AML/CFT

Compliance Program

ENTITY NAME: **PPK TECHNOLOGY GROUP LLC**

Business Identification Number: 412781002

Contact Details:
Managing Director: Peter Kritzer
Phone number +49 173 2926027 E-mail address: kritzer@ppk-tech- group.com

Head of the AML Department: Nikola Hariskov
Phone number +359887798765.
E-mail address: n.hariskov@ppk-technology-ltd.com

Authority for AML/CFT Reporting: **Financial Monitoring Service of Georgia (FMS), which operates as the country's Financial Intelligence Unit (FIU)**

Internal rules for the control and prevention of money laundering and terrorist financing compiled pursuant to Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing

Effective as 09.01.2024

.

These internal rules are prepared by **PPK TECHNOLOGY GROUP LLC** a Georgian Limited Liability Company, with Business Identification Number (BIN) 412781002 (hereinafter the "**Company**").

Subject to these rules, the Company shall apply the provisions and measures in carrying out its business as an obliged entity under the Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing. These rules of procedure are introduced to all employees whose duties include establishment of business relationships or carrying out transactions. The rules of procedure are also communicated to any third parties who will be conducting AML actions on behalf of the Company. The Company shall regularly check whether the established rules of procedure are up-to-date and establish new rules of procedure where necessary.

Internal rules for the control and prevention of money laundering and terrorist financing

Internal rules for the control and prevention of money laundering and terrorist financing

1. **Introduction**

1.1. These internal rules are prepared by **PPK Technology Group LLC** a Georgian Limited Liability Company, with Business Identification Number (BIN) 412781002 (hereinafter the "**Company**").

1.2. The Internal rules for the control and prevention of money laundering and terrorist financing are prepared to comply with the Law of Georgia on Facilitating the Prevention of Money Laundering and Terrorism Financing ("**Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing"**) and the Law of Georgia on Combating Terrorism (together referred to as the "**Georgian AML/CFT Legislation**")

2. Aim of the internal rules and their elements

2.1. The aim of these internal rules is to ensure the proper identification and verification of customers or persons participating in business relations and/or transactions, as well as ongoing monitoring of business relationships, including transactions carried out during business relationships, regular verification of data used for identification, update of relevant documents, data or information and, when necessary, identification of the source and origin of funds used in transactions.

2.2. Customer due diligence is one of the main tools for ensuring the implementation of legislationaimed at preventing money laundering and terrorist financing and at applying sound business practices. Customer due diligence comprises a set of activities and practices arising from the organizational and functional structure of the Company and described in internal procedures, which have been approved by the directing bodies of the Company and the implementation of which is subject to control systems established and applied by internal control rules.

2.3. The purpose of customer due diligence is to prevent the use of assets and property obtained in a criminal manner in the economic activities of credit institutions and financial institutions and in the services provided by them whose goal is to prevent the exploitation of the financial system and economic space of Georgia for money laundering and terrorist financing. Customer due diligence is aimed, first and foremost, at applying the Know-Your-Customer principle, under which a customer shall be identified and the appropriateness of transactions shall be assessed based on the customer's principal business and prior pattern of payments. In addition, customer due diligence serves to identify unusual circumstances in the operations of a customer or circumstances whereby an employee of the Company has reason to suspect money laundering or terrorist financing.

2.4. Customer due diligence ensures the application of adequate risk management measures in order to ensure constant monitoring of customers and their transactions and the gathering and analysis of relevant information. Upon applying the customer due diligence measures, the Company will follow the principles compatible with its business strategy and, based on prior risk analysis and depending on the nature of the customer's business relationships, apply customer due diligence to a different extent.

2.5. Upon establishing a business relationship, the Company will identify the person (and verify their right of representation- if applicable) based on reliable sources, and in case of company, identify the beneficial owner and the control structure, as well as identify the nature and purpose of possible transactions, including, if necessary, the source and origin of the funds involved in the transactions. Appropriate verification measures will be carried out.

2.6. Customer due diligence measures are appropriate and with suitable scope if they make it possible to identify transactions aimed at money laundering and terrorist financing and identify suspicious and unusual transactions as well as transactions that do not have a reasonable financial purpose or if they at least contribute to the attainment of these goals.

2.7. The first requirement for the measures of prevention of money laundering and terrorist financing is that the Company does not enter into transactions or establish relationships with anonymous or unidentified persons. Legislation requires that the Company waives a transaction or the establishment of a business relationship if a person fails to provide sufficient information to identify the person or about the purpose of the transactions or if the operations of the person involve a higher risk of money laundering or terrorist financing. Also, legislation requires the Company to terminate a continuing contract without advance notification term if the person fails to submit sufficient information for application of customer due diligence measures. The Company ensures that information concerning a customer (incl. gathered documents and details) is up to date. In the event of customers or business relationships falling in the high-risk category, the existing information will be verified more frequently than in the event of other customers/business relationships. The respective data shall be preserved in writing or in a form that can be reproduced in writing and made available to all relevant employees who need it to perform their employment duties (managing director, account managers, risk managers and internal auditors).

2.8. The principles and instructions provided for in the customer due diligence measures are set out in this document. Independent control mechanisms are established over adherence to these procedures and the relevant training of employees are ensured.

2.9. "Money laundering" - when committed intentionally is:

2.9.1. the conversion or transfer of property with knowledge that such property is derived from a criminal activity or from an act of participation in such an activity, in order to conceal or disguise the illegal origin of the property or to assist a person involved in the commission of such an act in order to avoid the legal consequences of that person's act;

2.9.2. the concealment or disguise of the nature, source, location, disposition, movement, rights in respect of or ownership of property with knowledge that such property is derived from criminal activity or from an act of participation in such activity

2.9.3. the acquisition, possession or use of property with knowledge at the time of receipt that such property was acquired from criminal activity or from an act of participation in such activity;

2.9.4. participation in an association with a view to committing, attempting to commit, or aiding, abetting, facilitating or counselling the commission of any of the acts referred to in paragraphs 2.9.1, 2.9.2 and 2.9.3.

2.9.5. Money laundering shall also occur where the activities from which the property referred to in 2.9.1 to 2.9.4 was acquired were carried out in the territory of another EU Member State or in the territory of a third country.

2.9.6. 'Terrorist financing' means the direct or indirect, unlawful and intentional provision and/or collection of funds and other financial assets or economic resources, and/or the provision of financial services, with the intention that they will be used, or with the knowledge that they will be used, in whole or in part, to commit terrorism, to finance terrorism, to recruit or train individuals or groups of individuals to commit terrorism, to leave or enter a country, or to unlawfully reside in a country, for the purpose of participating in terrorism.

3. Applicability of the Internal Rules

3.1. These Internal rules for the control and prevention of money laundering and terrorist financing include:

3.1.1. requirements for the identification and verification as well as methods for the collection of relevant data, including requirements for the data and documents on which the identification is based;

3.1.2. procedures for the identification of the purpose and intended nature of business relationships and transactions prior to the conclusion of such transactions or long-term contracts, and procedures for ongoing monitoring of business relationships;

3.1.3. a description of high-risk transactions and criteria for identification of high -risk clients;

3.1.4. procedures for updating the data and documents used for identification and verification;

3.1.5. other issues arising from the aim and scope of these internal rules.

4. General Obligatory Identification Rules

4.1. These internal rules require the identification and verification in case of:

4.1.1. establishing business relationships with new customers of the Company;

4.1.2. conducting transactions with persons with whom the relationship between the person and the Company will not constitute a business relationship and whereby the amount transferred is equal to or exceeds EUR 10 000, or an equal amount in any other currency, whether in one-time transfer or several related payments;

4.1.3. suspicion of money laundering, terrorist financing, or the presence of funds of criminal origin, irrespective of the transaction value or operation. doubt regarding the accuracy, timeliness, or adequacy of the credentials provided for customers and their beneficial owners, or upon receiving information of a change in such credentials, irrespective of the transaction value or operation.

5. Organisation structure and Internal Control

5.1. The managing director of the Company shall regularly (not less than once a quarter) review the efficiency of the internal procedures implemented for the purpose of complying with the Georgian AML/CFT Legislation and ensure internal control over application of the internal AML procedures. In addition, at the end of each calendar year, the managing director shall also conduct an annual internal control review. When conducting annual

internal control over the internal AML procedures, the managing director shall complete the internal control checklist, which is Schedule 2 to these rules.

5.2. The Company shall establish a dedicated department (the „**AML Department** ") responsible for developing, proposing for approval, and implementing training programs for employees regarding the application of the Georgian AML/CFT Legislation and other applicable acts and the Company's internal AML policies. Additionally, this department should organize, oversee, and supervise activities related to (where applicable):

5.2.1. The collection, processing, storage, and disclosure of information pertaining to specific operations or transactions.

5.2.2. Gathering evidence concerning the ownership of the property intended for transfer.

5.2.3. Requesting information regarding the origin of funds or valuables involved in transactions or operations, as well as the source of assets (where applicable).

5.2.4. Compiling information on customers and maintaining accurate and detailed records of their cash or valuables transactions. Providing the information gathered under points 5.2.1 - 5.2.4 to the Financial Intelligence Unit of the State Security Service of Georgia ("**FIU of FMS**"), following the conditions and procedures outlined in the Georgian AML/CFT Legislation. The AML Department shall provide information to the managing director of the Company who will perform the reporting obligation on behalf of the Company. However, all employees of the Company will be duly informed by the managing director that they may report directly to the authorities if they deem it appropriate.

