

EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT



European Center for
Not-for-Profit Law



PILnet



TURKEY

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.

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?

Generally, organizations do not have to be physically present in Turkey to open a bank account. That being said, in general, banks require the physical presence of a signatory authorized by the CSO. Banks allow authorized signatories of the non-resident legal entities to vest their powers through a power of attorney. Apart from these, in order for a non-resident CSO to carry out the following activities in Turkey, it must satisfy the conditions listed in here:¹

- to open a representative office;
- to establish a branch;
- to operate in Turkey;
- to cooperate with organizations operating in Turkey;
- to establish or to become a member of a Turkish association or a parent organization.

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)

Turkish banks do not impose any legal requirements specific for CSOs to open bank accounts. However, to ensure the legitimate and current activity of the CSO and to open an account in the name of the CSO; Turkish banks generally require the duly legalized and translated versions of the CSOs' corporate documents including but not limited to (depending on the requesting bank):

¹ Please click [here](#) to review the guide in Turkish.

- Association charter evidencing the CSO's incorporation;
- An original of the certificate of activity;
- A copy of the resolution of the competent body of the CSO approving the account opening and authorizing one or more signatories to sign the relevant documentation (including Banking Services Agreement) in its name and on its behalf (if required);²
- A specimen of signature of the authorized signatories as explained above;
- A power of attorney granting authority to third parties to enter into the relevant documentation on behalf of the CSO (this is only applicable if the CSO will be represented through a power of attorney);
- Documents identifying the authorized signatories (copies of identity cards or passports).

Also, Turkish banks require CSOs to obtain potential tax numbers from the Turkish Tax Offices and to provide contact and address information of the CSO's correspondences in Turkey.

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?

Who is authorized to open a bank account is a matter of the laws of the jurisdiction of the CSO. On the other hand, the CSO must provide legal evidence that the persons that will represent them vis-à-vis the bank are duly authorized to do so (i.e. a legalized power of attorney issued to these persons). Turkish banks do not allow online account opening by non-resident CSOs. Therefore, the persons authorized to represent the CSO must visit the bank in Turkey to sign the account opening documents.³ This person can be a Turkish resident person authorized through a power of attorney.

² Under Turkish Law, the competent body of CSOs is the Board of Directors. If the corporate documents of the relevant CSO requires the CSO's competent body to pass a resolution when entering into the Banking Services Agreement (or when opening the account), the relevant CSO must submit this resolution which also includes the authorization regarding the specific transaction alongside with documents submitted to the Bank. If the relevant CSO's corporate documents do not have such requirement, this item may be disregarded.

³ This can be a non-resident person, however, most of the banks require the CSO to have a contact person residing in Turkey who can be reached when needed.

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?

Estimated time of account opening may vary depending on the extent that the bank is satisfied with the KYC documents to be supplied to them. The account is immediately opened once the required documents are duly submitted. How long it would take to collect these documents is a matter of the laws of the jurisdiction of the CSO. As specified above, the persons authorized to represent the CSO in this process will need to visit the bank to submit the KYC documents and sign the account opening documents.

2. BANKING ACTIVITIES

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

Two main pieces of legislation regulate the due diligence obligation of Turkish banks when taking on new customers from an anti-money laundering perspective. They are (i) the Law No. 5549 on the Prevention of Laundering Proceeds of Crime (“[AML Law](#)”) and (ii) the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism (“[Measures Regulation](#)”).⁴ Both set out the know your customer obligations of Turkish banks. According to the relevant CSO’s legal characterization in Turkey (a labor union (*sendika*), union (*birlik*), association (*dernek*), foundation (*vakıf*)), Turkish banks may require different types of information to verify and authenticate the CSO’s identity. That said, banks generally require the name, purpose, registry number, tax identification number, full address, telephone number, fax number, and e-mail address of the relevant legal entity, representative’s name,

⁴ Both pieces of legislation define the obligated parties and regulate the procedures and principles of their obligations within the Turkish AML regulations to prevent the laundering of proceeds of crime. These obligations include but are not limited to the know your customer obligations, the suspicious transaction reporting obligations, the obligation to provide the information and documentation requested by the Financial Crimes Investigation Board (“MASAK”). The Measures Regulation lists banks as one of the obligated parties according to Article 4. Thus, banks are subject to various obligations outlined in the Measures Regulations and any other secondary legislation published by MASAK. Please click [here](#) to review the translation of AML Law and Measures Regulation. However, please keep in mind that English translations are not always up to date or good in quality.

surname, birthplace information, date of birth, nationality, ID type, and ID number and official documents that are issued in the CSO's jurisdiction, duly legalized and translated into Turkish, evidencing the accuracy of such information.

