RULES OF PROCEDURE AND INTERNAL REGULATION OF OÜ TKNBX

for the implementation of obligation to prevent money laundering and terrorist financing

Last updated on May 08, 2018

GENERAL DATA

Obligated person: OÜ TKNBX
Registration code: 14425430
Registered address: Tallinn, Kristiine linnaosa, Mustamäe tee 44, 10621
Types of activity: services for the exchange of virtual currency for money virtual currency wallet service.
Description of the service:
TKNBX OÜ is a person offering a **service for the exchange of virtual currency for money**, that in its business activities receives orders for the exchange of virtual currency through the electronic platform and exchanges it for money. TKNBX OÜ also provides, through the electronic platform, a service for the exchange of virtual currency for virtual currency.
Virtual currency wallet service:
TKNBX OÜ is a provider of virtual currency payment services that, through the electronic platform, creates and/or maintains encrypted keys for clients in an economic activity that can be used to store and transfer virtual securities.
Place of business: operates on the Internet
Mailing address: Tallinn, Kristiine linnaosa, Mustamäe tee 44, 10621

Place of activity on the Internet: tokenbox.io
Responsible board member: Vladimir Smerkis
Personal code of the responsible board member: date of birth 25.06.1984
Contact person: Salas Luzuriaga Pavel, 03.08.1985
Contact details of the contact person:
e-mail: salas@tokenbox.io
Phone: 7 926 381 85 43
E-mail address for sending and receiving messages: salas@tokenbox.io
The document is valid from: 08.05.2018

Signature of the responsible board member:
/digital signature/ date 08.05.2018
Signature of the contact person:
/digital signature/ date 08.05.2018

1. GENERAL PROVISIONS

1.1. According to clause 10 part 1 article 2 of the Money Laundering and Terrorist Financing Prevention Act (hereinafter referred to as "RahaPTS"), TKNBX OÜ is an obligated person, in whose economic activities the requirements established by RahaPTS shall be applied.

1.2. These rules of procedure establish in the TKNBX OÜ activities internal measures to counter money laundering and terrorist financing and establish suspicious transactions or business partners, with the application of the appropriate due diligence measure, the measure to assess the risks of money laundering and terrorist financing and their reduction, the rules for fulfilling the obligation of communication and the obligation of informing the management and their verification (hereinafter referred to as the Internal Regulation).

1.3. Rules of procedure determine the order of data collection, transmission and storage.

1.4. The objective of the rules of procedure is to provide the employees and the management of TKNBX OÜ with instructions for meeting the RahaPTS requirements, thereby effectively reducing and managing the risks of money laundering and terrorist financing, taking into account the risks arising from the activities of the obligated person. The purpose of the rules of procedure is to establish rules of action that counteract the use of property obtained by criminal means, the use of TKNBX OÜ for the purposes of money laundering and terrorist financing.

1.5. TKNBX OÜ confirms that the established rules of procedure shall apply to all business relations and clients in the amount and volume established by the rules of procedure.

1.6. When applying the rules of procedure, it is necessary to take into account the requirements arising from existing legal acts. In the event of mandatory requirements arising from legal acts, one shall proceed from those established by legal acts. In case of occurrence when implementing rules of procedure, one should proceed from the principle of reasonableness, taking into account the purpose of the RahaPTS and these rules of procedure, as well as to act in good faith, in accordance with the expected diligence from the obligated person.

1.7. TKNBX OÜ checks the conformity and appropriateness of the rules of procedure with the requirements of the RahaPTS regularly, but at least once a year and, if necessary, supplements them.

1.8. The representative of TKNBX OÜ is obligated to fulfill the requirements arising from the RahaPTS and these rules of procedure, if their job duties include the establishment of business relations or the performance of transactions.

1.9. The responsible board member of the obligated person shall provide employees, whose job duties include the establishment of business relations or the performance of transactions, with training to fulfill the duties arising from the RahaPTS.

2. TERMS AND ABBREVIATIONS USED IN THE RULES OF PROCEDURE

2.1. **Money laundering** is the transformation or transfer of property obtained as a result of criminal activity or received instead of it, if it is known that such property was obtained as a result of criminal activity or participation in it, in order to conceal the illegal origin of property or to provide assistance to a person, who participated in the criminal activity, so that they can evade the legal consequences of their actions, or the acquisition, possession or use of this property, if upon its receipt it is known that it has been received as a result of criminal activity or participation in it, or concealment of the true nature, origin, location, manner of disposal, transfer or ownership of property, or concealment of other rights related to property, or if it is known that such property was obtained as a result of criminal activity or participation in it. Money laundering is also participation in the above activities, connection with them, attempts to commit them, as well as complicity and incitement to their commission or assistance, or consultation on their commission. Money laundering takes place also in the cases when the property used in money laundering was obtained as a result of criminal activity committed in the territory of another state[1].

