EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT

European Center for Not-for-Profit Law

PILnet

MOLDOVA

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.

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?

Pursuant to Article 13(3) of Law no. 62/2008 on Currency Regulation, non-residents are entitled to open a bank account in Moldovan banks without restrictions. Organizations are not required to be physically present in the country (i.e. register a local legal entity or a branch) to open a bank account. The procedure can be performed by a statutory representative or an individual authorized by a power of attorney. Prior to opening a bank account, the non-residents have to obtain the tax registration number from the State Tax Service.

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)

No specific requirements for CSOs.

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?

The process of opening a bank account can be carried out either by its statutory representative or an individual authorized by a power of attorney. The physical presence of the statutory representative is required only if the CSO chooses to submit the documents through its statutory representative. The process shall be carried out face-to-face (online applications are not being processed). In both cases, some of the documents required to open a bank account (please see the answer to question iv.) need to be notarized and apostilled.

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 procedure to set up a bank account shall take up to one week, provided that the bank will not seek additional documents (for example regarding the ultimate beneficial owner). The request to open a bank account shall be accompanied by the following documents[1] translated into the Romanian language:

- authenticated sheet with signature specimen sheet and stamp imprint. The sheet shall contain the legal address and name of the CSO, name of the person who will be entitled to manage the bank account and sign fiscal documents;
- authenticated extract from the business register confirming the registration of the CSO in its country;
- authenticated incorporation documents (e.g. charter, regulation, and other mandatory documents according to the legislation in force of the respective country);
- authenticated statement on the beneficial owner of the foreign CSO;
- tax registration number assigned by the State Tax Service;
- confirmation from the State Tax Service that the foreign CSO has no debts towards the Moldovan budget;
- survey (questionnaire) of the foreign entity (it is completed during the visit in the bank). Each local bank has its own approved survey in this regard.

The fee to open a bank account is ca. EUR 5 (MDL 100).

2. BANKING ACTIVITIES

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

Pursuant to Article 4(1)a) of Law no. 308/2017 on Preventing and Combating Money-Laundering and Terrorist Financing, banks are considered a reporting entity. The reporting entities

1 The list of the documents is not provided by law, so each bank is entitled to the documents it deems relevant. The presented list represents the most common documents asked by the local banks in order to open a bank account.

shall apply simplified or increased customer precautions, in dependence on the identified risks of money-laundering and terrorist financing. Pursuant to Article 5(2) of the same law, customer precautions include:

- identifying and verifying the identity of customers based on identity documents, as well as documents, data, or information obtained from a credible and independent source;
- identifying the beneficial owner and taking appropriate and risk-based measures to verify his identity so that the reporting entity can be sure that he knows who the beneficial owner is, including taking reasonable steps to understand the ownership structure and control structure of the customer;
- understanding the purpose and desired nature of the business relationship and, if necessary, obtaining and evaluating information about them;
- continuous monitoring of the business relationship, including the examination of transactions, concluded throughout that relationship, to ensure that the transactions performed to comply with the information held by the reporting entities regarding the customer, business profile, and risk profile, including the source of the goods, and that the documents, data or information held are up to date.

Additionally to these measures, the bank will apply increased customer precautions if it identifies a higher risk of money laundering and terrorist financing. Pursuant to Article 8(3) of the same law, some of the relevant higher risk factors which the banks will consider are:

- customers are residing in jurisdictions with an increased risk of money laundering and terrorist financing;[2]
- transactions favor anonymity;
- payments are received from unknown or unrelated third parties;

2 The list of the high-risk jurisdictions is the one established by the European Commission and currently includes: Afghanistan, Barbados, Burkina Faso, Cambodia, Cayman Islands, Democratic People's Republic of Korea (DPRK), Haiti, Iran, Jamaica, Jordan, Mali, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen, Zimbabwe.

- transactions are made to jurisdictions that do not have effective systems to prevent and combat money laundering and terrorist financing or have a high level of corruption or other criminal activity.[3]

Provided that the CSO will have a transparent corporate formation, these requirements shall not have a significant impact on the CSO's banking activities.

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

Pursuant to Chapter 1 of the Annex to the Order of the Office for Prevention and Combating of Money-Laundering no. 15/2018 on approving the Guide on Identifying and Reporting Suspected Money-Laundering Activities or Transactions, the general criteria for identifying suspicious activities and money-laundering transactions are:

- The customer refuses to provide the information requested by the reporting entity, including information that is not provided for in the legislation, but which is required in accordance with banking practices. For example, it concerns a request for additional information regarding the subsequent destination of the money or the purpose/method of using the money in case of a specific transaction or request for additional information related to the purpose/method of using the money in case of a high volume cash withdrawals.);
- The customer presents contact details: addresses, telephone numbers, emails – which cannot be identified;
- The customer has an excessive interest in the internal control system and policies, as well as an excessive concern on the confidentiality of the operations carried out by the customer. This creates a suspicion that the customer wishes to adjust its activity in order to elude these provisions and implement specific methods of transacting to facilitate money laundering;

