EUROPEAN BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT

European Center for Not-for-Profit Law

PILnet

NETHERLANDS

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?

Generally, the organization does not have to be physically present in the Netherlands to open a bank account. However, internal Know-Your-Customer (KYC) and risk procedures of a bank may require this. Also, a registration with the trade register (*handelsregister*) of the Dutch Chamber of Commerce (*Kamer van Koophandel*) is often required.

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)

Generally, there are no requirements specifically for CSOs to open bank accounts. However, internal KYC and risk procedures of a bank may provide additional requirements (e.g. annual turnover) and can vary per bank.

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? In case of requirement of presence can this be fulfilled by signing the paperwork at an embassy or notary?

The person authorised to open a bank account on behalf of the CSO is the person duly authorised to represent the CSO, e.g. a director (*bestuurder*) of a foundation or his/her authorised representative. It is formally possible that the paperwork can be prepared through a civil notary, although this is not very common and can make the process more burdensome. Note that the bank can set additional requirements through its internal KYC and risk procedures.

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?

Each Dutch bank will need to determine whether the CSO is permitted to open a bank account. The application process can take quite some time (e.g. several months). During the application process, the bank will determine whether the CSO satisfies the KYC and risk procedures. It will be of vital importance that the bank gets a proper understanding of the identity of the CSO, its activities and operating cycle (flow of money, goods and services), its legal structure and directors, the ultimate beneficial owner(s), and the countries it will be sending funds to and receiving funds from. An interview is usually not required as long as the paperwork is in order.

2. BANKING ACTIVITIES

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

Banks must screen their customers before entering into a business relationship or carrying out a (incidental) transaction and carefully monitor the such business relationship, including scrutiny of transactions undertaken throughout the course of that relationship. Through customer due diligence, the customer is identified and screened. Once onboarded, the customer and all its financial transactions are permanently monitored. This Know Your Customer (KYC) principle is a basic principle in the Dutch financial services industry, which is laid down in the Dutch Financial Supervision Act (Wft)[1] and elaborated in the Dutch Money Laundering and Terrorist Financing (Prevention) Act (Wwft).[2] The Wwft is based on the European Anti-Money Laundering Directive (AMLD). The Dutch Central Bank (DNB) supervises compliance with the Wwft.

Customer Due Diligence

Banks are prohibited from entering into a business relationship or carrying out a transaction if these banks have not carried out customer due diligence (CDD) or if such investigation has not led

1 https://wetten.overheid.nl/BWBR0020368/2021-11-06.

2 https://wetten.overheid.nl/BWBR0024282/2021-07-01.

to the envisaged results (Section 5 Wwft). The Wwft contains three types of CDDs:

1. Regular CDD;
2. Simplified CDD; and
3. Enhanced form of CDD.

A CDD must be conducted by means of a risk-based approach. Additional measures need to be undertaken if the risk of money laundering or financing terrorism may be higher and vice versa.

Regular CDD

Pursuant to Section 3 (5) and Section 4 (1) Wwft, banks are required to carry out a Regular CDD to prevent money laundering and terrorist financing in any of the following instances:

a. prior to establishing a business relationship (more than one transaction) in or from the Netherlands;
b. prior to carrying out one or more one-off transaction(s) (non-cash) with a minimal (combined) value of EUR 15,000;
c. in case of a suspicion of a customer's involvement in money laundering or terrorism financing;
d. in case of doubts about the veracity or adequacy of previously obtained customer identification data;
e. in case of a suspicion of customer's involvement in money laundering and terrorism financing which gives reason to apply a CDD;
f. in case of a suspicion of money laundering and terrorism financing because of the country in which the customer is residing; and
g. in the event that a one-off transaction constitutes a transfer of funds in and/or from the Netherlands exceeding EUR 1,000.

