INTERNAL PROCEDURE

FOR COUNTERACTING MONEY LAUNDERING AND TERRORIST FINANCING

1. Activities and actions aimed at limiting the risk of money laundering and terrorist financing and proper management of the identified risk of money laundering or terrorist financing:

The purpose of the procedure is to introduce in the obligated institution financial security measures and other obligations specified by law, in accordance with the Act on Counteracting Money Laundering and Terrorist Financing. The procedure contains a set of internal regulations undertaken in the obligated institution in cooperation with dedicated national and international authorities for combating and preventing the above-mentioned crimes. Due to the fact that the purpose of the obligated institution is to operate in a transparent manner, in compliance with the law and principles of social coexistence, this procedure is intended to prevent the use of the services offered by it in a manner inconsistent with the law. The procedure therefore applies to employees, associates as well as contract, temporary or agency employees, interns, volunteers and trainees (hereinafter collectively referred to as “associates”). The basic activities and actions for the implementation of statutory obligations consist in applying financial security measures and ongoing risk analysis in order to prevent the occurrence of money laundering or terrorist financing.

The internal procedure is subject to ongoing verification and, if necessary, updating.

The procedure has been developed and is applied in the entity indicated below, which is simultaneously defined as the OBLIGATED INSTITUTION:

Name:	TRUSTPAY SP. Z O.O.
Address:	ul. Hoża 6/210, 00-682 Warsaw
NIP:	5272948997
Procedure update date:	27.10.2025

The Institution provides the following payment services:

1) accepting cash deposits and making cash withdrawals from a payment account and all activities necessary to maintain the account
2) execution of payment transactions, including transfer of funds to a payment account with the user’s provider or another provider:

2a) by executing direct debit services, including one-off direct debits

2b) using a payment card or a similar payment instrument

2c) by executing credit transfer services, including standing orders

3) execution of payment transactions referred to in point 2, charged to funds made available to the user under a credit agreement
4) issuing payment instruments
5) enabling acceptance of payment instruments and execution of payment transactions initiated by the payer’s payment instrument by the acceptor or through it, consisting in particular in handling authorization, transmitting to the issuer of the payment instrument or payment systems the payer’s or acceptor’s

Andrejs Saricevs

payment orders aimed at transferring funds due to the acceptor, excluding activities consisting in clearing and settlement of such transactions within a payment system within the meaning of the Act on Settlement Finality (acquiring)

6) provision of money remittance service

The Procedure consists of:
01_Internal procedure for counteracting money laundering and terrorist financing
02_Model of general rules together with instructions on the applied financial security measures
02a_Statement on BO and PEP_NATURAL PERSON
02b_Statement on BO and PEP_LEGAL PERSON AND OTHER
02c_PEP procedure
02d_Note for handling the PEP
03_Note on discrepancies in the procedure under art. 61a
04_Assessment of the business relationship
04a_Note from ongoing transaction analysis
05a_Client assessment card_NATURAL PERSON
05b_Client assessment card_LEGAL PERSON AND OTHER
06b_Company_Resolutions_appointment of employees responsible for AML
07_Risk assessment
08_Procedure for anonymous reporting of violations
09_Procedure for transaction monitoring, STR together with the process description
10_Confirmation of having completed training and familiarity with the procedure
11_Decision on implementation of the procedure AML_PL_signature

The above documents, as well as entries in this procedure, are intended to develop practical activities performed by individual persons within the scope of statutory obligations.

1) Definitions

AML (anti money laundering) – counteracting money laundering – a set of activities, procedures and regulations introduced in the institution to prevent the introduction of assets derived from crime into circulation.

Beneficial owner – a natural person exercising direct or indirect control over the client through powers arising from legal or factual circumstances, enabling decisive influence on activities or actions undertaken by the client, or any natural person on whose behalf a transaction or activity is carried out (meaning also transactions or activities carried out in relation to a trust), including:

a) in the case of a legal person other than a company whose securities are admitted to trading on a regulated market subject to disclosure requirements arising from European Union law or corresponding provisions of a third country:

– a natural person holding more than 25% of shares or stocks in that legal person,

– a natural person holding more than 25% of the total number of votes in the decision-making body of that legal person, including also as a pledgee or user, or under agreements with other authorized persons to vote,

– a natural person exercising control over the legal person or legal persons that jointly hold more than 25% of shares or stocks or more than 25% of the total number of votes in the decision-making body of that legal person, including also as a pledgee or user, or under agreements with other authorized persons to vote,

– a natural person exercising control over the legal person through personal connections referred to in art. 3 sec. 1 point 29 of the Accounting Act,

– a natural person holding a senior managerial position, in the case of documented inability to identify natural persons referred to in the above indents and in the absence of suspicion of money laundering or terrorist financing;

b) in the case of a trust:

– the founder, including the founder within the meaning of the Act of 26 January 2023 on the family foundation,

– the trustee, including a member of the management board within the meaning of the Act of 26 January 2023 on the family foundation,

– the supervisory board member, if established, including a member of the supervisory board within the meaning of the Act of 26 January 2023 on the family foundation,

– the beneficiary or – in the case where natural persons benefiting from the trust have not yet been designated – the group of persons in whose main interest the trust was established or operates,

– another natural person exercising control over the trust,

– another natural person exercising control over the legal person connected with the trust, including through ownership of shares or stocks, holding more than 25% of shares or stocks in that legal person, or through exercising control over that legal person.

c) in the case of a natural person conducting business activity, in respect of whom no premises or circumstances have been found that could indicate the fact of exercising control over them by another natural person or natural persons, it is assumed that such a natural person is simultaneously the beneficial owner.

Close associate of a politically exposed person (PEP) – a natural person who is a beneficiary of a legal person, organizational unit without legal personality or trust jointly with a politically exposed person, or who maintains close business relations with such a person, or is the sole beneficiary of a legal person, organizational unit without legal personality or trust, where it is known that the legal person, organizational unit without

legal personality or trust was established for the actual benefit of a politically exposed person.

Account blocking – temporary prevention of disposal and use of all or part of the assets accumulated in an account, including by a payment service provider.

Family member of a politically exposed person – spouse or person remaining in cohabitation with a politically exposed person, child of a politically exposed person and their spouse or cohabiting partner, parents of a politically exposed person.

CFT (combating the financing of terrorism) – counteracting the financing of terrorism – a set of actions, procedures and regulations created in order to prevent criminal activities related to terrorism;

Financing of terrorism – an offence against public security consisting in collecting, transferring or offering assets for the purpose of financing a crime of a terrorist nature or making assets available to a person or an organised group intending to commit such an offence (the act specified in detail in Article 165a of the Act of 6 June 1997 – Penal Code);

GIIF – General Inspector of Financial Information, the authority administering matters of counteracting money laundering and terrorist financing.

Obligated institution – entrepreneur within the meaning of the Act who is obliged to apply AML/CFT procedures, reports, transaction monitoring and implementation of measures arising from the Act.

Senior management – member of the management board, director or employee performing managerial functions in the obligated institution responsible for implementation of AML/CFT obligations.

Client – natural person, legal person or organizational unit without legal personality to whom the obligated institution provides payment services in connection with its business activity or professional activity.

Politically exposed person (PEP) – a natural person occupying a prominent public position, including:

a) head of state, head of government, minister, deputy or assistant minister, secretary of state,
b) member of parliament or similar legislative bodies,
c) member of governing bodies of political parties,
d) members of supreme courts, constitutional tribunals and other high-level judicial bodies whose decisions are not subject to appeal, except for extraordinary procedures,
e) members of courts of auditors or management boards of central banks,
f) ambassadors, chargés d'affaires and senior officers of the armed forces,
g) members of administrative, management or supervisory bodies of state-owned enterprises, companies with State Treasury participation in which more than half of the shares or stocks are held by the State Treasury or other state legal persons,

h) directors, deputy directors and members of governing bodies of international organisations or persons performing equivalent functions in such organisations,
i) directors general in supreme offices and central state authorities, as well as directors general of voivodeship offices,
j) other persons holding public positions or performing public functions in state authorities or central government administration bodies,
as well as persons indicated in the Regulation of the Minister of Finance, Funds and Regional Policy of 27 July 2021 on the list of domestic positions and public functions being politically exposed positions.

Employee – person performing duties for the obligated institution regardless of the legal basis of employment, including on the basis of civil law contracts.

Money laundering – action consisting in introducing into circulation property values derived from illegal or undisclosed sources in order to conceal their origin.

Entrepreneur – entity conducting business activity within the meaning of applicable regulations.

Ongoing monitoring – regular analysis of transactions carried out by the client and verification of the source of funds and consistency with declared business profile.

Transaction – legal or factual action based on which transfer of property values is carried out.

Occasional transaction – transaction carried out outside established business relations.