3 The list includes the same countries as the ones mentioned above.

- The customer presents information that arouses suspicion of being false and/or erroneous to the reporting entity, or the customer offers money, gifts, or other undue benefits for information or services that are of an unusual or suspicious nature or for not informing/reporting the business relationship/transaction;
- The customer presents confusing details regarding the transactions to be performed, shows a nervous state when performing the transactions, or when asking questions about his activity, at the same time tries to develop close relationships with the employees of the reporting entity;
- The customer is accompanied or supervised by a third party or acts through a third party, but does not communicate about it or refuses to present its data;
- The customer ignores offered more favorable conditions for provision of services;
- The customer performs operations without economic meaning, or transactions that do not correspond to the daily activity of the client or introduced in the scheme of the operation coordinated in advance, essential changes, immediately at the beginning of its execution, especially in the direction of money or other assets;
- The customer performs multiple transactions below the reporting limit (EUR 10000) by bank transfer or cash;
- Transactions with third parties from high-risk of money-laundering and terrorist financing jurisdictions are performed;
- Impossibility to establish the customer's partners, the name/name of the payer for the operations of registration in the current accounts of the funds;
- Difficulties that arose in the process of verifying the information submitted by the customer in accordance with the requirements established by law, the presentation by the customer of information that cannot be verified or the verification of which is difficult;
- Unjustified haste on the part of the customer when performing operations;
- Payments made with checks issued by third parties or with checks that have multiple signatures or such operations do not correspond to the customer's activity profile;

- The use of loan agreements between legal entities and individuals signed by one and the same person in different capacities (administrator and individual) or loan agreements are used to reflect the origin of funds or the applicability of such contracts have a repeated frequency for the customer;
- The customer's partner is registered in a different jurisdiction from the jurisdiction of the financial institution in which he holds the bank accounts;
- Carrying out non-economic banking operations with the involvement of politically exposed persons or transactions that do not reveal from their content the need to carry out such operations;
- A natural or legal person makes payments for the benefit of the politically exposed person or his family members for different types of services if such transactions are not relevant to the specific activity of these individuals or legal entities;
- In case of a company registered in high-risk jurisdictions (please see the list below under question c (i)), from the documents presented or from other sources, the bank understands that the beneficial owner is a politically exposed person or persons associated with him.

These criteria apply also to the CSOs. The criteria shall be interpreted for each case particularly, meaning that even if a specific case matches one criterion – it does not automatically mean that it will be suspected of money laundering and/or terrorist financing. The Office for Prevention and Combating of Money Laundering may decide that even if a specific case matches one criterion – it does not create suspicion of money laundering and/or terrorist financing, especially if the customer will have a convincing argument.

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).

Pursuant to Article 72 of the Regulation on the conditions and manner of conducting foreign exchange operations (approved by the National Bank of Moldova through the Decision of the Executive Committee no. 29/2018), the non-resident legal entities have a transfer limit abroad of EUR 10000 in order not to be required to present justifying documents. There are

no specific restrictions or limitations for transfers to certain jurisdictions. The risk of such transactions/transfers is to be deemed as a money-laundering and/or terrorist financing, which will lead to the suspension of the transfer/transaction for up to 30 days.

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

The list of the high-risk jurisdictions is established by the European Commission and can be found here.

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

The bank will report the transfer/transaction to the Office for Prevention and Combating of Money-Laundering, which will carry out the investigations. The transfer/transaction, in this case, might be suspended for up to 30 days. The bank may ultimately freeze the bank account until the investigations will be carried out if the Office for Prevention and Combating of Money-Laundering will request this.

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?

There are no other reports than the ones described in the answer to question 3. Generally, pursuant to Article 97(3) of the Law no. 202/2017 on the activity of banks, the information which constitutes bank secrecy shall be provided by the bank, only if the provision of this information is justified by the purpose for which it is requested, in the following cases:

- at the request of the bank's customer or his representative;
- at the request of the criminal investigation body, with the authorization of the investigating judge, regarding the concrete criminal case;
- at the request of the court, in order to resolve a pending case;

- at the written request of other public authorities or ex officio, if by special law these public authorities have the right, in order to fulfill their specific attributions, to request and/or receive such information from the bank;
- at the request of the bailiff, on the basis and within the limits provided by the court's writ;
- when the bank justifies a legitimate interest.

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

Pursuant to Article 96(1) of the Law no. 202/2017 on the activity of banks, the bank is obliged to maintain the confidentiality of all facts, data, and information related to its activity, as well as any facts, data, or information at its disposal regarding the clients' accounts (balances, turnovers, operations carried out), the transactions concluded by the clients, as well as other information about the clients that became known to them. All of this data is qualified as banking secrecy and can be disclosed only in the above-mentioned cases.

The personal data of the individuals representing the bank (e.g. statutory representatives, employees, empowered individuals) are protected by the provisions of Law no. 133/2011 on Personal Data Protection. Banks are obliged to ensure the confidentiality of personal data, unless:

- the processing refers to data made public voluntarily by the subject of personal data;
- personal data has been depersonalized.

For breaching the confidentiality of the personal data, Banks may be fined an amount of up to EUR 750 (MDL 15000) and eventually with deprivation of the right to carry out a certain activity for up to 1 year (which can be applied both – the employee responsible for the infringement and to the bank, as the case might be).

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

No specific reporting obligations on this end.

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

Moldovan authorities have not implemented any changes to the banking regulations/practices due to the Russian sanctions so far (confirmed in abstracto by the Office for Prevention and Combating of Money-Laundering and National Bank of Moldova).

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

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