ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

1. Activities and actions to reduce the risk of money laundering and terrorist financing and properly manage the identified risk of money laundering or terrorist financing:

The purpose of the procedure is to implement financial security measures and other regulatory obligations at the obligated institution, in accordance with the Act on anti-money laundering and combating the financing of terrorism. The procedure contains a set of internal regulations that are undertaken in the obligated institution in cooperation with dedicated state and international bodies to combat and prevent the above crimes. Since the goal of the obligated institution is to operate transparently, in accordance with the law and principles of social intercourse, this procedure is intended to prevent the use of the services it offers in an unlawful manner. The procedure therefore applies to employees, associates as well as contract, temporary or agency workers, interns, volunteers and trainees (hereinafter all collectively as "associates"). The basic activities and actions to implement statutory obligations are the application of financial security measures and ongoing risk analysis to prevent money laundering or terrorist financing. The internal procedure is subject to ongoing review and updating as necessary.

The procedure has been developed and is applied in the entity, indicated below, which is also referred to as an OBLIGATED INSTITUTION:

Name:	FINFERNO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Address:	HOŻA 86/210, 00-682 WARSAW, POLAND
TAX ID:	7011212502
Date of introduction of the procedure:	12.07.2024

The services the entity provides:
- exchange services between virtual currencies, as well as between virtual currencies and means of payment

Services that the entity does not provide:
- services of exchange of fiat currency for another fiat currency
- payment services according to the Payment Services Act (the entity especially does not accept deposits and does not transfer funds)

The obligated institution applies the General Principles Model operating in its business, which is also an instruction on the financial security measures applied, which is attached as an Annex to this Procedure. The procedure consists of:

01a_General Principles Model with instructions
02a_Declaration of BR and PEP_NATURAL PERSON
02b_Declaration of BR and PEP_LEGAL AND OTHER ENTITIES
02c_ PEP Procedure
02d_Note for PEP operation
03_Note on discrepancies under Article 61a
04_Evaluation of the business relationship
04a_Note of current transaction analysis
05_Declaration on legality of funds and source
05a_Client evaluation sheet_NATURAL PERSON
05b_Client evaluation sheet_LEGAL AND OTHER ENTITIES
06_Company_Regulations_designation of employees responsible for AML
07_Risk Assessment
08_Procedure for anonymous reporting of violations
09_Procedure for monitoring transactions, STR with description of the process
10_Confirmation of training and knowledge of procedure
11_Decision to implement the AML procedure_EN_signature

The above-mentioned documents, as well as the provisions of this procedure, are intended to develop a practical approach to performing individual AML/CFT duties.

1) Definitions

AML (anti-money laundering) – anti-money laundering – a set of activities, procedures and regulations created to prevent criminal activities related to money laundering;

Beneficial owner – a natural person or persons exercising direct or indirect control over a client through the powers they have, which arise from legal or factual circumstances, enabling them to exercise decisive influence over the actions or activities undertaken by a client or a natural person or persons on whose behalf business relationships are established or the occasional transaction is carried out;

PEP's close associate – a natural person who is the beneficial owner of a legal entity, organizational unit without legal personality or trust jointly with PEP or who has other close relations with PEP in connection with its business activities, as well as a natural person who is the sole beneficial owner of legal entities, organizational unit without legal personality or trusts known to have been established for the purpose of obtaining an actual benefit from PEP.

Account blocking – temporarily preventing the use and disposition of all or part of the assets accumulated in the account (in case the obligated institution provides account services);

PEP's family member – spouse or person in common cohabitation, child of PEP or his spouse or person in common cohabitation, parents.

CFT (combating the financing of terrorism) – counter-financing terrorism – a set of activities, procedures and regulations created to prevent criminal activities related to terrorism;

Terrorist financing – an offence against public security involving the accumulation, transfer or offering of assets in order to finance a terrorist offence, or the provision of assets to a person or an organised group with the aim of committing such an offence (in detail, an act defined in Article 165a of the Act of 6 June 1997, the Criminal Code);

GIIF – General Inspector of Financial Information, government administration body competent in anti-money laundering and combating the financing of terrorism;

Obligated institution – entrepreneurs, companies and institutions that are obliged to analyze transactions and provide information on suspicious transactions to the GIIF;

Senior management – management board member, director or employee of the obligated institution with AML/CFT expertise related to the organization's operations and decision-making that affects risk and as such, responsible for carrying out statutory obligations;

Client – a natural person, legal entity or organizational unit without legal personality, to whom the organization provides services or for whom it performs activities falling within the scope of its professional activity (including with whom the organization establishes business relationships or on whose behalf it carries out an occasional transaction);

Politically exposed person (hereinafter PEP) – natural person holding a significant position or performing a significant public function;

Employee – natural person performing duties for the obligated institution regardless of the legal form on the basis of which the cooperation was established (employment contract, contract of mandate, cooperation contract and others).