Transfer – any transaction carried out at least partly electronically on behalf of the payer via a payment service provider in order to make funds available to the payee via a payment service provider, regardless of whether the payer and the payee are the same person, and regardless of whether the payer's payment service provider is identical to the payee's payment service provider, including:

a) a credit transfer within the meaning of art. 2 point 1 of Regulation (EU) No 260/2012;
b) a direct debit within the meaning of art. 2 point 2 of Regulation (EU) No 260/2012;
c) a domestic or cross-border money remittance service within the meaning of art. 4 point 13 of Directive 2007/64/EC;
d) a transfer carried out using a payment card, an electronic money instrument, a mobile phone or another digital or IT device (in a subscription or prepaid system) with similar characteristics.

Act – Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing.

Property values – property rights or other property items, including cash, funds, securities, foreign exchange values.

Freezing of property values – temporary prevention of transfer, conversion, disposal or movement of property values.

2) **Scope of duties of senior management**

a) Establishes the scope of competences of persons responsible for the implementation and maintenance of an effective system for counteracting money laundering and terrorist financing, and also fulfills the obligations indicated in the Act on counteracting money laundering and terrorist financing;

b) Determines and supports the development of knowledge and competences of the AML/CFT employees;

c) Approves and trains and shapes employees' and associates' awareness in the field of counteracting money laundering and terrorist financing, and also compliance with the procedures and rules implemented in the organization in this scope.

d) Is responsible for building awareness among employees and associates in the field of counteracting money laundering and terrorist financing, as well as for compliance with the procedures and principles implemented in the organization in this respect.

3) **Person responsible for the implementation of obligations contained in the procedure:**

In the case of a single-member management board, acceptance of obligations by one person is assumed; all members of the management board of the obligated institution (senior management). Within the scope of responsibility for the implementation of obligations contained in the procedure and documentation concerning counteracting money laundering and terrorist financing, an appropriate person should be appointed, who monitors the implementation of the obligations imposed. This may be a separate function within the organizational structure of the obligated institution (e.g. person responsible for AML/CFT), who reports to the management board and ensures compliance of the institution's activities and employees' actions with the requirements for the benefit of the entity, as well as compliance with statutory obligations contained in the Act. The performance of statutory obligations contained in the Act may be entrusted to one or several persons depending on the legal form and scope of activity.

4) **Employees of the obligated institution:**

a) comply with the procedures implemented in the organization and transfer AML/CFT information;

b) take part in the assessment of the client's risk, apply financial security measures towards the client;

c) ensure that operations carried out comply with the provisions of AML/CFT law and internal regulations and report suspicious transactions or circumstances that may indicate money laundering or terrorist financing – regardless of the amount of the transaction;

d) inform the person responsible for compliance of the obligated institution with AML/CFT regulations about any suspicion related to circumstances of a transaction indicating money laundering or terrorist financing – regardless of the amount of the transaction;

e) take part in training on counteracting money laundering and terrorist financing.

In connection with the above, upon commencing cooperation/work with the obligated institution, these persons and persons performing duties related to AML/CFT become acquainted with this procedure and undergo training in the field of counteracting money laundering and terrorist financing (including in the form of e-learning).

5) Internal scope of the obligated institution's procedure

This internal procedure of the obligated institution defines, taking into account the nature and size of the activity, the rules of conduct applied in the obligated institution and includes in particular:

a) activities or actions undertaken in order to limit the risk of money laundering and terrorist financing and proper management of the identified risk of money laundering and terrorist financing;
b) principles of identifying and assessing the risk of money laundering and terrorist financing related to given business relationships or an occasional transaction, including the principles of classifying clients and business relationships by level of risk, taking into account the assessment of the risk of money laundering and terrorist financing;
c) financial security measures and proper risk management related to money laundering or terrorist financing associated with given business relationships or an occasional transaction;
d) principles of applying financial security measures;
e) principles of storing documents and information;
f) principles of performing obligations including the transfer to the General Inspector of Financial Information of information on transactions and notifications;
g) principles of disseminating among employees of the obligated institution knowledge in the scope of regulations on counteracting money laundering and terrorist financing;
h) principles of reporting by employees actual or potential violations of regulations in the scope of counteracting money laundering and terrorist financing;
i) principles of internal control or supervision of compliance of the obligated institution's activity with the regulations on counteracting money laundering and terrorist financing and with the rules of conduct specified in the internal procedure;
j) principles of recording discrepancies between information collected in the Central Register of Beneficial Owners and information on the client's beneficial owners determined in connection with the application of the Act;
k) principles of documenting difficulties identified in connection with verification of the identity of the beneficial owner and actions undertaken in connection with identifying as the beneficial owner a natural person occupying a senior managerial position.

2. Principles of identifying and assessing the risk of money laundering and terrorist financing related to given business relationships or an occasional transaction, including principles of verification and updating of the previously performed assessment of the risk of money laundering and terrorist financing.

1) Identification

Means collecting information about the client based on own sources, publicly available information and on the basis of information and documents provided by the client, as well as information received from law enforcement authorities, GIIF, UKNF, NBP. Information from other sources should also serve to verify information received from the client. The obligated institution documents the identified risk of money laundering and terrorist financing related to business relationships or an occasional transaction and its assessment, taking into account in particular factors concerning: the type of client; geographical area; purpose of the account; type of products, services and distribution channels; level of property values deposited by the client or the value of transactions carried out; purpose, regularity or duration of business relationships. The level of identified risk influences, among others, the intensity of application of financial security measures towards the client. The obligated institution identifies the risk at each stage of the business relationship. This means that in connection with receiving additional information about the client during the course of the business relationship, the obligated institution should perform a renewed identification and assessment of the risk related to the given client and undertake appropriate actions in order to adjust the possessed documents, information and knowledge about the client appropriately to the identified risk.

2) Risk assessment and risk documentation

Means assigning the client to an appropriate risk category (low, standard, high acceptable or high unacceptable) based on the methodology developed and applied in the organization. Before concluding an agreement with the client, the employee cooperating with or servicing the client performs the client's risk assessment by completing a risk assessment card, the template of which constitutes an annex to this procedure, and assigns the client to one of three groups of client risk related to the possibility of that client's participation in the process of money laundering or terrorist financing.

Documentation of the client's risk together with the assessment in the form of the so-called Client file (may be maintained in electronic form), which must include:

a) Type of client,
b) Geographical area,
c) Purpose of the account,
d) Type of products, services, provided services and their distribution channels,
e) Level of property values held by the client or value of transactions,
f) Purpose, regularity or duration of business relationships.

The obligated institution, during the course of the business relationship, documents every fact of receiving information about the client and assesses whether the given information affects the previously performed risk assessment related to the given client. If, in a given situation, a change in the assessment leads to an increase of the risk for the given client in relation to the previously identified one, then, in accordance with Art. 33 sec. 4 of the AML Act, the obligated institution is obliged to apply financial security measures to a new, broader extent resulting from the newly identified risk of money laundering and terrorist financing. The fact of receiving any information about the client is documented by the obligated institution, and the documents received concerning the client (after their analysis) are stored in the Client file.

3) Principles of verification of the risk assessment

For the purpose of determining the client's risk, in particular the following criteria should be taken into account:

a) Economic – assessment of the client in terms of the purpose of the activity conducted by him;
b) Geographical – analysis of the client's transactions, his business relationships with entities from third countries where there is an increased risk of money laundering and terrorist financing. In this place, the place of residence or conducting activity by the client should also be assessed;
c) Subject-related – what type of activity the client conducts, whether it is high-risk activity from the point of view of AML/CFT regulations?
d) Behavioral – atypical behavior of the client in a given situation.

In the risk analysis, the following are taken into account:

a) KNF communications 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) Updating of the previously performed risk assessment

Frequency of updating the client's risk assessment:

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

Identification, assessment and updating of risk are carried out on the basis of forms completed for each client, meeting the conditions for applying financial security measures towards him. Based on the established information, the client is assigned points, serving to assign the client to a specific risk group, including identification and assessment of the level of the identified risk. Documentation of these activities takes place by completing the Client risk assessment card. In the Card, through the creation of a scoring system, a weight has been assigned to individual criteria/risk assessment factors, influencing the final result of the analysis, as well as a list of warning signals, arousing vigilance, which translates into conduct towards the client or transaction in order to prevent incidents of money laundering or terrorist financing. Updating of the previously performed risk assessment may take place at each stage of cooperation with the client in connection with information received about the client that affects the previously identified level of risk related to the given client. In particular, updating of the previously performed risk assessment may take place in the event of receiving letters from public administration authorities (such as, for example, GIIF, KNF), banks, law enforcement authorities, border guard, etc.

