

AML/CFT/CFP Policy and Verification Procedure

TAKTONUM GROUP N.V.

17.03.2025

1. Company Policy

Money Laundering is the process of disguising the identity of money of illegal origin so that it appears to have originated from a legitimate source. Financing of terrorist provides funds for terrorist activity, terrorists and terrorist organizations. Financing of Proliferation of weapons of mass destruction is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials. The use of products and services by money launderers and terrorists exposes Taktonum Group N.V. (**Taktonum**) to significant criminal, regulatory and reputational risk.

This policy is designed to provide direction to staff on the approach and management of Anti-Money Laundering (**AML**), combating of the Financing of Terrorism (**CFT**) and Proliferation of weapons of mass destruction (**CFP**) within Taktonum. This policy supports management's objective of mitigating the following risks:

- Money laundering;
- Financing of terrorism;
- Financing of Proliferation of weapons of mass destruction (WMDs);
- Sanctions;
- Politically exposed persons (**PEPs**);
- Legal and regulatory risk.

For all AML/CFT/CFP matters mentioned in this policy, Taktonum appoints a Compliance Officer (+447418353460, legal@taktonum.com).

This policy applies to all individuals working and/or providing services at all levels of Taktonum, including acting as senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term workers, casual and agency staff, all of whom are collectively referred to as 'staff' in this document.

Senior management of Taktonum will provide direction to, and oversight of, the AML/CFT/CFP strategy as well as apply a risk-based approach across the business.

Taktonum will enforce a strict anti-money laundering policy with zero tolerance for money laundering activities.

All Taktonum partners will be obligated to comply with Taktonum's AML/CFT/CFP policy and with all applicable AML/CFT/CFP laws. Failure to comply can result in severe consequences such as criminal penalties and heavy fines.

Taktonum will implement a range of filtration operations for swift and accurate identification of any trading activities that may constitute or are related to money laundering. This will help reduce potential money laundering activities throughout the Taktonum system.

Taktonum has put in place Know-Your-Customer (KYC) programs as an essential element for service, risk management and control procedures.

Such programs include:

- Customer Registration/Acceptance;
- Customer Identification/Verification;
- On-going Monitoring of customers' activity;
- Risk Management;
- Reporting of suspicious activities to respective authorities.

Taktonum is obliged not only to establish the identity of its customers, but also to monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC constitutes a core feature of services' risk management and control procedures. The intensity of KYC programs beyond these essential elements is tailored to the degree of risk.

All Taktonum customers will acknowledge, undertake and agree to the following terms regarding their use of the website, entering into trading activities with Taktonum as a Taktonum customers:

1. The customer will comply (throughout the time as a Taktonum customer) with all relevant statutes pertaining to money laundering, financing of terrorism and proliferation of weapons of mass destruction, and proceeds from criminal activities;
2. Taktonum will operate under certain obligations known as "know-your-customer" obligations which grant Taktonum the right to implement anti-money laundering, combating of the financing of terrorism and proliferation of weapons of mass destruction procedures to help detect and prevent money laundering activities where money laundering may mean to handle any funds associated with any illegal activity regardless of the location of such activity;
3. The customer agrees to lend full cooperation to Taktonum with respect to anti-money laundering efforts. This involves providing information that Taktonum requests regarding account, website usage etc. to help Taktonum perform its duties as dictated by applicable laws, regardless of jurisdiction;
4. Taktonum reserves the right to freeze without delay and without prior notice any funds transfer or other assets, as well as freeze an account, if there is reason to believe that completing such a transaction may result in the violation of any applicable law or is contrary to acceptable practices;
5. Taktonum reserves the right to suspend or terminate any trading activity if there is reason to believe that services are used for activities that are deemed unlawful or fraudulent;

6. Taktonum has the right to use customer information for the investigation and/or prevention of fraudulent or otherwise illegal activities;
7. Taktonum has the right to share customer information with:
 - Investigative agencies or any authorized officers who are helping Taktonum to comply with applicable law, including anti-money laundering laws and know-your-customer obligations;
 - Organizations that help Taktonum provide the services it offers to its customers;
 - Government, law enforcement agencies and courts;
 - Regulatory bodies and financial institutions.