CDD should enable banks (Section 3 (2) Wwft):

a. to identify the customer and to verify his/her identity;
b. to identify the Ultimate Beneficial Owner (UBO) of the customer and to take risk based and adequate measures in order to verify his/her identity, and if the customer is a legal person, to take risk based and adequate measures in order to gain an insight into the ownership- and control structure of the customer; where the UBO is a senior managing official, banks must take the necessary reasonable measures to verify

the identity of the natural person who holds the position of senior managing official and must keep records of the actions taken as well as any difficulties encountered during the verification process;

c. to adopt the purpose and the intended nature of the business relationship;

d. to have the business relationship under an ongoing control and to have the on-off transaction that take place during the term of this business relationship under control, in order to ascertain that this is in line with the knowledge, which the bank has of the customer and his/her risk profile, with, if this is necessary, an investigation to the resources (*bron van de middelen*) that have been used in relation to the business relationship or the transaction;

e. to determine whether the natural person (*natuurlijke persoon*), who represents the customer, is entitled to represent such customer;

f. to take risk based and adequate measures in order to verify whether the customer is acting on behalf of him/herself or on behalf of a third party

Simplified CDD

In certain cases, a simplified due diligence (SDD) procedure will be sufficient. An SDD does not imply an exemption from any of the CDD measures. However, banks may adjust the amount, timing or type of each or all of the CDD measures in a way that is appropriate to the low risk they have identified.

Prior to entering into a business relationship or transaction, banks may conduct a SDD in the event that the business relationship or transaction potentially has a lower risk. Pursuant to Section 6 (1) Wwft, banks must take the list of factors into account as set out in Annex II to the 4th Anti-Money Laundering Directive (EU) 2015/849 (AMLD4) in order to determine whether there is a potential lower risk of money laundering or terrorist financing. This Annex II includes, amongst others, customer risk factors and geographical risk factors.

Enhanced CDD

If (i) a business relationship or a transaction is of a nature which involves a higher risk of money laundering or terrorist financing or (ii) a customer residing in a third-country jurisdiction which has strategic deficiencies in its national AML/CFT regime, an enhanced form of CDD (ECDD) must be performed (Section 8 (1) Wwft).

The Wwft refers to risk factors as set out in Annex III to the AMLD4 which banks must take into account in order to determine whether there is a potential higher risk of money laundering or terrorist financing (Section 8 (2) Wwft). This Annex III qualifies, amongst others, 'non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures' as a risk factor. Furthermore, Annex III to the AMLD4 includes customer risk factors, product, service, transaction or delivery channel risk factors and geographical risk factors.

Pursuant to Section 8 (3) Wwft, banks take reasonable measures to examine the background and purpose of (i) complex transactions, (ii) unusually large transactions, (iii) transactions with an unusual pattern or (iv) transactions with no apparent economic or lawful purpose. Banks must also increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual.

If a customer is not physically present for identification, banks may apply innovative solutions in order to verify the customer and his/her identity at distance. By using such innovative solutions banks must take the risk factors as set out in Annex III to the AMLD4 into account. Furthermore, the bank must ensure that it has (i) technical abilities to appropriately monitor these innovative solutions, (ii) a senior management and compliance officer which have sufficient knowledge regarding the innovative solutions and (iii) a contingency plan (*noodplan*) in place to ensure the continuity of the CDD.

An ECDD and the additional measures are also required if banks enter into a business relationship with, or carry out a transaction involving, (the family of) a politically exposed person. Banks should have proper procedures in place to determine whether politically exposed persons are involved (Section 8 (5) and (8) Wwft).

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

Banks must take measures to prevent money laundering and terrorist financing. To this end, they must pay particular attention to **unusual** transaction patterns and transactions of customers that due to their nature typically carry a higher risk of money

laundering and terrorist financing. If there are grounds for assuming that an actual or proposed transaction is linked to money laundering or terrorist financing, they must immediately report it as an unusual transaction to the Financial Intelligence Unit – the Netherlands (FIUN).[3] For completeness, it is noted that in the Netherlands unusual transactions must be reported to FIUN (instead of suspicious transactions as is the case for many other EEA Member States). Official monitoring criteria can be found in Annex 1 of the Implementation Decree Wwft and are summarized in English on the website of the FIUN.[4] Internal principles are generally not publicly available.