2.2. **Terrorist financing** is the financing and support of terrorist crimes and activities aimed at their commission within the meaning of Article 2373 of the Penal Code[2].

---

[1] RahaPTS § 4

[2] RahaPTS § 5

2.3. **Business relations** are relations that arise when a long-term contract is concluded by the obligated person in the economic or professional activity for the purpose of rendering a service or selling goods in another way or that are not based on a long-term contract, but during the establishment of contacts in connection with them, it is reasonable to assume a certain duration of the relationship, and during which the obligated person, in the provision of services, in performing official activities or offering goods, performs individual transactions repeatedly within the business, professional or official activity[3].

2.4. A **client** is a person, who is in business relations with the obligated person, that is, a person, who uses the service of a business association[4].

2.5. **Commercial association service** is, within the meaning of this instruction, the execution of a sales order, in the course of which the virtual currency is exchanged for some currency or another virtual currency. TKNBX OÜ does not offer a service for exchanging a virtual currency for cash and another service with cash.

2.6. A **politically significant person** is an physical person, who performs or performed important tasks of public authority, including the Head of State, the head of government, the minister and the deputy minister or an assistant minister, a member of parliament or a member of the legal institutional body similar to the parliament, a member of the governing body of the party, a member of the supreme court and the state court, a member of the state control and council of the central bank, an ambassador, a charge d'affaires and a senior officer of the Defense Forces, a member of the board and administrative or supervisory authority of the state commercial association, the head, the deputy head and a member of the governing body of an international organization or a person performing equivalent tasks that has no status of an official of the middle or lower level[5].

2.7. A **local politically significant person** is a person referred to in clause 2.6 that performs or performed important public authority tasks in Estonia, in another state under a contract of the European Economic Area or with the institution of the European Union[6].

---

[3] RahaPTS § 3 cl. 4

[4] RahaPTS § 3 cl. 5

[5] RahaPTS § 3 cl. 11

[6] RahaPTS § 3 cl. 12

2.8. A **family member** is a spouse or person deemed to be equivalent to the spouse of a politically significant person or a local politically significant person, a child or a spouse or a person deemed equal with the spouse of a politically significant person or a local politically significant person, as well as a parent of a politically significant person or a local politically significant person[7].

2.9. A **person considered to be a close colleague** is a physical person, who is known to be a real beneficiary of a judicial person or a legal entity or a joint owner together with a politically significant person or a local politically significant person or is in close business relations with a politically significant person or a local politically significant person, as well as a physical person, who is the sole beneficiary owner of a judicial person or a legal entity that is known to be established in favor of a politically significant person or a local politically significant person[8].

2.10. A **real beneficiary** is a physical person that, using their influence, controls the transaction, operation or other person, and in the interests, in favor of or at the expense of whom the transaction or operation is being performed. In the case of a business association, the real beneficiary is a physical person that ultimately owns or controls a legal entity by directly or indirectly owning a sufficient number of shares, equities, voting or ownership rights, including participation in the form of shares or bearer equities, or otherwise. Direct possession is a method of control, in which case a physical person owns 25% plus one share in a commercial association or over 25% of ownership. Indirect possession is a method of exercising control, in which case a business association has 25% plus one share in a business association or an ownership interest of more than 25%, a business association under the control of a physical person or several commercial associations under the control of the same physical person. If after the exhaustion of all possible methods of establishment it is impossible to establish the specified person and there is no suspicion that such person still exists, or if there is a suspicion that the established person is the real beneficiary, then the physical person, who is a member of the supreme governing body is considered to be the real beneficiary.

---

[7] RahaPTS § 3 cl. 13

[8] RahaPTS § 3 cl. 14

2.11. The **third state with a high risk** is the state adopted in accordance with part 2 of article 9 of Directive 2015/849 (i.e., the fourth anti-money laundering directive) in the delegated state. During the preparation of the rules of procedure, the list included the following States: Afghanistan, Bosnia and Herzegovina, Gwiana, Iraq, Lao People's Democratic Republic, Syria, Uganda, Vanuatu, Yemen, Iran, Democratic People's Republic of Korea (DPRK).

2.12. The **top management of the obligated person** is the head or an employee, who has sufficient knowledge of the risks of the obligated person in connection with money laundering and terrorist financing, as well as sufficient powers to make decisions about influencing risks, but that should not be a member of the management board[9].

2.13. **RahaPTS** is the Money Laundering and Terrorist Financing Prevention Act.