1.1. Money Laundering

There are several broad groups of offences related to money laundering that Taktonum needs to avoid committing. These are:

- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering;
- tipping off, or prejudicing an investigation.

1.2. Financing of Terrorism

There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organized criminal activity. However, there are two major differences between terrorist property and criminal property. More generally:

- often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;
- terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property. Money laundering, on the other hand, always involves the proceeds of illegal activity;
- while money laundering is concerned with obscuring the source of funds, financing of terrorism is mostly concerned with obscuring the end recipient of the funds.

1.3. Financing of Proliferation of weapons

Financing of terrorism and financing of proliferation of weapons of mass destruction are both serious international crimes, but they target different threats and have distinct characteristics:

- financing of terrorism supports violent acts targeting civilians and governments to achieve political or ideological goals. Financing of proliferation of WMDs supports the development and distribution of WMDs, posing a broader threat to global security;
- both are subject to international sanctions and legal frameworks, but the specific laws, treaties, and enforcement mechanisms differ, reflecting the distinct nature of the threats they address;

- financing of terrorism often has more immediate and localized effects, whereas financing of proliferation of WMDs has the potential for widespread, catastrophic consequences, especially if WMDs are deployed.

2. Risk-based Approach

Taktonum maintains a standardized risk rating model to conduct risk assessments related to the exposure to money laundering across all relationships with its customers.

The Risk-based Approach takes the most cost effective and proportionate way to manage and mitigate money laundering and terrorist financing risks. Where the risks are higher enhanced measures are taken. Where the risks are lower Taktonum may take simplified measures.

Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. Taktonum is fully committed to an effective KYC programme and procedures that ensures their effectiveness.

Explicit responsibility is allocated within the organization for ensuring that Taktonum's policies and procedures are managed effectively and are in accordance with local supervisory practice. The channels for reporting suspicious transactions are clearly specified and communicated to all personnel.

Taktonum maintains an ongoing employee training program so that the staff are adequately trained in KYC procedures. The timing and content of training for various staff categories is adapted by Taktonum for its own needs.

Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff are educated in the importance of KYC policies and the basic requirements at Taktonum.

Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an on-going basis and to detect patterns of suspicious activity. Regular refresher training is provided to ensure that employees are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

Applying Risk-based Approach means that Taktonum:

- Assesses the risks of money laundering or terrorist financing;
- Designs and implements policies, procedures and controls to manage and mitigate those risks;
- Monitors and seeks to improve the operation of these policies, procedures and controls;
- Records what has been done.

Taktonum implements policies, procedures and controls to manage and mitigate risks most efficiently and cost effectively. The policies, procedures and controls includes, but is not restricted to:

- Customer Due Diligence (CDD);
- monitoring of transactions;
- review of customers' data according to the risk level presented by the customer;
- employee training;
- producing appropriate management information;
- reporting upward;
- effective liaison with all parts of the business;
- maintaining up to date knowledge of regulation and legislation.

Taktonum recognises that risks change over time and will continually and regularly update its risk management procedures.

2.1. Business Risk Assessment (BRA)

Taktonum will identify the money laundering and terrorist risks presented by:

- Location of the customer;
- Type of the customers;
- Type of services.

Taktonum revises its business risk assessment whenever there are changes to the environment within which it is operating and within its business activities.

2.2. Customer Risk Assessment (CRA)

Taktonum will identify the money laundering and terrorist risks presented by:

- Location of the customer;
- Political Exposure;
- Source of funds;
- Account activity.

2.3. Technological developments risk assessment

Taktonum will identify the money laundering and terrorist risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used.

3. Structure of AML/KYC departments

For the purpose of fulfilling AML/KYC requirements, reducing the risk when handling fraud operations, and protecting customers' accounts and funds, Taktonum has the following structural units:

- **KYC department** verifies individuals and legal entities and ensures KYC requirements are met;

- **Compliance department (or Compliance)** monitors and scores customer deposit/withdrawal transactions; verifies whether any transactions are subject to reporting; reports unusual transactions;
- **Anti-Fraud department** monitors suspicious activity on customer accounts, uses different means to prevent illegal activities, investigates cases of hacking and fraud.