3. Measures applied for the purpose of proper management of the identified risk of money laundering or terrorist financing related to given business relationships or an occasional transaction, including actions or activities

undertaken in order to limit the risk of money laundering and terrorist financing

Characteristics of factors related to the analysis of the client's risk (example listing):

a) Type of client:
– natural person,
– natural person conducting business activity,
– commercial law company,
– commercial law company admitted to trading on a regulated market,
– non-profit organization.

b) Type of activity:
– scrap trade,
– fuel industry,
– car dealerships,
– entities providing virtual currency exchange services,
– pawnshops,
– entities engaged in fuel trade,
– entities engaged in trade of heating materials,
– intermediaries in trade of luxury goods, e.g. works of art, antiques,
– casinos,
– companies providing financial services,
– intermediaries in real estate trade,
– arms dealers,
– night clubs,
– foreign entities with registered office in tax havens.

c) Client's domicile – verification of the country of residence or registered office in terms of:
– level of corruption (comparison with corruption maps),
– deviation of the country of registered office from the client's usual place of residence,
– registered office in a tax haven (countries applying harmful tax competition),
– origin from high-risk countries indicated by the European Commission (which is understood as countries listed in Directive (EU) 2015/849 of the European Parliament and of the Council or in another currently applicable legal act) or recognized as such by the obligated institution, whereby as of the date of introduction of the procedure it is understood at least as:

1. Afghanistan
2. Barbados
3. Burkina Faso
4. Cayman Islands
5. Democratic People's Republic of Korea
6. Democratic Republic of the Congo
7. Gibraltar

8. Haiti
9. Iran
10. Jamaica
11. Jordan
12. Mali
13. Mozambique
14. Myanmar (Burma)
15. Nigeria
16. Panama
17. Philippines
18. Senegal
19. Republic of South Africa
20. South Sudan
21. Syria
22. Tanzania
23. Trinidad and Tobago
24. Uganda
25. United Arab Emirates

d) Client's behavior – behavioral factor

When assessing the client's risk, employees and associates of the obligated institution take into account the client's behavior and assess it in terms of deviation from the norm. In such a situation, the employee of the obligated institution should include this factor in the risk assessment. A situation that should draw particular attention of the employee is the presence of an additional person during the performance of a transaction, especially when that person instructs the client on what to do.

e) Client's transactions (amount and geography)

Assessment of the client in terms of concluded agreements and transactions inconsistent with the profile of his activity – if his behavior cannot be rationally explained, this should be taken into account in the risk assessment.

f) Client's presence

Absence of the client when concluding the agreement as well as during the course of the relationship is considered a factor indicating high risk.

g) New products, channels, technologies

If the client intends to provide new services, offer new products or distribution channels or technologies, this may lead to an increase in AML/CFT risk. This risk will not always relate directly to the client, but it requires assessment from the perspective of the security of the obligated institution.

h) Client status

If the client has the status of a politically exposed person, a member of such person's family or is a person known as a close associate, or the person is included on a warning list or a sanctions list, then the risk related to servicing such a client is recognized at a high level.

Lower risk may be indicated by the fact that the client is:

a) an entity 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 disclosure requirements regarding the beneficial owner or a company with a majority shareholding of such a company,
d) a resident of a Member State of the European Union, a Member State of EFTA – a party to the EEA Agreement,
e) a resident of a third country identified by reliable sources as a country with a low level of corruption or other criminal activity,
f) a resident of a third country in which, according to data from reliable sources, regulations on counteracting money laundering and terrorist financing are in force that meet the requirements resulting from European Union regulations in the scope of counteracting money laundering and terrorist financing.

Lower risk may also be indicated by linking business relationships or an occasional transaction with:
a) a Member State of the European Union, a Member State of EFTA – a party to the EEA Agreement,
b) a third country identified by reliable sources as a country with a low level of corruption or other criminal activity,
c) a third country in which, according to data from reliable sources, regulations on counteracting money laundering and terrorist financing are in force that meet the requirements resulting from European Union regulations in the scope of counteracting money laundering and terrorist financing.

Higher risk may be indicated in particular by:
a) establishing business relationships in atypical circumstances;
b) unjustified reluctance to provide required information or documents by the Client;
c) the fact that the client is:

– a legal person or an organizational unit without legal personality whose activity serves to store personal assets,
– a company in which bearer shares have been issued, whose securities are not admitted to trading on an organized market, or a company in which rights from shares or interests are exercised by entities other than shareholders or partners,
– a resident of a country referred to in letter k) below,
d) the subject of the activity conducted by the client's business activity including carrying out a significant number or high-value cash transactions or transactions inconsistent with the profile declared by the client,
e) an unusual or excessively complex ownership structure of the client, taking into account the type and scope of the business activity conducted by him,
f) the client's use of services or products offered within private banking,
g) the client's use of services or products favoring anonymity or hindering his identification,
h) establishing or maintaining business relationships or carrying out an occasional transaction without the physical presence of the client – where the higher risk of money laundering or terrorist financing related thereto has not been otherwise mitigated or the client uses services or products favoring anonymity or hindering identification,
i) commissioning by unknown or unrelated third parties transactions whose beneficiary is the client,
j) covering business relationships or transactions involving new products or services or offering products or services using new distribution channels,
k) linking business relationships or an occasional transaction with:
– a high-risk third country,
– a country identified by reliable sources as a country with a high level of corruption or other type of criminal activity, a country financing or supporting the commission of terrorist acts, or in which the activity of terrorist organizations is connected,
– a country in respect of which the United Nations Organization or the European Union have adopted a decision to impose sanctions or specific restrictive measures,
l) other circumstances indicating that the Client's activity may be related to money laundering or terrorist financing,
j) the Client uses services of a virtual office,
k) the same person appears as a representative of various entities or as a person with whom details of transactions concerning different entities are agreed,
l) the Client has its registered office or place of conducting business activity at an address at which there are no indications of conducting business activity,
m) the Client does not have organizational and technical facilities appropriate to the type and scale of the conducted business activity.

An absolutely high AML/CFT risk occurs in particular when the client has PEP status.

Limiting the risk is served by completing the client risk assessment card, including the introduced scoring supporting the determination of the level of identified risk and, depending on the determined level of risk, applying additional financial security measures in order to obtain broader information about the client. Additionally, with the

intention of limiting risk, the obligated institution uses the documentation presented in the Model of General Principles functioning in its activity, completes the introduced solutions and applies the transaction monitoring procedure and reporting of suspicious transactions (STR).

Therefore, the obligated institution, in order to limit the risk of money laundering and terrorist financing and properly manage the identified risk, undertakes the following actions:

1) Identification of risk by collecting information about the client based on public sources as well as information provided by the client;
2) Risk assessment and its documentation by completing the client risk assessment card;
3) Analysis of information about the client from the perspective of possible factors increasing or decreasing the risk related to the client, including from the perspective of the type of conducted activity, the client's domicile, etc.
4) Application of appropriate financial security measures, taking into account the level of identified risk related to the client;
5) Ongoing analysis of business relationships with the client in order to determine whether the previously identified level of the client's risk has changed, and also to ensure that the knowledge of the obligated institution about the client's activity and about the client is up to date.

4. Principles of applying financial security measures

1) Financial security measures are applied in the case of:

a) establishing business relationships (having features of durability);

b) carrying out an occasional transaction:

– with an equivalent value of EUR 15,000 or more, regardless of whether the transaction is carried out as a single operation or as several operations that appear to be linked, or

– which constitutes a transfer of funds exceeding the equivalent of EUR 1,000;

c) suspicion of money laundering or terrorist financing;

d) doubts as to the truthfulness or completeness of the identification data of the client obtained so far.

The application of simplified financial security measures is allowed in cases where the risk assessment confirms a lower risk of money laundering or terrorist financing. Simplified financial security measures are not applied in cases referred to in Art. 35 sec. 1 points 5 and 6 of the Act (in a situation of suspicion of money laundering or terrorist financing or in case of doubts as to the truthfulness or completeness of the identification data of the client obtained so far).

Enhanced financial security measures are applied in the case of a higher risk of money laundering or terrorist financing, in particular in the case of clients coming from a high-risk third country or having their registered office there, as well as in cases referred to in Art. 44–46 of the Act, including with respect to persons with PEP status. Enhanced protective measures may consist in particular in verifying the client by more than one of the required documents.

The obligated institution also applies financial security measures in relation to clients with whom it maintains business relationships, taking into account the identified risk of money laundering and terrorist financing, in particular when:

a) there has been a change in the previously established nature or circumstances of the business relationship;

b) there has been a change in the previously established data concerning the client or the beneficial owner;

c) during a given calendar year the obligated institution was required under legal provisions to contact the client in order to verify information concerning beneficial owners, in particular where such an obligation resulted from the provisions of the Act of 9 March 2017 on exchange of tax information with other countries.

2) Method of applying 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 undertaking justified actions in order to:

– verify his identity,

– determine the ownership and control structure – in the case of a client being a legal person, an organizational unit without legal personality or a trust;

c) assessment of business relationships and, depending on the situation, obtaining information about their purpose and intended nature;

d) ongoing monitoring of the client's business relationships, including:

– analysis of transactions carried out within business relationships in order to ensure that these transactions are consistent with the knowledge of the obligated institution about the client, the type and scope of his conducted activity and are consistent with the risk of money laundering and terrorist financing related to this client,

– examination of the source of origin of property values at the disposal of the client – in cases justified by circumstances,

– ensuring that the documents, data or information concerning business relationships held are kept up to date.