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 Measures Regulation also regulates suspicious transaction monitoring and reporting. Accordingly, Turkish banks are under an obligation to review the transactions to determine whether they are suspicious. If they suspect or have reasonable grounds that funds (subject of the transaction) are the proceeds of criminal activity or that the individual conducting the transaction will use the funds for illegal purposes, they must report these transactions to MASAK (Turkish Financial Crimes Investigation Authority). In line with the foregoing, Turkish banks must submit a suspicious transaction report to MASAK regardless of the value of the transaction in question. Furthermore, they may consider multiple transactions when necessary while considering whether a transaction is suspicious while evaluating a transaction.

There are publicly available guidelines on MASAK's website on suspicious transactions⁵ for banks. However, there is no English translation 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).

According to our knowledge, MASAK does not enforce a complete prohibition on transacting with any countries, provided that there are no national financial sanctions. However, according to the Measures Regulation, obligated parties are required to implement the tightened measures when conducting a transaction with high-risk countries. Within this context, banks are obliged to pay special attention to business relations and transactions with natural and legal persons, unincorporated entities, and nationals of risky countries and to collect and record as much information as possible about the purpose and

⁵ Please click [here](#) to review MASAK's guidelines on suspicious transactions in Turkish.

nature of transactions that do not have a reasonable legal and economic sense on the surface.

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

No, MASAK did not publish any list of high-risk jurisdictions. Banks often determine their own lists, however they are generally not publicly available (in practice they may also refer to FATF's grey list).

On a separate note, it might be significant to mention the problems with respect to certain physical limitations involving transactions with the Republic of Cyprus (also known as Southern Cyprus in Turkey). Turkey does not legally recognize the Republic of Cyprus as a sovereign state. Therefore, Turkish and Cypriote banking systems are not synchronized. As a result, a civil society organization wanting to transfer funds to an account in Cyprus from Turkey (or vice versa) might experience certain problems, such as the inability to transfer the funds directly. Therefore we recommend consulting the Turkish account bank to seek alternative options to complete these transactions. In practice, the Cypriot parties may tend to have accounts with Greek banks, and the transfer is made to or from such accounts.

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

Within the scope of the Measures Regulation, in high-risk situations to be identified within the framework of the risk-based approach, banks apply one or more or all of the following measures in proportion to the risk identified.

- Obtaining additional information about the client and updating the credentials of the client and the actual beneficiary more frequently.
- Obtaining additional information about the nature of the business relationship.
- Obtaining as much information as possible about the source of the assets subject to the transaction and the funds belonging to the client.
- Obtaining information regarding the main purpose of the subject transaction.
- Requiring the approval of a senior official while entering into a business relationship, continuing an existing business relationship or executing a transaction.

- Increasing the number and frequency of controls applied and keeping the business relationship under close supervision by identifying the types of transactions that require additional controls.
- Requiring the first financial transaction while establishing a continuous business relationship to be made from another financial institution to which the principles know the customer applying.

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 certain authorities that can request information from Turkish banks. In general, the client information is protected under the confidentiality obligation set forth under the Article 73 of the Banking Law No. 5411 ("Banking Law")⁶ and the Regulation on Disclosure of Confidential Information ("Disclosure Regulation").⁷ However, the data disclosure requests of competent authorities are excluded from the confidentiality obligation.

The Banking Regulatory and Supervisory Authority's ("BRSA") authority to require third parties to provide information under Turkish law is regulated under Article 95 and Article 96 of the Banking Law. In this respect, provided that the BRSA's request is limited to the fulfillment of its duties within the scope of the Banking Law and irrespective of any confidentiality obligation that may be applicable, the BRSA is entitled to require the following of any natural or legal person:

- Submit to the BRSA any data, information (including confidential information) and document that the BRSA requests

⁶ Please click [here](#) to review the translation of Banking Law. However, please keep in mind that English translations are not always up to date or good in quality.