Money laundering – an activity aimed at introducing into legal circulation money originating from illegal sources or used to finance illegal activities (specifically, an act defined in Article 299 of the Act of 6 June 1997, the Criminal Code);

Information processing – any operation performed on information, in particular, their acquisition, collection, consolidation, storage, editing, sharing and deletion (the term is also understood as information stored in a computer system);

Business relationships – relations of the organization with a client related to the company's professional activities, which, at the time of establishment, show the characteristic of permanence;

Transaction – a legal or factual act on the basis of which is made the transfer of ownership or possession of assets, or a legal or factual act made for the purpose of transferring ownership or possession of assets;

Occasional transaction – a transaction carried out not within the framework of economic relations;

Act – the Act of 1 March 2018 on anti-money laundering and counter-terrorist financing;

Assets – property rights or other movable property, real estate, means of payment, financial instruments, other securities, foreign exchange, virtual currencies (including cryptocurrencies);

Suspension of transactions – temporary restriction of the use and disposal of assets consisting in preventing a single transaction or more transactions;

2) Responsibilities of senior management

a) Establishes the responsibilities of those responsible for implementing and maintaining an effective anti-money laundering and combating the financing of terrorism system, and fulfils the statutory duties listed in the AML/CFT Act
b) Sets budget to support and develop internal AML/CFT countermeasure system,
c) Approves the training plan and expenditures for training and competence enhancement,
d) Responsible for building awareness among employees and associates on AML/CFT and also for adhering to the procedures and policies implemented in the organization in this regard.

3) The person responsible for carrying out the duties contained in the procedure:

In the absence of a written designation and the acceptance of these duties by another person, they are all members of the management board of the obligated institution (senior management). This provision should be treated as the designation of a responsible person in accordance with the statutory regulation. The primary person performing these duties is the President of the Management Board or the owner of the obligated institution in case the President of the Management Board has not been singled out. The responsibilities include implementing statutory regulations, ensuring compliance of the activities of the obligated institution and its employees and other persons performing activities for the entity, as well as providing notifications of statutory requirements. The Obligated Institution will appoint one or more persons to fulfil the statutory obligations contained in the Act, depending on the legal form of the business.

4) Associates of the obligated institution:

a) comply with the organization's AML/CFT policies and procedures implemented;
b) take an active part in assessing a client's risk, apply financial security measures to the client;
c) ensure that the company's operations comply with the act and meet AML/CFT security standards;
d) inform the person responsible for the compliance of the obligated institution with AML/CFT regulations and make available all data in their possession on the circumstances of transactions indicating a link to money laundering or terrorist financing – regardless of the size of the transaction;
e) participate in training courses on anti-money laundering and combating the financing of terrorism.

Accordingly, upon commencing work/cooperation with an obligated institution, these individuals and persons performing AML/CFT duties and become familiar with this procedure and receive training on AML/CFT (possibly in the form of an online video).

2. Principles for identifying and assessing the risk of money laundering and terrorist financing associated with a given business relationship or occasional transaction,

including the principles for verifying and updating a previously made assessment of the risk of money laundering and terrorist financing.

1) **Recognition**
   Means gathering information about the client based on own sources, publicly available information and based on information and documents provided by a client.

2) **Risk assessment and risk documentation**
   It means classifying a client into the appropriate risk category (low, standard, high) based on the methodology developed and used in the organization.

   Record of client risk with an assessment in the form of a so-called client file (may be maintained electronically), which must include:
   a) Client type,
   b) Geographic area,
   c) Purpose of the account,
   d) The type of products, services, services provided and their distribution channels,
   e) The level of assets held by the client or the value of the transaction, if the client qualifies as a high-risk client,
   f) The purpose, regularity or duration of the economic relationship.

3) **Principles of risk assessment verification**

   In particular, the following criteria should be taken into account to determine client risk:
   a) Economic – assessing a client in terms of the purpose of their business,
   b) Geographic – analysis of the client's transactions, its business relationships with entities in third countries where there is an increased risk of money laundering and terrorist financing. The client's place of residence or business should also be evaluated here.
   c) Substantive – what type of business does the client do, is it higher or high risk from the perspective of AML/CFT regulations?
   d) Behavioural – unusual client behaviour in a given situation.

   The risk analysis takes into account:
   a) KNF (The Polish Financial Supervision Authority) Announcements and Training,
   b) GIIF Annual Reports,
   c) National Risk Assessment,
   d) European Commission Report,
   e) Corporate memory and experience of the obligated institution,
   f) Media reports.