The performance of the above financial security measures takes place in a manual manner. The practical method of applying financial security measures is established on the basis of AML/CFT documentation, applied in order to fulfill obligations under the Act, including implemented cards, forms and notes. By means of these documents, practical application of the above measures takes place in accordance with the rules set out in those documents. Each person acting on behalf of the obligated institution

in fulfilling obligations related to counteracting money laundering and terrorist financing should use the relevant forms when servicing clients.

The obligated institution, applying the financial security measures referred to in the above letters a and b, identifies the person authorized to act on behalf of the client and verifies his identity and authorization to act on behalf of the client, in the case when it is identified that the person acts on behalf of a third-party entity.

The obligated institution documents the applied financial security measures and the results of the ongoing analysis of transactions carried out. At the request of the authorities referred to in Art. 130 of the Act, the obligated institution demonstrates that, taking into account the level of identified risk of money laundering and terrorist financing related to given business relationships or an occasional transaction, it applied appropriate financial security measures.

Before establishing business relationships or carrying out an occasional transaction, the obligated institution informs the client about the processing of his personal data, in particular about the obligations of the obligated institution resulting from the Act in the scope of processing such data.

3) **Identification of the client consists in obtaining, in the case of:**
   a) a natural person:
   I. first name and surname,
   II. citizenship,
   III. number of the Universal Electronic System for Registration of the Population (PESEL) or date of birth – in the case when a PESEL number has not been assigned, and the country of birth,
   IV. series and number of the document confirming the identity of the person,
   V. residential address – in the case of possessing such information by the obligated institution,
   VI. name (company name), tax identification number (NIP) and address of the principal place of business activity – in the case of a natural person conducting business activity;
   b) a legal person or an organizational unit without legal personality:
   I. name (company name),
   II. organizational form,
   III. address of the registered office or address of conducting activity,
   IV. NIP, and in the absence of such number – country of registration, name of the relevant register and number and date of registration,
   V. identification data referred to in point 3 letter a subpoints I and III, of the person representing that legal person or organizational unit without legal personality.

Determination whether the client is a politically exposed person takes place through submission by him of a statement before using the service and ongoing verification of the information obtained for the purpose of identification and verification of the person. The client submits a statement that he is not a person holding such a position with the clause “I am aware of criminal liability for submitting a false statement”.

4) **Identification of the beneficial owner and the authorized person:**

Includes determination of his first name and surname, and in the case of possession of data by the obligated institution, also the data indicated in point 3 above letter a, subpoints II–V. For this purpose, the obligated institution uses a form concerning identification of the beneficial owner.

Identification of a person authorized to act on behalf of the client includes determining the data referred to in point 3 above, letter a, subpoints I–IV.

5) Verification:

Verification of the identity of the client, the person authorized to act on his behalf and the beneficial owner consists in confirming the determined identification data on the basis of:
a) an identity document of a natural person;
b) a driving license (as an auxiliary document);
c) a passport;
d) a document containing current data from an extract from the relevant register;
e) or on the basis of another document, data or information originating from a reliable and independent source, including, where available, electronic identification means or appropriate trust services specified in Regulation 910/2014.

In the case of identification of a beneficial owner who is a person referred to in Art. 2 sec. 2 point 1 letter a fifth indent of the Act (a beneficial owner being a natural person occupying a senior managerial position), the obligated institutions document:

a) all difficulties causing the impossibility of determining or doubts as to the identity of the natural persons specified in Art. 2 sec. 2 point 1 letter a first–fourth indents of the Act;

b) all difficulties related to justified actions undertaken for the purpose of verifying the identity of the beneficial owner.

The rules of conduct in the case of identification of a beneficial owner being a person referred to in Art. 2 sec. 2 point 1 letter a fifth indent of the AML Act (a beneficial owner being a natural person occupying a senior managerial position) are described in point 12 of this procedure.

Verification of the identity of the client and the beneficial owner takes place before establishing business relationships or carrying out an occasional transaction.

Verification of the identity of the client and the beneficial owner may be completed during the establishment of business relationships if it is necessary to ensure continuity of conducting business activity and where there is a low risk of money laundering and terrorist financing. In such cases, verification is carried out as soon as possible after the commencement of establishing business relationships.

In the case of establishing business relationships or carrying out an occasional transaction with a client being an entity referred to in Art. 58 of the Act (entities obliged to report information on beneficial owners and their updating, in particular: general partnerships; limited partnerships; limited joint-stock partnerships; limited liability companies; simple joint-stock companies; joint-stock companies, with the exception of public companies within the meaning of the Act of 29 July 2005 on public offering and conditions for introducing financial instruments to organized trading system and

on public companies; trusts whose trustees or persons holding equivalent positions: a) have a place of residence or registered office in the territory of the Republic of Poland or b) establish business relationships or acquire real estate in the territory of the Republic of Poland on behalf of or for the benefit of a trust; partnerships; European economic interest groupings; European companies; cooperatives; European cooperatives; associations subject to entry into the National Court Register; foundations), or entities subject to the obligation to register information on beneficial owners resulting from the regulations of a Member State issued on the basis of Art. 30 or Art. 31 of Directive 2015/849, the obligated institutions obtain confirmation of registration or an extract from the Central Register of Beneficial Owners or a register maintained in the relevant Member State. These entities, at the request of the obligated institution applying financial security measures towards them, provide information or documents enabling identification of the identity of their beneficial owners.

6) **Assessment of business relationships and their ongoing monitoring consists in undertaking actions leading to the assessment whether:**
   a) Carrying out transactions by a person/entity does not show features of durability (in particular repeatability and regularity);
   b) Transactions are consistent with the original declarations and the established client profile;
   c) Transactions carried out by the client do not violate regulations related to the Act on counteracting money laundering and terrorist financing;
   d) Funds used for transactions do not originate from undisclosed or illegal sources;
   e) Identification data and possessed verification documents are kept up to date;
   f) No other irregularities occur resulting in possible violation of applicable regulations.

An important role is played here by the declaration submitted by the client to the obligated institution, related to the purpose of establishing the business relationship, or carrying out a transaction, the presented model of the client's activity including the risks determined in relation to this activity, declarations submitted during the course of the business relationship and atypical behavior of the client deviating from the originally declared nature and purposes of establishing the business relationship or carrying out the transaction. The purpose of the declaration submitted by the client is thorough determination of the subject of the client's activity and the business relationships concluded in connection therewith. Application of this financial security measure is documented by the obligated institution by completing the form "Assessment of business relationship".

During the establishment of the relationship, as well as during the course of the relationship with the client, the obligated institution determines (updates) the client's profile, which consists in particular of the following elements:

- value of transferred funds (the obligated institution ensures that the value of actual transactions does not deviate from the client's declaration or documents submitted by him, and therefore obtains from the client a declaration regarding the value of transactions carried out, e.g. PLN 5,000–10,000),
- frequency of carrying out transactions (the obligated institution ensures that the frequency of actual transactions does not deviate from the client's

declaration or documents submitted by him, and therefore obtains from the client a declaration regarding the frequency of transactions performed, e.g. 3–4 transactions daily),
• type of transactions (the obligated institution ensures that transactions carried out by the client are consistent with the types of transactions indicated in the client's declaration, and therefore obtains from the client a declaration regarding the type of transactions),
• subject of transactions (the obligated institution ensures that transactions carried out by the client are consistent with the activity profile declared by him, and therefore the obligated institution obtains a declaration regarding the conducted activity),
• direction/country of transactions (the obligated institution ensures that the direction/country of transactions carried out through the account is consistent with the directions/countries of transactions indicated in the client's declaration, and therefore obtains from the client an appropriate declaration, e.g. that the client serves foreign entities and therefore often receives foreign transfers).

For the purpose of fulfilling the obligation referred to in Art. 43 sec. 3 of the Act, the obligated institution conducts ongoing analysis of transactions, which process in practical terms has been included in the procedure for monitoring transactions and reporting suspicious transactions (STR).

The results of the ongoing transaction analysis are documented by the obligated institution in the form of a note in table form, where individual transaction amounts and the date of the transaction are entered, signed by the person making the entry, analyzing whether these transactions significantly deviate from the knowledge of the obligated institution about the client, the type and scope of activity conducted by him, and whether the transactions are consistent with the risk of money laundering and terrorist financing related to this client.

In order to conduct the analysis, the obligated institution obtains information both from the client and about the client from other sources (public databases, open sources of information).

The assessment of the business relationship is updated on an ongoing basis, and in the event of revealing a deviation from the originally declared activity profile by the client, the obligated institution updates information about the client, documenting the application of financial security measures, including performing a renewed assessment of business relationships, as well as the information obtained about their purpose and intended nature.

