

EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT



European Center for
Not-for-Profit Law



PILnet



AUSTRIA

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?

In general, bank accounts may be opened with Austrian banks also by organizations from other countries. The presence of a statutory representative is not necessarily required by law. However, in practice, banks will most likely demand a certain **nexus** of the organization and its business **to Austria** (e.g. the fact that the organization operates in Austria) based on their internal compliance provisions.

Furthermore, for organizations with their seat outside of Austria, an online account opening may not be possible due to compliance requirements but a physical meeting at the bank's branch may be demanded in order to open a bank account.¹

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)

Austrian banking law does not provide for any specific requirements for civil society organizations (“CSO”) to open bank accounts. This means that the **same provisions that are relevant for other customers** apply to CSOs as well (e.g. provisions for the prevention of money laundering and terrorist financing).

¹ E.g. https://www.bawagpsk.com/BAWAGPSK/businesskunden/SB/Business_Main_Channel/507106/businessbox-starter.html?int=BAWAGPSK|businesskunden|S-B|konten|konten,1,1

Some banks may however implement special rules for CSOs in their compliance strategy. For example, they may require CSOs to provide certain information to the bank on a regular basis (e.g. concerning annual turnover).²

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 **owner** of the bank account – be it a natural or (through its legal representative) a legal person – may open an account for himself. Furthermore, an account may be opened for the account owner by an **authorized representative**. Such representative needs to be authorized by means of a power of attorney that has been made explicitly for the opening of bank accounts (*Gattungsvollmacht*).³

A bank account may be opened either **physically** or, if special security measures are fulfilled and certain information about the client is provided to the bank (in case of legal persons: company name, registered office), **non-physically**.

According to [sec 6 \(4\) \(1\) Financial Markets Anti-Money Laundering Act \(FM-GwG\)](#), the need for proof of identity through the personal presentation of an official photo ID may be avoided through presentation of the official photo ID in the course of a video-based electronic procedure (online identification) in accordance with the requirements of the [Ordinance of the Financial Market Authority \(FMA\) on the Video-based Online Identification of Customers \(“Online-IDV”\)](#).

The possibility of an online identification is not limited by law to potential domestic clients or clients from member states.⁴ However, an Austrian bank might not allow foreign entities to open an account by online identification due to internal compliance rules.⁵ A bank might also require further security measures in the course of an online account opening such as for example the use of a qualified electronic signature.

2 <https://www.sparkasse.at/erstebank/unternehmen/produkte-firmenkunden/konto-karten/business-konto/vereinskonto-bonus>

3 RIS-Justiz RS0107010.

4 FMA Circular, Due Diligence for the Prevention of Money Laundering and Terrorist Financing (as per February 2022), 73.

5 E.g. https://www.bawagpsk.com/BAWAGPSK/businesskunden/SB/Business_Main_Channel/507106/businessbox-starter.html?int=BAWAGPSK|businesskunden|S-B|konten|konten,1,1.

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?

Basically, the opening of a bank account requires the conclusion of a contract between the bank and the account owner.

The bank has to conduct KYC (know your customer) processes. In such processes the client's identity has to be proven to the bank which may be made physically or, subject to certain requirements, non-physically (see previous question).

Furthermore, the bank will require certain information and respective evidence in particular about the client's ultimate beneficial owner ("UBO"). UBOs within the meaning of the FM-GwG are all natural persons who ultimately own or control a legal entity. The bank is obliged to verify the identity of beneficial owners (e.g. based on register extracts and/or photo IDs) as well as the holding structure of the client (e.g. based on register extracts, organizational charts and/or corporate documents of the holding companies) based on documents which have to be provided by the client. If the client is a legal entity according to [sec 1 \(2\) Beneficial Owners Register Act \("WiEReG"\)](#) which is obliged to report information about its beneficial owners to Statistics Austria (Bundesanstalt Statistik Österreich), the bank has to enquire the Austrian register of beneficial owners and thereby obtain certain information. In case the client is a legal entity comparable with a legal entity according to [sec 1 \(2\) WiEReG](#) which has to register its UBOs in another country, the bank has to obtain evidence of registration or an extract of the registry (if publicly available).⁶

The bank further requires information about the purpose of the opened bank account and the source of funds. The bank will also need to be informed whether the business relationship with the customer is commenced on the customer's own account (for more details see section 3 a. below).

In practice, the account opening proceedings offered by individual banks may differ. For example, not all banks allow an online account opening but some will require a personal meeting.

