

EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT



European Center for
Not-for-Profit Law



PILnet



LITHUANIA

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

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

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 ORGANIZATIONAL BANK ACCOUNT

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

i. Do organizations 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?

To set up a bank account it is not necessary to be physically present in the country, which means that foreign legal entities can open a bank account in Lithuania. At the same time, some banks might require to demonstrate a connection to Lithuania (e.g. operations in Lithuania) to understand the purpose for opening a bank account. The exact questions will depend on the particular bank and its internal policies.

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)

In principle, there are no special legal requirements for opening a bank account for non-profit organizations. However, some banks might require to provide further information such as years of operations, annual turnover, source of funds, etc. as a part of their customer due diligence procedures.

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?

Generally, one or more persons authorized to represent the entity (such representation may be authorized by power of attorney or statutory representation, e.g. manager (director) of the CSO) can

open a legal entity's bank account. An authorized representative is typically determined based on the internal organization of the CSO. Although legal regulation allows for setting up a bank account both remotely or in person, banks can have internal procedures requiring a physical presence for opening a bank account. It is important to note that in practice banks are more likely to demand the physical presence of the representative in order to set up an account for a legal entity (CSO).

It should be noted that some financial institutions established a practice of requiring a representative of the CSO to open a personal account with the bank in order to be able to set up a business account/account for a legal entity.

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?

To open a bank account, an application must be always completed and submitted to the bank together with the necessary supporting documents requested by the bank. Since timing depends on the individual bank's processes, it is difficult to estimate this, but in general, it may take up to a week or a few weeks. In extreme cases, it may take up to three months to open a bank account. For example, the bank may request additional documents due to enhanced risks or for explanation of unclear information, which naturally prolongs the process of opening a bank account. Processing times for foreign companies may also differ, e.g. depending on the client's country of origin. It may be sensible to inquire about the timeline with the selected bank. The process may be easier if the bank operates both within the client's country of residence and within Lithuania, and the client already has a bank account with this bank in its country of residence.

2. BANKING ACTIVITIES

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

Customer due diligence in place follows the general EU Anti-Money Laundering (AML) Legislation and Lithuanian Anti-Money Laundering And Counter-Terrorist Financing Legislation. There is no specific due diligence to be performed on civil society organizations.

Depending on the legal form of the organization, required information and documentation should usually include the following:

- Legal entity's name, type, registration number (if any), place of incorporation, the actual registered office of the head office, main business address, names of representatives;
- Public register extracts for the organization and its managing entity (if any);
- ID documentation for representatives, authorization for representation (power of attorney, etc.);
- Potentially group structure charts and other shareholding information (UBO).

As for CSOs established or connected to higher risk countries (Russia, Belarus included), banks will apply enhanced due diligence process. In such cases, banks will request additional information to comply with local regulations preventing money laundering and terrorist financing, e.g. information on the source of funds, additional information about transactions, purpose, and nature of the business relationship with the bank, beneficiaries, etc.

The purpose of providing the documentation is to establish with sufficient certainty the identity of the bank's new client, the person who is authorized to act on behalf of this new client and who is its ultimate beneficial owner, and also to understand the purpose and intended nature of the business relationship. Depending on the client, this can take various forms.

The bank will usually ask for such documents and information to the extent they are required. Please note that while it is expected that most banks are able to process documents in Lithuanian or English, depending on the bank, it may be more difficult to process documents in other foreign languages.

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

The main principles for identification of suspicious transactions follow the legal AML framework. Although there are a few suspicious transactions criteria established in regulation

provided by the Financial Crime Investigation Service (FCIS) that are relevant for the activities of CSOs, in most cases it will depend on the bank's internal transaction monitoring procedures to define whether transactions are suspicious or not (exact criteria/transaction monitoring scenarios will differ in each bank and are not publicly available). Some of the suspicious transactions criteria established by the FCIS include, but are not limited to:

- In the case of CSOs, suspicious transactions may be understood as monetary operations or transactions that do not correspond to the activities specified in CSO's founding documents;
- There is an unusual increase in the customer's cash settlement;
- The customer refuses to provide information requested by the financial institution clarifying the purposes for which the funds have been used when such transactions do not comply with the customer's normal cooperation with the bank;
- The Client endeavors to settle in cash in cases where it is common practice in the Client's settlement practice to settle in other ways.