4. Training

All employees who handle transactions that may be qualified as unusual are made aware, through the compulsory training programme, of:

- The risks of money laundering, financing of terrorism and proliferation of WMDs, the relevant legislation, and their obligations under that legislation;
- The identity and responsibilities of Taktonum's Compliance;
- Taktonum's procedures in how to recognise and deal with potential money laundering or terrorist financing transactions or activity.

Staff training details on anti-money laundering, and counter terrorist financing will be recorded.

The Compliance is responsible for oversight of Taktonum's compliance with its requirements in respect of staff training, and has overall responsibility for the establishment and maintenance of effective training arrangements.

Training covers, as a minimum, the following subjects focusing on the relevance to, and implications for, the company:

- the risks of money laundering, financing of terrorist and proliferation of WMDs, the relevant legislation, and obligations under that legislation
- the identity and responsibilities of Taktonum's Compliance
- Taktonum's procedures on how to recognise and deal with potential money laundering or terrorist financing transactions or activity.

5. Sanctions and PEPs Screening

"Sanctions" means any financial or trade sanctions enforced by the United Nations Security Council, the European Union, the UK Government (including, without limitation, Her Majesty's Treasury), the US Government, (including, without limitation, the Office of Foreign Assets Control of the US Department of the Treasury or the US Department of State), or any other relevant sanctions authority.

Taktonum will make use of an external service provider SumSub (www.sumsub.com) to screen applicants against recognised Sanctions Lists and Politically Exposed Persons (PEPs) lists. Individuals will be screened on a monthly basis as well as on initial sign up.

5.1. Sanctions Lists

While establishing business relationships with customers, Taktonum will take into account a variety of information sources, including published by:

- the Financial Action Task Force (FATF)

- the Caribbean Financial Action Task Force (CFATF)
- the Office of Foreign Assets Control (OFAC)
- European Union sanctions (EU)
- United Nations sanctions (UN)

Information leading to “fuzzy matches” will be investigated further, for example where the match was related to a name which can be deemed as popular, and this will be compared against the other information that is collected at point of registration. The full evaluation of the customers data will provide a result.

Any confirmed matches to sanctions lists will be declined or closed, and the necessary reports will be made.

5.2. PEPs Screening

Taktonum screens customers against PEP lists that helps to structure information about PEPs. Taktonum is using a provider SumSub (www.sumsub.com) .

According to 5th Anti-Money Laundering Directive ((EU) 2018/843) ‘Politically exposed person’ means a natural person who is or who has been entrusted with prominent public functions and includes the following:

- (a) heads of State, heads of government, ministers and deputy or assistant ministers;
- (b) members of parliament or of similar legislative bodies;
- (c) members of the governing bodies of political parties;
- (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- (e) members of courts of auditors or of the boards of central banks;
- (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- (g) members of the administrative, management or supervisory bodies of State-owned enterprises;
- (h) directors, deputy directors and members of the board or equivalent function of an international organisation.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.

‘Family members’ includes the following:

- (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

- (b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
- (c) the parents of a politically exposed person.

'Persons known to be close associates' means:

- (a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
- (b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

If a PEP were identified and it is validated, the customer's trading activities would be suspended immediately and the funds retained. Upon identification of a PEP, Enhanced Due Diligence will be applied. Executive management will decide on a case by case basis whether to proceed with PEP based on the risk to the business.

6. Regional Representation

6.1. FATF high-risk and other monitored jurisdictions

Taktonum takes all necessary steps to ensure that all customers/partners with whom Taktonum has business relations have been tested for compliance with the notices published by the FATF. Taktonum may also take into account a variety of sources of information produced by non-governmental well-known bodies.

6.2. List of jurisdictions which Taktonum does not provide its services in:

- Afghanistan
- Australia
- Austria
- Aruba
- Belgium
- Bonaire
- Bulgaria
- Belarus
- Belize
- Central African Republic
- Comoros
- Colombia
- Croatia
- Cuba
- Curacao
- Cyprus
- Czech Republic

- Democratic Republic of the Congo
- Democratic People's Republic of Korea (DPRK)
- Ethiopia
- Denmark
- Estonia
- France
- Georgia
- Germany
- Greece
- Hungary
- Islamic Republic of Iran
- Iraq
- Italy
- Ireland
- Latvia
- Lebanon
- Libya
- Lithuania
- Mexico
- Moldova
- Mali
- Myanmar
- Northern Korea
- Nicaragua
- Portugal
- Poland
- Romania
- Russian Federation
- Saba
- Somalia
- South Sudan
- Statia (Sint Eustatius)
- Singapore
- Slovakia
- Spain
- St. Maarten
- Sudan
- Syria
- Sweden
- Switzerland
- Ukraine (Crimea, Donetsk, Luhansk)
- the Netherlands
- the United Kingdom
- the United States of America

- Venezuela
- Yemen

IPs from the above jurisdictions are automatically blocked from accessing the Taktonum. The verification of customers from these jurisdictions (according to the provided documents) is not allowed.