5.3. The AML Department shall be overseen by an officer of the Company, occupying a senior management role, appointed by the managing director of the Company. The head of the AML Department shall ensure the application of customer due diligence measures based on the provisions in legislation and the Company's AML policies and documents and take into account that the measures applied are adequate, correspond to the operating profile of the Company and comply with the customer, nature and scope of the transactions and the related risks of money laundering or terrorist financing. The head of the AML Department shall regularly report to the managing director of the Company, as the internal control over AML compliance falls within the managing director's purview. The internal control is exercised by the managing director of the company who shall remain responsible for the implementation of these rules, which control includes: periodically informing the company's employees involved in the implementation of AML requirements of the possibility to directly inform the FMS in case of suspicion and/or knowledge of the presence of funds of criminal origin or money laundering or under the Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing; taking a decision to carry out a risk assessment where there is a risk of the company's activities being used for money laundering or terrorist financing; monitoring the terms and conditions for reviewing and updating the risk assessment; the storage of information collected under the Georgian AML/CFT Law and its implementing acts. The managing director shall perform the notification obligations of the Company and also will review and confirm the business relationships with PEPs or other high – risk clients. The managing director shall periodically review the files of the customers which shall be collected and stored by the AML Department of the Company.

5.4. The managing director of the Company ensures that the resources allocated to comply with the AML Acts are sufficient and that the employees directly involved in the fulfilment of the requirements of the AML Acts are fully aware of the requirements therein. The managing director of the Company shall conduct an annual review of the Company's AML procedures

and rules to ensure their compliance with AML requirements and their efficiency. If necessary, the managing director may seek assistance from external advisors and specialists in the field. The date of the most recent review by the managing director of the Company is indicated on the last page of these internal rules.

5.5. Each executive and employee directly involved in the implementation of the AML Acts shall have professional skills that allow them to fully and with sufficient accuracy adhere to the provisions of legislation in accordance with the scope of their responsibilities and they shall have completed the respective training or been otherwise instructed therein by the Company.

5.6. The Company shall mitigate and prevent conflicts of interests with internal rules, whereby the grounds of remuneration of executives and employees encourage them not to disregard or not to deviate from provisions of law.

5.7. Customer due diligence is part of the overall risk management framework where a clear distinction shall be made between the application of customer due diligence measures applied in business relationships and the application of measures for prevention of money laundering and terrorist financing in the Company's own operations.

5.8. The Company shall provide contractual partners (in the event of outsourcing) and all relevant staff, including staff whose duties include the establishment of business relationships and/or the execution of transactions, management of customer relationships, with regular training in and notification about the nature of the risks of money laundering and terrorist financing and any new trends in the field. First and foremost, staff shall be kept informed about the requirements governing the prevention of money laundering and terrorist financing with respect to the application of customer due diligence measures and reporting on suspected money laundering.

5.9. The managing director of the Company ensures that contractual partners (in the event of outsourcing) apply AML measures (including identification, verification, and risk assessment) on behalf of the Company in compliance with Georgian AML/CFT Legislation and other relevant legislation. Additionally, these partners commit to ensuring their staff is well-trained and informed about AML requirements

5.10. The Company shall ensure that the customer due diligence measures and data collection and preservation requirements applied in its third-country representations, branches or majority held subsidiaries (if any) comply with the Acts and the requirements set out in other acts and guidelines.

5.11. The Company will utilize at least two of the procedures below in order to assess the professional competence and reliability of the employees' part of the AML Department:

5.11.1. Competency-based Interviews: Conduct interviews focusing on assessing candidates' knowledge of AML regulations, understanding of risk management principles, and experience in conducting AML investigations.

5.11.2. Background Checks: Perform thorough background checks, which may include criminal record checks, credit checks, and verification of employment history, to ensure the integrity and reliability of candidates.

5.11.3. Reference Checks: Contact previous employers and professional references to verify candidates' qualifications, experience, and reputation in the field of AML compliance.

5.11.4. Skills Assessment: Administer assessments or tests to evaluate candidates' analytical skills, attention to detail, and ability to apply AML principles to real-world scenarios.

5.11.5. Behavioural Assessments: Use behavioural assessment tools to gauge candidates' suitability for roles requiring ethical decision- making, integrity, and adherence to compliance standards.

5.12. Rules for Conducting Checks and Training of the employees part of the AML Department:

5.12.1. Regular Monitoring and Review: Implement regular reviews and monitoring of employees' performance to ensure ongoing compliance with AML regulations and internal policies.

5.12.2. Continuous Training Programs: Provide regular training sessions covering updates to AML regulations, emerging trends in money laundering and terrorist financing, and best practices in AML compliance.

5.12.3. Scenario-based Training: Conduct scenario-based training exercises to simulate potential AML risks and challenges employees may encounter in their roles, and assess their ability to respond appropriately.

5.12.4. Certifications and Professional Development: Encourage employees to obtain relevant certifications such as CAMS (Certified Anti-Money Laundering Specialist) and provide opportunities for professional development to enhance their skills and knowledge in AML compliance.

5.12.5. Supervision and Oversight: Assign experienced supervisors or mentors to provide guidance and oversight to junior staff members, ensuring they adhere to established procedures and maintain high standards of professional conduct.

5.13. By implementing these procedures and rules, the Company can ensure it has competent and reliable employees in their AML departments who are well- equipped to identify and mitigate money laundering and terrorist financing risks effectively.

5.14. The Company may apply the procedures above to other employees whose duties, as determined by the Company or by the Head of the AML Department may relate to the control and prevention of money laundering and terrorist financing.

6. Economic or professional activities via agents and outsourcing

6.1. The Company has the right, taking into account the special requirements and restrictions provided by law, to use the services of a third party under a contract the subject of which is the continuing performance of activities and continued taking of steps required for the provision of (a) service(s) by the Company to its customers and that would normally be performed and taken by the Company itself. For the purposes of this section, third parties include, for instance, agents, subcontractors and other persons to whom the Company transfers the activities relating to the provision of the services provided as a rule by the Company in its economic activities.

6.2. The Company also has the right, subject to the special requirements and restrictions stipulated by law, to engage the services of a third party through a contract that involves outsourcing AML activities typically conducted by the Company itself. The Company shall choose the third party in order to ensure the ability of the person to fulfil the requirements provided for in the Georgian AML/CFT Legislation and to ensure the reliability and the required qualifications of such a person.

6.3. The third parties specified in section 6.1 and 6.2 are subject to all of the requirements provided by law for the prevention of money laundering and terrorist financing regarding outsourced activities. The Company who outsourced its activities is liable for infringement of the requirements.

6.4. Upon outsourcing an activity (activities), the Company shall ensure that the third party has the knowledge and skills required, above all, for the identification of situations of a suspicious and unusual nature and is able to meet all of the requirements for the prevention of money laundering and terrorist financing provided by law. To comply with the provisions in this section, the Company shall ensure the notification of the executives of the third party of the relevant requirements and the training of its staff in the prevention of money laundering and terrorist financing.

6.5. Upon outsourcing an activity to third parties, the Company shall ensure that any documents and information collected for the fulfilment of requirements arising from legislation are preserved in accordance with the procedure established in the AM Acts and any legislation issued on the basis thereof. The contract shall ensure that relevant information is handed over to the Company and that the relevant information and documents are archived in accordance with its rules of procedure. If any pertinent AML information and documents are stored by a third party on behalf of the Company, the outsourcing contract must stipulate that the Company shall have permanent and unrestricted access to this information and these documents. The Company should be able to download any information and documents without limitations at any given time. Moreover, the third party must be obligated to transfer all such stored information and documents to the Company in the event of the termination of the outsourcing contract.

6.6. The outsourcing contract shall specify the rights and duties of the Company upon reviewing compliance by the third party with the requirements provided by law. The outsourcing of economic activities or other activities (including AML measures) to a third party shall not impede state supervision over the Company and the latter shall, under contract, grant competent authorities access to the third party for supervisory purposes to whom the Company has outsourced its duties, tasks or functions.

6.7. Whilst services are provided by third parties, situations where the application of customer due diligence measures to the required extent is possible to an insufficient degree or entirely impossible shall be avoided. A third party shall be able to fully apply the required customer due diligence measures, thereby being able to notify the contact person of the Company immediately and to decline a transaction. The Company shall, under contract, ensure its right to terminate the contract with the third party if the latter fails to perform its contractual duties or obligations or performs the unduly.

7. Appointment of a Head of the AML Department

7.1. The managing director of the Company shall appoint a Head of the AML Department.

7.2. The position of a Head of the AML Department within the organisational structure of the Company shall allow for the performance of the requirements provided by law for the prevention of money laundering and terrorist financing. Upon establishment of the Head of the AML Department position, the Head of the AML Department shall be made directly accountable to the managing director of the Company and made as independent of business processes as possible.The internal control of the Company's AML compliance will remain with the managing director.

7.3. The head's independence from business processes does not mean that the officer is prohibited to advise or train colleagues for the purpose of ensuring the compliance of the actions of the executives and employees with the requirements of the AML Acts.

7.4. The professional qualifications and skills of the Head of the AML Department shall meet the requirements established in the AML Acts and the Head's professional and business reputation shall be impeccable.

7.5. The functions of the Head of the AML Department, among others, are as follows:

7.5.1. organisation of collection and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the Company (collection of information means collection of any and all suspicious or unusual notices received from the employees, contractual partners and agents of the Company, and systemising and analysis of the information contained in them);

7.5.2. reporting to the managing director in the event of suspicion of money laundering or terrorist financing;

7.5.3. periodic submission of written statements on implementation of the rules of procedure to the managing director of the Company; and

7.5.4. performance of other obligations related to the fulfilment of the requirements of the AML Acts by the Company.