3. RIGHTS AND OBLIGATIONS OF THE RESPONSIBLE BOARD MEMBER AND CONTACT PERSON

3.1. The member of the Board of TKNBX OÜ is responsible for the application of the RahaPTS and the legal acts and instructions established on its basis. If TKNBX OÜ has more than one member of the management board, the obligated person appoints the member of the management board responsible for the application of the RahaPTS and the legal acts and instructions established on the basis thereof by the relevant decision.

3.2. The management board of the obligated person may, in addition to a responsible member of the management board, appoint a contact person to perform duties related to combating money laundering and terrorist financing.

3.3. The duties of the contact person may be performed by an employee or a structural unit. If the duties of the contact person are performed by the structural unit, the head of this structural unit shall be responsible for the performance of duties of the contact person. The appointment of the contact person is notified to the Money Laundering Data Office.

3.4. Only a person, who has the education, professional suitability, necessary abilities, personality and experience, as well as an impeccable reputation, necessary for fulfilling the duties of the contact person can be appointed as a contact person.

---

[9] RahaPTS § 3 cl. 5

3.5. Prior to the appointment of a contact person, the functions of the contact person are performed by the responsible member of the management board.

3.6. The obligations of the contact person:

3.6.1. organization of collection and analysis of information indicating transactions or circumstances unusual or suspected money laundering or terrorist financing (collection of information means collection from employees, contractual partners and agents of the obligated person of suspicious or unusual messages received, systematization and analysis of information specified in them);

3.6.2. transfer of information to the Money Laundering Data Office, if there is suspicion of money laundering or terrorist financing;

3.6.3. periodic submission to the management of the obligated person of written reviews on the fulfillment of requirements arising from the RahaPTS;

3.6.4. briefing, consulting, training and informing employees of TKNBX OÜ on the requirements for combating money laundering and terrorist financing, as well as the application of appropriate monitoring mechanisms in the economic activities of the obligated person, including checking the compliance of the execution of transactions and actions by employees with the RahaPTS and these rules of procedure.

3.6.5. verification of the implementation of decisions/regulations containing international sanctions;

3.6.6. the submission of responses to inquiries, letters, requests for information to the Money Laundering Data Office, and the organization of enforcement of orders.

3.6.7. informing the Money Laundering Data Office of changes in contact data of the obligated person and/or a contact person.

3.7. The rights of the contact person:

3.7.1. to submit to the Board of TKNBX OÜ proposals for amendments and additions to the rules of procedure containing requirements for combating money laundering and terrorist financing, as well as organizing relevant training;

3.7.2. to obtain data and information necessary for the performance of the obligations of the contact person, among other things the contact person shall be provided with access to information that is the basis or prerequisite for the establishment of business relations, including information, data and documents reflecting the identity of the client and their economic activities;

3.7.3. to supervise the actions of employees and their compliance with the requirements of the RahaPTS, and also demand an immediate cessation of violations of the requirements for combating money laundering and terrorist financing or the elimination of identified deficiencies within a reasonable time;

3.7.4. to make suggestions on how to organize the process of submitting suspicious and unusual messages;

3.7.5. to receive training in the performance of obligations;

3.7.6. to transmit the information and data that have become known in connection with suspected money laundering and terrorist financing or the use of international sanctions to the Money Laundering Data Office, the institution of the preliminary investigation on the basis of an appropriate order or to the court on the basis of a court ruling or decision.

3.8. Before appointing a new contact person, TKNBX OÜ agrees the candidate with the Money Laundering Data Office.

4. RISK-BASED APPROACH

4.1. The obligated person, when applying the measures described in the rules of procedure, proceeds from a risk-based approach and constantly evaluates the risk of money laundering and terrorist financing in various activities and actions, and also applies, if necessary, enhanced due diligence measures.

4.2. In establishing business relations and monitoring business relations, the obligated person applies all the due diligence measures, established by the RahaPTS, but the scope and solidity depends on the client's risk profile, the nature of the business relationship and the service.

4.3. The steps taken to establish, evaluate and analyze risks shall be proportional to the nature, volume and complexity of the economic and professional activities of the obligated person.

5. RISK CATEGORIES

5.1. To establish, evaluate and analyze the risks associated with money laundering and terrorist financing, TKNBX OÜ takes into account the following risk categories:

5.1.1. the risk associated with the client;

5.1.2. the risk associated with states or geographical areas or jurisdictions;

5.1.3. the risk associated with services and transactions;

5.1.4. the risk associated with channels of mediation or communication between an obligated person and clients, or channels for the transfer of goods, services or transactions.

