INTERNAL ANTI-MONEY LAUNDERING
AND ANTI-TERRORIST FINANCING PROCEDURE
by
A&D Best Trade s.r.o., address Na Folimance 2155/15, Vinohrady (Praha 2), 120 00 Praha, company file number 19929943

Effective Date: 14.03.2024

1. Activities and actions to reduce the risk of money laundering, terrorist financing and to properly manage the identified risks of money laundering or terrorist financing:
   The purpose of the procedure is to introduce in the obliged institution financial security measures and other obligations stipulated by the regulations, in accordance with the Law on Anti-Money Laundering and Financing of Terrorism. The procedure contains a set of internal regulations, which are undertaken in the obliged institution in cooperation with dedicated state and international authorities to combat and prevent the above crimes. Since the aim of the obliged institution is to operate transparently, in accordance with the law and the principles of social coexistence, this procedure is intended to prevent the use of its services in an unlawful manner. The procedure therefore applies to employees, co-workers as well as contract, temporary or agency workers, interns, volunteers, and trainees (hereinafter all collectively "co-workers"). The primary activities and actions to meet the statutory obligations are the application of financial security measures and ongoing risk analysis to prevent money laundering or terrorist financing.

   Company provide P2P services in the virtual assets field, such as exchange virtual assets to fiat and vice versa.

   Company does not provide services of exchange of fiduciary currency into another fiduciary currency and payment services in accordance with the Payment Services Act (the entity, in particular, does not accept deposits and does not transfer funds)

   1) Definitions
   AML (anti-money laundering) - anti-money laundering - a set of activities, procedures, and regulations designed to prevent criminal activities related to money laundering.

   Ultimate Beneficial Owner - a natural person or natural persons exercising direct or indirect control over the client through their powers that result from legal or factual circumstances, enabling them to exert a decisive influence on the activities or actions undertaken by the client or natural person, or natural persons, on behalf of whose business relations are established or an occasional transaction is carried out;

   Close associate of PEP - a natural person who is the beneficial owner of a legal person, an organizational unit without legal personality or a trust jointly with PEP or having other close relationships with it related to the conducted business activity, as well as a natural person who is the sole beneficial owner of legal persons, organizational units without legal personality or a trust, known to have been created for the purpose of obtaining an actual benefit by the PEP;

   Account blockade - temporarily prevention of the use and disposition of all or part of the assets accumulated in an account (where the obligated institution provides account maintenance services).

PEP family member - spouse or cohabiting person, child of PEP or his spouse or cohabiting person, parents.

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

Financing of terrorism - a crime against public safety consisting in collecting, transferring, or offering property values in order to finance a terrorist crime or making property values available to a person, an organized group aimed at committing such an offense (in detail the act specified in Article 165a of the Act of 6 June 1997 Criminal Code).

FAU - Financial Analytical Unit, a government administration body responsible for counteracting money laundering and terrorist financing.

Obliged institution - entrepreneurs, companies and institutions that are obliged to analyze transactions and provide the FAU with information on suspicious transactions.

Senior Management - A board member, director, or employee of an obligated institution with AML/CFT expertise related to the organization's operations and decision-making impacting risk and as such, responsible for carrying out statutory obligations.

Customer - natural person, legal person, or organizational unit without legal personality, to whom organization provides services or for whom it performs activities falling within the scope of its professional activity (including with whom organization establishes economic relations or on whose behalf it carries out occasional transaction).

Politically Exposed Person (hereinafter PEP) - an individual who holds a significant position or public office.

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

Money laundering - an activity aimed at introducing to the legal turnover of money originating from illegal sources or used for financing illegal activity (in detail, Act No. 253/2008 Coll., on certain measures against money laundering and financing of terrorism and Decree No. 281/2008 Coll., on certain requirements for the system of internal policies, procedures and control measures against money laundering and terrorist financing).

Information processing - any operation performed on information, in particular its acquisition, collection, consolidation, storage, editing, sharing and deletion (the term also includes information stored in an IT system).

Economic relations - the relationship of the organization with the customer related to the professional activities of the company, which at the time of its establishment show the characteristic of permanence.

Transaction - a legal or factual act by which ownership or possession of property values is transferred, or a legal or factual act performed for the purpose of transferring ownership or possession of property values.

Occasional transaction - a transaction conducted not in the context of a business relationship.

Act - the Act of March 1, 2018, on counteracting money laundering and financing of terrorism.