⁷ Please click [here](#) to review the Regulation on Disclosure of Confidential Information in Turkish.

- Submit any commercial books and documents that the BRSA requests and have them available for the BRSA's examination
- Maintain their entire information processing system to be available for audit by the BRSA
- Provide to the BRSA access to all recordings on microfiche, microfilm, magnetic tape, disk and similar instruments related to any books, documents and reports that they are required to maintain, together with all systems and passwords necessary to enable access to the foregoing.

As mentioned above, the scope of the BRSA's discretion to request data from third parties is very broad, and the BRSA can require a third party to provide information even if such information is confidential to the extent that the BRSA's request is in furtherance of the fulfillment of its duties under applicable laws.

In addition to the BRSA's discretion specified above, the persons from whom the BRSA requests information are obliged to respond to the request within the time period to be determined by the BRSA and to provide the necessary convenience for the BRSA's examination.

On the other hand, the BRSA may not require a third party to provide information under any of the following circumstances:

- The provision of the concerned information would jeopardize the national security or the interests of the Turkish state.
- The concerned information is subject to professional secrecy (e.g., lawyer-client privilege).
- The provision of the concerned information would jeopardize the privacy of family life.
- The provision of the concerned information would jeopardize the right of defense.

Failure to comply with the BRSA's requests for information may trigger criminal liability. Article 153 of the Banking Law sets forth that the persons who fail to provide information upon the BRSA's request will be subject to imprisonment from one to three years and to a criminal monetary penalty of up to TRY 150,000. In addition, any person who prevents the audit of the BRSA will be subject to imprisonment from two to five years.

As per the Article 332 of the Criminal Procedure Law⁸ the public prosecutors, judgeships or courts can request information during investigation and prosecution of crimes. There is no limit for types of information that can be requested. The requests must be responded within 10 days and if it is impossible to provide the information within 10 days, the reasons for non-compliance must be disclosed to the requesting authority.

As per Article 89 of the Enforcement and Bankruptcy Law No. 2004,⁹ a secured creditor in an enforcement proceeding can collect a debtor's receivables from third parties. In this equation, banks may be the third party and the creditors may send the notices to collect any amount banks owe to the debtors, if any. The creditors are not obliged to check whether the debtors actually have receivables from the relevant third party but may send notices of attachment to companies they think may be relevant. In such a case, banks may need to disclose information about their clients.

In civil proceedings, the judge can request information from the parties of a civil lawsuit. Therefore, if banks are party to a lawsuit, they may need to disclose information to the relevant court. However, if they are not party to the lawsuit, then there is no specific statutory obligation to respond. However, in theory, failure to respond to the request may qualify as "disobedience of an order" under Article 32 of the Misdemeanors Law,¹⁰ and may lead to an administrative fine of TRY 581 (approx. USD 35).

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

There are certain requirements foreseen both under banking legislation and data protection legislation:

(i) Bank's confidentiality obligation

Under the Banking Law No. 5411, the data belonging to real and legal persons that has been generated following the establishment of a client relationship qualifies as client information. A Turkish bank can disclose client information to third parties (including the bank's affiliates registered abroad) only in case of (i) an exemption from confidentiality obligation or (ii) a specific request or instruction from the client to this effect. The obligation to obtain this request or instruction

8 Please click [here](#) to review the Criminal Procedure Law in Turkish.

9 Please click [here](#) to review the Enforcement and Bankruptcy Law in Turkish.

10 Please click [here](#) to review the Misdemeanors Law in Turkish.

applies even in cases where the client's explicit consent has been obtained.

The Disclosure Regulation, which entered into force on July 1, 2022 and is based on the Banking Law No. 5411, supplements the principles of the Banking Law No. 5411.

The Disclosure Regulation elaborates on these exemptions and introduces "proportionality principle" for data disclosures. Proportionality principle applies to all data disclosures and may require banks to take additional actions when transferring data. In this respect, in order for the disclosure of client secrets to be compliant, such disclosure must rely on one of the legal bases (i.e. client instruction/request or exemptions) and comply with the proportionality principle.