5.2. The **risk associated with the client** is the risk factors arising from the person participating in the transaction.

5.3. TKNBX OÜ considers the risk associated with the client to be **high** if the client:

5.3.1. is a person, who participates in a transaction in a business or professional activity or who participates in a business transaction, a person, a client using a service or their real beneficiary, a politically significant person or a member of the family of a politically significant person, or a person considered to be a close colleague of a politically significant person;

5.3.2. is a legal entity, the capital of which is formed by bearer equities or other bearer securities;

5.3.3. is a person who, with the establishment of a business relationship with whom the obligated person cannot perform the following due diligence measures: identification of the person and their verification in a reliable source; identification of the person's representative; establishment of a real beneficiary or establishment of structures of ownership and control of the person participating in the transaction;

5.3.4. is an physical person whose real beneficiary is a third party;

5.3.5. is a legal entity or other association of persons that does not have the status of a legal entity engaged in personal property management;

5.3.6. is an enterprise that makes a turnover of cash in large amounts;

5.3.7. a client or related business association have fictitious shareholders or bearer equities;
5.3.8. the ownership structure of a commercial entity that is a client, taking into account the activities of a business association, seems unusual or too complex;
5.3.9. the establishment of real beneficiaries of a legal entity is complicated, based on complex and opaque owner relations;
5.3.10. in the identification of the person or verification of the information provided, suspicion of the reliability of the submitted data or of the authenticity of documents or of establishing a real beneficiary arose;
5.3.11. is a person against whom the obligated person has a suspicion of money laundering or terrorist financing, or in the course of an earlier business relationship of whom suspicious transactions were established;
5.3.12. a person is subject to international sanctions[10];
5.3.13. is the person offering a service to anonymous clients in the course of economic activity;
5.3.14. is the person, the origin of the property or the source of the funds used for the transaction, and the origin of the wealth of whom cannot be properly established.

5.4. Persons who are on the list of international financial sanctions and those previously known for suspicion that persons may be associated with money laundering and terrorist financing do not receive services.

5.5. TKNBX OÜ considers the risk associated with the client to be **low**, if the client:
5.5.1. is a registered in a regulated market business association, for which disclosure obligations are applied that establish requirements to ensure that the beneficiary is sufficiently transparent;
5.5.2. is a public legal entity established in Estonia;

[10] The contact person shall immediately notify the Money Laundering Data Office if it turns out that a person, who wishes to enter into business relations, or a person, who has already entered into business relations with TKNBX OÜ, is subject to an international sanction or if it is suspected that the person concerned is subject to an international sanction. The client immediately loses access to services and falls under an international sanction, taking into account its content and scope.

5.5.3. is a government agency or other publicly performing institution of Estonia or a state party to the agreement on the European Economic Area;

5.5.4. is an institution of the European Union;

5.5.5. is a lending institution or financial institution operating in its own name, a lending institution or a financial institution, in a state party to the agreement on the European Economic Area or a third state, for which there are claims in the states at their location equivalent to the requirements of the Directive of the European Parliament and Council (EL) 2015/849, over which state supervision is exercised.

5.5.6. The value of the transaction is less than EUR 15,000 or an equivalent amount in another currency, for a period of one year

5.6. TKNBX OÜ establishes its clients and allows to make transactions anonymously. In a situation, where during the screening of transactions an unknown party to the transaction is established, the transaction instruction is not fully completed. TKNBX OÜ does not allow to make a service in cash. If an employee has a suspicion of money laundering or terrorist financing in relation to the transaction or the money which is its object, the origin of the property shall be established.

5.7. The **risk associated with states or geographical areas or jurisdictions** is risk factors arising from differences in the legal environment of different states.

5.8. TKNBX OÜ considers the risk associated with states and geographic areas to be **high**, if the client or the transaction is connected with:

5.8.1. with a person registered in an area with a low tax rate[11];

5.8.2. with a person participating in a transaction or an official act in a business or professional activity, with a person or client using a service from a third country with a high risk, or their place of residence or location, or the location of the person offering the payment service of the payee is located in a third state with high risk[12];

---

[11] List of territories that are not considered to be territories with a low tax rate (Decree of the Ministry of Finance dated 18.12.2014 No. 55 RT I, 19.12.2014, 15).

[12] At the time of the establishment of procedural rules, the third states with a high risk are Afghanistan, Bosnia and Herzegovina, Gwiyana, Iraq, Ethiopia, Serbia, Sri Lanka, Trinidad and Tobago, Tunisia, Lao PDR, Syria, Uganda, Vanuatu, Yemen, Democratic People's Republic of Korea (DPRK). http://www.fatf-gafi.org/countries/#high-risk

5.8.3. with a state of risk[13], which is credibly associated with the support of terrorism or where there is a high level of corruption;

5.8.4. with a state or territory, for which the UN or the European Union has established a sanction, embargo or similar measure;

5.8.5. with a state that finances or supports terrorism, or on whose territory there are terrorist organizations revealed by the European Union or the United Nations.