Property values - property rights or other movable property, real estate, means of payment, financial instruments, other securities, foreign exchange, virtual currencies (including cryptocurrencies).

Suspension of transactions - a temporary restriction on the use and disposition of property by preventing a single transaction or more transactions from taking place.

Board of directors - the person authorized to represent the obligated institution, including when the board of directors is not formally appointed or does not exist for reasons of organizational form

2) Responsibilities of senior management

a) Establishes the scope of competences for those responsible for implementing and maintaining an effective anti-money laundering and counter-terrorist financing system, and fulfills the statutory obligations listed in the AML/CFT Act.
b) Establishes a budget to support and develop an internal AML/CFT system.
c) Approves the training plan and expenditures for training and competency enhancement.
d) Is responsible for building awareness among employees and associates in the field of anti-money laundering and counter-terrorist financing and for adhering to the procedures and policies implemented in the organization in this regard.
e) Frequency of employee training in order to comply with the current legislation must be no less that once in 6 months.

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

In the absence of a written designation and the acceptance of these duties by another person, they shall be all members of the board of directors of the obligated institution (senior management). This provision shall be treated as the designation of the responsible person in accordance with the statutory regulation. The primary person performing these duties is the CEO or the owner of the obligated institution if the CEO has not been singled out. The responsibilities include implementing statutory regulations, ensuring compliance of the activities of the obligated institution and its employees and other persons performing activities for the entity, and providing notifications of statutory requirements.

4) Associates of the obligated institution:

a) comply with the AML/CFT policies and procedures implemented in the organization.

b) take an active part in the risk assessment of the client, apply financial security measures to the client.
c) ensure that operations conducted by the company are following the law and meet AML/CFT security standards.
d) inform the person responsible for the compliance of the obliged institution with the AML/CFT regulations and make available all available data on circumstances of transactions indicating the connection with money laundering or terrorist financing - regardless of the size of transaction.
e) participate in anti-money laundering and counter-terrorist financing training.

Accordingly, at the commencement of work/cooperation with the obliged institution, these persons and persons performing duties related to AML/CFT and familiarize themselves with this procedure and receive training in the subject of anti-money laundering and terrorist financing (possible in the form of an on-line video). Confirmation of these activities is the submission of a statement, possibly in accordance with Attachment 2.

2. Principles of identifying and assessing the risk of money laundering and terrorist financing associated with a given business relationship or occasional transaction, including the principles of verification, and updating of previously made money laundering and terrorist financing risk assessment.

1) Recognition

Means gathering information about the customer based on own sources, publicly available information and based on information and documents provided by the customer.

2) Risk assessment and risk documentation
Means classifying the customer to the appropriate risk category (low, standard, high) on the basis of methodology developed and applied in the organization.

Documenting the client's risk along with the assessment in the form of a so-called Client File (may be maintained in electronic form), which must include:
a) Type of customer,
b) Geographical area,
c) Type of products, services, services provided and their distribution channels,
d) The level of assets held by the client or the value of the transaction, if the client qualifies as a higher risk client,
e) Purpose, regularity, or duration of the business relationship.

3) Principles of verification of risk assessment

In order to determine the customer's risk, the following criteria should be considered in particular:
a) Economic - assessment of the customer in terms of the purpose of his business,
b) Geographical - analysis of the customer's transactions, its business relations with entities from third countries, where there is an increased risk of money laundering and terrorist financing. The customer's place of residence or business should also be assessed here.

c) Substantive - what type of activity does the client conduct, is it a higher or high-risk activity from the point of view of AML/CFT regulations?
d) Behavioral - unusual behavior of the customer in a given situation.

The risk analysis considers:
a) Communications and training with the AML officer,
b) Annual reports of FAU,
c) National Risk Assessment,
d) European Commission report,
e) Corporate memory and experience of the obliged institution,
f) Media reports.

4) Client's periodic review
Frequency of updating the customer risk assessment:
a) In the case of a low-risk customer - **5 years periodic review**
b) In case of a customer with medium level of risk - **3 years periodic review**
c) In case of a customer with a high-risk level - **1 year periodic review**
d) And also, each time if the obliged institution becomes aware of a change in significant issues that may affect the customer's risk level.

5) Regular screening

AML officer is checking our users activity on the monthly basis, including transaction monitoring, and if there is any suspicious activity the AML officer may conduct name screening in order to check legitimacy of our users. The actual name screening may appear no more than twice a year.