4) **Update of previously made risk assessment**

   Frequency of updating client risk assessment:
   a) For a low-risk client – once every 3 years,
   b) For a client with a standard risk level – once every 2 years,
   c) In the case of a high-risk client – once every 1 year,
   d) And also whenever the obligated institution becomes aware of a change in significant issues that may affect the client's risk level.

Recognition, assessment and updating of risk is carried out on the basis of forms filled out for each client meeting the conditions for the application of financial security measures to him. Based on the established information, points are assigned to the client, used to assign a client to a specific risk group, including the recognition and assessment of the level of identified risk. Recording of this activity is carried out by completing the Client Evaluation Sheet. In this Sheet, through the creation of a scoring system, the weight assigned to each risk assessment criterion/factor, influencing the final result of the analysis, as well as a list of alarm signals, arousing vigilance that translates into proceedings against a client or transaction to prevent incidents of money laundering or terrorist financing.

3. **Measures used to properly manage the identified risks of money laundering or terrorist financing associated with the business relationship or occasional transaction in question, including activities or actions taken to mitigate the risks of money laundering and terrorist financing**

Characteristics of factors related to client risk analysis (sample calculation):

a) Client type:
   - a natural person,
   - a natural person conducting a business activity,
   - a commercial company,
   - a commercial company admitted to trading on a regulated market,
   - non-profit organization.

b) Business object – industry:
   - scrap metal trading,
   - fuel industry,
   - services (e.g., car washes, laundromats, restaurants),
   - construction industry

c) Domicile of a client – verification of the country of residence of the registered office in terms of:
   - the degree of corruption (clash with corruption maps),
   - divergence of headquarters or residence from the usual client,
   - tax haven headquarters (countries with harmful tax competition)
   - origin from high-risk countries designated by the European Commission (by which is meant the countries listed in the Directive of the European Parliament and of the Council (EU) 2015/849 or any other current legal act) or recognized as such by the obligated institution, which as of the date of introduction of the procedure is meant at least:

1	Afghanistan
2	Bahamas
3	Barbados
4	Botswana
5	Cambodia
6	Ghana
7	Iran
8	Iraq
9	Jamaica
10	Democratic People's Republic of Korea (DPRK)
11	Mauritius
12	(deleted)
13	Myanmar/Burma
14	Nicaragua
15	Pakistan
16	Panama
17	Syria
18	Trinidad and Tobago
19	Uganda
20	Vanuatu
21	Yemen
22	Zimbabwe

d) Client behaviour – behavioural factor

In the case of a client risk assessment, the obligated institution's associates consider the client's behaviour and evaluate it for abnormal behaviour. In such a situation, an employee of the obligated institution should include this factor in the risk assessment. A situation that should draw the associate's special attention is the presence of an additional person at the transaction, especially when instructing the client on what to do.

e) Client transactions (size and geography)
Evaluate a client for contracts and transactions that are inconsistent with its business profile - if its behaviour cannot be reasonably explained, this should be included in the risk assessment.

f) Client presence
The absence of a client at the conclusion of the contract and also during the relationship is considered a higher risk factor.

g) New products, channels, technologies
If a client intends to provide new services, offer new products or distribution channels or technologies, this could lead to an increase in AML/CFT risk. This risk will not always relate directly to a client, but needs to be assessed in terms of the security of the obligated institution.

h) Client status
If a client has the status of a politically exposed person, a family member of such a person, or is a person known to be a close associate, or the person is on a warning or sanction list this is a significant factor for increased risk assessment.

The lower risk may be evidenced by the fact that a client is:

a) A unit of the public finance sector,
b) A state-owned enterprise or a company with a majority shareholding of the State Treasury, local government units or their associations,
c) A company whose securities are admitted to trading on a regulated market subject to beneficial owner disclosure requirements or a company with a majority stake in such a company,
d) Resident of a member state of the European Union, a member state of EFTA - a party to the EEA Agreement,
e) Resident of a third country described by reliable sources as a country with low levels of corruption or other criminal activity,
f) Resident of a third country where AML/CFT regulations are in force, according to reliable sources.

A lower risk may also be evidenced by linking the business relationship or occasional transaction to:

a) European Union member state, EFTA member state - party to the EEA agreement,
b) a third country described by reliable sources as having low levels of corruption or other criminal activity,
c) a third country with AML/CFT regulations in place, according to reliable sources.