7. Know Your Customer (KYC)

7.1. Simplified Due Diligence (SDD)

A verified individual customer will be offered an opportunity to enter into Taktonum, which is still subject to limits and ongoing monitoring based on the risk rating.

In order to become verified, individual customers may be screened manually and electronically using an e-KYC provider SumSub (www.sumsub.com). This will be achieved by requiring details that allow a KYC check as follows:

- one match on an individual's full name and current address, and
- a second match on an individual's full name and either his current address or his date of birth.

In the event that the customer's identity cannot be verified electronically, there is a manual process utilizing physical documents which the customer must submit for review.

Where Taktonum needs to verify the customer manually, applicants will be required to provide a proof of identity as well as a proof of address.

SDD measures are suspended where the customers' risk assessment changes and it no longer considers that there is a low degree of risk of ML/FT/FP. Under this circumstance, customers who successfully pass the registration process will be allowed to use Taktonum services.

Regulatory limits are set as follows:

- maximum turnover limit equal to or more than **EUR 2,000**, whether the deposit / withdrawal transaction is executed in a single operation or in several operations which appear to be linked.

7.2. Enhanced Due Diligence (EDD)

Enhanced due diligence is required in circumstances giving rise to an overall higher risk.

When assessing the ML/FT/FP risks the following factors will be considered:

- types of customer (PEPs);
- countries or geographic areas (countries identified by credible sources as not having adequate AML/CFT approaches);
- transactions (discrepancies between submitted and detected information);
- new delivery mechanism (businesses introduced by third parties).

Customers subject to EDD are required to provide a written confirmation regarding the legal origin of funds. As a result, senior management will take a decision to continue or terminate business relations with the respective customer.

8. Customer Journey

8.1. Registration

At point of registration within the website or mobile application, Taktonum will capture the following customer information:

- Name;
- Permanent address;
- Telephone number;
- Email address;
- Date of birth;
- Nationality;

At this stage, Taktonum screens applicants against geographical areas of operation (IP address detection).

In addition, the system will automatically detect if the personal details entered are already assigned to another customer.

8.2. Verification

Taktonum utilizes customer identification procedures to validate the true identity of its customer and proof of address. The first requirement of 'knowing your customer' for money laundering purposes is to be satisfied that a prospective customer is who they claim to be.

Taktonum carries out appropriate KYC procedures for all customers. The objective of the KYC process is to ensure Taktonum holds appropriate information to be able to satisfactorily know who Taktonum is dealing with.

Documenting and maintaining these identification procedures enhances Taktonum's ability to prevent money laundering activities. If Taktonum fails to verify a customer's identity within an acceptable time period, all activities will be suspended for that customer and any accounts opened will be terminated. In addition, the account and services attached to that customer will be under stricter scrutiny until the suspension and/or closure is carried out.

Who is subject to verification:

- Customers are subject to all aspects of identification in accordance with the standards of Know Your Customer (KYC) and Customer Due Diligence (CDD);
- Third parties who are service providers, such as providers of various services, owners of the rented premises, banks, payment service providers etc.

Taktonum's KYC procedure foresees the following steps:

- Customer identification and verification (Proof of Identity);
- Customer address verification (Proof of Address);
- Customer payment card verification.

Identity and address verification procedure requires the customers to provide with reliable, independent source documents, data or information according to the approved list of documents.

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, Taktonum will deactivate the account and, after considering the risks involved, consider closing any existing account. In either case, our Compliance will be notified so that we can determine whether we should report the situation to the authorities.

The customer may be offered to use an automotive system SumSub (<https://sumsub.com>) via Telegram channel for customer onboarding and verifying.