7.6. The Head shall have access to the information forming the basis or prerequisite for establishing a business relationship, including any information, data or documents reflecting the identity and business activity of the customer.

7.7. The managing director shall periodically review the performance of the AML Department and the Head of the AML Department as well as the files of the clients and the internal AML documentation and procedures of the Company.

8. Risk-based approach

8.1. The Company shall recognise, assess and understand money laundering and terrorist financing risks in its own activities and in the activities of its customers and take measures to mitigate the risks. The applicable measures shall correspond to the identified risk level.

8.2. In the event of the risk- based approach, the Company shall assess the probability of the realisation of risks and what the consequences of their realisation are. Upon assessment of probability, the chance of an increase in the threat and the possibility of occurrence of the respective circumstances shall be taken into account, e.g. the possible threats that may influence the activities of the customer and the service provider shall be taken into account.

8.3. The Company shall take all customer due diligence measures. Once customers are identified and their identification is duly verified, the Company shall also make the respective sanctions and PEP checks. Then, once the Company has obtained all the necessary information and documents about a customer, it will assess the customer's risk profile based on the criteria, risk categories and risk factors outlined in a separate document referred to as "RISK ASSESSMENT pursuant to the articles of the Georgian AML/CFT Law of PPK Technology Group LLC " (the "**Risk Assessment Document**"), which forms an integral part of the Company's internal AML procedures.

8.4. Upon identifying and substantiating the risk levels of a customer or a person participating in a transaction, the Company shall take into account, the following risk categories:

8.4.1. In identifying the risks associated with the customer and its beneficial owner, the Company considers risk factors related to the business or professional activities of the customer and the beneficial owner, the reputation of both the customer and the

beneficial owner, and the type and behaviour of both the customer and the beneficial owner. :

8.4.2. In identifying the risks associated with the services the Company offers to customers, the Company considers risk factors related to the level of transparency of the service; the complexity of the pertinent service, transaction, or operation; and the value or magnitude of the relevant product, service, transaction, or operation. :

8.4.3. In identifying the risks associated with the countries and geographic areas in which the customer or the customer's beneficial owner is incorporated, domiciled, resides or carries on its business or profession or with which it is otherwise associated, the Company considers risk factors related to the effectiveness of the systems for the prevention and deterrence of money laundering and terrorist financing in the country or geographical area concerned; the level of risk of terrorist financing in the country or geographical area concerned; the level of transparency and compliance with tax legislation in the country or geographical area concerned; and the level of money laundering predicate criminal activity in the country or geographical area concerned.

8.4.4. In identifying risks associated with delivery mechanisms, the Company considers risk factors related to the extent to which the business relationship is established and the transactions and dealings are privately conducted and the terms on which they are conducted; and the extent to which the Company uses agents or representatives and the manner in which these relationships are arranged.

8.5. Taking account of the aforementioned risk categories, the Company shall consider appropriate risk factors outlined in the Risk Assessment Document in order to determine the risk level of the person or customer participating in a transaction/business relationship, e.g. whether the customer's money laundering or terrorist financing risk level is low, normal or high or whether it corresponds to other risk level qualifications determined and used by the Company

8.6. Certain guidelines in the event of specifying a low level of risk:

8.6.1. The customer's risk level is generally considered low if there is no risk factor of impact in any risk category and it can therefore be claimed that the customer and its operations demonstrate elements that do not differ from those of an ordinary and transparent person; thereby there is no reason to suspect that the customer's operations may increase the probability of money laundering and terrorist financing.

8.6.2. In a situation where the application of the required measures of customer due diligence arises from legislation and information about the customer and its beneficial owner is publicly available, where the operations and transactions of the person are in line with its day- to-day economic activities and do not differ from the payment conventions and conduct of other similar customers or where the transaction is subject to quantitative or other absolute restrictions, the Company may deem the customer's estimated money laundering or terrorist financing risk to be lower. In a situation where at least one risk category can be qualified as high, the risk level of money laundering or terrorist financing cannot usually be low. Equally, a low risk does not necessarily mean that the customer's operations cannot be associated with money laundering or terrorist financing at all.

8.7. Certain guidelines in the event of specifying a high level of risk

8.7.1. The customer's risk level is usually high, when assessing the risk categories on the whole it seems that the customer's operations are not ordinary or transparent; there are risk factors of impact due to which it may be presumed that the likelihood of money laundering or terrorist financing is high or considerably higher. The customer's risk level is also high if a risk factor as such calls for this. A high risk does not necessarily mean that the customer is laundering money or financing terrorists.

8.8. If the Company feels that the risk level of a customer or a person participating in a transaction is high, the Company shall apply customer due diligence measures pursuant to the enhanced procedure in order to adequately manage the respective risks. Thereby enhanced due diligence measures shall be applied in accordance with article 18 of the Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing

8.9. The Company shall document the determination of the risk level, update it and make the data available to competent authorities, if necessary.

8.10. Once the relationship has been established, according to the risk profile of the client the Company shall perform periodic due diligence at a predetermined minimum interval as follows: for low risk – once every 2 years, for medium risk – once every 1 year and for high risk – once every 6 months. The Company may also update customer records more frequently.

8.11. In relation to the timeliness of the information collected, additional identification and verification actions are performed under the following circumstances:

8.11.1. Doubts arise regarding the accuracy, timeliness, or adequacy of the identification data provided for customers and their beneficial owners.

8.11.2. Information is received indicating a material change in the submitted identification data of customers and their beneficial owners. This includes changes in registration, ultimate ownership of the customer, the customer's business activity, or the identification of a prominent political figure or related person.

8.11.3. There is a change in the country or sector risk level.

8.11.4. A material change is identified in the type, value, volume, frequency, size, or manner of transactions and operations, or any other change that could affect the identified risk level.

8.11.5. Suspicion arises of money laundering, terrorist financing, or the presence of funds of criminal origin, regardless of the value of the transaction or the risk profile of the customer

9. Establishment of business relationships

9.1. The Company shall identify each customer upon establishment of a business relationship and upon making a random transaction if the value of the transaction is equal to or exceeds EUR 10000 or in the other cases specified in Art. 4.1 above.

9.2. The business relationships between Company and customers are regulated by contracts made in writing, in a form that can be reproduced in writing or electronically.

9.3. The prerequisite for the establishment of a business relationship is an explicit and recorded certification by the customer that it will fulfil the conditions established by the Company for the establishment of the business relationship and execution of transactions (including via the conclusion of an agreement).

9.4. Upon the establishment of a business relationship, the customer or its representative and the representative of the Company may be in the same place. This means that a potential customer or its representative has a direct contact with the representative of the Company. A direct contact calls for direct communication between the representative of the Company and the customer for the purpose of assessing the customer's true will. Thereby it is possible to specify the customer's risk level more accurately with the help of what is experienced in the course of the direct contact. The contact may occur outside the principal place of business of the Company if, in the course thereof, at least the same customer due diligence measures are performed as in ordinary instances.

9.5. A business relationship may be established without a direct contact (i.e. without being in the same place as the customer), though electronic means.

9.6. When establishing a business relationship without a direct contact, the Company must employ at least two of the following methods to verify the data submitted for customer identification:

9.6.1. collection of one or more of the following docs confirming the collected identification details:

9.6.1.1. other ID docs;

9.6.1.2. a copy of a document issued by a credit institution in BG/EU (to contain names, address and SSN/other identification number);

9.6.1.3. a document certifying utility billing or payment (to contain an address matching that of the ID doc);

9.6.1.4. collection of a notarized document (e.g. power of attorney);

9.6.1.5. electronic methods of identification, thereby verifying the validity of the electronic signature and certificate;

9.6.1.6. utilizing technical means to authenticate submitted documents;

9.6.1.7. confirming identification through another individual obligated to apply AML measures as per the Georgian AML/CFT Law, or by an individual obligated to apply AML measures in an EU Member State or third country whose legislation aligns with the requirements of the Georgian AML/CFT Law;

9.6.1.8. making inquiries in publicly accessible domestic and foreign official commercial, company, corporate, and other registers

9.6.1.9. consulting electronic websites and databases of domestic and foreign competent state and other authorities publicly accessible for validating the authenticity of identity documents and other personal documents, or verifying other collected data during identification;.

9.6.1.10. mandating that the initial payment to be conducted through an account opened in the customer's name with a credit institution from Georgia, an EU Member State, or a bank from a third country whose legislation aligns with the requirements of the Georgian AML/CFT Law;

9.6.1.11. using traditional methods of communication, such as sending a letter to the address on the ID, having a telephone conversation, exchanging electronic messages by e-mail specified by the customer, etc;

9.6.1.12. conducting a conversation with the customer via video conference by a trained employee of the Company or the external provider, if such services are used;

9.7. When establishing a business relationship without a direct contact, the identification and verification rules must be compliant with the following special procedures:

9.7.1. The Company is obliged to implement internal control systems containing measures aimed at limiting the possibility of:

9.7.1.1. providing false identification data by the identifiable natural person;

9.7.1.2. using foreign identification data and identity documents;

9.7.1.3. providing identification and identity documents under threat, duress, or similar circumstances.

9.7.2. The systems should incorporate measures to ensure that:

9.7.2.1. changes or failures of security features in identity documents are identified and located;

9.7.2.2. security features of identity documents are compared with pre-established security features in an internal specimen database or reliable external specimen databases;

9.7.2.3. the location of the identifiable person is established.