The increased risk may be evidenced in particular:

a) establishing business relationships in unusual circumstances;
b) that a client is:
- a legal entity or organizational unit without legal personality, whose activities are used to store personal assets,
- a company in which bearer shares have been issued, whose securities are not admitted to organized trading, or a company in which the rights of the shares are exercised by entities other than shareholders,
c) the subject of a client’s business involving the conduct of a significant number or high amount of cash transactions,
d) unusual or excessively complex ownership structure of a client, taking into account the type and scope of its business activities,
e) the client's use of services or products offered through private banking;
f) the client's use of services or products that promote anonymity or make it difficult to identify the client,
g) establishing or maintaining a business relationship or conducting an occasional transaction without the physical presence of the client,
h) the commissioning of transactions by unknown or unrelated third parties whose beneficiary is the client;

i) covering business relations or transactions with new products or services or offering products or services using new distribution channels;
j) linking a business relationship or occasional transaction to:
- a high-risk third country,
- a state described by reliable sources as a state with a high level of corruption or other criminal activity, a state that finances or supports the commission of terrorist acts, or with which the activities of terrorist organizations are linked,
- a country against which the United Nations or the European Union has decided to impose sanctions or specific restrictive measures.

Absolutely high AML/CFT risk occurs in particular when:
a) The client is from or based in a high-risk third country,
b) The client has PEP status,
c) Correspondent banking relationships are being established,
d) The transaction has the status of an unusual transaction.

Risk mitigation is achieved by completing a client assessment sheet, including the introduced scoring, to assist in determining the degree of risk identified. In addition, with the intention of mitigating risk, the Obligated Institution uses the records presented in the General Principles Model operating in its business, completing the solutions introduced, and applies the procedure for monitoring transactions and reporting suspicious transactions (STR).

4. Principles of application of financial security measures

1) Financial security measures are in place for:

a) establishing economic relations (showing the characteristic of permanence);
b) conducting an occasional transaction:
- of the equivalent of EUR 15,000 or more, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related, or
- which represents a transfer of funds for an amount exceeding the equivalent of EUR 1,000;
- **with the use of virtual currency of the equivalent of EUR 1,000 or more - in the case of mandatory institutions referred to in Article 2, section 1, item 12 of the Act**
c) carrying out an occasional cash transaction of the equivalent of EUR 10,000 or more, regardless of whether the transaction is carried out as a single operation or several operations that appear to be interrelated - in the case of mandatory institutions referred to in Article 2, section 1, item 23;
d) betting on stakes and receiving winnings of the equivalent of EUR 2,000 or more, regardless of whether the transaction is carried out as a single operation or several operations that appear to be interrelated - in the case of obligated institutions referred to in Article 2, section 1, item 20;
e) suspected money laundering or terrorist financing;
f) doubts about the veracity or completeness of client identification data obtained to date.

Simplified financial security measures are allowed at where a risk assessment confirms a lower risk of money laundering or terrorist financing.

Enhanced security measures are applied in case of a higher risk of money laundering or terrorist financing and, in particular, in case of clients coming from or based in a high-risk third country. Enhanced safeguards may consist, in particular, of verifying the client with more than one of the required documents.

2) How to apply financial security measures

Financial security measures include:
a) Identification of the client and verification of his identity, including in particular whether he is a politically exposed person;
b) identification of the beneficial owner and taking reasonable steps to:
- verify his identity,
- determine the structure of ownership and control - in the case of a client that is a legal entity, an organizational unit without legal personality or a trust;

c) assessing business relationships and, as appropriate, obtaining information on their purpose and intended;
d) ongoing monitoring of the client's business relationships, including:
- analysis of transactions carried out within the framework of the business relationship to ensure that these transactions are consistent with the obligated institution's knowledge of the client, the type and scope of its business, and consistent with the money laundering and terrorist financing risks associated with that client,
- investigation of the source of assets at the disposal of the client - in cases justified by the circumstances,
- ensuring that the documents, data or information in its possession regarding business relations are kept up to date.

The execution of the above financial security measures is done manually. The practical manner in which financial security measures are applied is determined by the AML records used to fulfil the obligations of the Act, including the charters, forms and notes introduced. With the help of these documents, the practical application of the above measures is carried out based on the principles established in these documents. Any person acting for the Obligated Institution in fulfilling its AML/CFT obligations should use the forms in question when dealing with clients.

3) Identification of a client involves determining in the case of:

a) natural person:
   i. name and surname,
   ii. citizenship,
   iii. the Universal Electronic System for Registration of the Population (PESEL) number or date of birth, and if no PESEL number has been assigned, the date of birth and country of birth,
   iv. the series and number of the person's identification document,
   v. address of residence - in case the obligated institution has this information,
   vi. the name (company), tax identification number (NIP) and address of the main place of business - in the case of a natural person conducting a business activity;
b) legal entity or organizational unit without legal personality:
   i. (company) name,
   ii. organizational form,
   iii. registered office or business address,
   iv. NIP, and in the absence of such a number - the country of registration, the name of the relevant registry, and the number and date of registration,
   v. identification data referred to in item 1 letters a and c, of the person representing that legal entity or organizational unit without legal personality.