5.9. TKNBX OÜ considers the risk associated with states and geographical areas to be low, if the client from the state mentioned below or their place of residence or location is in the following state:

5.9.1. in the state party to the agreement on the European Economic Area[14];

5.9.2. in a third state, where there are effective systems for combating money laundering and terrorist financing[15];

5.9.3. in a third state, where, according to reliable sources, the level of corruption and criminal activity is low;

5.9.4. in a third state where, according to reliable sources, such as mutual evaluations, reports or subsequent disclosures, requirements are set for countering money laundering and terrorist financing that comply with the changed recommendations of the Financial Action Task Force, and where these requirements are effectively applied[16].

5.10. The **risk associated with services or transactions** is the risk factors that result from the client's economic activity and the openness of a particular product or service to the possible risks of money laundering.

---

[13] A state of risk is a state or territory where there is an increased danger of terrorism or which is associated with a greater risk of terrorist financing. Information on high-risk states can be found here: http://www.fatf-gafi.org/countries/#high-risk

[14] **In the European Economic Area (EEA):** From the European Union France, Italy, Germany, Belgium, Luxembourg, Holland, Denmark, Ireland, Great Britain, Greece, Spain, Portugal, Finland, Sweden, Austria, Estonia, Latvia, Lithuania, Poland, Czech Republic , Slovakia, Slovenia, Hungary, Malta, Cyprus, Romania, Bulgaria, Croatia and the EFTA states: Iceland, Norway and Liechtenstein. **NB! Switzerland is not part of the EEA.**

[15] Australia, South Korea, Brazil, Mexico, Canada, Singapore, Hong Kong, Switzerland, India, South Africa, Japan, United States of America (Directive 2005/60 / EU)

[16] **List of states:** http://www.fatf-gafi.org/countries/#FATF

5.11. TKNBX OÜ considers the risk associated with a service or transaction to be **high** if:

5.11.1. If the appearance and behavior of the person does not correspond to the nature of the person's transaction or the person's conduct causes suspicion, among other things the person cannot describe their possible cooperation partners or the purpose of the transaction, as well as there is suspicion of a dummy in relation to the person wishing to use the services.

5.11.2. The person does not wish to divulge the origin of money at the request of TKNBX OÜ, but there is reason to believe that it may originate from a third high-risk state.

5.11.3. When rendering a service, the person does not want to disclose the real beneficiaries of the enterprise, but there is reason to believe that they can be associated with a third state with high risk.

5.12. TKNBX OÜ considers the risk associated with a service or transaction to be **low** if:

5.12.1. The purpose of the service desired by the person is clear and proper;

5.12.2. The person wishing to use the service of TKNBX OÜ is the ultimate beneficiary and there are no other risk factors in relation to them (e.g., state risk and geographical risk);

5.12.3. The origin of the money used during the service is clear and, if necessary, documented;

5.12.4. The **risk associated with mediation or communication channels between TKNBX OÜ and clients or service or transaction transfer channels** is a risk factor arising from the way the client communicates with or provides services that may indicate possible money laundering risks.

5.13. TKNBX OÜ considers the risk associated with mediation or communication channels between the obligated person and clients, or goods, services or transactions transfer channels to be **high** if:

5.13.1. the communication channel allows to remain anonymous. TKNBX OÜ does not use the channel, allowing the person to remain anonymous, when establishing business relations and in the future communication. If TKNBX OÜ cannot get acquainted with the original documents, one can use a notarized or officially certified document or information from a reliable and independent source (for example, request a copy of the

document to be sent via an electronic channel) to verify the identity, using at least two sources (e.g. ask for an account for your phone or housing costs).

5.14. TKNBX OÜ considers the risk associated with mediation or communication channels between an obligated person and clients, or goods, services or transactions transfer channels to be **low** if:

5.14.1. The person uses the electronic platform of TKNBX OÜ and there is no suspicion regarding the employee's document transmitted through the platform.

5.14.2. The person has confirmed on the electronic platform that they are available through various communication channels.

5.15. TKNBX OÜ considers the degree of the client's risk to be generally low, if there is no risk factor present in any risk category, and therefore it can be argued that the client and their activities correspond to the characteristics that are not different from the person with normal and transparent activities, and there is no suspicion that the activities of the client can increase the likelihood of money laundering and terrorist financing.