6) Transactions monitoring
All transactions are carefully monitored by our AML officer manually. We plan to implement integration with KYCaid transaction monitoring AML tools and we notify our users and partners when this will occur. Until then, the transactions are monitored by our AML officer manually.. The threshold which user have to exceed to apply additional screening is EUR 10,000 in either single transaction or several during the month. AML officer is conducting the monitoring of transactions on the daily basis to verify users and then to monitor the transactions of such users. In case if there is a suspicious transaction in place (over EUR 10,000 or a lot of small transactions during short period) we conducting an additional check and in case if we cannot verify the source of funds or such user our AML officer have to inform Financial analytical Unit (FAU) regarding such transaction.

We are considering KYCaid LLC as our transaction monitoring provider is. It is the outsourced service provider with whom we have signed agreement.

The rules of the transaction monitoring (TM) are simple. Our dedicated AML officer is monitoring transactions through the KYCaid or other third-party tools implemented into our website. In case if the EUR 10,000 threshold is exceeded either in single or in several transactions from one user, the AML officer is sending the additional verification link to such user. Through this link such a user has to answer to additional questions and provide with additional documents (source of funds, residency, agreements etc.)

The transactions will be monitored through the KYCaid or other third-party AML/KYC provider we may choose by our in-hose certified AML officer. Our AML officer is trained and certified and go through additional trainings every 6 months. In case of unusual/suspicious activity the AML officer have to contact user, which conducted such unusual activity. In case if such user fails to provide additional information, our AML officer have to report to Czech Republic Financial Analytical Unit (FAU). As we just started we have only one dedicated AML officer monitoring the transactions.

We do not use any on-chain analysis tool to help detect illicit activity on the blockchain.

We may implement a platform which is an automated transaction monitoring system into our website. Additional transaction monitoring policies will be implemented together with such a platform solution.

3. Measures applied to properly manage the identified risk of money laundering or terrorist financing related to the given economic relations or occasional transaction

Characteristics of factors associated with the customer risk analysis (sample listing):

a) Type of customer:
   - a natural person,
   - a natural person conducting a business activity,
   - commercial law company,
   - a commercial law company admitted to trading on a regulated market,
   - non-profit organization.
b) Business object - industry:
   - scrap metal trading,
   - fuel industry,
   - services (e.g., car washes, laundries, restaurants),
   - construction industry
c) Client domicile - verification of the country of residence of the head office with respect to:
   - degree of corruption (clash with corruption maps),
   - deviation of the place of residence or domicile from the usual customer,
   - residence in tax haven (countries applying harmful tax competition)
   - origin from high-risk countries designated by the European Commission (by which is meant the countries listed in the Directive of the European Parliament and of the Council (EU) 2015/849 or any other legal act currently in force) or recognized as such by the obliged institution, whereby as of the date of introduction of the procedure is meant at least:

1	Afganistan
2	Bahamas
3	Barbados

4	Botswana
5	Kambodża
6	Ghana
7	Iran
8	Irak
9	Jamajka
10	Democratic People's Republic of Korea
11	Mauritius
12	Morocco
13	Mjanma/Birma
14	Nikaragua
15	Pakistan
16	Panama
17	Russia
18	Syria
19	Trinidad i Tobago
20	Uganda
21	Vanuatu
22	Jemen
23	Zimbabwe
24	Belarus
25	Sudan
26	Cuba
27	Haiti
28	Gwatemala
29	Argentina
30	Belize
31	Crimea, Donetsk and Luhansk (Ukrainian regions)

d) Customer behavior - behavioral factor
In the case of customer risk assessment, the obliged institution's co-workers take into account the customer's behavior and assess it in terms of abnormal behavior. In such a situation, the obliged institution's employee should take this factor into account in the risk assessment. A situation that should draw

the associate's special attention is the presence of an additional person at the transaction, especially when instructing the client on what to do.

e) Client transactions (size and geography)
Assess the client for agreements and transactions that are inconsistent with the client's business profile - if the client's behavior cannot be reasonably explained this should be included in the risk assessment.

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

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

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

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

a) Public sector entity,
b) State-owned enterprise or a company with a majority stake held by the State Treasury, local government units or their associations,
c) A company whose securities are admitted to trading on a regulated market subject to beneficial ownership disclosure requirements, or a company with a majority stake in 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 that is determined by reliable sources to be a country with a low level of corruption or other criminal activity,
f) Resident of a third country where according to reliable sources AML/CFT regulations are in force.

