GLOFFIX
GLOBALLY YOURS

# ANTI MONEY LAUNDERING POLICY

**ANTI MONEY LAUNDERING POLICY**

## 1. INTRODUCTION

This Policy is issued by Gloffix as the main guidance for its employees and management for combating the financing of terrorism and preventing money laundering.

The term “money laundering” includes all schemes to conceal the origins of criminal incomes so that they appear to originate from a legal source. Gloffix aims to recognize, control and mitigate the risks associated with money laundering and terrorism funding.

This Policy will be applicable for all operations, local and international. The objective of this policy is to ensure that the services of Gloffix are not used to launder the proceeds of crime and that all of the staff is aware of their obligations and the need for vigilance in the fight against money laundering and terrorist financing.

The policy of the Company – not to enter into business relationships with criminals and/or terrorists, not to process transactions which result from criminal and/or terrorist activity and not to facilitate any transactions involving criminal and/or terrorist activity including the financing of terrorism.

The Company undertakes to implement all policies and procedures necessary to prevent money laundering and to comply with all applicable legislation in this regard, such as the regulatory instructions, laws, and regulations (issued from time to time) of the countries where Gloffix operates.

The Company is obliged to regularly monitor the risk exposure level of money laundering and terrorism funding.

The Company maintains the know-your-client policy and understands Anti Money Laundering directions thoroughly in order to evaluate risks and identify unusual actions.

## 2. GENERAL AND SPECIFIC PROVISIONS

## 1. GENERAL PROVISIONS CONCERNING MONEY LAUNDERING

Money laundering involves the placement of illegally obtained money into legitimate financial systems so that monetary proceeds derived from criminal activities are transformed into funds with an apparently legal source. Money laundering has many destructive consequences both for society as a whole and for those entities involved in money laundering activities.

A money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means most serious offences under the Penal Code or any other Act. It includes, but is not limited to those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement.

Terrorist financing refers to the processing of funds to sponsors involved in or those who facilitate terrorist activity. Terrorist individuals/ groups/ organization derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income.

## 2. CLIENT CONFIDENTIALITY

It is important to stress out that the reporting of the suspicion of money laundering does not constitute a breach of client confidentiality.

## 3. SPECIFIC MONEY LAUNDERING PROVISIONS FOR CONDUCTING THE REGULATED ACTIVITIES

The following points apply to the Company in order to facilitate recognition of suspicions of money laundering and reporting of the foregoing to the authorities and so that the Company may produce its part of the audit trail to assist in an official investigation. In particular, the Company is obliged to:

1. Have procedures to verify the identity of new counterparties;

2. Have procedures for employees to report any suspicious transactions;
3. Have record-keeping procedures relating to the identity of clients and transactions effected for them;
4. Responsibility of ensuring that employees are suitably trained and made aware of the above procedures and in the recognition and handling of suspicious transactions;
5. Appoint a senior person as a designated MLRO to whom reports of suspicious transactions are to be made. This person must be free to act on his/her own authority and to make further investigations to determine whether a suspicion can be discounted or must be reported. The MLRO will be able to delegate duties, but will be responsible for the activities of such delegates;
6. Stress the employees of the Company the potential of personal liability as well as that of the Company for failure to observe any aspect of the Regulations.

### 4. COMPLIANCE

The implementation of a compliance regime is a legislative requirement and a good business practice for anyone subject to the Anti-Money Laundering and Counter-Terrorism Financing. A welldesigned applied and monitored regime will provide a solid foundation for compliance with the legislation.

The Compliance Officer is responsible for establishing and conducting Employee training programs to ensure that all appropriate Employees are aware of the applicable Laws and Regulations, Policies & procedures and their responsibilities with respect to these policies.

## 3. PROCEDURES AND OBLIGATIONS OF THE COMPANY

### 1. DUTY ON ESTABLISHING BUSINESS RELATIONSHIPS

The Company may not carry out a one-off transaction or form a business relationship in the course of a relevant financial business unless:

1. It has money laundering procedures in place, meaning:

1. identification procedures;
2. record-keeping procedures; and monitoring;
3. recognition of suspicious transactions;
4. internal reporting procedures and such other procedures of internal control and communication as maybe appropriate for the purpose of forestalling and preventing money laundering;

2. It makes its employees aware of the statutory duties and of the Company's procedures; and it maintains training procedures.