5.16. In situations where the application of scrutiny measures is derived from legal acts and information about the client and their real beneficiary is publicly available, where the person's activities and transactions correspond to their daily business activities and do not differ from the payment and behavioral traditions of other similar clients, or where there are quantitative or other absolute restrictions to the transaction, TKNBX OÜ believes the perceived risk of money laundering and terrorist financing is low.

5.17. TKNBX OÜ considers the degree of the client's of risk to be generally high if, when assessing the risk categories in the aggregate, there is a suspicion that the client's activity is not normal or transparent, and there are risk factors present, which suggests that the likelihood of money laundering and terrorist financing is great or has increased significantly. The client's risk level is always high, if the person participating in a transaction or official act in a business or professional activity, a person or a client using a service from a third state with a high risk, or their place of residence or location, or the location of the person offering the payment service of the payee specified in clause 5.8, the state or the person is subject to international sanctions. If a client relationship is established with a person, for whom enhanced

measures of thorough verification should be applied, the employee shall immediately notify the contact person by e-mail or telephone.

5.18. Given the above risk categories, TKNBX OÜ determines the degree of risk of the person, involved in the transaction: high, ordinary or low. TKNBX OÜ documents a certain degree of risk to a client and updates it as applicable, and, if necessary, makes it available to competent institutions.

5.19. If the client refers to a high risk degree, TKNBX OÜ shall apply enhanced measures of thorough verification. In the event that TKNBX OÜ assesses the degree of risk of the person participating in the transaction as low, TKNBX OÜ may apply the scrutiny measures in a simplified manner. In such a case, TKNBX OÜ determines the scope of the due diligence measures independently.

6. ESTABLISHMENT OF BUSINESS RELATIONS AND MONITORING OF BUSINESS RELATIONS

6.1. TKNBX OÜ clients are legal entities using the established electronic platform for the exchange of virtual currency and with whom TKNBX OÜ is in business relations.

6.2. Establishment of business relations with the client takes place on the electronic platform of TKNBX OÜ, where the client is requested to fill out an application for opening an account and an identification form before opening an account.

6.3. In the event that the client wishes to make only transactions on the electronic currency exchange (virtual currency to virtual currency) on the electronic platform TKNBX OÜ, the client is asked to fill only the application for opening an account (*services, in which one virtual currency is exchanged for another virtual currency, within the meaning of the new edition of the RahaPTS, which entered into force on 27.11.2017, do not need permission to operate and persons providing such services are not obligated persons any more within the meaning of the RahaPTS*).

6.4. In the event that a client wishes to use the service of exchanging a virtual currency for a virtual currency, the identity of the client shall be established. The client shall unconditionally fill in the application for opening an account and the personal identification form. In this case, the client shall attach a photo from the identity document in the .PDF or .JPG format to the completed form. The attached photo shall be of high quality. The following

data shall be read and clear from the photo presented: name and patronymic, date of birth and/or personal identity code, photograph and/or image of the person, signature of the person, validity period and number of the document, name of the issuing institution, citizenship and place of birth. The document must be complete and not be damaged[17]. In addition to the identity document, the client shall present their photo along with the submitted identity document in their hands.

6.5. TKNBX OÜ verifies the data submitted by the client, based on these rules of procedure and guided by the established RahaPTS. After the rules of procedure are fulfilled and the data are verified, TKNBX OÜ opens an account for the client on the electronic platform, through which the person can perform virtual currency exchange services for virtual currency.

6.6. When the client completes the application for opening an account on the electronic platform of TKNBX OÜ and the identification form, it is considered that the person has agreed with the general terms and conditions for the provision of services by TKNBX OÜ. From the moment of the client account opening, it is considered that a long-term agreement has been concluded between TKNBX OÜ and the client on general terms in electronic form (articles 9, 35 of the General Explanatory Note).

6.7. As TKNBX OÜ allows to establish business relationships without direct contact, the identity shall be established based on the data received from the client and the information received shall be verified in reliable and independent sources.

6.8. TKNBX OÜ concludes a long-term contract with the client via the electronic platform to provide services. In the case of a high-risk client, TKNBX OÜ enters into the contract staying at one and the same place with the client or taking into account additional due diligence measures that allow direct contact with a representative of TKNBX OÜ (e.g. a recorded Skype Online conversation) to a potential client or their representative. The contact can occur at the location of the TKNBX OÜ's permanent business or outside of it, if at least the same duties of thorough verification as in the ordinary cases are met in the course of it.

