UAB GLOBIANCE LT

(Trading as *Globiance*)

Anti-Money Laundering and Counter-Terrorism Financing Information

May 2023

TABLE OF CONTENTS

1 Overview

1.1 The purpose of this Anti-Money Laundering and Counter-Terrorism Financing Informational Document (hereinafter referred to as the "*Policy*" and "*Guidelines*") and applicable Sanctions measures is to ensure that **UAB Globiance LT** (hereinafter referred to as "***Globiance***", the "*Company*", "*we*" and/or "*us*" for the purposes of this document) has internal guidelines in place to prevent the use of its business for activities involving Money Laundering and Terrorist Financing and internal guidelines for the implementation of international sanctions, and is reviewed and updated when the need arises to comply with new rules and regulations or at least annually – whichever arises soonest.

1.2 These Guidelines have been adopted to ensure that Globiance complies with the rules and regulations as set out in the Republic of Lithuania *Law on the Prevention of Money Laundering and Terrorist Financing* (hereinafter referred to as the "*Law*") and other applicable legislation including, but not limited to, the following:

i. Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission approved by the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on November 30th of 2016 by Resolution No. V-314 (hereinafter referred to as the "*Technical Requirements*");[1]

ii. Resolution No. V-240 of December 5th of 2014 of the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on the "Approval of the List of Criteria for Money Laundering and Suspicious or Unusual Monetary Operations or Transactions Identification";[2]

iii. Resolution No. V-5 of 5 January 10th of 2020 of the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on the "Approval of Guidelines for the Depositary virtual currency wallet operators and virtual currency exchange operators to prevent money laundering and/or terrorist financing";[3]

iv. Resolution No. V-273 of October 20th of 2016 of the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on the "Approval of Guidelines for the Supervision of Financial Crimes for the Implementation of International Financial Sanctions in the Field of Regulations of the Ministry of Internal Affairs of the Republic of Lithuania";[4]

v. The Minister of the Interior of the Republic of Lithuania October 16th of 2017 by order no. 1V-701 on the "Suspension of Suspicious Monetary Transactions or Transactions and Submission of Information on Suspicious Monetary Transactions or Transactions to the Financial Crime Investigation Service under the Description of Procedure of the Ministry of the Interior of the Republic of Lithuania and Information on Cash Transactions or Transactions equal to or exceeding **15,000 euros** or submission of the corresponding amount in foreign currency to the Financial Crime Investigation Service under the approval of the description of the procedure of the Ministry of the Interior of the Republic of Lithuania";[5] and

vi. The Director of the Financial Crime Investigation Service May 21st of 2015 by order no. V-129 on the "Approval of Information Forms, Submission Schemes and Recommendations for the Completion of Information Provided in Accordance with the Requirements of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania."[6]

[1] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[2] https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9
[3] https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194
[4] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f
[5] https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4
[6] https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac

2 Definitions and Interpretations

2.1 Beneficial Owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation, step, or exercises control in another manner over a transaction, act, action, operation, step, or over another person and in whose interests, or for whose benefit, or on whose account a transaction, act, action, operation, or step is made. In the case of a legal entity, the *Beneficial Owner* is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the legal person, exceeds 25 percent (%), including holdings in the form of shares or other forms.

2.2 Business Relationship means a relationship that is established upon the conclusion of a long-term contract by the Company in economic or professional activities for the purpose of provision of a service or distribution thereof in another manner; or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of the establishment of the contact and during which the Company repeatedly makes separate transactions in the course of economic or professional activities whilst providing a service.

2.3 Company means the legal entity bearing the following data:

i. Company name: **UAB Globiance LT**;
ii. Registration country: **Lithuania**;
iii. Registration number: **306059802**;
iv. Email address: **lt@globiance.com**.

2.4 Custodian Virtual Currency Wallet means Virtual Currency Address(es) generated with the public key[7] for storing and managing Virtual Currencies entrusted to the Company but remaining their property.

2.5 User means a natural person or a legal entity which has a Business Relationship with the Company.

2.6 Company's Representative(s) refers to the Company's employee(s) and any other person who is involved in the application of these Guidelines within the Company.