9.7.2.4. the reasons for a customer from another country or jurisdiction using the services of the Company are clarified;

9.7.2.5. Imposing restrictions on accepted documents by fulfilling at least two of the following criteria:

9.7.2.5.1. accepting solely official identity documents with security features;

9.7.2.5.2. accepting solely official identity documents containing biometric data;

9.7.2.5.3. mandating the use of a qualified electronic signature;

9.8. The purpose of application of customer due diligence measures is not merely the identification of the customer. Sufficient application of customer due diligence measures means a situation where, among other things, the customer's risk level is determined.

9.9. In the event of extraordinary termination of a business relationship on grounds resulting from the Georgian AML/CFT Law, different time limits for provision of services (above all, restrictions on making transactions) and termination of a business relationship (long-term contract) may be established. In the event of extraordinary termination of a business relationship, the Company shall set out a procedure for the subsequent use of the customer's assets (e.g. allowing for a payment to be made to the account of a credit institution in another contracting state of the European Economic Area or in an equivalent third country) in accordance with the requirements of the AML Acts. No disbursements in cash are allowed.

10. Customer identification

10.1. The Know-Your-Customer (KYC) principle shall be followed upon customer identification. This principle means that the operating profile, purpose of operation, beneficial owner of the person as a potential customer and, if necessary, the source and origin of the funds used in the transactions/business relationships and other similar information essential for the establishment of a business relationship shall be identified in addition to the customer.

10.2. The Company shall identify the customer, its representatives and proxies and the beneficial owner (in case of companies) within a reasonable period of time prior to the commencement of the steps for entry into a long-term contract.

10.3. Any information and documents concerning establishment of identity shall be preserved in a manner making it possible to respond fully and without unreasonable delay to relevant enquiries from the FIU, investigating body or court. To this end, the Company shall set up a system enabling, in view of the characteristics of its activities, the prompt retrieval from databases and documents of the required information or documents concerning identification of the customer or person participating in the transaction.

10.4. Identification and verification of persons upon the establishment of a business relationship are mandatory in the event of the use Company's services, regardless of whether a long-term contract is entered into with the person participating in the transaction or not, thereby taking into account the exceptions arising from the Georgian AML/CFT Law.

11. General requirements regarding identification of individual upon establishment of business relationship

11.1. The establishment and verification of the identity of an individual (a natural person) shall be carried out, as a general rule, in one step on the basis of an identity document.

11.2. An individual shall be identified based on an identity document in accordance with the Georgian AML/CFT Law. A document submitted to the Company for identification shall be assessed as follows:

11.2.1. validity of the document based on the date of expiry;

11.2.2. the outward likeness and age of the person match the appearance of the person represented on the document; the personal identification code matches the gender and age of the submitter (if applicable);

11.2.3. with respect to the information contained in codes assigned to individuals of a foreign country, foreign missions or other competent authorities shall be consulted in the case of doubt as to the authenticity of the document or identity.

11.3. A copy of the page containing personal data and photo shall be made of the identity document in accordance with the Georgian AML/CFT Law. The copy made of the document shall be of a quality allowing the details included on it to be read legibly.

11.4. The following details must be available in the collected ID document (and respectively recorded by the AML Department of the Company):

11.4.1. Names;

11.4.2. Date and place of birth;

11.4.3. Official personal ID number or another unique element for establishing identity contained in an official identity document, whose validity has not expired and which includes a photograph of the customer;

11.4.4. Any citizenship held by the person;

11.4.5. Country of permanent residence and address (a post office box number is not sufficient).

11.5. If the official identity document does not contain all the data mentioned above, then the missing data shall be obtained by presenting additional official identity documents or other valid official identity documents with a client photograph, and a copy shall be taken.

11.6. Such "*other valid official identity documents*" may be: driving license, residence documents or a registration card of an alien seeking or granted protection.

11.7. When no other alternatives are available, data collection may be carried out by presenting alternative official documents or documents from a reputable and independent source. In such cases, the Company may register the occupation and address of the individual in the course of identification of identity on the basis of a utility bill or other similar document provided by the person. As for the place of residence, not the address recorded in the population register or another similar register but the permanent or primary place of residence of the person is important. If it is difficult to determine a person's permanent place of residence (e.g. the person's place of residence cannot be identified or there are several of them), the person's habitual residence shall be identified. A post office box number or poste restante address cannot be considered a habitual residence.

11.8. Upon identifying the permanent place of residence or habitual residence of an individual, it is also necessary to register the address of the place to which the Company can send notices on paper.

11.9. In addition to the address of the place of residence of the individual, the Company may record other contact details, including an e-mail address, phone number, Facebook account, Skype account and other similar data, and agree on the submission of information via these telecommunications channels.

11.10. If the provided ID documents do not include any of the other mandatory details specified in Article 11.4 above, then the latter may also be collected from the documents specified in Article 11.7.

11.11. Determining field of activity, job or profession gives the Company the opportunity to assess whether the business relationship or transactions are in compliance with the customer's normal participation in commerce and whether the business relationship or transaction has a clear economic reason. For the purpose of prevention of the movement of illegally acquired funds, the customer's operating profile needs to be identified upon establishment of a business relationship. To this end, the customer's main fields of work and activity and possible payment habits need to be identified. This will be achieved through the utilization of documents, data, or information from a reliable and independent source, completion of a questionnaire, or other suitable methods.

11.12. Upon identifying an individual, it shall be identified whether the person is a politically exposed person or related to such person.

11.13. Upon identifying an individual, it shall be identified whether the person is:

11.13.1. from a country which does not comply or does not fully comply with the international standards on combating money laundering and financing of terrorism;

11.13.2. or belongs to any of the following categories/lists:

11.13.2.1. legal persons, groups and organizations upon which sanctions for terrorism or its financing have been imposed with a Regulation of the European Parliament or of the Council;

11.13.2.2. natural or legal persons, groups and organizations indicated by the United Nations Security Council as ones that are connected to terrorism or its financing or upon which sanctions for terrorism or its financing have been imposed with a Resolution of the United Nations Security Council;

11.13.2.3. natural and legal persons, groups and organizations which are included in a List of the natural and legal persons, groups and organizations upon which the measures under the Measures against Financing of Terrorism Act adopted with Decision No. 265 of 2003 of the Council of Ministers and amended with decision No. 445 of 3 June 2016 are applied.

11.14. Enhanced due diligence measures shall be undertaken towards customers who are identified to be politically exposed persons or related to such persons.

11.15. The Company will not enter into relationship with customers who belong to any of the lists in 11.13.2 above or who are from countries which does not comply or does not fully comply with the international standards on combating money laundering and financing of terrorism.

11.16. Any details and references required to identify a person shall be verified on the basis of at least two of the following source/methods:

11.16.1. collection of one or more of the following docs confirming the collected identification details:

11.16.1.1. other ID docs;

11.16.1.2. a copy of a document issued by a credit institution in GE (to contain names, address or identification number);

11.16.1.3. a document certifying utility billing or payment (to contain an address matching that of the ID doc);

11.16.1.4. collection of a notarized document (e.g. power of attorney);

11.16.1.5. confirming identification through another individual obligated to apply AML measures as per the Georgian AML/CFT Law (a bank, a notary, an attorney-at - law, etc.);

11.16.1.6. consulting e- websites and databases of domestic and foreign competent authorities publicly accessible for validating the authenticity of identity documents and other personal documents;

11.16.1.7. mandating that the initial payment for the operation or transaction be conducted through an account opened in the customer's name with a credit institution from Georgia, an EU Member State, or a bank from a third country whose legislation aligns with the requirements of the Georgian AML laws;

11.16.1.8. utilizing technical means to authenticate submitted documents.

11.16.1.9. using traditional methods of communication, such as sending a letter to the address on the ID, having a telephone conversation, exchanging electronic messages by e-mail specified by the customer, etc;

11.16.1.10. conducting a conversation with the customer via video

11.17. In the event of persons whose active legal capacity is limited (incl. minors), the Company shall also follow the identification procedure. Upon identification of the personal data of minors, the Company shall, in addition to the instructions given in this document and provisions of the Georgian AML/CFT Law, follow the provisions of the General Part of the Civil Code Act and the Family Act. In addition to the personal data of a person of restricted active legal capacity, the personal data of the legal representative (parent(s) or guardian(s)) shall be verified.

11.18. The Company will compile an identification file (identification card) for each customer, encompassing all client-related information (including identification data such as names, address, ID number, etc., details of the utilized ID or other documents such as type of document, registration numbers, date of issuance, etc., and sources utilized for identification and verification purposes such as databases, websites, etc.).

11.19. The date and time of the identification and verification operations, along with the name and title of the person conducting them, should be recorded in the identification cards of the customers.

11.20. The Company shall regularly update the customer's personal data and operating profile, ensuring that they are up to date and based on the customer's risk level.

11.21. The Company may opt to outsource the identification and verification process to a third party under a contractual agreement. In such instances, the third party will be responsible for identifying and verifying the Company's customers in accordance with the procedures outlined in this document and the requirements of the Georgian AML/CFT Law and the other applicable legal acts. The Company's AML Department will oversee the customer identification and verification processes, ensuring compliance. If deemed necessary, the AML Department will implement additional measures for identification and verification purposes.

11.22. When third parties are entrusted with the task of identification and verification, they will generate client reports encompassing all information and documents pertaining to the identified customers of the Company. These reports must include details regarding the date and time of identification and be readily available and accessible to the AML Department at all times. The AML Department will download and retain all pertinent information and documents collected by the third party.

11.23. Even in cases where identification and verification are outsourced to a third party under a contractual agreement, the AML Department will compile customer files as outlined in Article 11.21. These files will include all information and documents collected by the third party on behalf of the Company, as well as any additional documents and information gathered by the AML Department as per Article 11.23. Additionally, the files will record the date and time of identification, the date and time of AML Department review, the date and time of any additional actions undertaken by the AML Department, and the names of the AML Department officers involved.