(ii) Technical and organizational measures under banking legislation

Turkish banks must ensure data security and implement necessary technical organization measures foreseen under the provisions of the Regulation on Banks IT Systems and Electronic Banking Services¹¹ relating to data confidentiality and security, which include but not limited to:

- Maintaining a risk management process for monitoring IT systems;
- Implementing effective authentication and access management systems;
- Conducting controls and tests for information security;
- Identifying and remedying security vulnerabilities;
- Conducting operations to increase awareness of employees/ service providers on data security;
- Maintaining and reviewing information security policies, processes or procedures;
- Establishing roles and duties for information security;

¹¹ Please click [here](#) to review the Regulation on Banks IT Systems and Electronic Banking Services. However, please keep in mind that English translations are not always up to date or good in quality.

- Implementing additional security measures based on the degree of the data's sensitivity/importance;
- Implementing encryption methods and algorithms to ensure data security and network security.

(iii) Technical and organizational measures under data protection legislation

Under the Turkish Data Protection Law No. 6698 data controllers (such as Turkish banks) are obliged to take all necessary technical and organizational measures to (i) prevent the unlawful processing of personal data; (ii) prevent the unlawful access to personal data; and (iii) to maintain personal data in a secure way. The Turkish DPA published a guideline regarding organizational and technical measures.¹² In addition, DPA's decision dated January 31, 2020 and numbered 2018/10¹³ lists the relevant measures in detail regarding special categories of data. In addition to the data security requirements under banking legislation, banks, as data controllers, are also required to take necessary technical and organizational measures to protect its client's data.

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

From the AML perspective there are two reporting obligations imposed on Turkish banks. One of them is the suspicious transaction reporting obligation as described under 3.b. The other one is continuous reporting obligation. According to the Measures Regulation, besides the suspicious transaction reporting obligation, MASAK requires banks to report certain transactions continuously. Within the scope of the AML Law, banks must report transactions that exceed the amount determined by the Ministry of Treasury and Finance to MASAK. However, the Ministry of Treasury and Finance has not yet determined a threshold for the continuous reporting obligation. Therefore, this obligation does not apply in practice. Apart from these there are no specific reporting obligations under MASAK.

On the other hand, the legal entities residing in Turkey are allowed to transfer foreign exchange or Turkish lira abroad through banks in Turkey. There is no monetary limitation on

¹² Please click [here](#) to review the DPA Guideline in Turkish.

¹³ Please click [here](#) to review DPA's Decision numbered 2018/10 in Turkish.

the amount of funds to be transferred. Banks intermediating the transfer of funds abroad are, however, under the obligation to report any transfers in Turkish or foreign currency exceeding the equivalent of USD 50,000 (including transfers from foreign exchange deposits) to the Central Bank of the Republic of Türkiye (“CBRT”) within 30 (thirty) days of the transfer.

Pursuant to the Decree No. 32,¹⁴ it is free to import funds to Turkey in Turkish lira or foreign currency. However, in order to determine whether unidentified foreign currency fund transfers made from abroad to a Turkish entity’s account, for USD 50,000 or more, are in respect of the loans utilized by such an entity, Turkish banks are required to obtain the related entity’s written declaration as well as information and documents substantiating the declaration. If the entity fails to provide the written declaration and/or information and documents substantiating the declaration, the bank will not complete the transfer and will return the foreign currency amount. The Turkish bank is obliged to verify the nature of the transfer even if the entity’s statement is obtained. Therefore, the bank may require further documents and information from the entity to make sure that the transferred amount does not relate to loans made to the entity.

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

Up to now, the Turkish government did not adopt any sanctions against Russia regarding the Russia – Ukraine conflict. Moreover, under Turkish law, Turkey is not under an obligation to implement or comply with the sanctions adopted by the US, UK, or the EU. That said, banks with international connections (i.e., banks with foreign shareholders or foreign banks with Turkish subsidiaries or branches) often attempt to comply with the sanctions adopted by the US, UK, or the EU, even though, as per Turkish law, they are under no obligation to comply with them. Since many countries started adopting various sanctions against Russia, banks in Turkey began to carry out more systematic and strict due diligence processes against Russian and Belarusian customers to avoid any potential collateral impact of sanctions or reputational risks in their businesses.

¹⁴ Please click [here](#) to review the Decree No.32 on the Protection of the Value of Turkish Currency. However, please keep in mind that English translations are not always up to date or good in quality.



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