A lower risk may also be evidenced by having a business relationship or occasional transaction with:

a) A Member State of the European Union, an EFTA Member State party to the EEA Agreement,
b) A third country described by reliable sources as a country with a low level of corruption or other criminal activity,
c) A third country, where according to reliable sources AML/CFT regulations are in force.

Increased risk may be indicated in particular by:

a) the establishment of business relationships in unusual circumstances.
b) that the client is:
- a legal person or an unincorporated organizational unit whose business is used to hold personal assets,
- a company in which bearer shares have been issued whose securities are not admitted to organized trading, or a company in which the rights from shares are exercised by entities other than shareholders or members,

c) the subject of the client's business activity involving a significant number or high value of cash transactions,
d) unusual or excessively complex ownership structure of the client, considering the type and scope of its business activity,
e) the customer's use of private banking services or products,
f) use by the customer of services or products that promote anonymity or make it difficult to identify the customer,
g) establishing or maintaining a business relationship or conducting an occasional transaction without the physical presence of the customer - where the associated higher risk of money laundering or terrorist financing has not been mitigated otherwise, including by the use of electronic identification means,
h) ordering by unknown or unrelated third parties of transactions benefiting the customer.
i) to extend the business relationship or transactions to new products or services or to offer products or services through new distribution channels,
j) linking the business relationship or occasional transaction to:
- a high-risk third country,
- a business relationship or occasional transaction with a high-risk third country, a country that is identified by reliable sources as a country with a high level of corruption or other criminal activity, a country that finances or supports the commission of terrorist acts, or with which the activity of a terrorist organization is associated
- a state with respect to which the United Nations or the European Union has decided to impose sanctions or specific restrictive measures.

Absolutely high AML/CFT risk occurs in particular when:
a) The Client is from or based in a high-risk third country,
b) The Client has a PEP status,
c) Relationships are concluded under correspondent banking,
d) The transaction has the status of an unusual transaction.

4. Principles of applying financial security measures

1) Financial security measures shall be applied when:
a) The establishment of a business relationship (showing the characteristic of permanence).
b) conducting an occasional transaction:
- of the equivalent of 15,000 euros or more, regardless of whether the transaction is conducted as a single operation or several operations that appear to be linked, or
- which represents a transfer of funds for an amount exceeding the equivalent of 1,000 euros.
- with the use of virtual currency of the equivalent of 1,000 euros or more - in the case of mandatory institutions referred to in Article 2, paragraph 1, point 12;
c) conducting an occasional cash transaction of the equivalent of EUR 10,000 or more, regardless of whether the transaction is conducted as a single operation or as several operations that appear to be linked - in the case of obliged institutions referred to in Article 2, paragraph 1, point 23.

d) placing bets and collecting winnings of the equivalent of EUR 2,000 or more, regardless of whether the transaction is conducted as a single operation or as several operations that appear to be linked - in the case of obliged institutions referred to in Article 2, paragraph 1, point 20.
e) suspicion of money laundering or terrorist financing.
f) doubts as to the accuracy or completeness of customer identification data obtained to date.

Simplified financial security measures may be applied where a risk assessment confirms a lower risk of money laundering or terrorist financing.

Enhanced security measures shall apply where there is a higher risk of money laundering or terrorist financing, and in particular, in the case of customers from or established in a high-risk third country. Enhanced security measures may consist, in particular, in verifying the customer with more than one of the required documents.

2) The manner of applying financial security measures

Financial security measures include:
a) Identification of the customer and verification of his identity, including in particular whether he is a politically exposed person.
b) Identification of the beneficial owner and verification of the beneficial owner.
c) Assessment of business relationships and their ongoing monitoring.

3) Customer identification consists of obtaining, in the case of:

a) an individual:
   i. first and last name,
   ii. citizenship,
   iii. ID number or date of birth - in case the ID number has not been assigned and country of birth,
   series and number of the document confirming identity of the person,
   iv. the address of residence - if the obliged institution has this information,
   v. name (company), tax identification number and address of the main place of business activity - in case of a natural person conducting business activity.
b) a legal person or an organizational unit without legal personality:
   i. name (business name),
   ii. organizational form,
   iii. registered office or business address,
   iv. Tax identification number, and if there is no such number - the country of registration, the name of the relevant register and the number and date of registration,
   v. identification data referred to in item 1 letters a and c of the person representing that legal person or organizational unit without legal personality.

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

Identification of the person authorized to act on behalf of the customer is based on the determination of the data in point 3 above letter a, designation ii-iv.

4) Identification of the beneficial owner:

   Includes establishing his/her name and, where possible, the data indicated in point 3 above designation ii-vi.

5) Verification of individuals:
   Verification shall consist of confirming the established identification of the persons in point 3 above, based on:
   a) identity document.
   b) driver's license.
   c) passport.
   d) bank account statement.
   e) bank transfer confirmation.
   f) or on the basis of any other document, data or information coming from a reliable and independent source.
6) Verification of corporates:
   Verification shall consist of confirming the established identification of the legal entity in point 3 above, based on:
   a) legal representative information
   b) UBO's passports/ID's
   c) certificate of incorporation
   d) articles of association with disclosure of any affiliates (if any)
   e) confirmation of the address
   f) UBO declaration
   g) confirmation of source of funds
   h) bank account statement
   i) bank transfer confirmation

   The documents listed above must be submitted all together as a package.

   j) The assessment of economic relations and their ongoing monitoring consists in taking actions leading to the assessment whether:

   a) The making of transactions by a person/entity does not show the characteristics of permanence (especially repetition and regularity).
   b) Transactions made by the customer do not violate regulations related to the Money Laundering and Terrorist Financing Act.
   c) The funds used for the transaction do not come from undisclosed or illegal sources.
   d) Identification data and verification documents held are updated on an ongoing basis.
   e) There are no other irregularities resulting in possible violations of applicable laws.

   k) When one of the financial security measures cannot be applied, what does the obliged institution do?

   a) Does not establish business relations.

b) Does not conduct an occasional transaction.
c) does not conduct a transaction through a bank account.
d) terminates the business relationship.

l) Business relations with a politically exposed person

In accordance with the applicable regulations, if a risk analysis is carried out showing that a transaction is to be carried out with a politically exposed person (as customer or beneficial owner), the obliged institution MAY carry out such a transaction. However, in such a case, the person conducting the transaction shall obtain senior management approval for such action, and the obligated institution shall:

1) apply appropriate measures to determine the source of the customer's property and the source of the property values at the customer's disposal under the business relationship or transaction.
2) intensify the application of financial security measures.

For these purposes, the obliged institution may use Attachment No. 1.

m) The effect of the existence of the Client on the sanction lists

The obliged institution also applies financial security measures in the following areas Establishing business relations and conducting transactions with Customers on sanction lists, including in particular:

a) Those designated by the Financial Analytical Unit (FAU) of Czech Republic (Supervisory Authority in the Czech Republic) (https://www.financnianalytickyurad.cz/en),
b) The list included in OFAC (https://sanctionssearch.ofac.treas.gov/),
c) Other lists selected on an ongoing basis, according to the existing risks and information acquired.

In the case of a Client's appearance on one of such lists, the Obligated Institution shall not establish a relationship or conduct transactions with it. If the Obligated Institution is in the process of a transaction, then it shall apply the detention of funds and transfer to a depository designated by the competent Prosecutor. In case the Obligated Institution has a relationship then it shall terminate such economic relationship.

The fact that controls are applied is recorded on an ongoing basis in the Notes in Customers reports.

5. Rules for retention of records and information.

An obliged institution and its employees are obliged to document the applied financial security measures, e.g., by making copies of documents, screenshots with the date, or in any other way. The documentation is kept for 5 years, counting from the date of termination of business relations with the customer or from the date of execution of an occasional transaction. Documents are stored in a manner ensuring their safety and in accordance with regulations on personal data protection. These issues are regulated by separate internal procedures.

6. The principles of performing duties involving the transmission of information on transactions and notifications to the FAU.

The purpose of the procedure is to determine events and situations that require an obliged institution to report to the FAU. The reporting obligation of an obliged institution consists in:

a) Reporting of suprathreshold transactions,
b) Reporting to the FAU on suspicious circumstances.

The organization cooperates with the authorities also in the situation of request for information.

1) The Management Board:
   a) receives reports and assesses the appropriateness of further reporting to the supervisory authority,
   b) is responsible for training employees on how to inform and report necessary events,
   c) cooperate with the authorities and provide them with the necessary documents and information.

2) Associates:
   a) Report the events described in the procedure,
   b) in case of becoming aware of a person who made a report - ensure that his/her data is not disclosed to other employees and that the reporting person does not bear negative consequences related to the report,
   c) where they become aware of a person who has been reported as potentially or actually responsible for a breach of AML/CFT rules, ensure that this information is kept confidential.

3) Situations in which an obliged institution submits information to the FAU:
   a) accepted deposit or executed withdrawal of funds of the equivalent of more than EUR 10 000,
   b) executed transfer of funds of an amount exceeding the equivalent of EUR 15,000, with exceptions specified by law.