2.7 Guideline(s) refers to this document including all annexes as provided for at the end of this document. The Guidelines include *inter alia* the Company's internal control procedure regarding the Guidelines and the Company's Risk Assessment Policy regarding risk-based approach for mitigating ML/TF risks and appropriate appetites.

2.8 Management Board refers to the management board of the Company.

2.9 MLRO means the Money Laundering Reporting Officer, who is appointed by the Company as a person responsible for receiving internal disclosures and making reports to the Financial Crime Investigation Service (hereinafter referred to as "*FCIS*") and other duties as prescribed for within this document.

2.10 Monetary Operation refers to any payment, transfer, and/or the receipt of money.

2.11 Money Laundering ("*ML*") means the concealment of the origins of illicit funds through their introduction into the legal economic system and transactions that appear to be legitimate. There are three (3) recognized stages in the Money Laundering process:

i. Placement, which involves placing the proceeds of crime into the financial system;
ii. Layering, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds; and
iii. Integration, which involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

[7] **Public key** means a code of letters, numbers and/or symbols designed to identify the customer and generate the client's Virtual Currency Address

2.12 Occasional Transaction means the transaction performed by the Company in the course of economic or professional activities for the purpose of provision of a service, the sale of goods, or the distribution thereof in another manner to the User outside the course of an established Business Relationship.

2.13 Politically Exposed Person ("*PEP*") means a natural person who performs or has performed prominent public functions, and with regard to whom related risks remain.

2.14 Sanctions mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy, and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security Policy of the European Union. Sanctions include:

i. international Sanctions which are imposed with regard to a state, territory, territorial unit, regime, organization, association, group, or person by a resolution of the United Nations Security Council, a decision of the Council of the European Union or any other legislation imposing obligations on Lithuania;
ii. Sanctions of the Government of the Republic of Lithuania which is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clause in order to protect the security or interests of Lithuania.

International Sanctions may ban the entry of a subject of an international Sanction in the state, restrict international trade and international transactions, and impose other prohibitions or obligations.

The subject of Sanctions is any natural or legal person, entity, or body, designated in the legal act imposing or implementing Sanctions, with regard to which the Sanctions apply.

2.15 Terrorist Financing (TF) means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.

2.16 Third Country means a state that is not a member state of the European Economic Area ("*EEA*").

2.17 Virtual Currency means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.

2.18 Virtual Currency Address means the address/account generated from letters, numbers and/or symbols in the blockchain, by which the blockchain allocates the Virtual Currency to the owner or recipient.

3 Customer Due Diligence ("*CDD*") and Know Your Customer ("*KYC*") Measures

Customer Due Diligence (hereinafter referred to as "*CDD*") and Know Your Customer (hereinafter referred to as "*KYC*") measures are required for verifying the identity of a User, as well as for the performance of risk-based ongoing monitoring of the Business Relationship held with the User.

The CDD measures consist of three (3) levels, including basic and enhanced due diligence measures.

3.1 Main Principles

The CDD measures are taken and performed to the extent necessary considering the User's risk profile and other circumstances in the following cases:

i. Upon establishment of the Business Relationship and during the ongoing monitoring of the Business Relationship;
ii. Upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data; and
iii. Upon suspicion of Money Laundering or Terrorist Financing, regardless of any derogations, exceptions or limits provided for in these Guidelines and applicable legislation.

The Company does not establish or maintain the Business Relationship and does not perform the transaction if:

i. The Company is not able to take and perform any of the required CDD measures;
ii. The Company has any suspicions that the Company's services or transactions will be used for Money Laundering or Terrorist Financing; and
iii. The risk level of the User or of the transaction does not comply with the Company's risk appetite.

In the case of receiving information in foreign languages within the framework of CDD implementation, the Company may request to demand translation of the documents to another language applicable for the Company. The use of translations should be avoided in situations where the original documents are prepared in a language applicable to the Company.

The Company has applied CDD measures adequately if the Company has the inner conviction that they have complied with the obligation to apply due diligence measures.

