's relationship with the institution;
- Disclosure of information to the Bank of Portugal, within the scope of its competence;
- Disclosure of information to the Portuguese Securities Market Commission (CMVM), within the scope of its powers;
- Disclosure of information to the Insurance and Pension Funds Supervisory Authority, within the scope of its powers;
- Disclosure of information to the Deposit Guarantee Fund, the Investor Compensation Scheme and the Resolution Fund, within the scope of their respective powers;
- Disclosure of information to the judicial authorities, within the scope of criminal proceedings;

- Disclosure of information to the parliamentary inquiry committees of the Assembly of the Portuguese Republic, to the extent strictly necessary to fulfil their purpose, which specifically includes the investigation or examination of the actions of the authorities responsible for the supervision of credit institutions or legislation relating to such supervision;
- Disclosure of information to the Portuguese tax authority, within the scope of its powers; and
- Any other legal provision which expressly limits the duty of secrecy.

More concretely, during AML proceedings, the duty to report to the relevant authorities all information concerning suspicious transactions or activities is expressly foreseen as an exception to the duty of secrecy mentioned above.

Other exceptions to the duty of secrecy under the AMLFT Law include article 56, according to which obliged entities shall make available all information, documents and other elements necessary for full compliance with the duties listed in articles 43, 45, 47 and 53 of the AMLFT Law, even if subject to any duty of secrecy imposed by law, regulation or contract.

c. Are there specific reporting obligations for banks to inform governments on civil society banking in certain circumstances?

There are no reporting obligations specifically applicable to civil society banking. The general rules apply.

d. Are you aware of any change in regulation/practice due to the Russian sanctions?

Under article 5b of Council Regulation (EU) 2022/328 of 25 February 2022, in order to limit commercial relations between Russian banks and European banks, new restrictions were imposed on Russia which also affect CSO clients, prohibiting EU banks from accepting deposits equivalent to more than EUR 100,000 from Russian citizens or legal entities established in Russia.

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt, 2513 AM
The Hague, Netherlands
www.ecnl.org
twitter.com/enablingNGOlaw

PILnet
199 Water Street, 11th Floor
New York, NY 10038 U.S.A.
https://www.pilnet.org
twitter.com/PILnet