In the case of identifying transactions:

1) complex, or
2) involving high amounts that are not justified by the circumstances of conducting the transaction, or
3) carried out in an unusual manner, or
4) appearing to lack legal or economic justification

– the obligated institution undertakes actions to clarify the circumstances under which these transactions were carried out, and in the case of transactions conducted within business relationships, intensifies the

application of the financial security measure referred to in Art. 34 sec. 1 point 4 of the Act (within the framework of ongoing monitoring of business relationships), with respect to the business relationships within which these transactions were carried out.

If the collected information does not allow establishing that the transactions correspond to the established client profile, the obligated institution should take steps aimed at limiting the risk. If the obligated institution is unable to determine justification for the transactions carried out by the client, in particular where these are complex transactions or involving high amounts, or carried out in an unusual manner, or appearing to lack legal or economic justification, this means the impossibility of applying financial security measures. It is therefore necessary to take actions indicated in Art. 41 of the AML Act (referred to in the next point 7). The obligated institution, if it obtains information that is insufficient to determine the nature of the transaction, should take steps related to the inability to apply financial security measures.

Client service may not be continued until explanations are obtained from the client demonstrating the economic justification of the client's transactions. The mere attempt to contact the client, e.g. by sending a letter, does not constitute application of financial security measures or determination of justification for the transactions carried out.

After reapplying financial security measures and updating documents, data and information about the client, as well as after the client provides all necessary explanations, the obligated institution may resume servicing the client. The obligated institution follows the principle according to which it should know and understand the economic justification of transactions carried out by the client.

In order to ensure that the possessed documents, data or information concerning business relationships are kept up to date, a person acting on behalf of the obligated institution completes the "Note on updating client data and information".

7) **What does the obligated institution do in the case of inability to apply one of the financial security measures?**
   a) does not establish business relationships;
   b) does not carry out an occasional transaction;
   c) does not carry out a transaction through a bank account;
   d) terminates business relationships.

The obligated institution assesses whether the inability to apply financial security measures constitutes grounds for submitting a notification to the General Inspector referred to in Art. 74 or Art. 86 of the Act.

8) **Business relationships or carrying out a transaction with a person holding a politically exposed position and application of enhanced financial security measures**

In order to determine whether the client or beneficial owner is a person holding a politically exposed position, the obligated institution obtains from the client a statement in written form or documentary form that he is or is not a person holding such a position.

In accordance with the applicable regulations, in the case where the risk analysis indicates that a business relationship will be established or a transaction will be carried out with a person holding a politically exposed position (as a client or beneficial owner) or a member of the family of such a person or a person known as 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 in order to determine the source of the client's assets and the source of origin of property values at the disposal of the client within business relationships or transactions;
2) intensifies the application of financial security measures;
3) intensifies the application of the financial security measure referred to in Art. 34 sec. 1 point 4 of the Act.

From the date of cessation of holding a politically exposed position until the determination that a higher risk is no longer associated with that person, however not shorter than 12 months, the obligated institution applies measures taking into account the risk in relation to such a person.

The above regulations apply accordingly to members of the family of a person holding a politically exposed position and to persons known as close associates of a person holding a politically exposed position.

The obligated institution determines whether the beneficial owner is a person holding a politically exposed position by obtaining a written statement using a form used for client identification.

The obligated institution applies enhanced financial security measures in cases of a higher risk of money laundering or terrorist financing, as well as in cases referred to in Art. 44–46 of the Act.

Application of enhanced financial security measures consists in:

a) obtaining additional information about:
– the client and the beneficial owner,
– the intended nature of business relationships;
b) obtaining information about the source of the client's assets and the beneficial owner and the source of origin of property values at the disposal of the client and the beneficial owner within business relationships or transactions;
c) obtaining information about the reasons and circumstances of intended or carried out transactions;
d) obtaining the approval of senior management for establishing or continuing business relationships;
e) intensifying the application of the financial security measure referred to in Art. 34 sec. 1 point 4 of the Act, by increasing the number and frequency of monitoring of business relationships and increasing the number of transactions selected for further analysis.

In the case of a transaction related to a high-risk third country identified by the European Commission, the obligated institution, in addition to applying financial

security measures referred to in Art. 44 sec. 1 of the Act, undertakes at least one of the following actions limiting the risk related to such transaction:

a) undertakes additional actions within the applied enhanced financial security measures;

b) introduces intensified obligations related to the transfer of information or reporting of transactions;

c) limits the scope of business relationships or transactions.

Enhanced financial security measures are applied in situations referred to in sec. 3 of this procedure in the case of identification of higher and absolutely high risk related to the client.

5. Principles of storing documentation and information

The obligated institution and its employees are obliged to document the applied financial security measures, for example by making copies of documents, screenshots together with the date or in any other manner. Documentation is stored for a period of 5 years, counted from the date of termination of business relationships with the client or from the date of carrying out an occasional transaction. Documents are stored in a manner ensuring their security and in accordance with regulations on personal data protection. These matters are regulated by separate internal procedures. The General Inspector of Financial Information may request storage of documentation for an additional period not longer than 5 years, counted from the date on which the 5-year period expires, if it is necessary to ensure the correctness of conducted proceedings in matters concerning counteracting money laundering or terrorist financing or for the purposes of criminal proceedings.

The obligated institution stores for a period of 5 years, counted from the date of termination of business relationships with the client or from the date of carrying out an occasional transaction:

a) copies of documents and information obtained as a result of applying financial security measures, including information obtained by means of electronic identification means and trust services enabling electronic identification;

b) evidence confirming transactions carried out and transaction records, including original documents or copies of documents necessary to identify the transaction.

The obligated institution stores the results of the ongoing analysis of transactions carried out for a period of 5 years, counted from the date of their performance.

In the case of liquidation, merger, division or transformation of the obligated institution, the provisions of Art. 76 sec. 1 of the Act of 29 September 1994 on accounting apply to the storage of documentation.

6. Principles of performing obligations including transferring to the General Inspector information on transactions and notifications and cooperation with the General Inspector of Financial Information

The purpose of the procedure is to define events and situations that cause the obligation of the obligated institution to report and notify GIIF. The reporting obligation of the obligated institution consists of:

a) reporting threshold transactions,
b) reporting to GIIF circumstances of suspicion,
c) notifying GIIF of suspicion of committing a crime,
d) providing information and performing actions at the request of GIIF.

In a situation of reasonable suspicion that a specific transaction or specific property values may be related to money laundering or terrorist financing or in a situation of suspicion of committing these crimes (or also other crimes), notification to GIIF is made, fulfilling the obligation under Art. 74, 86, 89 and 90 of the Act on counteracting money laundering and terrorist financing.

By way of example, notification to GIIF is submitted in the following cases:

- lack of economic justification for numerous transactions carried out by the client;
- lack of documents confirming the source of origin of property values at the disposal of the client;
- frequent and numerous transactions carried out by the client within one day;
- high transaction amounts;
- splitting transaction amounts within one day;
- the entity's address is the address of a so-called virtual office, where other business entities are also registered;
- connection with conducting unregistered business activity (without formal entry into the register).

Suspicion may also be raised by situations other than those listed above, in justified circumstances, e.g. similarity of IP addresses from which transactions are carried out, use of e-mail with the domain @protonmail.com, carrying out transactions with the same user logging in from different accounts.

Notifications are made electronically via the website https://www.giif.mofnet.gov.pl/#/glowna

The organization cooperates with public authorities also in the event of a request to provide information.

1) **Management Board:**
   a) receives notifications and assesses the validity of their further reporting to the supervisory authority,
   b) is responsible for training employees in the scope of informing and reporting necessary events,
   c) cooperates with authorities and provides them with necessary documents and information.
2) **Associates:**
   a) report events described in the procedure,

b) in the event of obtaining information about the person who made the notification – ensure that their data are not disclosed to other employees and that the reporting person does not suffer negative consequences related to the notification,
c) in the event of obtaining information about a person who has been reported as potentially or actually responsible for a violation of AML/CFT regulations – ensure confidentiality of this information.

3) **Situations in which the obligated institution provides information to GIIF:**
a) accepted deposit or made withdrawal of funds in an amount exceeding the equivalent of EUR 15,000,
b) transfer of funds exceeding the equivalent of EUR 15,000, with exceptions specified by law.

The organization is obliged to immediately notify GIIF in the event of a justified suspicion that a given transaction or property values may be related to money laundering or terrorist financing. An employee, associate, trainee and any other person who has a justified suspicion of the above shall provide the Management Board with information on this matter by e-mail or orally. The deadline for providing information is immediate. The Management Board makes a decision without undue delay on the further course of action regarding the notification. From the moment of confirmation of receipt of the notification, the obligated institution does not carry out the transaction.