Determination of whether a client is a politically exposed person is made by the client's declaration before using the service and ongoing checking of the information obtained to identify and verify the person. The client shall make a declaration that he is not a person holding such a position with the clause "I am aware of the criminal liability for making a false declaration".

4) Identification of the beneficial owner:

Includes the determination of his name and, where possible, the data indicated in point 3 above designation ii-vi.

5) Verification:

Verification consists in confirming the established identification data of the persons in item 3 above, based on:
a) identity document;
b) driver's license (as a supporting document);
c) passport;
d) or on the basis of another document, data or information from a reliable and independent source.

6) Evaluation of economic relations and their ongoing monitoring consists of taking actions leading to an assessment of whether:

a) The performance of transactions by a person/entity does not show the characteristic of permanence (especially repetition and regularity);
b) The client's transactions do not violate regulations related to the Act on anti-money laundering and combating the financing of terrorism;
c) Funds used for transactions do not come from undisclosed or illegal sources;
d) Identification data and verification documents held are updated on an ongoing basis;
e) There are no other irregularities resulting in possible violations of applicable regulations.

An important role is played here by the declaration made by the client of the obligated institution, related to the purpose of establishing a business relationship or carrying out a transaction, the presented business model of the client including the established risks associated with this activity, the declaration made during the course of the business relationship, and unusual behaviour of the client deviating from the originally declared nature and purposes of establishing a business relationship or carrying out a transaction.

In order to fulfil the obligation referred to in Article 43, section 3 of the Act, the Obligated Institution conducts ongoing analysis of transactions, a process that in practical terms is included in the procedure for monitoring transactions and reporting suspicious transactions (STR).

The results of the ongoing analysis of the transactions The obligated institution documents a note in the form of a table, where it enters the individual transaction amounts, the date of the transaction, with the signature of the person making the entry, analysing whether the transactions deviate significantly from the obligated institution's knowledge of the client, the type and scope of its business, and whether the transactions are consistent with the money laundering and terrorist financing risks associated with that client.

7) What does an obligated institution do if one of the financial security measures cannot be applied?

a) does not establish business relationships;
b) does not carry out the occasional transaction;
c) does not conduct transactions through a bank account;
d) dissolves business relationships.

8) Business relationships or carrying out a transaction with a politically exposed person and applying enhanced financial security measures

According to the current regulations, if a risk analysis is conducted showing that a transaction is to be carried out with a politically exposed person (as a client or beneficial owner) or a family member of such a person or a person known to be a close associate of such a person, the obligated institution MAY carry out such a transaction. In such a case, however, the person conducting the transaction obtains the approval of senior management for such action, and the obligated institution:

1) applies appropriate measures to determine the source of the client's property and the source of the assets at the client's disposal in the course of business relations or transactions;
2) intensifies the use of financial security measures;
3) intensifies the application of the financial security measure referred to in Article 34, section1, item 4 of the Act.

An obligated institution shall apply enhanced financial security measures in cases of higher risk of money laundering or terrorist financing, as well as in cases referred to in Articles 44-46 of the Act.

The application of enhanced security measures involves:

a) obtaining additional information about:
   - the client and the beneficial owner,
   - the intended nature of the business relationship;
b) obtaining information about the source of the client's and the beneficial owner's assets and the source of the assets at the client's and the beneficial owner's disposal within the framework of a business relationship or transaction;
c) obtaining information on the reasons and circumstances of the intended or conducted transactions;
d) obtaining approval from senior management to establish or continue business relationships;

e) intensify the application of the financial security measure referred to in Article 34, section 1, item 4 of the Act, by increasing the number and frequency of monitoring of economic relations and increasing the number of transactions typified for further analysis.

In the case of a transaction related to a high-risk third country identified by the European Commission, an Obligated Institution, in addition to applying the financial security measures referred to in Article 44, section 1 of the Act, shall take at least one of the following actions to mitigate the risk associated with such transaction:

a) undertakes additional activities as part of the enhanced financial security measures in place;
b) introduces intensified obligations to provide information or report transactions;
c) limits the scope of economic relations or transactions.

Enhanced financial security measures are applied in the situations referred to in section 3 of this procedure in the event of identification of elevated and absolutely high client risk.

6. Rules for the storage of records and information.

The obligated institution and its employees are required to document the financial security measures in place, e.g. by making copies of documents, screen shots with the date, or in any other way. Records are kept for a period of 5 years from the date of termination of business relations with the client or from the date of the occasional transaction. Documents are stored in a manner that ensures their security and in accordance with data protection regulations. These issues are governed by separate internal procedures.