Usually, the opening of a bank account does not require lengthy proceedings and takes about one to two days.

⁶ FMA Circular, Due Diligence for the Prevention of Money Laundering and Terrorist Financing (as per February 2022), 49 f.

2. BANKING ACTIVITIES

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

Provisions regarding customer due diligence are contained in the [Austrian Banking Act \(BWG\)](#) as well as in the [FM-GwG](#).

According to sec 5 FM-GwG, banks shall apply customer due diligence in the following cases:

- when establishing a **business relationship** (including for example the opening of current accounts or credit accounts⁷),
- when executing any transactions which are not conducted within the scope of a business relationship (occasional transactions), which
 - either involve an amount of at least EUR 15 000 or a euro equivalent value, regardless of whether the transaction is carried out in a single operation or in multiple operations between which there is an obvious connection; or
 - which involves a transfer of funds as defined in Article 3 (9) of Regulation (EU) 2015/847 exceeding EUR 1 000,
- for each deposit into savings deposits, and for each withdrawal of savings deposits if the amount deposited or withdrawn is at least EUR 15 000 or a euro equivalent value;
- if the bank suspects or has reasonable grounds to suspect that the customer belongs to a terrorist organization (sec 278b Austrian Criminal Code, “StGB”) or the customer objectively participates in transactions that serve the purpose of money laundering (sec 165 StGB – including asset components which stem directly from a criminal act on the part of the perpetrator) or terrorist financing (sec 278d StGB);
- when there are doubts as to the veracity or adequacy of previously obtained customer identification data.

⁷ FMA Circular, Due Diligence for the Prevention of Money Laundering and Terrorist Financing (as per February 2022), 13.

The scope of **due diligence obligations** is contained in sec 6 (1) FM-GwG. It contains the following:

- identifying the customer and verifying the customer's identity (as well as the identity of any person acting on behalf of the customer),
- identifying the beneficial owner and taking reasonable measures to verify that person's identity including measures to understand the ownership and control structure of the customer,
- assessing and obtaining information on the purpose and intended nature of the business relationship,
- obtaining and checking information about the source of the funds used,
- identification and verification of the trustor and the trustee (in case of a trusteeship),
- conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, the business, and risk profile, including where necessary the source of funds,
- regular checking of the availability of all required information, data, and documents that are required under the FM-GwG, and updating of such information data and documents.

A bank has to enquire its customer about whether he intends to conduct the business relationship or the occasional transaction on its own account or for the account of others or on behalf of a third party, as well as about the identity of its beneficial owner(s). The customer is **obliged to cooperate** with the bank and provide the required information.

In order to determine the extent of due diligence obligations in individual cases, banks have to **assess the risks** of money laundering and terrorist financing and assign each customer to a risk class. Where a bank identifies areas with a lower risk of money laundering or terrorist financing (taking into account, amongst others, types of customers, geographic areas, and particular products, services, transactions, or distribution channels), it may apply **simplified customer due diligence** according to sec 8 FM-GwG. On the other hand, according to sec 9 -12 FM-GwG, **enhanced customer due diligence** shall be applied by a bank in cases where a higher risk of money

laundering or terrorist financing exists (e.g. in cases with a connection to high risk countries or the involvement of politically exposed persons).

Particular reference should be made to sec 41 BWG in connection with sec 16 FM-GwG, which stipulates a comprehensive **reporting obligation**. According to these provisions, banks are obliged to report to the money laundering office if they have **knowledge, a suspicion or a justified reason** to believe that one of the following cases defined in sec 16 (1) FM-GWG has occurred: transaction in connection with money laundering, funds derived from money laundering offence, failure to disclose a trusteeship, transaction or funds in connection with a criminal organization, a terrorist organization, a terrorist offence or terrorist financing.

The opening of a bank account by a CSO would be regarded as the establishment of a business relationship. Therefore, the account opening bank would have to apply customer due diligence. The CSO should be aware of its duty to cooperate with the bank with regard to the conducted due diligence.