---

[17] When the document is considered damaged or corrupted: the photo is crumpled; the photo became blurred; the photo was partially or completely separated from the document; the photo detached from the document, is reattached by the user; the protective film covering the photo and personal data is detached or torn; covers are cut to a smaller size or one or more corners are missing.

6.9. When establishing a business relationship with a person, with whom TKNBX OÜ has not entered into a valid long-term contract through the electronic platform, TKNBX OÜ shall apply careful verification measures appropriate to a particular risk degree of the person, and among other things it is always necessary to establish the identity of the person, the real beneficiary and the purpose of the transaction.

6.10. TKNBX OÜ does not create business relations with anonymous clients and does not allow making transactions (exchanging virtual currency for money) anonymously. TKNBX OÜ does not allow the client to make transfers (withdraw official money received during the exchange of virtual currency for money) to third-party bank accounts.

6.11. TKNBX OÜ does not create business relations with anonymous clients and does not allow to make transactions (exchange of virtual currency for money) anonymously. TKNBX OÜ does not allow the client to make transfers (withdraw official money received during the exchange of virtual currency for money) to third-party bank accounts.

6.12. During the term of the long-term contract concluded with the client, TKNBX OÜ organizes ongoing supervision over business relations, that is, monitoring of business relations.

6.13. Monitoring of business relations shall be documented and cover the following actions:

6.13.1. verification of transactions made in business relations to ensure that transactions correspond to the knowledge of the obligated person about the client, their activities and risk profile;

6.13.2. regular updating of appropriate documents, data and information collected during the application of the due diligence measures;

6.13.3. determination of the source and origin of the funds used in the transaction.

6.14. TKNBX OÜ shall always pay more attention to business transactions, client activities and circumstances pointing to criminal activity, money laundering or terrorist financing, or linking them to money laundering or terrorist financing, when establishing business relations and monitoring business relations probably based on the client's degree of risk[18], including special attention to complex, high-value and unusual transactions and transaction

[18] https://www2.politsei.ee/dotAsset/258254.pdf

methods that do not have reasonable or vivid economic or legal purpose, or that are not typical for particular business specifics, as well as to a business relationship and transaction, if a client is from a third state with a high risk or a state or territory, specified in clause 5.9 of these rules, or has the citizenship of that state, or their place of residence or location, or the location of the person offering the payment service of the payee is located in the specified state or territory.

6.15. TKNBX OÜ is forbidden to establish a business relationship or allow even from time to time to make a transaction or bring it to the end, if it cannot perform the following measures of thorough verification: establishing the identity of the person and its verification in a reliable source; establishing the identity of the person's representative; establishing the real beneficiary or establishing the ownership structure and control of the person participating in the transaction, or if TKNBX OÜ has a suspicion of money laundering or terrorist financing. TKNBX OÜ is prohibited from establishing a business relationship or making a deal with a person whose capital forms bearer equities or other bearer securities.

6.16. If in the case specified in clauses 6.13 and 6.14 TKNBX OÜ is in business relations with the client, the client's refusal to provide the necessary information for verifying information or documents is considered to be a material breach of the contract and TKNBX OÜ is obliged to refuse from the long-term contract being the basis of business relationship exceptionally without observing the terms of the notification and to report on a suspicious transaction related to the client to the Money Laundering Data Office.

6.17. TKNBX OÜ has the right to refuse to conclude a transaction, if the person participating in the transaction or service act, the person or client using the service, in spite of the relevant requirement, does not submit documents and proper information or data or documents being the subject of the transaction to confirm the origin of the property, or if on the basis of the submitted data and documents, the obligated person has a suspicion that there may be money laundering or terrorist financing, or the commission of the related crime, or an attempt to perform such an activity. In such a case, TKNBX OÜ has the right to terminate the long-term contract being the basis of business relationship on an exceptional basis without observing the terms of the advance notice.

6.18. TKNBX OÜ has the right to cancel a long-term contract in the usual manner, having notified the client about it in writing within a reasonable time.

6.19. Business relations are deemed to have ceased by the submission of a refusal to the client for notification, after which TKNBX OÜ restricts the provision of services to the client in full.

6.20. TKNBX OÜ may, upon termination of the contract with the application of clauses 6.16, 6.17, transfer the client's property only to an account opened in a credit institution or a branch of a credit institution registered in Estonia in a foreign country or in a credit institution registered or whose place of business is located in the member state of the agreement on the European Economic Area or the state where the requirements equivalent to the requirements of the directive of the European Parliament and Council (EL) 2015/849 have effect. In an exceptional case, the property can be transferred to an account different from that of the client, giving advance notice to the Money Laundering Data Office about this, at least **seven working days in advance** and provided that the Money Laundering Data Office does not give a different order.