7. Rules for the performance of duties involving the submission of information on transactions and notifications to the Inspector General.

The purpose of the procedure is to identify events, situations that trigger the obligation of the obligated institution to report, report to the GIIF. The reporting obligation of the obligated institution consists of:

a) Reporting of transactions exceeding the threshold,
b) Reporting to the GIIF on suspicious circumstances.

In a situation where a reasonable suspicion is raised that a certain transaction or certain assets may be related to money laundering or terrorist financing, or in a situation where there is a suspicion that these crimes have been committed, notifications are made to the GIIF, fulfilling the obligation under Articles 74, 86 and 90 of the Act on anti-money laundering and combating the financing of terrorism.

For example, notification to the GIIF is given in the following cases:

- Lack of economic purpose to justify the numerous transactions performed by the client;
- Lack of documents confirming the source of assets at the client's disposal;
- Frequent and numerous transactions performed by the client on a single day;
- High transaction amounts;
- Splitting transaction amounts in one day;
- The address of the entity is that of a so-called virtual office, where other business entities are also registered;
- Linking the conduct of non-registered business activities (without formal registration).

Suspicion may also be aroused by situations other than those mentioned above, in case of reasonable circumstances, such as the coincidence of IP addresses from which transactions are carried out, the use of e-mail with the @protonmail.com domain, making transactions with the same user logging in from different accounts.

Registration is done electronically via the website https://www.giif.mofnet.gov.pl/#/glowna
The organization also cooperates with authorities when information is requested.

1) Management Board:

a) accepts reports and evaluates the appropriateness of their further reporting to the supervisory authority,
b) is responsible for training employees on how to inform and report necessary events,

c) cooperates with the authorities and provides them with the necessary documents and information.

2) Associates:

a) report the events described in the procedure,
b) in the event that they become aware of the person who made the report - ensure that his or her data is not disclosed to other employees and that the reporting person does not suffer negative consequences related to the report,
c) in the event that they become aware of a person who has been reported as potentially or actually responsible for an AML/CFT violation - ensure that this information is kept confidential.

3) Situations in which the obligated institution provides information to the GIIF:

a) accepted deposit or made withdrawal of funds with an equivalent value of more than EUR 15,000,
b) made transfer of funds with an equivalent value of more than EUR 15,000, with exceptions specified by law.

The organization is obliged to immediately notify the GIIF in case of a reasonable suspicion that a particular transaction or assets may be related to money laundering or terrorist financing. An employee, associate, trainee and any other person who will have a reasonable suspicion of the above shall provide the Management Board with information on the subject by e-mail or verbally. The deadline for submitting the information is immediate. The Management Board shall decide without undue delay on the further fate of the application. Since the confirmation of acceptance of the notification, the obligated institution does not carry out transactions.

4) Notice of suspected crime

An obligated institution, excluding domestic banks, branches of foreign banks, branches of credit institutions and cooperative savings and credit unions, shall immediately notify the competent public prosecutor if it has a reasonable suspicion that the assets transacted or accumulated in the account originate from or are related to a crime other than the crime of money laundering or terrorist financing or a fiscal crime.

The obligated institution shall apply the formal requirements, related to the application, specified in the Act.

8. Principles of dissemination of knowledge of anti-money laundering and counter-terrorist financing regulations among associates (employees) of the obligated institution.

Senior management provides access to knowledge of anti-money laundering and combating the financing of terrorism regulations among their associates, including employees. This involves, in particular:

a) Sending current guidelines and other courses of action,
b) Providing written, electronic and oral information and explanations,
c) Informing about changes in regulations,
d) Providing at least initial access to training (possibly in the form of an online video) on the topic of anti-money laundering and combating the financing of terrorism.

The obligated institution shall ensure that employees participate in training programs on the implementation of AML obligations, taking into account issues related to the protection of personal data. The training programs referred to above shall take into account the nature, type and size of the activities carried out by the obligated institution and shall provide up-to-date knowledge in the implementation of the obligations of the obligated institution, in particular the obligations referred to in Articles 74, section 1, 86, section 1 and 89, section 1 of the Act.

The completion of training by an employee, is documented by the issuance of a certificate by the training provider and a declaration of training, signed by the employee.