12. Politically Exposed Persons (PEP's)

12.1. The Company shall establish the following procedures in order to decide whether a potential customer or its beneficial owner and/or legal representative (in case of legal entities) is a politically exposed person (PEP) or a close associate of a PEP as per the meaning of the FATF

12.2. The AML Department is responsible for collecting declarations under FATF from each customer. In the case of customers who are legal entities, the declarations must be obtained from the legal representatives, Ultimate Owners (UBOs), and proxies (if applicable). These declarations are required to be signed in the presence of an AML Department officer or electronically using an e- signature.

12.3. Checks will be conducted on external databases and PEP lists.

12.4. The Company has the option to outsource the checks outlined in Article 12.1.2 to a third party through a contractual agreement. In these instances, the AML Department will assess the results of the PEP checks conducted by the third party and appropriately document them in the customers' identification files. The Company may also outsource the collection of the declaration under the Georgian AML/CFT Law to a third party through a contractual agreement.

12.5. The Company apply enhanced due diligence measures to customers who are identified to be (currently or during the last 12 months) PEPs or associated to PEPs.

12.6. Politically exposed persons within the meaning of para. 1 are individuals who perform or have been entrusted with the following prominent public functions:

12.6.1. heads of state, heads of government, ministers and deputy ministers or assistant ministers;

12.6.2. members of parliament or of other legislative bodies;

12.6.3. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to appeal, except in exceptional circumstances;

12.6.4. members of a court of auditors;

12.6.5. members of the managing bodies of central banks;

12.6.6. ambassadors and chargés d'affaires;

12.6.7. high-ranking officers in the armed forces;

12.6.8. members of the administrative, management or supervisory bodies of State-owned enterprises and solely owned by the State commercial entities;

12.6.9. municipality mayors and deputy mayors, district mayors and deputy mayors and chairpersons of a municipal council;

12.6.10. members of the managing bodies of political parties;

12.6.11. heads and deputy heads of international organisations, members of the management or supervisory bodies of international organisations or persons performing an equivalent function in such organisations.

12.6.12. The categories defined in Items 1 to 7 of para. 2 shall include respectively and as far as applicable, positions in the institutions and bodies of the European Union and in international organisations.

12.6.13. The categories defined in Items 1 to 8 of para. 2 shall not cover middle-ranking or more junior officials.

12.6.14. For the purposes of para. 1, the following shall be considered "related persons":

12.6.15. the spouses or the de facto cohabitants;

12.6.16. the first-degree descendants and the spouses or the de facto cohabitants thereof;

12.6.17. the first-degree ascendants and the spouses or the de facto cohabitants thereof;

12.6.18. the second-degree correlative relatives and their spouses or the de facto cohabitants thereof;

12.6.19. any natural person who is known to be beneficial owner jointly with any person referred to in para. 2 of a legal person or other legal enterprise or to be in other close commercial, professional or other business relationships with any person referred to in para (2);

12.6.20. any individual who is a sole owner or a beneficial owner of a legal entity or the

13. Identification of representatives and third parties

Upon identifying an individual, the Company shall, identify any representatives or other third parties who act on behalf of the customer.

If the customer acts on behalf of third parties, the company shall also identify any such third persons.

14. Civil law partnerships and other contractual associations

14.1. Upon identification of civil law partnerships, all of the members of the partnership or their representatives shall be identified on the grounds applicable to individuals. The beneficial owners of the partnership shall be identified.

14.2. In the case of civil law partnerships, the purpose of their activity and, if necessary, the origin of the funds used shall be identified. Thereby one may rely, among other things, on clarifications and statements given by the representative of the partnership. The Company shall make sure that the use of funds by the partnership corresponds to the purposes of activity declared by it previously.

14.3. **Data of the members of the partnership and their representatives shall be preserved and regularly updated.**

15. General requirements regarding identification of legal entity

15.1. The business name, registry code, seat, registered office, address for correspondence and place of business, information about the legal form, passive legal capacity, term of existence, control bodies, management bodies (type and composition of the collective management body) and representatives (legal representatives and proxies), and beneficial owners shall be identified upon identifying legal entities. The business activity, purpose of operation, purpose of establishment and other similar information required for the establishment of business relationships shall be identified as well.

15.2. Upon determining the seat of a legal entity, both the theory of the country of foundation as well as the theory of the seat shall be used to identify whether the legal entity may involve country and geographical risks.

15.3. The place of business of a legal entity shall be determined on the basis of factual circumstances, i.e. where production is based or a service is

15.4. As regards legal entities, incorporated in the EU, the identification of the identity (i.e., collection of all mandatory identification details mentioned in art. 15.1) and passive legal capacity of a legal entity shall be carried out, as a general rule, on the basis of the information contained in the commercial register (in Georgia) or another equivalent register3 (in EU) or a copy of the registration certificate or an equivalent document (for instance, in countries where there is no national register, foundation documents certified by a notary are considered equivalent) submitted in accordance with the procedure provided by law. Documents issued by a register or their equivalents shall have been issued no earlier than 6 months prior to their submission to the Company.

15.5. Documents issued in a foreign state shall be legalised or apostilled, i.e. in order to use an official document issued in one country in another, an internationally recognized certificate of the authenticity of the document is given in another.

15.5.1. Documents issued by EU authorities and officials do not require legalisation or an apostille.

15.5.2. To be legalised, a document shall go through the legalisation authorities of the issuing state as well as those of the receiving state (usually, foreign ministries).

15.6. As regards legal entities, incorporated in the EU, upon identification, legal entities are not required to submit an extract of their registration if the Company has access to the required extent via the computer network to the data in the commercial register or register of non-profit organisations and foundations (including access to data in respective registers in the foreign country) as long as all mandatory identification information is available on the file of the legal entity in the respective register.

15.7. When it comes to legal entities incorporated in third countries, the Company will obtain a certificate of good standing (original or notarized copy) and a certified copy of the memorandum of association. If any mandatory identification details are missing from the obtained documents, additional documentation will be required.

15.8. Upon identification of a legal entity, the Company is required to register the names of the executive of the legal person or members of its management board or another body substituting for it, their powers in representing the legal entity and the principal field of activity of the legal entity. If the aforesaid details are not indicated in the relevant EU register and/or the register extract or another relevant document, the relevant information shall be obtained by using other documents and/or reliable sources of information. All executives, board members, and representatives must be identified according to the rules applicable for the identification of natural persons. If the representative of a legal entity is another legal entity, then information regarding the names of the natural persons participating in its control body must also be collected.

15.9. The need for use, the criteria of use and/or the list of reliable sources of information shall be specified by the Company (e.g. information issued by national registers, public authorities, credit institutions, foreign missions of the Georgia and foreign missions in Georgia may be used).

15.10. The Company shall identify the existence of politically exposed persons related to the legal entity as per the rules outlined in Art. 12

15.11. In the case of international organisations, the documents serving as the basis for their activities (including in Georgia) shall be determined and the submission of relevant documents shall be requested. If necessary, information required for the establishment of the business relationship

which is contained in the documents shall be verified.

15.12. When documenting a register check, it must include, at a minimum, the date and time of the check, the individual who conducted it, and the most recent update date on the identified legal entity's account.

15.13. The Company shall collect copies of relevant licenses/permissions if the customer's activity is regulated.

15.14. The Company shall verify the identification of legal entities, its executives, UBOs and representatives in accordance with the procedures outlined in Article 11.16, utilizing at least two reliable sources.

15.15. The Company will compile an identification file (identification card) for each customer- legal entity, its executives, UBOs and proxies (if any) - encompassing all identification information.

15.16. The date and time of the identification and verification operations, along with the name and title of the person conducting them, should be recorded in the identification cards of the customers.

15.17. The Company shall regularly update the customer's data and operating profile, ensuring that they are up to date and based on the customer's risk level.

15.18. The Company may opt to outsource the identification and verification process to a third party under a contractual agreement. In such instances, the third party will be responsible for identifying and verifying the Company's customers in accordance with the procedures outlined in this document and the requirements of the AML/CTF Law of Georgia and other applicable legal acts. The Company's AML Department will oversee the customer identification and verification processes, ensuring compliance. If deemed necessary, the AML Department will implement additional measures for identification and verification purposes.

15.19. When third parties are entrusted with the task of identification and verification, they will generate client reports encompassing all information and documents pertaining to the identified customers of the Company. These reports must include details regarding the date and time of identification and be readily available and accessible to the AML Department at all times. The AML Department will download and retain all pertinent information and documents collected by the third party.

15.20. Even in cases where identification and verification are outsourced to a third party under a contractual agreement, the AML Department will compile customer files as outlined in Article 15.15. These files will include all information and documents collected by the third party on behalf of the Company, as well as any additional documents and information gathered by the AML department as per Article 15.18. Additionally, the files will record the date and time of identification, the date and time of AML Department review, the date and time of any additional actions undertaken by the AML Department, and the names of the AML Department officers involved.

16. Agency

16.1. The Company shall verify if the person is acting on their own behalf or on behalf of another (natural or legal) person. If the person is acting on behalf of another person, the Company shall also identify the person on behalf of whom transactions are performed.

16.2. Documents required to identify a legal entity shall be submitted by the legal representative or authorized representative of the entity. The Company shall make certain that the right of representation complies with legislation. If the submitted documents do not indicate the right of representation of the individual submitting them and/or the authority is not compliant, the

identification process (and thus also the establishment of the business relationship or performance of the transaction) cannot be continued.