   The organization is obliged to immediately notify the FAU in case of reasonable suspicion that a given transaction or assets may be related to money laundering or financing of terrorism. An employee, associate, trainee, and any other person who will have a reasonable suspicion of the above shall communicate the information to the Board of Directors by email or verbally. The deadline for providing the information shall be immediate. The Board of Directors shall decide without undue delay on the further fate of the notification. Since the acknowledgement of the notification, the obliged institution shall not conduct transactions.

4) Notification of a suspected crime
   An obliged institution, excluding domestic banks, branches of foreign banks, branches of credit institutions and cooperative savings and credit unions, shall immediately notify the competent public prosecutor if it has a reasonable suspicion that the property values transacted or accumulated in the account are derived from or related to an offence other than the offence of money laundering or terrorist financing or a fiscal offence.

7. Principles of dissemination of knowledge of the anti-money laundering and terrorist financing regulations among employees of the obliged institution.
   Senior management provides access to knowledge of the AML and terrorist financing regulations among its co-workers, including employees. This involves, in particular:
   a) Providing updated guidance and other courses of action,
   b) Providing written, electronic, and verbal information and explanations,
   c) Informing about changes in regulations,

d) Providing at least initial access to training (possibly in the form of an on-line video) on the subject of anti-money laundering and terrorist financing.

8. Rules for employees to report actual or potential violations of anti-money laundering and terrorist financing regulations

A procedure has been implemented in the obliged institution, which allows employees and other persons performing activities (hereinafter referred to as "other persons") for the benefit of the obliged institution to report actual or potential violations of regulations in the field of anti-money laundering and terrorist financing. The procedure is that these persons have been provided with an e-mail address to which they can make reports. Reports can therefore also be made anonymously. In connection with the above:

a) The persons acting as members of the Board of Directors are the persons responsible for receiving reports.
b) Reports shall be received by reading the e-mail and taking appropriate action thereon.
c) The data of the employee or other person are subject to special protection, so that the contents of the notification are not made available to anyone outside the management board. The obliged institution is obliged to ensure such working conditions that the person making the report does not experience any negative actions, including discriminatory, repressive ones, in connection with the report.
d) If the identity of the persons making the report or to whom the report relates is disclosed and the identity of those persons can be ascertained, senior management shall determine the circle of persons who may have had access to it and instruct them of their duty of confidentiality and the consequences of not complying.
e) Upon receipt of a report, senior management shall review the report and, if the report is found to be legitimate, shall take appropriate action, including but not limited to:
- suspend the transaction,
- notification of suspicion of committing a crime,
- notification of the FAU.

9. Principles of internal control or supervision of the compliance of the obliged institution with the anti-money laundering and counter-terrorist financing regulations and the rules of conduct set forth in the internal procedure.

Senior management:

a) Analyze changes in AML and terrorist financing regulations on an ongoing basis to ensure compliance with the procedure,
b) In case of changes or perceived inconsistencies or lack of precision, they take actions resulting in adjustments to the procedure,
c) Supervise on an ongoing basis how the procedure is being used in practical terms to ensure that it is as effective as possible.

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

10. Rules for noting discrepancies between the information collected in the Central Register of Beneficial Beneficiaries and the information on the customer's beneficial owners determined in connection with the application of the Act.

    In the case of risk analysis, as well as customer identification and verification, in case of recording discrepancies between the information collected in the Central Register of Beneficial Owners and information on the customer's beneficial owners established in connection with the application of the Act, an annotation to this effect is made in the Customer File.

11. Rules for documenting impediments identified in connection with verification of the identity of the beneficial owner and actions taken in connection with identification as a beneficial owner of an individual holding a senior management position.

    In the case of difficulties identified in connection with verification of the identity of the beneficial owner and actions taken in connection with identification of a natural person holding a senior managerial position as the beneficial owner, a note is made in the Client's File.

12. Rules for AML officer advanced training

    Once in 6 months (Training Period) the responsible for compliance AML officer have to go through the additional trainings in order to obtain necessary qualification and development of skills. AML officer trainings have to be selected by the A&D Best Trade s.r.o. or by the responsible AML officer one month prior to the Training Period. Selected AML officer trainings have to be certified either by government or by special authority responsible for certification of such trainings. After Training Period, the responsible AML officer have to provide A&D Best Trade s.r.o. with the confirmation of completion of the compliance trainings.

14 of March, 2024