9. Rules for employees to report actual or potential violations of anti-money laundering and combating the financing of terrorism regulations

A procedure has been implemented at the obligated institution that allows employees and other persons performing activities (hereinafter referred to as "other persons") for the benefit of the obligated institution of actual or potential violations of AML and CFT regulations. The procedure is that these people have been provided with an e-mail address to which they can make submissions. Submissions can also be made anonymously in this regard. Accordingly:

a) Persons serving as management board members are the persons responsible for receiving applications;
b) Notifications are received by reading the e-mail message and taking appropriate actions in connection with it;
c) The data of an employee or other person is subject to special protection, so the contents of the application are not shared with anyone outside the management board. The obligated institution is obliged to provide such working conditions that the reporting person does not suffer negative actions, including discriminatory, repressive actions, in connection with the report;
d) In the event that the identity of the persons reporting or affected by the report is disclosed, as well as the possibility of determining the identity of these persons, senior management shall determine the circle of persons who may have had access to this and instruct them on their duty of confidentiality and the consequences of not complying;
e) Upon receipt of the application, senior management reviews it and, if it is found to be valid, takes appropriate action, including, in particular:
   - stopping the transaction,
   - reporting suspected crimes,
   - reporting to the GIIF.

In the above regard, this procedure also refers to the introduced procedure for anonymous reporting of AML/CFT violations.

10. Principles of internal control or supervision of compliance of the activities of the obligated institution with the provisions on anti-money laundering and combating the financing of terrorism and the rules of conduct set forth in the internal procedure.

Senior management:

a) On an ongoing basis, it analyses changes in anti-money laundering and counter-terrorist financing regulations to ensure compliance with the procedure,
b) In the event of changes or observation of inconsistencies or lack of precision, they take action resulting in the correction of the procedure,
c) On an ongoing basis, they oversee how the procedure is used in practical terms to ensure maximum efficiency.

For this purpose, an internal control and supervision report is prepared in accordance with the requirements and development of the obligated institution.

11. **Rules for noting discrepancies between information collected in the Central Register of Beneficial Owners and information on the client's beneficial owners established in connection with the application of the Act.**

In the case of the risk analysis performed, as well as the identification and verification of the client, if a discrepancy is noted between the information collected in the Central Register of Beneficial Owners and the information on the client's beneficial owners established in connection with the application of the Act, an annotation is made in the client Profile.

If discrepancies are discovered between the information collected in the Central Register of Beneficial Owners and the established information on the beneficial owner from the client, there is an obligation to note these discrepancies and to take steps to clarify the reasons for the discrepancies. The obligated institution is required to contact the client, explain the client's determination of the beneficial owner, explain the client's determination of the ownership and control structure, explain whether the obligated institution's determination of the beneficial owner and ownership and control structure of the client was correct, explain for what reason the client considered the person to be the beneficial owner, collect new information and documents.

If the recorded discrepancies are confirmed, t is mandatory to provide the authority in charge of the Registry with verified information on these discrepancies, together with the reasons and records for

the recorded discrepancies. Applications are made electronically via the website https://crbr.podatki.gov.pl/adcrbr/#/ under the "Report a discrepancy" tab.

One type of **discrepancy is the failure to report information on beneficial owners to the CRBR (CRBR - Central Register of Beneficial Owners).** This is because the failure to report the information to the Central Register of Beneficial Owners should be read as a declaration by the client that the natural person is not the beneficial owner of the entity required to report the information to the Central Register of Beneficial Owners.

Verification of the beneficial owner can be done not only on the basis of a document from the registry, but also on the basis of, for example, a memorandum of association or a company's share transfer agreement.

The Obligated Institution shall make a note of the above activities.

12. **Rules for documenting impediments identified in connection with verification of the identity of the beneficial owner and actions taken in connection with the identification as the beneficial owner of a natural person in a senior management position.**

In the event of difficulties in connection with the verification of the identity of the beneficial owner and actions taken in connection with the identification as the beneficial owner of a natural person holding a senior management position, an annotation to this effect is made in the client Profile. This is an exceptional situation, so the rule is to determine the beneficial owner in accordance with the earlier provisions of this procedure.

The obligated institution uses this method of determining the beneficial owner in situations:

1) in which there is a complex and multi-level ownership structure, and the analysis of the client's ownership structure leads to the conclusion that it is impossible to determine or there are doubts about the identity of the natural persons defined in Article 2, section 2, item 1, letter a, first through fourth indents of the AML Act;

2) in which the ownership structure includes entities located in countries that do not make detailed information available to the public - for example, about the beneficial owners).