16.3. The Company shall identify the basis, scope and term of the representative's right of representation. The representative shall be asked to submit a document proving the right of representation. Further attention shall be paid to the verification of the identity and right of representation of authorized representatives operating or residing in a jurisdiction different from the legal entity's jurisdiction or whose rights of representation are valid for more than a year.

16.4. Clarification shall be sought on the scope of the right of representation granted to the authorized representative (for instance, whether a one-off transaction or recurring transactions over a certain period are involved). The Company shall take notice of the terms of the right of representation granted to the authorized representative and provide services only to the extent of the right of representation.

16.5. The company shall request that the representative of a legal entity of a foreign country submit documents proving their right of representation, notarised or certified in an equivalent manner and legalised or certified with an apostille, unless provided for otherwise in an international agreement or verifiable through other reliable sources.

16.6. Upon handling the right of representation of authorized and legal representatives, it shall be made certain whether the representative knows their customer. To identify the true nature of the relationships between the representative and the represented, the representative shall know the intentions related to the business relationship with the Company of the represented party and be able to answer other relevant questions about the seat of operations, fields of activity, sales and transaction partners, other related persons and beneficial owners. In addition, where applicable, the representative shall confirm with their signature that they are aware and convinced of the source and legal origin of the funds used in the transaction of the represented entity.

17. Identification of beneficial owner

17.1. Upon the identification of a legal entity, the Company shall register the beneficial owner of the entity.

17.2. "Beneficial owner" shall be any individual or individuals who ultimately owns or controls a legal entity or other legal enterprise, and/or any individual or individuals on whose behalf and/or for whose account an operation, transaction or activity is being conducted and who complies with at least one of the following conditions:

17.3. In the case of legal entities and other legal enterprises, the beneficial owner shall be the person who directly or indirectly owns at least 25% of the stocks, shares or voting rights in that legal entity or other legal enterprise, including through holding bearer shares, or through control via other means, with the exception of the cases of a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate level of transparency of ownership information.

17.4. The stock or share ownership interest in a legal entity or other legal enterprise held by a legal entity or other legal enterprise which is under the control of one and the same individual/s or by multiple legal entities and/or legal enterprises which are ultimately under the control of one and the same individual/s, shall be considered an indication of indirect ownership.

17.5. In respect of trust ownership, including trusts, trust funds and other similar foreign legal entities established and existing under the law of the jurisdictions allowing such forms of trust ownership, the beneficial owner is:

17.5.1. the founder

17.5.2. the trustee

17.5.3. the protector, if any

17.5.4. the beneficiary or class of beneficiaries,

17.5.5. Person exercising ultimate effective control over a legal entity or other legal entity by means of exercising rights through third parties conferred, inter alia, by virtue of authorisation, contract or another type of transaction, as well as through other legal arrangements conferring the possibility of exercising decisive influence through third parties, shall be an indication of "indirect control".

17.5.6. Where, after having exhausted all possible means and provided there are no grounds for suspicion, no individual can be identified as beneficial owner or where doubts exist that the identified individual/s is/are not the beneficial owner, the individual acting as senior managing official shall be considered "beneficial owner". The Company shall keep records of the actions taken for the identification of the beneficial owner

17.5.7. The ultimate beneficial owners of legal entities shall be identified through the respective commercial/UBO registers of the countries where the legal entities are registered. If the Company cannot access the relevant register, the AML Department shall request an excerpt from the register showing the UBOs or another similar document.

17.5.8. In the case of legal entities with nominee directors, nominee secretaries, or nominee owners of capital, the Company shall obtain certificates, contracts, or other valid documents in accordance with the legislation of the jurisdiction in which they are registered. These documents must be issued by a central registry or registering agent and must accurately identify the beneficial owners of the legal entity.

17.5.9. Identified UBOs will undergo verification through the examination of the collected identification documents, ensuring that their presence is clearly evident in such documentation.

17.5.10. Identified UBOs will further undergo verification through a written UBO declaration under the Georgian AML/CFT Law (where the wording of the declaration may be included in another document – such as a questionnaire collected and signed by the customer).

17.5.11. Ultimate Beneficial Owners will be identified according to the rules for individuals' identification outlined in this document. The UBO identification process must be thoroughly documented, along with any other identification procedures conducted by the Company or a third party to whom such tasks have been delegated. Additionally, the AML Department shall generate identification cards for the UBOs, along with ID cards for the legal entities and their representatives and proxies (if applicable).

17.5.12. The Company and/or the third party entrusted with such responsibilities shall verify whether the UBOs of legal entities are Politically Exposed Persons or associated with PEPs in accordance with the regulations outlined in Article 12 of this document. The checks and their outcomes shall be accurately recorded in the ID cards of the UBOs.

17.5.13. For customers - legal entities, and/or the legal entities that own or control them, whose equity securities are admitted to trading on a regulated market or on a market of a third country that is subject to disclosure requirements in accordance with European Union law or equivalent international standards ensuring an adequate degree of transparency with respect to ownership, data on shareholders and information on their shareholdings subject to disclosure shall be collected.

18. Requirements for identification of non-resident legal entities

18.1. In the event of the identification of legal entities that are non-residents, the Company shall comply, to the greatest extent possible, with the same requirements as in the event of customers that are residents, taking into account the specifications arising from the country of origin and legal form of the non-resident customer.

18.2. Upon identifying the passive legal capacity of a non- resident legal entity and handling documents certifying the powers of representatives, it shall be verified whether the documents meet the requirements established in Georgian legislation with respect to legalisation of foreign documents.

18.3. Due to differences in legal regulations in different countries, the Company shall pay attention, above all, to companies founded in countries or territories with a low tax rate, because it is not always abundantly clear whether they have passive legal capacity. In many countries, the standards for identifying a customer and registration and preservation of documents are lower than in Georgia, as a result of which particular attention shall be paid to the content of the documents of the companies registered in such countries and to the manner of their submission.

18.4. Particular attention shall be paid to information and documents submitted in the case of persons whose country of origin is on the FATF's list of countries that do not contribute sufficiently to the prevention of money laundering. The Company shall avoid business relations with persons whose place of residence or location is in the country listed by FATF high risk and non- cooperative countries. That list can be seen at: https://www.fatf-gafi.org/countries/#highrisk.

18.5. In the event of foreign- language documents, the Company is entitled to request a translation of the documents into a language understood by it. The Company shall arrange translation in Georgian language to any such documents.

19. Special requirements regarding trusts

19.1. As regards beneficiaries of a trust, including trusts, grantor trusts, and similar entities where beneficiaries are designated based on specific characteristics or class, the Company must collect, upon establishing a business relationship, the information regarding the beneficiary necessary for identification and verification of the beneficiary's identity prior to or at the time of disbursing the trust's own funds.

20. General requirements regarding the application of customer due diligence measures upon execution of transactions

20.1. In addition to the establishment of a business relationship, customer due diligence measures shall also be taken if:

20.1.1. in the event of any kind of transaction, incl. in the event of an offer made in the course of provision of a counselling service whose price exceeds the limit specified in the Georgian AML/CFT Law;

20.1.2. the amount of a single transaction or the total amount of consecutive transactions exceeds the limit provided by law (or the internal procedure rules of the Company). The obligation shall be performed upon occasional transactions made by a non-customer;

20.1.3. the Company has doubts about the correctness or sufficiency of the data collected upon establishment of the business relationship and if the actions of the other party are not ordinary or transparent as well as if the Company suspects money laundering or terrorist financing; and

20.1.4. the Company does not suspect money laundering or terrorist financing for the purposes of the Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing and does not have a reporting obligation for the purposes of the Georgian AML/CFT Law, but the transaction is complex and extraordinarily large or the transaction scheme is unusual and does not have an obvious economic or legal purpose.

20.2. The Company shall constantly assess changes in the customer's operations and whether these may raise the risk level so that additional customer due diligence measures need to be taken.

20.3. The application of customer due diligence measures also calls for the existence of the respective monitoring systems whose purpose is to detect reaching the transaction limit or the existence of risk factors and inform the appropriate persons thereof for the purpose of identifying suspicious or unusual transactions. If the Company comes to suspect money laundering in the course of monitoring transactions, the FIU shall be informed thereof.

21. Following transactions

21.1. The following of unusual and suspicious transactions is an important part of the set of customer due diligence measures and allows for the identification of circumstances that may point to money laundering or terrorist financing in the economic activities of customers. Also, the purpose of following a customer's transactions is to identify transactions with subjects of international sanctions and politically exposed persons and detect and notify of transactions whose limit or other parameters exceed the prescribed value over a certain period of time.

21.2. Transaction-following measures can be divided into two. One can use measures which enable, based on parameters or features developed with the help of the Company's prior work experience, transactions to be followed in real time as well as analysed afterwards.

21.3. Screening

21.3.1. In the event of following transactions in real time, the Company executives or other employees observe, upon performing their duties, the customer's behaviour and transactions with the aim of detecting unusual or suspicious transactions or transactions exceeding the prescribed limits.

21.3.2. Upon following transactions in real time, information technology tools which, using predefined parameters, select transactions made over a certain period may be used. The screening parameters depend on information technology possibilities and established goals. What shall be identified is as follows:

21.3.3. politically exposed persons involved in transactions;

21.3.4. transactions with persons whose name, date of birth etc. match data disclosed in lists of persons subject to international sanctions;

21.3.5. transactions with persons whose country of operation or origin is included on the list of higher (terrorist) risk countries; and persons whose transactions are subject to one- off temporary monitoring.

21.4. Monitoring

21.4.1. The Company shall conduct ongoing monitoring of its business relationships and customer activities in accordance with Georgian AML requirements.