## 2. CUSTOMER DUE DILIGENCE

Effective Customer Due Diligence ("CDD") standards are crucial for managing risks related to money laundering and terrorism funding. CDD suggests actions and procedures directed to recognize the customer and verify his/her authentic identity. Customers must provide documents, data, or information both at the moment of beginning the business relationship with the Company and on an ongoing basis if needed. The required steps to finalize CDD measures include the acquisition of data and efforts to verify that information given by customers.

Individual customers must provide the following credentials to the Company during the registration process:

1. Customer's a full name;
2. Country of residency/location;
3. The mobile phone number and e-mail address.
4. The Company's staff has to verify the credentials received from the customer by requesting relevant documents.
5. The list of verification documents includes, but is not limited to, the following:
6. For an individual customer: A copy of the passport or any other national ID. Images must be made with a high-resolution (scan or photo), indicating surname and name(s), date and place of birth, passport number, issue and expiry dates, country of issue and Client's signature;
7. For a corporate customer: a high-resolution copy of documents confirming the entity existence, such as Certificate of
   Incorporation and Certificate of Good Standing, Articles of

Incorporation, or a government-issued business license (if applicable), etc.

The Company requires to verify the Customer's location. One of the following documents must be provided by the Customer as proof of address, which must include the Customer's name and address indicated:

8. Any utility bill (fixed-line phone, water, electricity) issued within the last 3 months;
9. Any bank statement (current account, deposit account, or credit card account);
10. Bank reference letter. A high-resolution image is a must.

The Customer is required to provide a scanned copy or photo of the credit/debit card (front and backside) for any transactions related to funds deposit or withdrawal via credit/debit card. The front side of the card must confirm the cardholder's full name, the expiration date and the first six and the last four digits of the card number (all of the rest digits must be hidden). The copy or scan of the reverse side of the credit/debit card should indicate clearly the cardholder's signature, while the CVC2/CVV2 code must be masked.

If a customer has authorized another person, un additional documentation is required. These include:

11. Attested copies of ID document of Authorized person
12. Power of Attorney duly attested by Notary Public on the prescribed format duly signed by all Account Holders with the following minimum information:

    1. Name of Authorized person and his/her Relationship
    2. Passport number
    3. Contact Details and email address
    4. o Specimen Signature of the person so authorized.

The authorized person is only allowed to issue an instruction for buy or sale of securities on behalf of the client and all payments or receipt of funds must be made to or from the client own accounts

If the high-risk level of the business relationship with a Customer has been estimated by the Company, the following additional measures can be imposed:

13. The Customer will be required to provide additional information related to the funds or source of wealth (e-mail or phone notification);
14. The Company can conduct independent research and/or use third-party sources in order to clarify or update the Customer's information, obtain any further or additional data, define the Customer's transaction intentions and purposes with the Company.

In case of an existing customer either refuses to provide the information described above or if a Customer has deliberately provided incorrect information, the Company will consider closing any of the existing Customer's accounts after acknowledging the risks involved.

The Company's staff is allowed to ask for and examine details of the person's employment status or business/occupation when obtaining verification data of the customer's statements about the source of funds or wealth. In particular, the list of appropriate documents to confirm the Customer's employment/occupation can include employment agreements, bank statements, letters from employer or business, etc.

The Company will conduct continuous Customer's due diligence and monitor Customer's accounts in all business relationships, involving regular reviews and updates of the Company's prospect of customers' actions, the risk-level imposed, and any contradictory information or assumptions previously provided by the customer. It can also include anything that resembles to be a significant change in the nature or purpose of the Customer's business relationship with the Company.

In order to the obligation to verify identity, Gloffix using the best evidence and means available. In cases where our Compliance officer is not satisfied with the documentary evidence provided or with the results of public inquiries, he can approach another institution, on a non-competitive basis, specifically for the purpose of verifying identity.