The principle of reasonability is observed in the consideration of inner conviction. This means that the Company must, upon the application of CDD measures, acquire the knowledge, understanding and assertation that they have collected enough information about the User, the User's activities, the purpose of the Business Relationship and of the transactions carried out within the scope of the Business Relationship, the origin of the funds, etc., so that they understand the User and the User's (business) activities, thereby taking into account the User's risk level, the risk associated with the Business Relationship, and the nature of such relationship.

All documentation and/or information obtained in respect of a User's personal data, transaction records, and correspondence in respect thereof will be retained by the Company for at least ten (10) years after the provision of services by the Company.

3.2 The Services Provided

The Company's main economic activity is the provision of Virtual Currency services. For this reason, the Company offers to their Users the following transaction types:

i. Providing Custodian Virtual Currency Wallet operator service, which allows the User to open a Custodian Virtual Currency Wallet on the User's name and make transactions with this wallet: to deposit Virtual Currency and to withdraw deposited Virtual Currency to another wallet(s); and
ii. Providing Virtual Currency exchange operator service, which allows the User to exchange, purchase and sell Virtual Currency.

The Company does not offer the above transaction types as Occasional Transactions.

3.3 The Verification of Information used for the User's Identification

Verification of the information for the User's identification means using data from a reliable and independent source to confirm that the data is true and correct, also confirming, if necessary, that the data directly related to the User is true and correct. This, *inter alia*, means that the purpose of verification of information is to obtain reassurance that the User, who wants to establish the Business Relationship is the person they claim to be.

3.4 Verification Procedures

Globiance has established systematic procedures for identifying an applicant for business and ensuring that such identity is verified on the basis of documents, data, and/or information obtained from a reliable and independent source.

Globiance is required to identify the beneficial owner of each user on its platform, taking reasonable measures to verify the identity such that Globiance is satisfied of knowing who the beneficial owner is and, in the case of a body corporates, reasonable measures are to be taken to understand its ownership and control structure.

Enhanced due diligence procedures shall be applied to those Users which pose a higher risk.

3.5 Identification of the User – Natural Person

The Company identifies the User who is a natural person and, where relevant, their representative and retains the data on the User.

3.6 Identification of the User – Legal Entity/Juristic Personnel

The Company identifies the User which is a legal entity and their representative(s) and retains the data on the User.

3.7 The Identification of the User's Beneficial Owner

The Company must identify the Beneficial Owner of the User and take measures to verify the identity of the Beneficial Owner to the extent that allows the Company to make sure that they know who the Beneficial Owner is.

The Company shall request from the User information to the User's Beneficial Owner (e.g., providing the User with an opportunity to specify their Beneficial Owner when collecting data about the User).

3.8 Political Exposed Persons' ("*PEPs*") Identification

The Company shall take measures to ascertain whether the User, the Beneficial Owner of the User, or the representative of this User is a PEP, their family member[8] or close associate,[9] or if the User has become such a person.

[8] **family member** means the spouse, the person with whom partnership has been registered (i.e.
the cohabitant), parents, brothers, sisters, children, and children's spouses,
children's cohabitants

[9] **close associate** means a natural person who, together with PEP, is a member of the same legal entity or of a body without legal personality or maintains other business relationship; or a natural person who is the only the Beneficial Owner of the legal

The Company shall request from the User information to identify if the User is a PEP, their family member or close associate (e.g., providing the User with an opportunity to specify the relevant information when collecting data about the User).

The Company shall verify the data received from the User by making inquiries in relevant databases or public databases or making inquiries or verifying data on the websites of the relevant supervisory authorities or institutions of the country in which the User has place of residence or seat. PEP must be additionally verified using international search engine (e.g., Google) and the local search engine of the User's country of origin, if any, by entering the User's name in both Latin and local alphabet with the User's date of birth.