It determines authenticity of ID, including customer's documents, compares the photo in the document with a customer selfie, determines customer's age and national origin, automatically flags fake or forged documents, identifies the liveliness of a real human face versus a hologram and checks photos with internal databases of fraudulent materials and cases to protect your service from professional fraud and cybercrime.

Once personal data and documents are received, Taktonum 24/7 Verification department screens applicants verifiers potential customers on the presence in the recognized worldwide "black lists" (e.g. OFAC) and sanctions and PEP lists using system SumSub (<https://sumsub.com>). The customers who are intended to use payment cards have to go through card verification.

After a customer has been approved Taktonum performs a comprehensive process of customers activity monitoring once the deposit from the customer is received.

8.2.1. Verification of identity (Proof of Identity)

The aim of verification of identity is to establish the following about the customer: first, middle (if any), and last names, date and place of birth, nationality and details of the document of identity issued in accordance with the legislation of the country issuing the document.

The customer undergoing verification must provide a photo/scan copy of the original document that certifies the identity. Any document from the following list can be accepted:

- ID card;
- Passport;
- Permanent resident card.

The document provided for verification must contain the following information:

- Country issuing the document;
- Serial number;

- Date of issue;
- Expiry date;
- Customer's first name;
- Customer's last name;
- Date of birth of the customer.

All scanned copies or photos of the document provided for verification must meet the following quality criteria:

- Scanned copies or photos must be made from the original documents;
- Scanned copies or photos of documents must be in color;
- Scanned copies or photos of documents must not be edited using a photo editor software;
- Scanned copies or photos of documents should not have scanning/photographing artifacts such as glare from the flash or blur;
- Scanned copies or photos of documents must be in good quality, and the document data clearly visible.

8.2.2. Verification of address

Verification of addresses is confirmation of a permanent and (or) temporary residence of the customer.

The customer can provide one of the following documents as proof of address:

- Bank statement about the customer's account;
- Utility bill;
- Tax documents;
- Document confirming registration at the address issued by local authorities;
- Rental agreement;
- Documents issued by the government or other competent authorities;
- Court documents.

Document confirming the customer's permanent and (or) temporary residence must contain:

- Full name of the customer;
- Postal address of the customer;
- Date of issue of the document that is not older than 6 month old;
- Document must be stamped and signed by the organization's employee (where applicable).

8.2.3. Verification with a selfie photo

Verification with a selfie photo is used to confirm that the verification documents really belong to the customer in question. The customer must provide a photo of themselves holding the document that had been used to verify their identity (proof of identity) next to the face.

A selfie photo must meet the following requirements:

- Photo must show a customer holding the verification document;
- Customer's face must fully fit in the frame;

- Customer must hold the document vertically, and all the data on the document is clearly visible.

9. Suspicious Activity Reporting

When any member of staff either knows, suspects or has reasonable grounds for knowing or suspecting that a money laundering offence has been or is being committed they must make a suspicious activity report (**SAR**) to the Compliance.

Staff are not required to actively search for indications that money laundering offences are occurring. However if they become aware of, or suspect that, such offences are occurring during the course of their normal duties then they shall make a SAR to the Compliance.

9.1. Internal Reporting

All staff must report any activity that they see in the course of their duties and that they think may be suspicious to the Compliance; all such reports must be documented by the member of staff making the report. Taktonum will provide all necessary training and guidance to ensure that staff are aware of:

- Their obligations in this area;
- Possible offences and penalties;
- Procedures to be followed;
- Documentation to be used to make reports;
- Where to access further advice and guidance.

9.2. Suspicious Activity Reports – Internal Procedure

Taktonum has made a SAR template available to staff, all reports must be made using this template to ensure consistency. All reports must be fully documented and must include at a minimum the following information:

- Name and contact details of person making the report;
- The customers personal details;
- The suspicious activity details;
- Date, amount and transaction identifier;
- Details of any related activities (as above);
- The reasons for the suspicions.

The fact that a report has been made and the content of the report must remain confidential at all times. A member of staff who forms or is aware of a suspicion of money laundering shall not discuss it with any outside party or any other member of staff unless directly involved in the matter causing suspicion.

No member of staff shall at any time disclose a money laundering suspicion to the person suspected. If circumstances arise that may cause difficulties with a customer contact, the member of staff must seek and follow the instructions of the Compliance.