A standard format can be used for making such inquiries. It may be necessary to obtain the prior consent of the prospective client for disclosure of their information by the other financial institution. For additional screening and verifying the Company can use services of https://complyadvantage.com/ from time to time.

The Company's Client Identification Procedures are based on the premise that the Company will accept funds from a new and existing Client only after the Client's identity is confirmed and it's known for sure that the Client is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made.

The Client Identification Procedures should be reviewed in light of the specific characteristics presented by a Client and in any instance, the Compliance Officer may determine to apply enhanced measures for reasons other than those discussed in the section below. As a reference tool, an Individual Client KYC Checklist is used.

Following are the examples of Clients who pose a high money laundering risk:

15. Customers belonging to countries where CDD/KYC and antimoney laundering regulations are lax or if funds originate or go to those countries;
16. Customers whose business or activities present a higher risk of money;
17. Customers with links to offshore tax havens;
18. High net worth customers with no clearly identifiable source of income;
19. There is a reason to believe that the customer has been refused brokerage services by another brokerage house;
20. Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations; and
21. Politically Exposed Persons (PEPs) or customers holding public or high-profile positions.

3. **POLITICALLY EXPOSED PERSON (PEP)**

A politically exposed person (PEP) is defined as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions

that potentially can be abused for the purpose of committing money laundering (ML) offenses and related predicate offenses, including corruption and bribery, as well as conducting activity related to terrorist financing (TF). This has been confirmed by analysis and case studies. The potential risks associated with PEPs justify the application of additional preventive measures with respect to business relationships with PEPs.

It includes, but is not limited to, the following:

1. heads of state, heads of government, ministers, and deputy or assistant ministers; members of parliament or of similar legislative bodies;
2. members of the governing bodies of political parties;
3. 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;
4. members of courts of auditors or of the boards of central banks;
5. ambassadors, charge affairs, and high-ranking officers in the armed forces;
6. members of the administrative, management, or supervisory bodies of state-owned enterprises;
7. directors, deputy directors, and members of the board or equivalent function of an international organization.

A person who is a PEP should continue to be treated as a PEP for a period of at least three (3) years after the date on which that person ceased to be entrusted with that public function, or for such longer period as the relevant person considers appropriate to address risks of money laundering or terrorist financing in relation to that person.

The Company's Back-office staff can check if the client is PEP in open internet sources such as https://namescan.io/FreePEPCheck.aspx

Regulation defines 'family members' of a PEP to include the following:

8. a spouse or partner of that person
9. children of that person and their spouses or partners; 10. parents of that person. This is not an exclusive list.

"Known close associate" of a PEP to include the following:

11. an individual is known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a politically exposed person;
12. an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP;

A known close associate of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

4. **HIGH-RISK INDICATORS – GEOGRAPHICAL:**

A client may pose a greater risk if she/he is from, or closely connected to, a country with some of the following characteristics:

1. associated with high levels of corruption
2. political instability
3. weak state institutions
4. weak anti-money laundering defenses
5. armed conflict
6. non-democratic forms of government
7. widespread organized criminality
8. a political economy dominated by oligopolistic actors with close links to the state
9. lacking a free press and where legal or other measures constrain journalistic investigation
10. a criminal justice system vulnerable to political interference
11. lacking expertise and skills related to book-keeping, accountancy, and audit, particularly in the public sector
12. weaknesses in the transparency of registries of ownership for companies, land, and equities

List of countries having strategic deficiencies:

13. Afghanistan,
14. American Samoa,
15. The Bahamas,
16. Botswana,

17. Democratic People's Republic of Korea,
18. Ethiopia,
19. Ghana,
20. Guam,
21. Iran,
22. Iraq,
23. Libya,
24. Nigeria,
25. Pakistan,
26. Panama,
27. Puerto Rico,
28. Samoa,
29. Saudi Arabia,
30. Sri Lanka,
31. Syria,
32. Trinidad and Tobago,
33. Tunisia,
34. US Virgin Islands,
35. Yemen.

## 5. MEASURES TO BE APPLIED IN WORKING WITH PEPs AND CLIENTS FROM HIGH-RISK COUNTRIES

The following measures can be appropriate in lower-risk situations:

1. Undertake customer due diligence to establish whether the customer is a family member or has a close relationship with a PEP.
2. Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of family members or known close associates of a PEP; for example, only use information already available to the Company (such as transaction records or publicly available information) and do not make further inquiries of the individual unless anomalies arise.

3. Oversight and approval of the relationship take place at a less senior level of management.
4. A business relationship with a PEP or a PEP's family and close associates is subject to less frequent formal review.

The following measures can be appropriate in higher-risk situations:

5. Assessing the Client's business reputation through review of financial or professional references, generally available media reports, or by other means;
6. Considering the source of the Client's wealth: including the economic activities that generated the Client's wealth, and the source of the particular funds intended to be used to make the investment;
7. Reviewing generally available public information, such as media reports, to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations, or any investigation, indictment, conviction, or civil enforcement action relating to the financing of terrorists;
8. Take more intrusive and exhaustive steps to establish the source of wealth and source of funds of family members or known close associates of a PEP
9. Oversight and approval of the relationship take place at a more senior level of management.
10. A business relationship with a PEP or a PEP's family and close associates is subject to more frequent and thorough formal review as to whether the business relationship should be maintained.

## 6. COMPLIANCE OFFICER APPROVAL

Once completed, the Client Identification Questionnaire should be completed and signed by the employee or the person designated by the Company and must be handed over to the Compliance Officer for record-keeping. For each applicant, the Compliance Officer must also countersign the forms and will be responsible for deciding what further information, including documentation, is required prior to conducting business for the applicant.

## 7. COMPLIANCE AND REPORTING OFFICER

The Company has appointed a dedicated CRO to oversight the Compliance function who will be reporting to the Board of Directors. The officer has the appropriate qualifications, experience, competence, authority, and independence to be able to effectively and independently fulfill the reporting obligations.
The reports must include any information related to the Company's internal AML policy violations and the Regulations procedures breaches, as well as principles and standards of good practice infringements.

Any Employee shall immediately notify the CRO if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed. Employees are encouraged to seek the assistance of the Compliance Officer with any questions or concerns they may have with respect to the Policy & Procedures

AML Compliance and Reporting Officer's responsibilities include:

1. Ensuring the Company's compliance with the Regulations requirements;
2. Establishing and maintaining internal AML application;
3. Establishing an audit function to test its anti-money laundering and opposing the terrorism funding schemes and systems;
4. Ensuring that all officers, employees, and agents are screened by the CRO and other appropriate officers before recruitment;
5. Training employees to recognize suspicious and unusual transactions;
6. Investigating internal suspicious activity, getting transaction reports from staff and reporting if needed;
7. Ensuring that conventional AML records are kept and stored;
8. Obtaining and updating the list of countries with poor AML rules, laws, or standards.

The degree of decision-making responsibility placed on the CRO is significant. Informing an independent judgment about whether there are reasonable grounds for suspicion, he/she should consider all other relevant information available within the reporting entity concerning the person or business to which the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to the identification and other records held. If after completing this review, the CRO decides that reasonable grounds for suspicion exist, then he/she must immediately proceed to make an STR to

the VFIU. All STRs must be made within two working days of forming the relevant suspicion (or knowledge).

All STRs should be hand-delivered to the office of the VFIU. When submitting an STR the Company should provide the VFIU as a matter of course with all information that it has about the transaction or attempted transaction and the parties to the transaction, including the records prescribed under the AML Act. If it is not possible to provide this information with the STR then it should follow as soon as reasonably practicable.

## 8. EMPLOYEES' AML DUTIES

All Company employees, managers, and officers must be aware of this policy. The knowledge of any officer, employee or agent of the Company is taken to be knowledge of the entity.

Employees, managers, and directors who are engaged in AML-related duties must be vetted to meet the AML policy requirements. This includes an examination of potential criminal activity of the employee and continuous monitoring during the work contract. Any violation of this policy or the AML management rules must be reported confidentially to the AML Compliance Officer unless the violation involves the AML Compliance Officer himself, in which case the employee must report about the violation to the Chief Executive Officer.

Employees, working in positions that are susceptible to money laundering or terrorism funding schemes, must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism funding risks and what actions are needed to be made once the risks are identified.
This policy and procedures are intended to ensure that, prior to accepting funds from Clients, all reasonable and practical measures are taken to confirm the Clients' identities. Gloffix may take assistance from the bank or other financial institutions for completing the client identification process. The assistance shall not relieve Gloffix for the identification process to be conducted by the company.

Employees are encouraged to provide the Compliance Officer with any revisions they consider appropriate. The Compliance Officer shall retain copies of all documents reviewed or checklists completed in connection with its Client Identification Procedures in accordance with the Company's Client Records Retention policy.

## 9. EMPLOYEE TRAINING PROGRAMME

The Company provides AML training to employees who will be dealing with customers or will be involved in any AML tests, verification, or monitoring processes. The Company will conduct its training internally once every six (6) months and also will hire external third-party consultants (once every two years). It can be https://www.intcomp.com/ or any other appropriate and a respectful training company that can prove its high educational level and will be accepted by management.

A supervisor will be assigned to every Company's employee. The supervisor's duties are to teach employees in relation to all policies, procedures, customer documentary forms, and requirements, forex markets, trading platforms, etc. A training plan for every new employee must be developed with examines which are being held for 2-3 months (depending on the level within the business).

The Company's AML training programs are aimed to ensure its employees to get an appropriate training level with regards to any possible AML/TF risks.

Training that will be provided for employees is:

1. Relevant to today's challenging working environment.
2. Practical so everyone can apply his learning to the role immediately.
3. Global with an emphasis on international best practice but using local expertise.
4. Interactive with a combination of first-class online materials and face to face teaching.

Content of the training:

5. Understanding Money Laundering, Terrorist Financing, and Sanctions.
6. Vulnerabilities of the Company to Money Laundering and Terrorist Financing.
7. Anti Money Laundering and Combating Terrorist Financing in Practice.
8. Anti Money Laundering and Combating Terrorist Financing – Legal and Regulatory Structures.
9. Management Obligations and the Risk-based Approach to Money Laundering and Terrorist Financing.

As mentioned above, the Company will provide extra AML\CTF training every six (6) months for all employees. This training will include the following content:

10. The Company's commitment to the prevention, detection, and report of ML and TF crimes.
11. Examples of ML and TF cases that have been detected in similar structures, to create an awareness of the potential ML and TF risks, which may be faced by the Company's employees
12. Well known or recognized typical activities, especially according to the FATF or AML Supervisors.
13. The consequences of ML and TF for the Company, including potential legal charges.
14. The Company's commitments ML Act and Regulations.
15. Exact employee's responsibilities as identified in this AML Policy and the way employees are expected to follow the Company's AML procedures.
16. Necessary steps to identify and report unusual activities that may be suspicious transactions or attempts for ML crime.
17. The rules that appeal to illegal disclosure of suspicious transactions ("tipping off"). After training the employees will:
    1. Understand the AML risks inherent to the Company;
    2. Have the knowledge to detect unusual activity and recognize red flags; and
    3. Can escalate unusual or suspicious activity to their supervisor or compliance officer.

## 10. RECORD KEEPING

Copies of all documents related to Gloffix's Client Identification Procedures will be retained for an appropriate period of time and, at a minimum, the period of time required by applicable law or regulation. The documents the Company retains are copies of documents reviewed in connection with Client Identification Procedures or enhanced due diligence procedures, Client identification checklists if any, or similar due diligence documentation, and any other documents required to be retained by applicable anti-money laundering legislation.

Gloffix will retain documents for so long as a Client is a client of the Company and for a minimum of 5 (five) years after this relationship ends. Gloffix shall, however, retain those records for a longer period where transactions, customers, or accounts involved litigation or it is required by the court or other competent Authority. The Company shall satisfy, on a timely basis, any inquiry or order from the relevant competent authorities including the VFIU and the VFSA for a supply of information and records as per law.

All records must be kept in a form which is immediately accessible upon request. Records do not have to be kept in hard copy. Retention may be by way of original documents, or by way of copies in any machine-readable or electronic form from which a paper copy can be readily produced.

## 11. REPORTING PROCEDURES

The Compliance Officer on behalf of the organization is nominated to receive disclosures under this regulation.

Anyone in the organization, to whom information comes in the course of the relevant business as a result of which he suspects that a person is engaged in money laundering, must disclose it to the Compliance Officer;
Where a disclosure is made to the Compliance Officer, the officer must consider it in the light of any relevant information which is available to AFS and determine whether it gives rise to suspicion: and

Where the Compliance Officer determines in consultation with the Senior Management, the information must be disclosed to the Regulatory Authority after obtaining independent legal advice.

## 12. SUSPICIOUS TRANSACTIONS

Below are some examples of suspicious activity that reporting entities in the course of conducting business.

### 1. Suspicious customer behavior

1. Customer is secretive, has an unusual, nervous, or excessive demeanor.
2. Customer insists that a transaction be done quickly or volunteers the information that a transaction is „clean".
3. Customer shows uncommon curiosity or level of knowledge about record keeping or reporting requirements.
4. Customer attempts to deter compliance with recordkeeping or reporting duties, through threats or otherwise.
5. Customer presents inconsistent or confusing details about a transaction or does not appear to understand it.
6. Customer appears to have only informal records of significant or large volume transactions.
7. Customer is reluctant to proceed with a transaction after being told it must be reported

8. Customer suggests payment of a gratuity or unusual favor.
9. Family members or close associates of public officials (PEPs) begin making large transactions not consistent with their known legitimate sources of income.

2. **Suspicious customer identification**

1. Agent, attorney, or financial advisor acts for another person without proper proof of authority.
2. Customer is unwilling to provide personal identity information or wants to establish identity using unofficial documents.
3. Customer furnishes unusual, suspicious, or inconsistent identification documents.
4. Customer is unusually slow in providing supporting documentation or cannot provide properly certified copies.
5. Customer spells name differently from one transaction to another, uses alternative names, or uses a consistent address but frequently changes the names of persons involved.
6. Customer's telephone is disconnected.

3. **Suspicious employee activity**

1. Employee exaggerates the credentials, background, financial ability, and/or resources of a customer in internal reporting.
2. Employee lives a lifestyle that cannot be supported by his/her salary.
3. Employee frequently overrides internal controls or established approval authority or circumvents policy.
4. Employee permits or facilitates transactions where the identity of the ultimate beneficiary or counterparty is not disclosed.
5. Employee avoids taking holidays.

## 13. CONFIDENTIALITY

Reporting a suspicion is a defense to a claim for breach of confidence. However, any statements to the press or other publicity must be routed through the MLRO or his deputy. Similarly, any requests for information or statements should be referred to him or his deputy for a reply. Confidentiality whilst an investigation is ongoing is of the utmost importance and employees are reminded of the offense of "tipping-off".

## 14. SANCTIONS

All officers and employees need to understand that they could be personally liable for non-compliance with AML obligations. They should be supported and

encouraged by the CRO and other senior officers to participate in relevant training, to make prompt reports of all suspicious transactions, and to cooperate fully with the VFIU and other regulatory agencies.

It is a criminal offense for any person to make a false or misleading statement (or to mislead by omission) in any STR or other reports to the VFIU, or to authorize the opening or operation of an account with a reporting entity in a fictitious, false or incorrect. Where anybody corporate is convicted of an offense under the AML Act or Regulations, and where the act or omission is shown to have taken place with the knowledge, authority, permission, or consent of any director, controller, or other officer concerned in the management of the corporate, that person is also guilty of the offense.

If there are suspects or there are reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorist financing, the Company / MLRO will as soon as possible, yet no later than during 2 (two) days, report promptly his/her suspicions to the Laundering and Counter-Terrorism Financing.

In the process of carrying out its activity, including as part of own risk management, Gloffix shall focus on applicable legislation of Laundering and Counter-Terrorism Financing, & regulatory legal acts.