At least the following persons are deemed to be PEPs:

i. The head of the state, the head of the government, a minister, a vice- minister or a deputy minister, a secretary of the state, a chancellor of the parliament, government, or a ministry;
ii. A member of the parliament;
iii. A member of the Supreme Court, the Constitutional Court, or any other supreme judicial authorities whose decisions are not subject to appeal;
iv. A mayor of the municipality, a head of the municipal administration;
v. A member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank;
vi. Ambassadors of foreign states, a chargé d'affaires ad interim, the head of the Lithuanian armed forces, commander of the armed forces and units, chief of defence staff or senior officer of foreign armed forces;
vii. A member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state;
viii. A member of the management or supervisory body of a municipal undertaking, a public limited company, or a private limited company whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state, and which are considered as large enterprises in terms of the Law on Financial Statements of Entities of the Republic of Lithuania;
ix. A director, a deputy director or a member of the management or supervisory body of an international intergovernmental organisation; and/or
x. A leader, a deputy leader, or a member of the management body of a political party.

The Company shall identify close associates and family members of PEPs only if their connection with PEP is known to the public or if the Company has reason to believe that such a connection exists.

Where the User who is a PEP no longer performs important public functions placed upon them, the Company shall at least within twelve (12) months consider the risks that remain related to the User and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of PEPs no longer exist in the case of the User.

3.9 Identification of the Purpose and Nature of the Business Relationship or a Transaction

The Company shall understand the purpose and nature of the establishing Business Relationship or performing transaction. Regarding the services provided, the Company may request from the User information for understanding the purpose and nature of the Business Relationship or transaction.

entity or a body without legal personality set up or operating de facto with the aim of acquiring property or another personal benefit for the PEP.

3.10 Monitoring of the Business Relationship

The Company shall monitor established Business Relationships where ongoing due diligence (hereinafter referred to as "*ODD*") measures are implemented.

The Company shall regularly **check and update the documents, data and information** collected within the course of the implementation of CDD measures and update the User's risk profile. The regularity of the checks and update must be based on the risk profile of the User.

The collected documents, data and information must also be checked if an event has occurred which indicates the need to update the collected documents, data, and information.

In the course of the **ongoing monitoring of the Business Relationship**, the Company shall monitor the transactions concluded during the Business Relationship in such a manner that the latter can determine whether the transactions to be concluded and correspond with the information previously known about the User (i.e., what the User declared upon the establishment of the Business Relationship or what has become known in the course of the Business Relationship).

The Company shall also monitor the Business Relationship to ascertain the User's activities or facts that indicate criminal activities, Money Laundering or Terrorist Financing or the relation of which to Money Laundering or Terrorist Financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question. In the course of the Business Relationship, the Company shall constantly assess the changes in the User's activities and assess whether these changes may increase the risk level associated with the User and the Business Relationship, giving rise to the need to apply EDD measures.

In the course of the ongoing monitoring of the Business Relationship, the Company applies the following measures:

i. Screening i.e., monitoring transactions in real-time;
ii. Monitoring i.e., analysing transactions later.

The objective of **screening** is to identify:

i. Suspicious and unusual transactions and transaction patterns;
ii. Transactions exceeding the provided thresholds;
iii. Politically exposed persons and circumstances regarding Sanctions.

If the User gives order for transaction which exceeds the threshold established or for transaction to the Virtual Currency wallet with high-risk score (e.g., wallets related to fraud, crime, etc.), the transaction shall be manually approved by the Company's Representative, who shall assess, before the approval, the necessity to apply any additional EDD measures (e.g., applying EDD measures, asking source and origin of funds or asking additional information regarding the transaction).

The Company **identifies the source**[10] **and origin**[11] **of the funds** used in transaction(s) if necessary. The need to identify the source and origin of funds depends on the User's previous activities as well as other known information. Thereby the identification of the source and origin of the funds used in transaction shall be performed in the following cases:

i. The transactions exceed the limits established by the Company;
ii. The transactions do not correspond to the information previously known about the User;

[10] **the source of the funds** used in the transaction is reason, explanation, and basis (legal relationship and its content) why the funds were transferred

[11] **the origin of the funds** used in the transaction is the activity by which the funds were earned or received

iii. The Company wants to or should reasonably consider it necessary to assess whether the transactions correspond to the information previously known about the User;

iv. The Company suspects that the transactions indicate criminal activities, Money Laundering or Terrorist Financing or that the relation of transactions to Money Laundering or Terrorist Financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

The Company performs reviews of the User and their allocated risk rating on an annual basis, or when the Company deems fit due to internal alerts and escalations, whichever is soonest.