4) **Notifications to the General Inspector of Financial Information and the obligation to provide or make available documents or information and to perform actions at the request of the General Inspector of Financial Information**

a) Notification to the General Inspector of circumstances that may indicate suspicion of committing the crime of money laundering or terrorist financing (Art. 74 of the Act)

The institution, in the case of grounds for notifying the General Inspector of circumstances that may indicate suspicion of committing the crime of money laundering or terrorist financing, submits a notification. The notification is submitted immediately, however not later than within 2 working days from the date of confirmation by the obligated institution of the suspicion referred to in the preceding sentence.

The notification shall include:

1) identification data referred to in Art. 36 sec. 1 of the Act of the client of the obligated institution;
2) available identification data referred to in Art. 36 sec. 1 of the Act, of natural persons, legal persons and organizational units without legal personality who are not clients of the obligated institution;
3) number of the account maintained for the client of the obligated institution, marked with the IBAN identifier or an identifier containing the country code and account number in the case of accounts not marked with IBAN;
4) type and amount of property values and the place of their storage;
5) available information referred to in Art. 72 sec. 6 of the Act, in relation to the transaction or attempts to carry it out;

6) indication of the European Economic Area country with which the transaction is connected, if it was carried out within cross-border activity.
7) available information on the identified risk of money laundering or terrorist financing and on the prohibited act from which the property values may originate;
8) justification for submitting the notification.

Notifications are made through the IT system of the General Inspector of Financial Information.

b) Transfer to the General Inspector of Financial Information of information on an accepted deposit or made withdrawal of funds in an amount exceeding the equivalent of EUR 15,000 and on a transfer of funds exceeding the equivalent of EUR 15,000 (Art. 72 of the Act).

The obligated institution transfers to the General Inspector information on an accepted deposit or made withdrawal of funds in an amount exceeding the equivalent of EUR 15,000 and on a transfer of funds exceeding the equivalent of EUR 15,000. The entity provides the information within 7 days from the date of acceptance of the deposit, making the withdrawal, executing the transfer of funds or making funds available to the payee.

The transferred information includes:

1) unique transaction identifier in the entity's register;
2) date or date and time of carrying out the transaction;
3) identification data referred to in Art. 36 sec. 1 of the Act, of the client issuing the instruction or order to carry out the transaction;
4) available identification data referred to in Art. 36 sec. 1 of the Act, of the other parties to the transaction;
5) amount and currency of the transaction;
6) type of transaction;
7) transaction title;
8) method of issuing the instruction or order to carry out the transaction;
9) account numbers used to carry out the transaction marked with the International Bank Account Number (IBAN) identifier or an identifier containing the country code and account number in the case of accounts not marked with IBAN.

Transfer of information takes place in accordance with the Regulation of the Minister of Finance on providing information on transactions and the form identifying the obligated institution of 4 October 2018 (Journal of Laws of 2018, item 1946) via the platform: https://www.giif.mofnet.gov.pl

c) Notification to GIIF in the event of a justified suspicion that a specific transaction or specific property values may be related to money laundering or terrorist financing (Art. 86 of the Act).

The obligated institution, in the event of circumstances giving rise to notification of the General Inspector, by means of electronic communication, in the case of justified suspicion that a specific transaction or specific property values may be related to money laundering or terrorist financing, immediately notifies the General Inspector. In

the notification, the entity provides the information in its possession related to the suspicion and information on the expected date of carrying out the transaction. The notification shall include:

1) identification data referred to in Art. 36 sec. 1 of the Act (sec. 4 point 3 of this procedure) of the client of the obligated institution;
2) available identification data referred to in Art. 36 sec. 1 of the Act (sec. 4 point 3 of this procedure), of natural persons, legal persons and organizational units without legal personality who are not clients of the obligated institution;
3) number of the account maintained for the client of the obligated institution, marked with the IBAN identifier or an identifier containing the country code and account number in the case of accounts not marked with IBAN;
4) type and amount of property values and the place of their storage;
5) available information referred to in Art. 72 sec. 6 of the Act (sec. 6 point 4 letter b of this procedure), in relation to the transaction or attempts to carry it out;
6) indication of the European Economic Area country with which the transaction is connected, if it was carried out within cross-border activity;
7) available information on the identified risk of money laundering or terrorist financing and on the prohibited act from which the property values may originate;
8) justification for submitting the notification.

If the General Inspector considers that the transaction referred to above may be related to money laundering or terrorist financing, he submits to the obligated institution a request to suspend the transaction or block the account for a period not longer than 96 hours, counted from the date and time indicated in the confirmation of receipt of the notification. Immediately after receiving this request, the obligated institution suspends the transaction or blocks the account. In the request, the General Inspector specifies the property values covered by the request. Until receipt of the request referred to in the preceding sentence or release from the obligation not to carry out the transaction, however not longer than 24 hours from the moment of confirmation of receipt of the notification, the obligated institution does not carry out the above-mentioned transaction to which the justified suspicion relates, or other transactions debiting the account on which the property values referred to above have been accumulated.

The General Inspector may release the obligated institution from the obligation to suspend the transaction if the available information does not provide grounds for notifying the prosecutor of suspicion of committing the crime of money laundering or terrorist financing or if he considers that suspension of the transaction or blocking of the account could hinder the performance of tasks by judicial authorities and services or institutions responsible for protection of public order, citizens' security or prosecution of perpetrators of crimes or fiscal crimes.

The request or release is transmitted by the General Inspector by means of electronic communication.

Immediately after transmitting the request to the obligated institution to suspend the transaction or block the account, the General Inspector notifies the competent

prosecutor of suspicion of committing the crime of money laundering or terrorist financing. After receiving this notification, the prosecutor may, by decision, suspend the transaction or block the account for a specified period, not longer than 6 months, counted from the date of receipt of the notification. The decision on suspension of the transaction or blocking of the account referred to above may also be issued despite the lack of notification made by the General Inspector. In the prosecutor's decision on suspension of the transaction or blocking of the account, the scope, method and period of suspension of the transaction or blocking of the account are specified. A complaint against the decision may be lodged with the court competent to examine the case. The prosecutor may extend the suspension of the transaction or blocking of the account for a further specified period, not longer than another 6 months. In this case, the scope, method and period of suspension of the transaction or blocking of the account are also specified, and a complaint against this decision may be lodged with the court competent to examine the case.

At the request of the client issuing the instruction or order to carry out the transaction to which the justified suspicion relates, or being the holder or owner of the property values to which such suspicion relates, the obligated institution may inform the client about the submission by the General Inspector of the request to suspend the transaction or block the account. In this case, the provision of Art. 54 of the Act (sec. 13 of this procedure) does not apply. Suspension of the transaction or blocking of the account ceases if, before the expiry of the period of their application, no decision on property security or decision regarding material evidence has been issued.

The obligated institution shall immediately notify the General Inspector, by means of electronic communication, of carrying out a transaction to which suspicion relates, in the event that submission of the notification was impossible prior to its execution. In the notification, the obligated institution justifies the reasons for the earlier failure to submit the notification and provides the remaining information in its possession confirming the suspicion referred to in sec. 1. The provision of Art. 74 sec. 3 of the Act (sec. 6 point 4 letter a of this procedure) shall apply accordingly.

Persons acting in the name and on behalf of the obligated institution, before making the notification, should familiarize themselves with the GIIF communication: https://www.gov.pl/web/finanse/komunikat-nr-22-w-sprawie-praktycznych-aspektow-stosowania-srodkow-bezpieczenstwa-finansowego-oraz-przekazywania-zawiadomien-o-ktorych-mowa-w-art-74-i-art-86-ustawy-aml2

d) Request to suspend a transaction or block an account by GIIF (Art. 87 of the Act)

If the General Inspector considers that a specific transaction or specific property values may be related to money laundering or terrorist financing, he transmits to the obligated institution, by means of electronic communication, a request to suspend the transaction or block the account. In the request for blocking the account, the General Inspector specifies the property values covered by the request.

The obligated institution suspends the transaction or blocks the account for a period not longer than 96 hours, counted from the moment of receipt of the request referred to above.

Immediately after transmitting the request to the obligated institution, the General Inspector notifies the competent prosecutor of suspicion of committing the crime of money laundering or terrorist financing.

After receiving this notification, the prosecutor may, by decision, suspend the transaction or block the account for a specified period, not longer than 6 months, counted from the date of receipt of the notification. The decision on suspension of the transaction or blocking of the account referred to above may also be issued despite the absence of a notification made by the General Inspector. In the prosecutor's decision on suspension of the transaction or blocking of the account, the scope, method and period of suspension of the transaction or blocking of the account are specified. A complaint against the decision may be lodged with the court competent to examine the case. The prosecutor may extend the suspension of the transaction or blocking of the account for a further specified period, not longer than another 6 months. In this case, the scope, method and period of suspension of the transaction or blocking of the account are also specified, and a complaint against this decision may be lodged with the court competent to examine the case.