There might be certain cases of banks de-risking and refusing to work with certain types of CSOs due to increased money laundering/terrorist financing risks, especially where connections/funds related to Russia/Belarus are discovered. On the other hand, the Bank of Lithuania (central bank and supervisory institution of banks in Lithuania) emphasized recently the importance of ensuring that non-profit organizations operating in the field of development cooperation, democracy support, expansion of the security and stability area as well as sustainable development in the EU countries can engage in their activities in Lithuania and use the services provided by the country's financial system. In the Bank of Lithuania's opinion, financial institutions, same as in other cases, should not establish or should terminate business relationships with non-profit organizations only when they are unable to manage ML/TF risks posed by these organizations. Although, it is difficult to evaluate further actions by financial market participants (banks) in the near future due to the political crisis and war in Ukraine.

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).

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

Yes, transfers to certain high-risk countries, e.g. North Korea, are prohibited due to sanctions and embargoes. It is important to mention, that only the application of restrictive measures (international sanctions) imposed by the EU or UN is mandatory for banks established (operating) in Lithuania. However, most of the banks voluntarily chose to comply with sanctions imposed by the United States of America (OFAC) as well. As for the other higher-risk countries and jurisdictions (E.g. FATF high-risk countries¹ or FATF monitored jurisdictions,² European Commission high-risk countries³), transactions to/from are allowed, however, due to increased money laundering and terrorist financing risks, application of enhanced due diligence measures for such transactions is required. As a result, many banks choose to refuse to carry out such transactions or allow them with certain limitations that are subject to banks' internal policies.

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

The bank would apply sanction and embargo schemes for its CSO client as it would for any other clients. No difference would be made as there is no specific regulation for CSOs.

1 <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html>

2 <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html>

3 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counteracting-financing-terrorism/eu-policy-high-risk-third-countries_en

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?

No special regime in respect of CSOs, because there is no specific CSO regulatory authority in Lithuania.

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

Under banking laws in Lithuania, the bank and its employees have an obligation to protect and not to disclose client's information, including whether a specific person (both natural or legal, CSO included) is a client of the bank, transactions performed by the client, etc. Information constituting a bank secret may be provided only to a bank client to whom the information constituting a bank secret relates, or to other persons at the written request or written consent of the client, specifying to whom and what information may be provided.

Although banks have an obligation to protect and not disclose clients' information, there are some exceptions. For example, banks have the right to provide information constituting a bank secret to a court, arbitration, or other persons on its own initiative, if it is necessary for the protection of the bank's legitimate interests and only to the extent necessary to protect the bank's interests. Also, banks may provide information to state institutions for crime prevention purposes, e.g., FCIS and others without the court's approval in case it is needed for money laundering and terrorist financing prevention functions.

Additionally, the bank may provide information to notary public and bailiffs, if they are necessary for the performance of the functions of notary public and bailiff established by the law.

In other cases, if it is not meant for the purposes described above, the information constituting a bank secret shall be provided only based on a reasoned court order, if the court determines that such information is necessary due to the legitimate interest pursued by the court.

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

There is no specific regulation under which bank has a reporting obligation on CSO banking.

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

In relation to recent sanctions imposed on Russia, no changes occurred in local regulation/legislation as EU sanctions are directly applicable. However, in practice, the risk tolerance of financial institutions in Lithuania has lowered towards clients related to Russia. Compliance checks and screenings might take longer, sending/receiving payments to/from Russia might take a longer time to process or some institutions might even voluntarily refuse to execute such payments. Also, supporting documentation for each financial transaction (if it is related to Russia or Russian persons) might be requested, which may cause delays due to increased workload and checks.



European Center for
Not-for-Profit Law

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