EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT

European Center for Not-for-Profit Law

PILnet

SLOVENIA

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 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, no. The presence of a statutory representative of an organization is generally not required in order to open an organization's bank account in Slovenia. For the opening of accounts, the provisions of the Slovenian AML Act (Prevention of Money Laundering and Terrorist Financing Act; *Zakon o preprečevanju pranja denarja in financiranja terorizma*) must be observed. Under certain conditions,[1] video identification is possible under the AML Act. Note, however, that banks have their own AML/KYC policies which differ with regard to accepted solutions and the actual manner of KYC procedures.

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)

There are no such special requirements for CSOs to open a bank account. Most banks will treat CSOs as standard corporate clients.

1 Video identification is possible provided that: (i) no increased risk of money laundering or terrorist financing has been identified; (ii) the identity of the customer, legal representative or proxy is established and verified solely on the basis of an official identity document bearing a photograph from which the customer's face is clearly identifiable, which contains at least the customer's name and date of birth; (iii) the customer, legal representative or proxy is domiciled or established in a Member State or in a third country which has an effective system in place for the prevention and detection of money laundering and terrorist financing; and (iv) the client, legal representative or proxy does not have his/her permanent residence or registered office in the high risk countries or in the countries where is a higher risk for money laundering or terrorist financing.

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, the opening of a bank account for a legal entity can be done by a person authorized to represent the entity. Whether the physical presence of the persons authorized to represent is required for opening an account depends on the respective bank at which an account is to be opened and its AML/KYC policies.

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 has to be completed and submitted to the bank together with the necessary supporting documents requested by the bank. While the list of documents to be provided may differ from one bank to another, at least the following documents will need to be provided:

- proof of tax identification no.,
- extract from the court/business register (or other relevant register),
- identification documents of authorized representative or a person concluding the agreement on behalf of a CSO.

Note that specifics of the whole process and timing differ from bank to bank.

2. BANKING ACTIVITIES

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

Customer due diligence is required in line with the AML Act which implements the EU Anti-Money Laundering Directive. There are no specific due diligence rules with respect to CSOs.

The general rules regarding customer due diligence are:

a. Identification of the customer
b. Identification of the ultimate beneficial owner
c. Obtaining information on the purpose and intended nature of the trade

d. Determining whether the customer or the customer's ultimate beneficial owner is a politically exposed person or a sanctioned person

In accordance with the AML Act if, on the basis of a risk assessment, any client, any type of business or any particular line of business constitutes a higher risk of money laundering or terrorist financing, the bank is obliged to perform "enhanced" customer due diligence that involves undertaking additional customer due diligence measures, while under certain conditions a "simplified" customer due diligence may be sufficient. In case of a simplified due diligence, a bank is still required to carry out all measures prescribed under customer due diligence, except that the measures may be slightly simplified, which allows for the following:

i. a reduced set of information about the customer, the statutory representative, or the proxy;
ii. information on the purpose and intended nature of the business relationship is only required if it is not evident from the business relationship itself;
iii. a lower frequency of transaction monitoring (annual); and
iv. a longer period for reviewing and updating information and documentation about the customer (three to five years).

Enhanced due diligence on the other hand requires the following:

i. additional review of information about the customer's business activities;
ii. additional review of information about the purpose and intended nature of the business relationship (in particular the scale and purpose of cash transactions and the destination of cross-border transactions);
iii. approval of the business relationship by a responsible person in a senior management position;
iv. in certain cases also assessment of the compliance of the business relationship by the AML/CFT department;
v. more frequent transaction monitoring (monthly); and
vi. a shorter period for reviewing and updating information and documentation about the customer (one to two years).

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 banking activities of CSOs do not have specific monitoring rules. The monitoring rules for all clients derive from requirements of the AML Act and the Guidelines on the assessment of the money laundering and terrorist financing risk issued by the Bank of Slovenia. The latest version of the Guidelines (from May 2022) is available in Slovenian language here, while the previous version (from November 2019) is available also in English language here. Further, each bank will have its own monitoring regime and internal rules which are not publicly available.

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?

First, restrictive measures (sanctions regimes) which prohibit certain transactions concerning sanctioned countries or sanctioned persons should be considered. In Slovenia, restrictive measures are regulated by the Act Regulating Restrictive Measures Introduced or Implemented by the Republic of Slovenia in Accordance with Legal Acts and Decisions Adopted by International Organizations (*Zakon o omejevalnih ukrepih, ki jih Republika Slovenija uvede ali izvaja skladno s pravnimi akti in odločitvami, sprejetimi v okviru mednarodnih organizacij*). The Government of the Republic of Slovenia is responsible for the issuance of regulations introducing or implementing restrictive measures under this Act. According to the amendment of the law, which entered into force on 13 April 2022, the direct applicability of EU decisions is established and the immediate implementation of amendments to the UN sanctions lists is made possible. The overview of restrictive measures and the list of countries and persons is available here.

Second, under the AML Act, all enhanced customer due diligence measures must be applied to all business relationships and transactions involving high-risk third countries. The European Commission Regulation (EU) 2016/1675 as amended from time to

time (with the last amendment in January 2022) specifies which countries are considered to be high-risk third countries.

Third, the Slovenian AML office publishes the list of countries with an increased risk of money laundering or terrorist financing. In case of such countries, one or more enhanced customer due diligence measures must be applied.

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 all clients. No difference would be made.

Possible sanctions include (without limitation):

- The bank may be obliged to inform authorities of suspicious transactions.
- The bank may refuse to make a specific transfer or 'freeze' all or certain funds, i.e. refuse to transfer them (generally in cooperation with competent authorities).
- The bank may also terminate the banking relationship with the client.
- A fine.

Specific procedures and measures depend on the individual bank and the situation at hand.

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, there is no such specific requirement either with respect to CSOs or in general. In general, all information, facts and circumstances about a particular customer in the bank's possession is subject to confidentiality under the Slovenian Banking Act (*Zakon o bančništvu*; ZBan-3). Upon specific request of the relevant authorities (police, prosecutors, regulators, courts etc.), a bank is obliged to provide the public authorities with information required (regardless of the confidentiality).

However, note that in Slovenia there is a register of all bank accounts opened with the payment service providers in Slovenia. This register contains information on who holds which accounts at which payment service provider, irrespective of whether the account holder is a resident or a non-resident, and whether the accounts are held by a private individual or a legal entity. Information (account number and the institution at which an account is opened) with respect to legal entities is public.

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

Under the Slovenian Banking Act (*Zakon o bančništvu*; ZBan-3), confidential information is all information, facts and circumstances about a particular customer in the bank's possession and the bank has a duty to protect such confidential information.

Members of the bank's bodies, shareholders of the bank, employees of the bank or other persons who, in connection with their work in the bank or in the performance of services for the bank, are in any way in possession of the confidential information may not communicate such information to third parties, nor may they allow such information to be used by third parties, nor may they use such information themselves for their own purposes.

The exceptions to the confidentiality are specifically listed and include, among others:

- explicit written consent of a client;
- if the Bank of Slovenia, the European Central Bank or a supervisory authority needs this information for the purposes of supervision of the bank carried out within the scope of its competence;
- if the Commission for the Prevention of Corruption requests such information in writing or if a court, prosecutor's office or the police request it in writing for the purpose of conducting pre-trial or criminal proceedings, except in cases where the provision of confidential information is expressly ordered by an investigating judge by law; and
- in certain cases, to exchange information on the creditworthiness of clients for the purpose of credit risk management.

For each disclosure of confidential information, a bank shall ensure that it is possible to establish at a later date which confidential information was disclosed, to whom, when and on what basis, for a period of 10 years after the disclosure of that information.

Further, a bank as controller of personal data must comply with its obligations under the GDPR. This includes, but is not limited to:

i. lawful, fair and transparent processing of personal data;
ii. personal data is collected for specified, explicit and legitimate purposes;
iii. appointment of the data protection officer;
iv. notification of the Data Protection Authority and data subject in case of a data breach.

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

No, there are no specific reporting obligations in this context. The general rules apply.

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

Banks need to closely follow the current sanctions regime against Russia.

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