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

There are no specific rules for CSOs. In general, sec 6 (1) (6) FM-GwG provides that banks are obliged to conduct **ongoing monitoring of the business relationship** with its customer including transactions undertaken throughout the course of that relationship. Thereby it shall be ensured that the transactions being conducted are consistent with the bank’s knowledge of the customer, the business and risk profile, including where necessary the source of funds. Such monitoring is conducted via special software systems. In the course of the monitoring proceedings, customers are rated based on their risk profile and categorized in certain risk classes⁸ taking into account aspects regarding the customer (sector, legal form), country and geographic region (nationality, residence/seat), product-, service- and transaction risk, distribution channels and new

⁸ The available sources do not explicitly state how CSOs/the nonprofit sector are rated. This may depend on different criteria such as whether the respective organization deals with cash money a lot, whether there is a high risk of corruption (e.g. in the health sector), whether payments are received by unknown or unrelated parties or whether there is a connection to branches that have typically a higher risk of being associated with money laundering of terrorist financing (e.g. trade with precious metals).

technologies. Intensified monitoring is needed where politically exposed persons, persons with residence/seat in high-risk countries or corresponding banks in non-EU/EEA countries are involved.^{9 10} Furthermore, banks have to determine monitoring measures for each risk class. The specific design of the systems used by individual banks is not publicly available.¹¹

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).

Austrian banks are subject to special auditing requirements for transactions with **certain non-EU/EEA countries** (“high risk third countries”). The European Commission Regulation (EU) 2016/1675 as amended from time to time specifies which countries are covered. In addition to this regulation, Austria also follows the list published by the FATF (Financial Action Task Force), which is updated on a monthly basis.¹²

It is imperative that **enhanced customer due diligence** measures pursuant to sec 9 – 10 FM-GWG be applied to all business relationships and transactions involving **high-risk third countries**.

These measures **include, but are not limited to**, verifying additional information about the customer and its beneficial owners, the purpose and nature of the business relationship, the source of funds used, the reasons for the transaction, and the approval of the customer’s senior management.

In addition to the third countries named in the above-named Regulation, enhanced due diligence requirements must be applied where there is an increased risk of money laundering or terrorist financing due to a geographic risk. Here, the factors for a potentially increased risk listed in [Annex 3 of the FM-GWG](#) must be taken into account in particular.

9 High risk countries named in the annex to Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)Text with EEA relevance in its current version (recently amended by Commission Delegated Regulation (EU) 2022/229).

10 This concerns cross-border relationships between a correspondent bank institution and a respondent bank institution where the latter is incorporated outside of EU/EEA.

11 Trautmann in Hörtner/Trautmann (Hrsg), Praxishandbuch FM-GwG (2020), sec 6 Rz 24.

12 <http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-march-2022.html>

The FMA also publishes an annual circular on due diligence for the prevention of money laundering and terrorist financing.

For CSOs, this means an increased effort with regard to transactions connected to high-risk third countries.

In this context, also current sanctions regimes (e.g. EU-sanctions against Russia) which prohibit certain transactions concerning sanctioned countries or sanctioned persons should be considered.¹³

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?

On the one hand, reference should be made here to item 4b below regarding the Austrian banking secrecy. On the other hand, Austria has a so-called **account register** (*Kontenregister*).¹⁴ This register contains information on who holds which accounts at which Austrian credit institution, irrespective of whether the account holder is a resident or a non-resident, whether he or she is tax resident in Austria or abroad, and whether the accounts are held by a private individual or a legal entity.¹⁵

However, no account balances and account movements are visible.

Inspection of these is only permitted in the course of criminal proceedings, in tax matters, for the purposes of preventing and combating money laundering and terrorist financing, and for the purposes of sanctions by the Austrian National Bank.

¹³ E.g. with regard to sanctions against Russia and Belarus the following overview by the Austrian National Bank: https://www.oenb.at/dam/jcr:ed237fdb-347c-4947-9d89-5cffe119b540/OeNB_Leitfaden_Russland-Belarus-Sanktionen_20220405.pdf

¹⁴ It is not a public register, only public prosecutors, criminal courts and fiscal authorities have access and may conduct enquiries under certain conditions.

¹⁵ Edelhauser/Gaubinger, Geplante Neuerungen im Kontenregister- und Konteneinschaugesetz - KontRegG, kritische Analyse des Ministerialentwurfs zur KontRegG-Novelle, JEV 2020, 96

The purpose of this regulation is to enable the authorities in the aforementioned circumstances to obtain knowledge of whether or not a person has an account in Austria.¹⁶

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

In Austria, the confidentiality of banking information is given a particularly high priority. The **banking secrecy** according to sec 38 BWG provides that certain (confidential) information arising from the business relationship with a customer may not be disclosed or used.

Sec 38 BWG includes, above all, a fundamental right to withhold information from public authorities, which can only be deviated from in a few exceptional cases.

The banking secrecy applies to all persons who work for the bank, regardless of their position, shareholders and members of the bank's governing bodies. The scope of application may also extend to third parties if information has been entrusted or made accessible to them.