The first step in the transaction monitoring process is risk identification. During the identification process banks systematically analyse the money laundering and terrorist financing risks. The results of this analysis are recorded in the systematic analysis of the integrity risks (SIRA). Drawing up a SIRA is an obligation that was initially imposed by the Wft but is now also included as an obligation in the Wwft.

Section 2b of the Wwft requires financial institutions to draw up a systematic risk analysis. This obligation applies to all institutions referred to in the Wwft, including banks. The obligation for certain financial institutions to conduct a systematic integrity risk analysis also results from Sections 3:10 and 3:17 of the Wft, Article 10 of the Prudential Rules (Financial Supervision Act) Decree, Article 19 of the Decree on the Financial Assessment Framework for Pension Funds and Article 14 of the Pensions Act Implementation Decree.

The risk analysis under the Wwft focuses on money laundering and terrorist financing, whereas the risk analysis under the Wft has a broader scope. When drawing up the SIRA, institutions take account of the risk factors relevant to them. The SIRA means as a minimum that the institution performs the assessment periodically in accordance with a predetermined protocol. The institution then records the results of the assessment in writing

As shown above, the financial institution then monitors its transactions and activities for suspicious or unusual situations. These situations may include amounts, times, locations and devices used. Do the transactions fit the customer's risk profile and

3 See Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act, paragraph 5.1 <https://www.dnb.nl/media/i1xjqk52/dnb-guidance-anti-money-laundering-and-anti-terrorist-financing-act-and-the-sanctions-act-december-2019.pdf>

4 https://www.fiu-nederland.nl/en/meldergroep/8

do the activities not deviate too much from what is customary for this customer? In that case, data from before, during and after the transaction is taken into account. Nowadays, financial institutions, including banks, increasingly combine information obtained internally with data from public sources. More information can be found in the 'Know Your Customer In Brief' section of the Dutch Payments Association.[5]

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).

Yes.

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

A list of third-country jurisdictions which are considered to have strategic deficiencies in their anti-money laundering (AML) and countering the financing of terrorism (CFT) regimes that pose significant threats to the financial system can be found in the Annex to Commission Delegated Regulation (EU) 2016/1675.[6] A list of black listed countries that are identified by the Financial Action Task Force (FATF) to have strategic AML/CFT deficiencies can be found on the website of the FATF.[7] Banks can also make use of internal lists of high risk jurisdictions, which are not publicly available.

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

In case a customer of the bank is resident in geographical areas of higher risk, the bank will take this into account as a factor of potentially higher-risk situation. This means that an ECDD must be performed.

A transaction or intended transaction to a high risk jurisdiction must be reported as unusual transaction to the FIUN.

By way of derogation from the general prohibition against

5 https://www.betaalvereniging.nl/en/know-your-customer-in-brief/

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A02016R1675-20210207

7 https://www.fatf-gafi.org/countries/#high-risk.Also see the website of the FIU: https://www.fiu-nederland.nl/en/which-countries-have-been-designated-high-risk-countries-by-the-fatf.

carrying out unusual transactions, banks are able to carry out unusual transactions before informing the competent authorities where refraining from such carrying out is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, is without prejudice to any applicable obligations pursuant to the Dutch Sanctions Act 1997 (Dutch Sanctions Act) (e.g. the obligations to freeze without delay funds or other assets of terrorists, terrorist organizations or those who finance terrorism).

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?

Banks are required by law to share customer account information with domestic and foreign tax authorities. For example, data needed to determine whether and how much tax a customer has to pay, but also information to determine in which country a customer has to pay tax. Also, customer data is shared with the Dutch Central Bank (DNB) pursuant to the Dutch Sanctions Act. This concerns data of persons and/or organizations that are on the Dutch, European and United Nations sanctions lists as referred to under the Dutch Sanctions Act (and European sanctions legislation).