At the request of the client issuing the instruction or order to carry out the transaction to which the justified suspicion relates, or being the holder or owner of the property values to which such suspicion relates, the obligated institution may inform that client about the submission by the General Inspector of the request to suspend the transaction or block the account. In this case, the provision of Art. 54 of the Act (sec. 13 of this procedure) does not apply. Suspension of the transaction or blocking of the account shall cease if, before the expiry of the period of their application, no decision on property security or decision regarding material evidence has been issued.

e) Notification of the prosecutor of suspicion that property values originate from a crime other than the crime of money laundering or terrorist financing (Art. 89 of the Act)

1) The obligated institution shall immediately notify the competent prosecutor in the event of a justified suspicion that the property values being the subject of the transaction or accumulated in the account originate from a crime other than the crime of money laundering or terrorist financing or a fiscal crime, or are related to a crime other than the crime of money laundering or terrorist financing or a fiscal crime. In the notification, the obligated institution provides the information in its possession related to the suspicion and information on the expected date of carrying out the transaction.
2) Until receipt of a decision on suspension of the transaction or blocking of the account, not longer than 96 hours from the moment of submission of the notification referred to in point 1, the obligated institution does not carry out the transaction referred to in sec. 1 or other transactions debiting the account on which the property values referred to in point 1 have been accumulated.
3) Immediately after receiving the decisions referred to in Art. 89 sec. 4 and 7 of the Act, the obligated institution transmits to the General Inspector, by means of electronic communication, information on the notifications referred to in point 1 and copies of those decisions.

4) The obligated institution shall immediately notify the competent prosecutor of carrying out the transaction referred to in point 1 in the event that submission of the notification about that transaction was impossible prior to its execution. In the notification, the obligated institution justifies the reasons for the earlier failure to submit the notification and provides the remaining information in its possession confirming the suspicion referred to in sec. 1. The provision of point 3 shall apply accordingly.
5) The obligated institution, when submitting the notification, uses the notification template referred to in sec. 1. The template may also be used in the situation referred to in point 4 to supplement the notification with the reasons for the earlier failure to submit it.

f) Obligation to provide or make available documents or information at the request of the General Inspector (Art. 76 of the Act)

1) At the request of GIIF, the obligated institution shall immediately provide or make available the information or documents in its possession necessary for the performance of GIIF's tasks specified in the Act, including concerning:
   a) clients;
   b) carried out transactions, within the scope of data specified in Art. 72 sec. 6 of the Act;
   c) the type and amount of property values and the place of their storage;
   d) application of the financial security measure referred to in Art. 34 sec. 1 point 4 of the Act;
   e) IP addresses from which connection to the IT system of the obligated institution was made and the times of connection to that system.
2) In the request referred to in point 1, GIIF may indicate:
   a) the deadline and form of providing or making available the information or documents;
   b) the scope of information and the deadline for obtaining it by the obligated institution in connection with application of the financial security measure referred to in Art. 34 sec. 1 point 4 of the Act or in connection with specific occasional transactions.
3) The information and documents referred to in point 1 are provided and made available free of charge.

7. Principles of disseminating among associates (employees) of the obligated institution knowledge of regulations on counteracting money laundering and terrorist financing

Senior management ensures access to knowledge of regulations on counteracting money laundering and terrorist financing among its associates, including employees. This consists in particular of:
a) providing current guidelines and other directions of activity;
b) providing written, electronic and oral information and explanations;
c) informing about changes in regulations;
d) ensuring at least at the initial stage access to training (possible in the form of an online film) on counteracting money laundering and terrorist financing.
The obligated institution ensures employees' participation in training programs concerning the implementation of AML/CFT obligations, including issues related to personal data protection. The training programs referred to above take into account

the nature, type and size of the activity conducted by the obligated institution and ensure up-to-date knowledge regarding the implementation of the institution's obligations, in particular the obligations referred to in Art. 74 sec. 1, Art. 86 sec. 1 and Art. 89 sec. 1 of the Act.
Completion of training by an employee is documented by issuance of a certificate by the entity organizing the training and by a declaration of completion of training signed by that employee. Each newly employed employee, before commencing performance of official duties, is obliged to familiarize himself with this procedure and complete dedicated training.

8. Principles of reporting by employees actual or potential violations of regulations on counteracting money laundering and terrorist financing

In the obligated institution, a procedure has been implemented which enables employees and other persons performing activities (hereinafter "other persons") on behalf of the obligated institution to report actual or potential violations of regulations on counteracting money laundering and terrorist financing. The procedure consists in making available to such persons an e-mail address to which reports may be submitted. Reports may also be made anonymously. In connection with the above:

a) Receipt of reports takes place by reading the e-mail message and undertaking appropriate actions in connection with this activity;
b) Data of the employee or other person are subject to special protection, therefore the content of the report is not disclosed to anyone outside the management board. The obligated institution is obliged to ensure such working conditions that the person making the report does not experience negative actions, including discriminatory or repressive actions, in connection with the report;
c) In the event of disclosure of the identity of the reporting persons or persons to whom the report relates, as well as the possibility of determining their identity, senior management determines the circle of persons who may have access to such information and instructs them on the obligation to maintain confidentiality and the consequences of failure to comply therewith;
d) After receiving the report, senior management verifies it and, in the event of recognizing its validity, undertakes appropriate actions, including in particular:
– suspension of the transaction,
– notification of suspicion of committing a crime,
– notification to GIIF.

In this respect, this procedure also refers to the implemented procedure of anonymous reporting of violations of regulations on counteracting money laundering and terrorist financing.

The obligated institution ensures employees and other persons performing activities related to the implementation by the obligated institution of obligations referred to in Art. 74, Art. 86, Art. 89 and Art. 90 of the Act protection against actions of a repressive nature or actions adversely affecting their legal or factual situation, or consisting in directing threats against them.

The obligated institution, its employees and other persons performing activities on behalf of the obligated institution do not undertake against employees and other persons referred to above actions of a repressive nature or adversely affecting their

legal or factual situation, or consisting in directing threats against them, in particular actions negatively affecting their working or employment conditions.

Employees and other persons performing activities on behalf of the obligated institution exposed to actions referred to above are entitled to report to the General Inspector cases of such actions. The provisions of Art. 80 sec. 1 and 2 of the Act shall apply accordingly.

9. Principles of internal control or supervision of compliance of the obligated institution's activity with regulations on counteracting money laundering and terrorist financing and with the rules of conduct specified in the internal procedure.

Senior management:

a) on an ongoing basis analyzes changes in regulations on counteracting money laundering and terrorist financing in order to ensure compliance with the procedure;

b) in the event of changes or identification of inconsistencies or lack of precision, undertakes actions resulting in correction of the procedure;

c) on an ongoing basis supervises the manner of using the procedure from a practical perspective, in order to ensure its maximum effectiveness.

For this purpose, the obligated institution may prepare a report on internal control and supervision in accordance with the requirements and development of the obligated institution. Also, not less frequently than every 2 years, the obligated institution prepares a risk assessment referred to in Art. 27 of the Act, with a detailed analysis of the entity's activity and application of regulations on counteracting money laundering and terrorist financing.

When performing the risk assessment related to the activity of the obligated institution, the following are taken into account in particular:

a) the national risk assessment prepared by GIIF, as well as the report of the European Commission;

b) the results of individual risk assessments related to particular clients.

2. The risk assessment of the obligated institution includes at least:

a) description of the methodology of assessing the risk of money laundering and terrorist financing;

b) description of the system used to control the identified risk of money laundering and terrorist financing;

c) assessment of the risk of the obligated institution;

d) implementation of organizational mitigants limiting the risk of money laundering and terrorist financing;

e) indication of the level of risk of money laundering and terrorist financing and conclusions resulting from the risk assessment.

10. Principles of recording discrepancies between information collected in the Central Register of Beneficial Owners and information on the client's beneficial owners determined in connection with application of the Act

The obligated institution, when applying a financial security measure in the scope of identification and verification of the beneficial owner (Art. 34 sec. 1 point 2 of the Act),

does not rely exclusively on information originating from the Central Register of Beneficial Owners or a register maintained in the relevant Member State.

In the case of risk analysis, as well as identification and verification of the client, in the event of identifying discrepancies between information collected in the Central Register of Beneficial Owners and information on the client's beneficial owners determined in connection with application of the Act, an annotation thereof is made in the Client Profile.

In the event of identifying discrepancies between information collected in the CRBR and the determined information on the beneficial owner originating from the client, there is an obligation to record such discrepancies and to undertake actions in order to clarify the reasons for the discrepancies. The obligated institution is obliged to contact the client, clarify the method of determining the beneficial owner by the client, clarify the method of determining the ownership and control structure by the client, clarify whether the method of determining the beneficial owner and the ownership and control structure by the obligated institution was correct, clarify the reason why the client recognized a given person as the beneficial owner, and collect new information and documents.