3.11 Termination of the Business Relationship

The Company is prohibited to establish a Business Relationship and the established Business Relationship or transaction shall be terminated (unless it is objectively impossible to do) in case when:

i. The Company suspects Money Laundering or Terrorist Financing;

iii. It is impossible for the Company to apply the CDD measures, because the Customer does not submit the relevant data or refuses to submit them, or the submitted data gives no grounds for reassurance that the collected data are adequate;

iv. The Customer which capital consists of bearer shares or other bearer securities wants to establish the Business Relationship;

v. The Customer who is a natural person behind whom is another, actually benefiting person, wants to establish the Business Relationship (suspicion that a person acting as a front is used);

vi. The Customer's risk profile has become inappropriate with the Company's risk appetite (i.e., the Customer's risk profile level is "*prohibited*").

Globiance will retain records of the Users for at least five (5) years after the termination of the Business Relationship.

4 Sanctions

Upon the entry into force, amendment or termination of Sanctions, the Company shall verify whether the User, their Beneficial Owner or a person who is planning to have the Business Relationship or transaction with them is a subject of Sanctions.

5 Reporting Obligations

The Company has established efficient processes for the reporting of suspicious transactions and/or activities; and must suspend the transaction disregarding the amount of the transaction (except for the cases where this is objectively impossible due to the nature of the Monetary Operation or transaction, the manner of execution thereof or other circumstances) and through its MLRO must report to the FCIS on the activity or the circumstances that they identify in the course of economic activities and whereby:

i. The Company has established that the User is carrying out a suspicious transaction; and

ii. The Company knows or suspects that assets of any value are obtained directly or indirectly from criminal activity or participation in such activity.

The minimal characteristics of suspicious transactions are provided in the guidelines made by the FCIS.

The Company will retain in-depth and sufficient records of any reports of suspicious transactions and/or activities.

6 Training of Globiance Representatives

The Company ensures that its Employees, its contractors, and others participating in the business on a similar basis and who perform work tasks that are of importance for preventing the use of the Company's business for Money Laundering or Terrorist Financing (hereinafter referred to as "*Relevant Persons*") have the relevant qualifications for these work tasks.

In accordance with the requirements applicable to the Company on ensuring the suitability of Relevant Persons, the Company makes sure that such persons receive appropriate training and information on an ongoing basis to be able to fulfil the Company's obligations in compliance with the applicable legislation. It is ensured through training that such persons are knowledgeable within the area of AML/CFT to an appropriate extent considering the person's tasks and function. The training must provide, first and foremost, information on all the most contemporary money laundering and terrorist financing methods and risks arising therefrom.

This training refers to relevant parts of the content of the applicable rules and regulations, the Company's risk assessment, the Company's Guidelines and procedures and information that should facilitate such Relevant Persons detecting suspected Money Laundering and Terrorist Financing. The training is structured on the basis of the risks identified through the risk assessment policy.

The content and frequency of the training is adapted to the person's tasks and function on issues relating to AML/CFT measures. If the Guidelines is updated or amended in some way, the content and frequency of the training is adjusted appropriately.

For new Employees, the training comprises of a review of the content of the applicable rules and regulations, the Company's risk assessment policy, the Company's internal AML/CFT Policy, the Company's Transaction Monitoring Program, and other relevant procedures.

The Employees and the Management Board members receive training on an ongoing basis under the auspices of the MLRO in accordance with the following training plan:

i. Periodicity: at least once a year for the Management Board members. At least once a year for the Company's Employees and Relevant Person engaged.

ii. Scope: review of applicable rules and regulations, the Company's Guidelines, and other relevant procedures. Specific information relating to new/updated features in the applicable rules and regulations. Report and exchange of experience relating to transactions reviewed since the previous training.

In addition to the above, Relevant Persons are kept informed on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of Money Laundering and Terrorist Financing.

The training held is to be documented electronically and confirmed with the Relevant Person signature. This documentation should include the content of the training, names of participants and date of the training.

IF YOU HAVE ANY QUESTIONS OR CONCERNS, PLEASE FEEL FREE TO CONTACT OUR COMPLIANCE DEPARTMENT AT AML@GLOBIANCE.COM