21.4.2. The Company shall place complex or unusually large transactions or dealings, as well as transactions and dealings with no apparent economic or legitimate purpose that can be ascertained from available customer information,

under ongoing and extended surveillance.

21.4.3. In connection with the above, it shall assess the transactions and operations on the basis of the information gathered on their nature, their consistency with the customer's usual business and its object, the value of the transactions and operations, their frequency, the customer's financial situation, the means of payment used.

21.4.4. Where complex or unusually large transactions or operations, as well as transactions and operations with no apparent economic or legitimate purpose, are identified, collect information on the essential elements and value of the transaction or operation, relevant documents and other identifying data.

21.4.5. The Company shall document its assessment of the existence of the conditions for notification to the FMS under the Georgian AML/CFT Law as a result of the information collected.

22. Conduct in case of suspicion of money laundering and fulfilment of reporting obligation

22.1. In a situation where the Company, based on documents collected in the course of application of customer due diligence measures, develops a suspicion of money laundering or terrorist financing upon the establishment of a business relationship or upon occasional making of transactions, the Company shall not establish the business relationship or make the occasional transaction.

22.2. If unusual circumstances or circumstances whereby an employee of the Company suspects money laundering or terrorist financing become evident in relationships with a customer, the managing director shall be immediately informed thereof and the managing director will decide the immediate forwarding of the information to the FIU and the need to postpone or refuse to make the transaction. In a situation that entails a high risk of money laundering or terrorist financing, an employee of the Company may decide to postpone the transaction and thereafter inform the managing director of the situation.

22.3. The background of each individual suspect or unusual instance shall be investigated as much as reasonably necessary, thereby recording the details of the transaction and analysing the circumstances with the aim of identifying the typical features of more frequent transactions.

22.4. The main circumstances to which attention should be paid when suspect and unusual transactions are analysed are as follows:

22.4.1. What is suspicious about the steps, transactions or other circumstances?

22.4.2. Is the Company convinced that it knows its customer sufficiently or is it necessary to collect additional information about the customer?

22.4.3. Upon taking a step or making a transaction involving Company shall make certain that it follows the prescribed procedure. Was all the required information submitted or did additional information needs to be requested or otherwise clarified?

22.4.4. Have there been repeated instances of suspicious steps and transactions?

22.4.4.1. Criteria for Identifying Suspicious Transactions and Customers:

22.4.4.1.1. Transactions that lack a clear or legitimate economic purpose;

22.4.4.1.2. Transactions that are unusually large given the customer's known profile and expected activities;

22.4.4.1.3. Frequent or unexpected transfers between accounts, especially if the funds are moved to or from high-risk jurisdictions;

22.4.4.1.4. Sudden changes in the customer's financial behavior or transaction patterns;

22.4.4.1.5. Transfers to or from countries known for high levels of

corruption, money laundering, or terrorism financing;

22.4.4.1.6. Transactions involving foreign trusts or companies where the customer is the ultimate beneficiary but no clear business purpose is evident;

22.4.4.1.7. Customers with previous criminal records related to financial crimes;

22.4.4.1.8. Customers with a history of legal or regulatory actions against them or their businesses;

22.4.4.1.9. Documents that appear to be forged, altered, or improperly authenticated;

22.4.4.1.10. Inconsistencies in information provided by the customer, such as differing names, addresses, or identification numbers;

22.4.4.1.11. Lack of verifiable documentation for sources of funds or wealth;

22.4.4.1.12. Customers who show an unusual level of secrecy or request unusual levels of confidentiality;

22.4.4.1.13. Any activity that appears to be an attempt to obscure the origin, ownership, or destination of funds.

22.5. If the postponement of a transaction may prevent the interception of the potential perpetrator of money laundering or terrorist financing, the transaction or official act shall be performed and thereafter a report shall be forwarded to the FIU.

22.6. The Company shall preserve in a form that can be reproduced in writing all of the information received from staff about suspicious or unusual transactions and any information collected to analyse these reports and other related documents and any reports forwarded to the FIU along with information about the time of the forwarding of the report and the employee that forwarded it.

22.7. No customer or party participating in a transaction (including its representative or other related parties) with respect to whom suspicion is being communicated to the FIU may be notified of this.

22.8. The Company shall immediately fulfil the reporting obligation. The purpose of immediate fulfilment is to give the FIU the chance to develop the suspicion as per the Georgian AML/CFT Law and for taking its own measures. Money laundering is a process where criminal proceeds, above all, financial assets may be transferred via credit institutions and financial institutions of multiple states in a single day and therefore swift reporting helps to track down illegal funds more effectively.

23. Foreign affiliates and subsidiaries

23.1. The Company registered in Georgia applies customer due diligence measures and the requirements for information collection and preservation that are at least equivalent to the provisions of the Georgian AML/CFT Law in all foreign offices, branches and majority-held subsidiaries of the companies of the consolidation group, if such affiliates and subsidiaries are founded.

23.2. If the legislation of the third country does not permit the application of equivalent measures, the Company shall apply supplementary measures to prevent money laundering or terrorist financing.

23.3. The Company operating in several different countries, including in a third country, shall avoid in their activity the application of standards differing by country. Standards approved in the European Union provide guidance.

24. Measures Against Terrorism Financing

24.1. The measures to prevent the use of the financial system for money laundering and terrorist financing purposes are:

24.1.1. freezing of funds and other financial assets or economic resources;

24.1.2. prohibition on the provision of financial services, financial funds and other financial assets or economic resources;

24.1.3. notification of suspicion or implementation of the measures referred to in points 24.1.1 and 24.1.2.

25. Enhanced Due Diligence Measures

25.1. The Company shall apply enhanced due diligence measures in the following cases:

25.1.1. PEPs or persons related to PEPs

25.1.2. Customers from countries which do not comply or do not fully comply with the international standards on combating money laundering and financing of terrorism;

25.1.3. new products, business practices and delivery mechanisms where these are assessed as high risk;

25.1.4. new technologies in new or existing products, business practices and delivery mechanisms where these are assessed as high risk;

25.1.5. complex or unusually large transactions or operations, transactions or operations which are carried out in unusual patterns, and transactions and operations without an apparent economic or legitimate purpose;

25.1.6. in all other cases where a higher risk of money laundering or terrorist financing is established.

25.2. Enhanced due diligence measures may include:

25.2.1. Requesting and/or collecting additional data, documents, and information on the customer. If necessary, this may extend to collecting additional data on its beneficial owners, the intended nature of the business relationship, the grounds and/or relevant supporting documents for planned or completed transactions, and the origin of funds, especially in cases involving countries that do not fully apply international standards in the fight against money laundering and terrorist financing.

25.2.2. Gathering information through another customer.

25.2.3. Commissioning investigations or other necessary actions by reputable individuals with proven expertise and practical experience in the prevention and suppression of money laundering and terrorist financing.

25.2.4. Making enquiries of registers or other sources to ascertain whether the company is or has been undergoing insolvency, annulment, liquidation, or dissolution proceedings.

25.2.5. Conducting further enquiries or Internet checks for adverse information and negative press reports.

25.2.6. Requesting bank references or references from individuals who have or had a commercial or professional relationship with the client or the client's group.

25.2.7. Making contact at the customer's premises, by telephone, by post, or by email.

25.2.8. Inspecting the customer's business, including visiting the customer's business or administrative premises, or gathering information from the customer's contractors.

25.2.9. Requesting data, documents, and information provided or certified by

various independent parties and sources to collate, compile, and/or verify the data, documents, and information already collected.

25.2.10. Carrying out initial and subsequent periodic verification of related parties against mandatory reference lists (e.g., sanctions and IDP lists).

25.2.11. Dating and notarizing the shareholders' ledger, copying temporary bearer share certificates, requiring a special declaration from the client for mandatory notification prior to any change of ownership in the temporary bearer share certificates, including a special clause in the loan agreement for non-fulfilment of conditions regarding the temporary certificates, and conducting periodic checks at the client's office of the shareholders' ledger and temporary certificates.

25.2.12. Implementing measures contained in instructions issued by the Director of the FIU of the FMS.

25.2.13. Employing other measures deemed appropriate.

26. Origin of Funds

26.1. In case of high risk of money laundering (including in case of PEPs), the Company shall establish the origin of funds by two of the following methods:

26.2. Analysing the customer's financial history and transactions to identify any inconsistencies or unusual patterns.

26.3. Consulting public records or other reliable sources to verify the customer's financial background and the origin of the funds.

26.4. Reviewing documents and records that demonstrate the origin of the funds, such as bank statements, contracts, invoices, or proof of income.

26.5. Requesting detailed information from the customer about the source of the funds.

26.6. Consulting public records or other reliable sources to verify the customer's financial background and the origin of the funds.

26.7. Conducting interviews or meetings with the customer to discuss and confirm the origin of the funds.

26.8. Gathering information from the customer about his core business, including the actual and expected volume of the business relationship and the transactions or dealings anticipated within that relationship, through the completion of a questionnaire or other appropriate means.

26.9. If the origin of funds cannot be established through the means described in sections 26.1.1 to 26.1.7 of these rules, the Company shall rely on the collected origin of funds declaration under the Georgian AML/CFT Law which shall be collected from customers as part of the identification procedure.

27. Source of wealth

27.1. Under Article 6 of the Georgian AML/CFT Law, The Company is required to take appropriate action to clarify the source of wealth:

27.1.1. to a customer or beneficial owner of a customers who is found to be a person referred to in the abovementioned law (a PEP or a person related to PEP);

27.1.2. to customers and beneficial owners from high-risk third countries;

27.1.3. where the Company has determined that the use of this measure is appropriate in the case of enhanced due diligence measures.

27.2. The clarification of the source of wealth shall be carried out:

27.2.1. in the presence of a mechanism for public disclosure of the client's assets - by periodic review and comparison between the information on the declared assets of the client - natural person, or the beneficial owner of the client - legal person or other legal entity, and the information established as a result of the application of the due diligence measures (for example, comparison between the information indicated by the person in his annual declaration of assets and interests under of The Law of Georgia on Countering Corruption)

27.2.2. in case of impossibility to apply the actions referred to in point 27.2.1, or in case of establishing inconsistencies or deficiencies in the information when performing the actions referred to in point 27.2.1, the Company requires a written declaration of the client's financial situation.

27.2.3. The actions shall be documented and updated within the timeframes referred to in these rules, or at shorter intervals if the Company deems it necessary, or if so directed by the Director of the Financial Monitoring Service of Georgia.

27.2.4. The update under par. 27.2.3 shall be carried out in shorter periods when:

27.2.4.1. the customer or the beneficial owner of the customer, who has been identified as a PEP or a person associated with PEP, is from a country for which there is information about an identified high level of corruption or about identified significant gaps in the anti-money laundering and anti-terrorist financing enforcement mechanisms;

27.2.4.2. the customer or the beneficial owner of the customer, who has been identified as a PEP or a person associated with PEP, is associated with a sector in relation to which a higher risk of corruption or money laundering has been identified in the European Commission's supranational money laundering and terrorist financing risk assessment, in the national risk assessment, in the Company's own risk assessment or in the sectoral risk assessment, if applicable.

28. Electronic means

28.1. The Company may utilize the services of third parties for identification and verification of customers. If such third parties conduct identification, verification and/or other anti-money laundering measures through electronic means, then the safety measures undertaken by such third providers shall be described as Schedule 1 to these internal rules.

29. Collection, Storage and Disclosure of Information

29.1. Collection of Information

29.1.1. The data and information collected in connection with the customer identification and verification shall be kept on file as per the requirements of the rules of this document. The AML Department of the Company shall be responsible for the collection of identification cards of all customers (including UBOs and representatives in case of companies) and proxies (if any) together with all collected documents from customers (including copies of ID documents, declarations, questionnaires, company documents, PoAs, copies of checks in sanctions and other lists, etc).

29.1.2. For the purpose of conducting due diligence the Company collects documents, data and information at its discretion in light of the specific case in accordance with the requirements in these rules. The documents, data and information shall be relevant to the identification and verification of the identification of the customers and the persons to be identified and their collection shall not contravene the provisions of the Georgian

AML/CFT Law and the Rules on the application of the Georgian AML/CFT Law or any other legal act. The additional documents collected shall be used only for the purpose of conducting due diligence under the Georgian AML/CFT Law, within the framework, under the terms and subject to the conditions and limitations of the Georgian AML/CFT Law and other applicable anti-money laundering and anti-terrorism financing legal acts.

29.2. Book of suspicious transactions and customers

29.2.1. The Company shall prepare and maintain a special register in which it shall be entered:

29.2.1.1. any report of suspicion of money laundering, terrorist financing and/or the presence of funds of criminal origin, regardless of the manner in which the report was made, together with a conclusion on the need for notification under the Georgian AML/CFT Law; This rule applies also to reports and conclusions made to a representative of the AML Department or to the managing director of the Company

29.2.1.2. A conclusion as to the purpose and nature of the operations or transactions which fall within the scope of the Georgian AML/CFT Law, and a conclusion as to the existence of suspicion of money laundering or the presence of funds of criminal origin

29.2.2. In the event of doubt, the managing director shall open a file in which all documents relevant to the acts committed by him or his servants shall be collected and arranged in the order in which they are received.

29.2.3. The Company may maintain the log in paper or electronic form and shall be responsible for its proper preservation.

29.3. Storage or Preservation

29.3.1. The Company shall retain for a period of 5 years all documents, data and information collected and prepared pursuant to these internal rules. In the case of the establishment of a business relationship (i.e., establishment of a trust with a customer), the 5-year period shall commence at the beginning of the calendar year following the year of termination of the relationship (i.e., the termination of the trust). In the case of an incidental transaction, it shall commence at the beginning of the calendar year following the year in which it occurs.

29.3.2. The Internal Rules for the Control and Prevention of Money Laundering and the Financing of Terrorism with all related documents and their amendments, supplements and updates shall be kept throughout the duration of the activities of the Company and for a period of one year from the cessation of such activities.

29.3.3. In cases of disclosure of information pursuant to the Georgian AML/CFT Law, the time limit shall commence at the beginning of the calendar year following the year of disclosure of the information.

29.3.4. All documents, data and information collected and prepared in accordance with the Georgian AML/CFT Law, and these internal rules shall be collected and stored by the Company in such a way as to be available to the FIU, as well as to other competent state authorities, in accordance with their powers and competences provided for in a legal act.

29.3.5. All documents, data and information collected and prepared in accordance with these rules and the Georgian AML/CFT Legislation, shall be kept by the Company so that it can perform its activities and obligations under the Georgian AML/CFT Legislation without hindrance.

29.3.6. Information, documents and data on individual transactions, operations and customers shall be stored in a manner that permits their timely retrieval if they are to be provided for use as evidence in judicial and pre-trial proceedings.

29.3.7. Internal access to certain documents, data and information collected and prepared

pursuant to these rules and the Georgian AML/CFT Legislation and other related legal acts shall be available to employees of the Company whose official duties relate to the implementation of the Georgian AML/CFT Legislation and these rules.

29.4. Personal Data

29.4.1. The collection and storage of information pursuant to the Georgian AML/CFT Law, the Rules for the Application of the Georgian AML/CFT Law, and these internal rules which contains personal data within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1 of 4 May 2016).), and the Personal Data Protection Act, does not contravene the provisions of the aforementioned data protection legislation, insofar as it is carried out in fulfilment of an obligation established by a statutory instrument, namely Georgian AML/CFT Law, the Rules for the Application of the Georgian AML/CFT Law. The processing of personal data for the purposes of the prevention of money laundering and terrorist financing is processing with a legal basis of a matter of public interest under the General Data Protection Regulation and cannot be limited by the requirements of Articles 12 to 22 and 34 of that Regulation.

29.5. Disclosure of Information

29.5.1. In the event of suspicion and/or knowledge of money laundering, terrorist financing and/or the presence of funds of criminal origin, the Company shall immediately notify the FIU of the FMS prior to the execution of the operation or transaction by delaying its execution within the legally permissible time limit. Where the delay of the transaction or operation is objectively impossible or is likely to frustrate actions to pursue the beneficiaries of a suspicious transaction or operation, the Company shall notify the FIU of the FMS immediately after the transaction or operation has been carried out, stating the reasons why the delay was impossible.

29.5.2. Notification under the Georgian AML/CFT Law shall be made by filling in a form published on the FMS website in the section Measures against money laundering and terrorist financing

29.5.3. In urgent cases, notification may be made orally, followed by written confirmation within 24 hours.

29.5.4. The Company does not make/accept cash payments in contravention of the statutory restrictions under the Restriction of Cash Payments Act and has no obligation to make the notifications under the Georgian AML/CFT Law.

29.5.5. The Company and its employees may not notify their customer or third parties of a disclosure of information.

30. Trainings

30.1. The Company provides induction and ongoing training to employees in relation to their AML/CFT activities, including ongoing training programmes aimed at identifying suspicious transactions, transactions, sources and customers and taking appropriate action in cases of suspected money laundering and terrorist financing.

30.2. The Head of the AML Department shall prepare, approve and implement an employee training plan on the application of the AML Acts on an annual basis.

31. Procedure for Anonymous and Independent Internal Reporting

31.1. It is permissible for the managing director of the Company to receive an internal report disclosing information about suspected money laundering and/or the presence of funds of criminal origin, as well as violations of the Georgian AML/CFT Legislation, and these rules.

31.2. Internal reports can be submitted either in writing or through electronic communication means to the electronic addresses of the managing director of the Company.

31.3. The managing director of the Company is obliged to maintain the anonymity of the person submitting the report, both to other employees of the Company and to the competent authorities to whom the information related to the internal report is disclosed.

31.4. The managing director of the Company is prohibited from disclosing information about received internal reports, according to the procedure described above, except in accordance with the requirements of the AML Acts, while adhering to all applicable legal and internal regulations for the protection of data, information, and individuals.

31.5. If the report concerns information about suspected money laundering and/or violations of the Georgian AML/CFT Legislation, or these rules, committed by the managing director of the Company, the report may be submitted directly to the Financial Intelligence Directorate of the Financial Monitoring Service of Georgia in accordance with the Georgian AML/CFT Law and/or to the relevant competent state authority, in compliance with the applicable legal provisions in the specific case, without notifying the managing director of the Company.

32. Changes

32.1. The Company shall from time to time review these rules in order to comply with the applicable law.

33. Transitional and Final Provisions

33.1. These internal rules and their appendices have been adopted by PPK Technology Group LLC. with Decision/Order No. PPK01/01/2024 dated 09/01 / 20 24.

33.2. Upon their adoption in accordance with the prescribed legal procedures, these internal rules for the control and prevention of money laundering and terrorist financing become mandatory for application by PPK Technology Group LLC. and all its employees involved in fulfilling the obligations under the Georgian AML/CFT Legislation and these rules.

33.3. The Company through its managing director, is authorized to issue internal acts for the implementation of these Rules.

Last review by the managing director of the Company conducted on:

Date:

X

Peter Kritzer
Managing Director