The process of recording discrepancies and making the notification referred to in Art. 61a sec. 1 of the Act is divided into stages during which the obligated institution should:

- **apply the financial security measure specified in Art. 34 sec. 1 point 2 letter a of the Ac**t, consisting in identifying the beneficial owner and undertaking justified actions in order to verify their identity;
- **apply the financial security measure specified in Art. 34 sec. 1 point 2 letter b of the Act**, consisting in identifying the beneficial owner and undertaking justified actions in order to determine the ownership and control structure – in the case of a client that is a legal person, an organizational unit without legal personality, or a trust;
- **determine and record discrepancies** between information collected in the CRBR and the established information on the client's beneficial owner;
- **undertake actions to clarify the reasons for discrepancies** (for example: contact the client, clarify the method of determining the beneficial owner by the client, clarify the method of determining the ownership and control structure by the client, clarify whether the method of determining the beneficial owner and the ownership and control structure by the obligated institution was correct, clarify why the client recognized a given person as the beneficial owner, collect new information and documents);
- **confirm the recorded discrepancies** (for example: confirm that the obligated institution did not make an error when determining the beneficial owner and the ownership and control structure of the client; where possible, confirm that the information on beneficial owners in the CRBR is incorrect; confirm the reasons for the discrepancy; determine whether the discrepancy is apparent or factual);
- **prepare a justification of the discrepancy** (for example: indicate and document what actions the obligated institution undertook to identify and verify the beneficial owner and the ownership and control structure of the client; what information and documents formed the basis for determining the client's beneficial owner and ownership and control structure; what information or documents formed the basis for identifying the discrepancy; what actions the

obligated institution undertook to confirm the recorded discrepancies; what information the institution obtained during the confirmation process; what conclusions result from the analysis of the collected information and documents; on what grounds the obligated institution concluded that the discrepancy is factual);

• **provide the competent authority with verified information about the discrepancies together with justification and documentation** regarding the recorded discrepancies – the institution submits the justification prepared in accordance with the above instructions and sends complete documentation related to determining the beneficial owner and confirming the recorded discrepancies.

If the recorded discrepancies are confirmed, there is an obligation to provide the authority competent in matters of the Register with verified information on these discrepancies together with justification and documentation regarding the recorded discrepancies. The notification is made electronically via the website https://crbr.podatki.gov.pl/adcrbr/#/ in the "Report discrepancy" tab.

One type of **discrepancy is the lack of reporting information on beneficial owners to the CRBR**. The absence of reporting information to the CRBR should be interpreted as a declaration by the client that a given natural person is not the beneficial owner of the entity obliged to report information to the CRBR.

Verification of the beneficial owner may take place not only on the basis of a document from the register, but also on the basis of, for example, the company agreement or an agreement transferring ownership of company shares.

The obligated institution makes every effort not to provide the competent authority with:

• information on possible minor typographical errors in the CRBR (for example, an obvious spelling mistake in the beneficial owner's name);

• information on possible minor inaccuracies in the excerpt from the client's National Court Register (for example, an insignificant error in the value of the client's shares);

• information on the lack of reporting to the CRBR by entities not obliged to make such a report (for example, an ordinary association);

• information on inaccuracies that do not affect the determination of the beneficial owner (for example, failure to enter the beneficial owner's middle name).

The obligated institution, when fulfilling its reporting obligation, assumes that clients approach the issue of determining the beneficial owner in a reliable manner and does not assume in advance that clients have made errors when reporting information on beneficial owners to the CRBR. Therefore, any ambiguities will be resolved by the obligated institution through the application of financial security measures.

For the purpose of fulfilling the obligation referred to in Art. 61a of the Act, the obligated institution completes the form "Note regarding identification of discrepancies referred to in Art. 61a of the AML Act." The note is also completed when no discrepancies are identified; in such a case, the note documents the analysis performed and the fulfillment of the institution's obligations under Art. 61a of the Act.

11. Rules for documenting difficulties identified in connection with the verification of the identity of the beneficial owner and actions undertaken in connection with identification as the beneficial owner of a natural person holding a senior management position.

In the event of difficulties related to the verification of the identity of the beneficial owner and actions undertaken in connection with identification as the beneficial owner of a natural person holding a senior management position, a record of this fact is made in the Client Profile. This is an exceptional situation, since as a rule the beneficial owner is determined in accordance with the earlier provisions of this procedure.

The obligated institution applies the above method of determining the beneficial owner in situations:

1) where 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 that there are doubts as to the identity of the natural persons specified in Art. 2 sec. 2 point 1 letter a indents one to four of the AML Act;
2) where entities located in countries that do not publicly provide detailed information – for example on beneficial owners – appear in the ownership structure.

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

1) Actions undertaken to determine the identity of the natural persons specified in Art. 2 sec. 2 point 1 letter a indents one to four of the AML Act (for example, obtaining an excerpt from the client's National Court Register, the client's articles of association, agreements transferring ownership of the client's shares, preparing a note from a telephone conversation with the client's representative);
2) Circumstances recognized by the obligated institution as causing the inability to determine, or doubts as to the identity of, the natural persons specified in Art. 2 sec. 2 point 1 letter a indents one to four of the AML Act (for example, determining that each shareholder of the client – a natural person – holds 20% of shares);
3) Difficulties related to justified actions undertaken in order to verify the identity of the beneficial owner, i.e. a natural person holding a senior management position (for example, failure to report information on the beneficial owner to the Central Register of Beneficial Owners; difficulties related to the lack of the beneficial owner's physical presence; difficulties related to video verification).

In order to fulfill the above obligation, the obligated institution has introduced a form used to comply with this obligation. It contains, among other things, a field to be completed in connection with the identification of difficulties in verifying the identity of the beneficial owner.

12. Obligation of confidentiality

The entity is obliged to keep confidential the fact of providing the General Inspector or other competent authorities with information specified in Chapters 7 and 8, as well as information about the planned initiation and the conduct of analyses concerning money laundering or terrorist financing. All documents and information related to the performance of obligations under the Act are confidential and must be stored in a secure manner ensuring data confidentiality and accessible only to authorized persons. An employee is also obliged to maintain confidentiality of all information regarding concluded transactions.

Information about forming a suspicion that specific assets may originate from criminal activity or be connected with terrorist financing is shared between entities within the same group. The General Inspector may require an obligated institution that is part of a group to keep confidential the fact that such suspicion has been formed.

13. Sanctions Policy

In order not to execute transactions or enter into business relationships with persons included on sanctions lists, and to fulfill the obligations under Articles 117–119 of the Act, the obligated institution verifies client data in sources available at the following 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 a client against sanctions lists is performed by one or several of the following methods:

1) marking in the electronic system of the obligated institution;
2) confirmation on the risk assessment card;
3) a note (which may be individual or collective).

The obligated institution may retain a screenshot; however, this is not required for verification purposes. The obligated institution may document fulfillment of this obligation by means of a note.

Verification of the client against sanctions lists is carried out at the moment of establishing a business relationship or performing a transaction in relation to which financial security measures are applied. Updating client information in this respect is performed when other client information related to the nature and purpose of the business relationship is updated.

If a client is identified on the above-mentioned lists (with regard to special restrictive measures), the following measures are applied:

a) freezing of assets owned, held, or controlled directly or indirectly by persons and entities, as well as proceeds derived from such assets, which is understood as preventing their transfer, alteration, use, as well as conducting any operation involving such assets in any manner that could result in a change in their

quantity, value, location, ownership, possession, nature, purpose, or any other change that could enable benefits to be obtained from them;

b) making assets unavailable, directly or indirectly, to persons and entities or for their benefit, which in particular includes not granting loans, consumer credit or mortgage loans, not making donations, and not making payments for goods or services.

At the same time, the obligated institution may use a broader catalogue of sanctions lists, especially in the case of applying enhanced financial security measures or any other need to determine such necessity, applying them according to the circumstances or the established/identified risk. The full catalogue of sanctions lists (including the above) includes:

1) Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (OJ EU L 229, 31.7.2014, as amended);
2) Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (OJ EU L 78, 17.3.2014, 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 the involvement of Belarus in Russia's aggression against Ukraine (OJ EU L 134, 20.5.2006, 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 restrictive measures list - 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) Sankcije World Bank - https://www.sanctions-intelligence.com/global-lists/
16) EU Country Sanctions - https://www.sanctionsmap.eu/#/main

The obligated institution may select additional lists on an ongoing basis, even if they are not included in the procedure (sanctions policy), based on the existing risk and information obtained. Sanctions lists are updated by the Company by re-screening Clients with whom business relationships have been established (during their duration).

In the event that a Client appears on any of the above lists, the Company:

1) does not establish business relationships and does not carry out Transactions;
2) if the Company is in the course of a Transaction, it applies a hold on funds;
3) applies the restrictive measures specified in the Act;
4) if the Company maintains an existing relationship, it terminates such business relationship.