The obligated institution shall document the following actions taken to verify the identity of the beneficial owner and the actions taken in connection with the identification as the beneficial owner of a natural person in a senior management position:

1) Actions taken to establish the identity of natural persons as defined in the first through fourth indents of Article 2, section 2, item 1, letter a of the AML Act (for example, obtaining a duplicate of the client's KRS, the client's company deed, the client's share transfer agreement, an employee's transcription of a note of a telephone conversation with a client's representative);
2) Circumstances that have been determined by the obligated institution as causing the impossibility of determining or doubting the identity of the natural persons specified in the first through fourth indents of Article 2, section 2, item1, letter a) of the AML Act (for example, the determination that each partner of the client - a natural person - holds 20% of the shares);
3) Impediments related to legitimate actions taken to verify the identity of the beneficial owner, i.e. a natural person in a senior management position (for example, failure to report information about the beneficial owner to the Central Register of Beneficial Owners, impediments related to the lack of physical presence of the beneficial owner, impediments related to video verification)**.**

In order to fulfil the above obligation, the Obligated Institution has introduced a form to fulfil the obligation in question. Among other things, it contains a field to be filled out in connection with the identification of difficulties with verifying the identity of the beneficial owner.

13. **Sanction policy**

With the purpose of not executing transactions or entering into business relations with persons who are on sanction lists, as well as fulfilling the obligations of Articles 117-119 of the Law, the Obliged Institution checks clients data in the sources located at the following web addresses:

1) https://www.gov.pl/web/finanse/lista-osob-i-podmiotow-wobec-ktorych-stosuje-sie-szczegolne-srodki-ograniczajace-na-podstawie-art-118-ustawy-z-dnia-1-marca-2018-r-o-przeciwdzialaniu-praniu-pieniedzy-i-finansowaniu-terroryzmu

2) https://www.gov.pl/web/finanse/sankcje-miedzynarodowe-giif
3) https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami

Verification of the client on the sanction lists is carried out by one or more methods:
1) Marking in the electronic system of the Obliged Institution;
2) Confirmation on the risk assessment card;
3) Note (possible on an individual or aggregate basis).

The Obligated Institution may retain a screenshot, but this is not required.

Verification of the client on the sanction lists takes place at the time of establishing a business relationship/conducting a transaction for which financial security measures are carried out. The updating of client information in the above-mentioned regard is carried out at the time of updating other client information related to the nature and purpose of the business relationship.

If a client is disclosed on the above-mentioned lists (in terms of specific restrictive measures), the following are applied:
(a) the freezing of property values owned, held, controlled directly and indirectly by persons and entities, as well as the benefits derived from such property values, by which is meant the prevention of their transfer, alteration or use, as well as the carrying out of any operation with the participation of such values in any way that may cause a change in their size, value, place, ownership, possession, nature, purpose or any other change that may enable benefits to be derived from them;
(b) not making property values directly or indirectly available to or for the benefit of persons and entities, which means, in particular, not granting loans, consumer credit or mortgages, not making donations, not making payments for goods or services.

At the same time, the obliged institution may use a broader catalog of sanction lists, especially in the case of the application of increased financial security measures or any other need in view of the determination of such a need, applying to the circumstances or established/established risks. The full catalog as to sanction lists (also listed above) includes:
1) Council Regulation (EU) No. 833/2014 of July 31, 2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine (OJ.EU.L.2014.229.1 as amended),
2) Council Regulation (EU) No. 269/214 of March 17, 2014 on restrictive measures with regard to actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (OJ.EU.L.2014.78.6 as amended),
3) Regulation (EC) No. 765/2006 of the European Parliament and of the Council of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and Belarus' participation in Russia's aggression against Ukraine (OJ.EU.L.2006.134.1, as amended),
4) US BIS Denied Persons List - https://www.bis.doc.gov/index.php/the-denied-persons-list
5) Canada Sanctions List - https://www.international.gc.ca/world-monde/international_relations- relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng
6) Australian DFAT Sanctions List - https://www.dfat.gov.au/international-relations/security/ sanctions/consolidated-list
7) Polish Sanctions List - https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami
8) Polish list of restrictive measures - https://www.gov.pl/web/finanse/lista-osob-i-podmiotow- wobec-ktorych-stosuje-sie-szczegolne-srodki-ograniczajace-na-podstawie-art-118-ustawy-z- dnia-1-marca-2018-r-o-przeciwdzialaniu-praniu-pieniedzy-i-finansowaniu-terroryzmu
9) EU Sanctions List - https://www.sanctions-intelligence.com/global-lists/
10) Sanctions Targets UK - https://www.gov.uk/government/publications/financial-sanctions- consolidated-list-of-targets/consolidated-list-of-targets
11) French Freezing of Assets - https://www.opensanctions.org/datasets/fr_tresor_gels_avoir/
12) SDN List - https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated- nationals-and-blocked-persons-list-sdn-human-readable-lists
13) UN Sanctions List - https://www.un.org/securitycouncil/content/un-sc-consolidated-list
14) Netherlands Sanctions List - https://www.sanctions-intelligence.com/global-lists/
15) World Bank Sanctions - https://www.sanctions-intelligence.com/global-lists/
16) EU Country Sanctions - https://www.sanctionsmap.eu/#/main