No copies or records of money laundering suspicion reports are to be made, except by the Compliance who will keep such records secure, and separate.

9.3. Compliance Acknowledgement and Evaluation

All members of staff, anywhere within Taktonum, shall respond in full to all enquiries made by the Compliance for the purposes of evaluating a SAR. Information provided to the Compliance in response to such enquiries does not breach customer confidentiality or professional privilege, and no member of staff shall withhold information on those grounds.

The Compliance will acknowledge every report made. This confirms to the member of staff who raised the matter that their legal obligation to report has been fulfilled. This response will:

- Acknowledge receipt of the report;
- Remind the initiator of the report of their obligation to do nothing that might prejudice an investigation or tip off the customer;
- Provide feedback on the quality of the report and suggest areas of improvement for future reports.

The Compliance will then conduct his own evaluation of the information provided within the report and decide whether or not to make a disclosure to the competent authority.

Any internal enquiries made in relation to the report will be documented.

9.4. Tipping-Off

In some circumstances it may be necessary to obtain information from the customer before deciding whether or not to make a disclosure to the competent authority. In these cases the Compliance may request an appropriate person (such as a Fraud and Security, Marketing or Customer Services Supervisor) to make discreet enquiries of a customer. In such circumstances care will be taken to ensure that the offence of 'tipping-off' will be avoided.

9.5. External Reporting

The Compliance shall receive and evaluate internal suspicion reports and decide whether a formal disclosure is to be made to the authorities. If so deciding, the Compliance will make the formal disclosure on behalf of Taktonum.

Prior to making any such report the Compliance will undertake internal enquiries to satisfy themselves that, based on the information in the report and the result of their enquiries, they know or suspect, or have reasonable grounds to know or suspect, an offence of money laundering.

Where the Compliance does not have immediate access to such information it will be provided as soon as is practicable by any relevant employee of Taktonum or any relevant employee of any organisation that provides outsourced services on behalf of Taktonum. The need to examine any additional information will not unnecessarily delay any report.

The decision whether or not there is knowledge, suspicion or reasonable grounds for knowledge or suspicion of a money laundering offence will rest with the Compliance or their delegated representative alone. Such a decision will not be subject to the consent of any other person within Taktonum.

From the moment a suspicion of money laundering arises, no further work will be carried out on the matter that gave rise to the suspicion. Neither commercial considerations, nor the difficulty in responding to the customers enquiries on the matter shall be permitted to take precedence over Taktonum's legal obligations in this regard.

10. Record-Keeping

Taktonum will retain the following records for five years after the end of the customer relationship or the date of the occasional transaction:

- Copies of, or references to, the evidence obtained of a customer's identity;
- Details of customer trading activities;
- Details of actions taken in respect of internal and external suspicion reports;
- Details of information considered by the Compliance in respect of an internal report where no external report is made.

Taktonum will ensure that the above requirements are adhered to, and that the documents are able to be produced on request.

Signature of Managing Director:

Eduards Kalnins

A handwritten signature in blue ink, appearing to be 'EK', is written over a horizontal line.

Date: March 17, 2025

Internal Suspicious Activity Report Form

To: Compliance department

From: (name of employee)

Date:

This SAR is (circle which applies):

1. A request for consent for a transaction which is not yet completed
2. A report on a transaction which has taken place which I consider suspicious
3. Report on other business related activity which I consider suspicious

I consider the following transaction suspicious and report to you under the internal reporting procedure:

- 1) Date of transaction: _____
- 2) Amount: _____
- 3) Customer name/ID: _____
- 4) Transaction number: _____
- 5) Reason for suspicion: _____

Signature of reporting staff _____

Annex 2

Suspicious Activity Report Form- Compliance Resolution

Private and Confidential

From: Compliance department

Transaction number:

Customer:

Amount:

Internal SAR received from:

Date SAR received:

I confirm that I have reviewed the internal SAR and customer ID for this customer plus transaction history (all documents attached)

I confirm that, based on the information received and reviewed, I have:

1. submitted a Consent request to the following authority _____

2. submitted a post transaction SAR to the following authority _____

3. decided not to submit any kind of SAR to the following authority _____ for the following reason: _____

Signature of the representative of Compliance department:

Date: