

EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT



European Center for
Not-for-Profit Law



PILnet



ESTONIA

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?

There is no legal prohibition to open bank accounts for non-residents, so the permanent presence of a statutory representative in Estonia is generally not required to open an organizational bank account. However, additional requirements may be placed by banks themselves. The most important prerequisite for opening a bank account is the organization's connection with Estonia. Banks may impose special restrictions for certain countries e.g. offshore or high-risk countries (see question 3(c)), to comply with laws and reduce the risk of money laundering.

The relevant due diligence requirements can be found in the [Estonian Money Laundering and Terrorist Financing Prevention Act](#) (AML Act) (also described in 2. a below).

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 special legal requirements for opening a bank account on the basis of non-profit status. However, banks may set their own requirements depending on the risk appetite.¹

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?

Bank account may be opened by the representative of the company. Representation right may be proved by a document

¹ More information on risk appetite can be found in § 10 of the AML Act.

certifying the right of representation (e.g. power of attorney, extract from the register of the person entitled to representation, decision of the competent authority, etc.)

The law allows credit institutions (banks) the use of information technology means for identification of person and verification of data in the framework of due diligence measures.² In practice, it depends on the particular bank. Most of the process can usually be done online. However, for example, Swedbank recommends that non-residents [open an account in an office](#), and the LHV bank at the last stage requires a [physical presence to verify identity of the representative](#).

Although the assistance of a notary may be required in the process of opening a bank account, especially certifying documents originating from another country, signing the paperwork at an embassy or notary does not replace personal presence if it is required.

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 always be 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 the timeline. Some banks provide for a deadline, e.g. that the documents will be reviewed within 10 working days. The process, however, may take more than two weeks. Opening an account online may take a little longer.

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 the [Estonian AML Act](#). There is no specific due diligence to be performed on civil society organizations.

The obliged entity (a bank) apply the following due diligence measures:

² § 31 of the AML Act.

1. identification of a customer or a person participating in an occasional transaction and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronic transactions;
2. identification and verification of a representative of a customer or person participating in an occasional transaction and their right of representation;
3. identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer or of the person participating in an occasional transaction;
4. understanding of business relationships, an occasional transaction or operation and, where relevant, gathering information thereon;
5. gathering information on whether a person is a politically exposed person, their family member or a person known to be their close associate;
6. monitoring of a business relationship.

The obliged entity identifies a foreign legal person and retains the following details on the legal person:

1. the name or business name of the legal person;
2. the registry code or registration number and the date of registration;
3. the names of the director, members of the management board or other body replacing the management board, and their authorization in representing the legal person;
4. the details of the telecommunications of the legal person.

The obliged entity identifies a legal person based on the following documents:

1. the registry card of the relevant register;
2. the registration certificate of the relevant register; or
3. a document equivalent to these documents.

A representative and a beneficial owner are identified in accordance with the provisions on the identification of natural persons.

The obliged entity identifies natural person and retains the following data on the person:

1. the person's name;
2. their personal identification code or, where the person does not possess one, their date of birth and the place of residence or location;
3. information concerning recognition and verification of the right of representation and scope thereof and, where the right of representation does not arise from the law, the name of the document serving as the basis for that right, its date of issue, and the name of the issuer;
4. particulars of the person's means of telecommunication.

The obliged entity identifies a natural person based on the following documents:

1. an identity document;³
2. a valid travel document issued in a foreign country;
3. a driving license, if the name, photograph or facial image, signature or image of signature and date of birth or personal identification code of the holder are entered therein; or
4. a birth certificate⁴ in the case of a person below the age of seven years.

Please take into account that the beneficial owner is a natural person:

1. who, via ownership or another type of control, has the final dominant influence over a natural or legal person, or
2. in whose interests, for the benefit of whom, or in whose name a transaction or operation is made.

The purpose of the documentation is to establish with sufficient certainty the identity of the bank's new client, who is authorized to act on behalf of that new client, and who is its ultimate beneficial owner. Depending on the client, this can take various forms.

Additionally, the bank may require tax-related information such as tax ID numbers or information and documentation relating to the taxability of its new client and that client's funds, especially to the extent they are kept with that bank.

3 More information can be found in subsection 2 of § 2 of the Identity Documents Act

4 § 30 of the Vital Statistics Registration Act.

The bank will usually ask for such documents and information if and to the extent they are required.

Please note that in the case of founding documents in foreign languages, the bank has the right to request translations into Estonian that have been notarized or translated by a sworn translator. If the founding documents are in English or Russian, no translation is required.

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

Internal and official principles of the identification follow the legal AML framework. The banking activities of civil society organizations are monitored in the same way as the activities of other business clients of a bank. Monitoring rules may vary depending on the risk level. The legal framework in Estonia is set by the [Estonian Money Laundering and Terrorist Financing Prevention Act](#). The framework of due diligence is set by Chapter 3.

Each bank will have its own monitoring regime in place,⁵ which is not publicized. For example, banks may have varying thresholds for money transfers to determine which transfers will be subject to individual review before processing them.

The monitoring of a business relationship must include at least the following:

1. checking of transactions made in a business relationship in order to ensure that the transactions are in concert with the bank’s knowledge of the customer, its activities, and risk profile;
2. regular updating of relevant documents, data or information gathered in the course of application of due diligence measures;
3. identifying the source and origin of the funds used in a transaction;
4. in economic, professional or official activities, paying more attention to transactions made in the business relationship, the activities of the customer and circumstances that

⁵ Based on the Money Laundering and Terrorist Financing Prevention Act. Due diligence procedure requires bank to monitor a business relationship (§ 20(1)). Further information on monitoring requirement can be found in § 23.

refer to a criminal activity, money laundering or terrorist financing or that a likely to be linked with money laundering or terrorist financing, including to complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or lawful purpose or that are not characteristic of the given business specifics;

5. in economic, professional or official activities, paying more attention to the business relationship or transaction whereby the customer is from a high-risk third country or whereby the customer is a citizen of such country or whereby the customer's place of residence or seat or the seat of the payment service provider of the payee is in such country or territory.

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?

There are certain limitations for transfers to high-risk countries, however transfers to these countries are not prohibited by law. At the same time, enhanced due diligence measures⁶ shall be applied by banks if the risk is higher than usual, meaning that transaction is related to the high-risk third country.

The obliged entity is not allowed to establish a business relationship or enable an occasional transaction or a transaction in a business relationship where at least one of the following circumstances occurs:

1. the obliged entity is unable to apply the due diligence measures;
2. the obliged entity suspects money laundering or terrorist financing.

Upon assessment of factors referring to a higher risk the following is deemed a factor increasing the geographical risk:

1. that, according to credible sources such as mutual evaluations, detailed evaluation reports, or published follow-up reports, has not established effective AML/CFT systems;

6 § 39 of the AML Act.

2. that, according to credible sources, has significant levels of corruption or other criminal activity;
3. that is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
4. that provides funding or support for terrorist activities, or that has designated terrorist organizations operating within their country, as identified by the European Union or the United Nations.⁷

Banks also have their own lists of high-risk countries. These countries usually include:

- Iraq;
- Democratic Republic of the Congo;
- Libya;
- North-Korea;
- Sudan and South Sudan;
- Syria;
- Central African Republic;
- Somalia.

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 transfers.
- 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.

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

You can find a more comprehensive information on measures applied by credit institutions [in this guideline](#) by the Estonian

⁷ § 37(4) of the AML Act.

Financial Supervision Authority.

Additionally, please note that undertaking transactions which are prohibited due to sanctions and embargoes may render those transactions void under Estonian law and may also incur penalties and punishment under regulatory and criminal law.

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 – especially because there is no specific CSO regulatory authority in Estonia.

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

On one hand, banks have the duty to maintain professional secrecy on any customer related facts and evaluations they are aware of. Banks may only disclose customer-related information if they are legally required to do so or if the customer has consented thereto or if the banks are authorized to disclose banking affairs.

Each bank has detailed information about why and what information they collect, how they protect it and in which case they have the right to disclose. Such information can be found online on the bank's website.

Important disclosure obligations include:

- Disclosure to other companies of the same Group for the purpose of provision customers with better and more convenient services.⁸
- Disclosure to other parties in order to execute transactions

⁸ There are several reasons to provide data to other companies of the same Group. For example, for identifying the Customer, updating Customer Data, evaluating the Customer's expertise, risk management and hedging of risks, and compliance with fiduciary regulations, including capital and liquidity requirements, and assessing creditworthiness. The data are transmitted for the purpose of fulfilling an obligation imposed by law, based on legitimate interest or based on the Customer's consent. For detailed information it would be better to check with a particular bank.

or to provide products a client have requested.

- A bank is obliged to disclose and to convey Customer Data for the purpose of performing obligations arising from legal acts and international and mutual legal assistance (e.g. forwarding data to investigative bodies, notaries, trustees in bankruptcy, the Tax and Customs Board, Financial Intelligence Unit, Financial Supervision Authority, Estonian Motor Insurance Bureau, Estonian Funded Pension Registry).

On the other hand, the General Data Protection Regulation (GDPR) protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

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?

Restrictions apply to bank transactions with certain Russian banks (list of sanctioned banks can be found here: <https://swedbank.ee/private/home/more/newsandblog/news#newsId=20220303155004667>), the financing of Russian state and state-owned enterprises and the movement of capital between the European Union and Russia.

Some banks decided to suspend payment services to and from Russia and Belarus and end quotations for the Russian ruble (RUB) and providing financial services in rubles - including initiating and receiving payments, as well as converting RUB to other currencies upon the client's order. For example, the relevant announcement can be found on the Swedbank website.

Banks began to check payments more carefully, especially those related to Russia and Belarus, because there is a high risk of falling under sanctions. It means that any bank may have to hold the customer's transactions and ask them to provide supporting documents to investigate whether the transaction is related to

the sanctions imposed by respective authorities.

Some banks offer more favorable conditions for businesses opened by Ukrainian citizens. If a Ukrainian citizen starts a new company in Estonia (from 24 February 2022) and wants to open an account, the account opening fee will be waived. Other services will be charged according to the ordinary price list, and whether a bank agree to open the account depends on the bank's risk appetite.



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