Central Bank (DNB) pursuant to the Dutch Sanctions Act. This concerns data of persons and/or organizations that are on the Dutch, European and United Nations sanctions lists as referred to under the Dutch Sanctions Act (and European sanctions legislation).

The Dutch government is cooperating with many countries to combat tax evasion. Internationally, members of the Organization for Economic Cooperation and Development (OECD) have agreed to automatically exchange financial account information. The Common Reporting Standard (CRS) was developed for this purpose. The CRS is a system designed to identify account holders living or domiciled abroad. It is also designed to annually exchange financial account information among countries that

have signed an agreement for this purpose. The Netherlands is a participant in this agreement together with other EU member states. The CRS has been incorporated into the Dutch International Assistance (Levying of Taxes) Act (WIB). This act obliges financial institutions in the Netherlands to be aware and register where all account holders, private and commercial customers, reside or are domiciled for tax purposes. In addition, the tax identification number of their country of tax residence must be registered.[8]

In addition, banks must take measures to prevent money laundering and terrorist financing. To this end, they must pay particular attention to unusual transaction patterns and transactions of customers that due to their nature typically carry a higher risk of money laundering and terrorist financing. If there are grounds for assuming that an actual or envisaged transaction is linked to money laundering or terrorist financing, they must immediately report it as an unusual transaction to the FIUN.[9]

Furthermore, banks may face demands from the Public Prosecution Department to supply customer information as part of a criminal investigation into a customer or a third party. The bank is subject to a confidentiality obligation. A demand may be grounds for banks to conduct more detailed and possibly ECDD and to carry out additional monitoring of the customer's transactions. The results of the more detailed customer due diligence may be grounds for banks to take control measures or report unusual transactions to the FIUN without discussing the demand with the customer.[10]

Directive (EU) 2019/1153 enhances the use of financial information by giving law-enforcement authorities direct access to information about the identity of bank-account holders

8 For more information: See Q&A 'Common Reporting Standard and your personal or business tax residence' of the Dutch Banking Association <https://www.nvb.nl/media/1981/001277_q-and-a-common-reporting-standard-and-your-personal-or-business-tax-residence.pdf>

9 See Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act, paragraph 5.1 <https://www.dnb.nl/media/i1xjqk52/dnb-guidance-anti-money-laundering-and-anti-terrorist-financing-act-and-the-sanctions-act-december-2019.pdf>

10 See Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act, paragraph 5.9 <https://www.dnb.nl/media/i1xjqk52/dnb-guidance-anti-money-laundering-and-anti-terrorist-financing-act-and-the-sanctions-act-december-2019.pdf>

contained in national centralized registries. In addition, it gives law enforcement the possibility to access certain information from national Financial Intelligence Units (FIUs) – including data on financial transactions – and also improves the information exchange between FIUs as well as their access to law enforcement information necessary for the performance of their tasks.

Finally, banks have a joint warning system. In it they register data of persons and legal entities that have committed fraud or have tried to do so. This involves privacy-sensitive information. Banks process these data in accordance with the Protocol on the Incident Warning System for Financial Institutions (PIFI). The protocol has been approved by the Data Protection Supervisor.

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

There is no specific legal provision on banking secrecy in the Netherlands. As a general principle, Dutch law requires banks to keep all customer data confidential and are obliged to observe the European General Data Protection Regulation (GDPR). Several exceptions apply. The more general exception provides that a bank is authorised to disclose customer data to third parties, including regulatory authorities or supervisors, if it is under a statutory obligation to do so. For example, personal data may be processed for the purposes of the prevention of money laundering and terrorist financing as referred to in the aforesaid legislation and may not be further processed in a way that is incompatible with those purposes. The processing of personal data for any other purposes, such as commercial purposes, is in principle prohibited..

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

None that we are aware of.

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