Furthermore, the banking secrecy covers any secrets that have been entrusted, known or made accessible to someone exclusively in the context of a business relationship. These may not be disclosed or exploited.

The only **exceptions to this rule** are named in sec 38 (2) BWG being amongst others, the initiation of judicial or financial authority criminal proceedings, the provision of information in connection with money laundering and deposit insurance, explicit written customer consent, the provision of general information regarding the economic situation of a company customary in banking if such company does not explicitly refuse such information, the clarification of legal matters concerning the relationship between credit institutions and customers, the obligation to provide information to the FMA according to the [Securities Supervision Act \(Wertpapieraufsichtsgesetz\)](#) or the [Stock Exchange Act \(Börsegesetz\)](#), the obligation to transmit and provide information, and reporting obligations under the Capital Outflow Reporting Act (*Kapitalabfluss-Meldegesetz*).

Particularly relevant is the initiation of criminal proceedings by the courts and financial authorities, which primarily relate to financial offenses, and the provision of information in connection with money laundering pursuant to sec 41 (1) and (2) BWG.

16 Edelhofer/Gaubinger, Geplante Neuerungen im Kontenregister, JEV 2020, 96

In addition to the Austrian banking secrecy, certain further provisions concerning confidentiality may be of relevance, e.g. the General Data Protection Regulation (*Datenschutz-Grundverordnung*) and the Austrian Data Protection Act (*Datenschutzgesetz*).

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

There exist reporting obligations in the event of suspected money laundering. For more details, please refer to section 3.

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

Yes,¹⁷ banks will pay increased attention to current sanctions against Russia. This includes in particular but not exclusively current EU-sanctions.¹⁸ Such sanctions affect different areas of daily life and economy and a wide variety of people. Therefore, when engaging in business with a client, banks will review whether such client, its affiliates or the transactions conducted by the client are subject to any sanctions or whether a link to a sanctioned country (e.g. Russia or Belarus) or any sanctioned person (according to given sanction provisions) exists. In general, banks will be very careful not to enter into any transactions that might conflict with existing sanctions regulations.

A comprehensive presentation of the various sanctions provisions would go beyond the scope of this questionnaire. However, we point out some of the sanctions that are especially essential in the given context:

- **Asset freeze**

A considerable number of persons have recently been added to the EU's financial sanctions list. This list is based on [Regulation \(EU\) No 269/2014](#) (as amended from time to time and especially multiple times since February 2022).

All funds and economic resources belonging to, owned, held or controlled by any natural or legal persons, entities or bodies named on such list are frozen and no funds or economic resources shall be made available, directly or indirectly, to or for the benefit of any listed person.

¹⁷ Please note that similar sanctions provisions might exist for other countries (e.g. Belarus).

¹⁸ In addition, e.g. US- and UK-sanctions can be of relevance.

A bank will refuse to enter in a business relationship with any listed person.

- **Restrictions on deposits**

According to Art 5b of [Regulation \(EU\) No 833/2014](#) (as amended from time to time and especially multiple times since February 2022). It shall be prohibited to accept any deposits from Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia, if the total value of deposits of the natural or legal person, entity or body per credit institution exceeds EUR 100 000. There are however certain exceptions to that rule. For example, the competent authorities may authorise the acceptance of such a deposit if (a) it is necessary for humanitarian purposes, such as delivering or facilitating the delivery of assistance, including medical supplies, food, or the transfer of humanitarian workers and related assistance or for evacuations; or (b) it is necessary for civil society activities that directly promote democracy, human rights or the rule of law in Russia.

- **Full transaction ban**

Art 5aa para 1 of [Regulation \(EU\) No 833/2014](#) (as amended from time to time and especially multiple times since February 2022) prohibits to directly or indirectly engage in any transaction with certain explicitly named Russian persons, entities or bodies which are publicly controlled or with over 50 % public ownership or in which Russia, its Government or Central Bank has the right to participate in profits or with which Russia, its Government or Central Bank has other substantial economic relationships. This transaction ban is extended to certain subsidiaries of the named persons and any persons who act on their behalf or at their direction. A bank will refuse to enter in a business relationship with any such person.

- **Trade sanctions**

[Regulation \(EU\) No 833/2014](#) (as amended from time to time and especially multiple times since February 2022) contains a considerable number of trade sanctions prohibiting different kinds of transactions (e.g. concerning the import of certain raw material to the EU or the export of certain technology to Russia. Such sanctions also concern the provision of financing or financial assistance to sanctioned persons.)



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