7. DUE DILIGENCE MEASURES

7.1. TKNBX OÜ applies the due diligence measures established by these rules of procedure and the RahaPTS when establishing business relations and during business relations.

7.2. TKNBX OÜ applies the following due diligence measures:

7.2.1. establishment of the identity of the client or the person participating in the transaction from time to time, as well as verification of the information provided in a reliable and independent source, on the basis of the information obtained, including by means of reliable e-identification services and e-transactions;

7.2.2. establishment and verification of the identity and right of representation of a representative of a client or a person participating in the transaction from time to time;

7.2.3. establishment of a real beneficiary and taking measures to verify their identity to the extent that the obligated person fully realizes that they know who the real beneficiary is and understands the ownership and control structure of the client and the person participating in the transaction from time to time;

7.2.4. understanding of the business relationship, the transaction or action performed from time to time and, if appropriate, collecting additional information about this;

7.2.5. obtaining information about the circumstance whether a person is a politically significant person, a member of their family or a person considered to be their close colleague;

7.2.6. monitoring of business relations.

7.3. TKNBX OÜ shall, in addition to the due diligence measures established in clause 7.2, evaluate the content and purpose of the transactions and actions of the client comprehensively, and establish a permanent location, place of activity or residence, profession or field of activity, important partners in transactions of the person, paid taxes and in case of the legal entity also experience and, if necessary, the source and origin of the funds used in the transactions, as well as other important information for establishing business relations.

7.4. TKNBX OÜ will, if necessary, require the person to provide the documents necessary for the application of the due diligence measures and appropriate information. If there is a suspicion, TKNBX OÜ will require the person to confirm the accuracy of the information and documents provided with their signature, including digital signature, or provide notarized or officially certified documents.

7.5. In the establishment and continuation of business relations, TKNBX OÜ shall fulfill the “know your client” principles, considering the risk categories and choose the conformity, the appropriate scope and method of performing the due diligence.

7.6. TKNBX OÜ establishes the identity of the client and the real beneficiary prior to the commencement of actions on conclusion of a long-term contract.

7.7. **The representative of TKNBX OÜ establishes the identity of all persons and their representatives in the following cases:**

7.7.1. when establishing business relations (in transactions for the exchange of virtual currency for money);

7.7.2. in the commission or mediation of transactions from time to time outside business relations, if the value of the transaction is more than EUR 15,000 or an equivalent amount in another currency, regardless of whether the monetary obligation is fulfilled by one payment or several interconnected payments in a period of up to one year;

7.7.3. in case of suspicion of insufficiency or reliability of documents or data previously collected during the verification of information or updating of the relevant data;

7.7.4. if there is a suspicion of money laundering or terrorist financing, irrespective of any exception or ceiling amount specified in the law of concession.

7.8. TKNBX OÜ verifies the correctness of client data and applies monitoring of business relations at least once a year. In the case of a high-risk client, the risk degree / profile of the client shall be re-evaluated no later than six months after the establishment of the business relationship.

7.9. TKNBX OÜ keeps information and documents relating to the identity of persons in a manner that allows to respond to the relevant requests of the Money Laundering Data Office, the investigative institution, the court or the supervisory institution (corresponding CMR system) fully and without undue delay.

7.10. TKNBX OÜ cannot provide services that can be used without identifying the person participating in the transaction and verifying the information provided, except when providing a service for the exchange of virtual currency for virtual currency.

7.11. TKNBX OÜ is required to open an account and maintain an account on behalf of the account holder.

8. ESTABLISHMENT OF THE IDENTITY OF THE PHYSICAL PERSON WHEN CREATING BUSINESS RELATIONS

8.1. TKNBX OÜ establishes the identity of the person and, if applicable, also the identity of the representative of the person in the cases specified in clause 7.7 and saves the following information about the person and their representative:

8.1.1. full name;

8.1.2. personal identification code, in its absence, the date and place of birth, as well as the place of residence or location;

8.1.3. information on the right of representation and the establishment and verification of its scope, as well as if the right of representation does not follow from the law, the title, date of issue and the name of the person that issued the document which is the basis of the right of representation.

8.1.4. The client sends the data necessary to establish identity via an electronic platform (a normal client or a low-risk client). In case of dealing with a high-risk client, the client shall send the data necessary to establish identity through an electronic platform, however TKNBX OÜ applies additional due diligence measures (request for additional information, telephone conversation, Skype Online conversation or, if necessary, direct contact with the client being in one place).

8.2. TKNBX OÜ establishes the identity of an physical person based on the following documents:
- 8.2.1. identity card: digital identity card or residence permit card;
- 8.2.2. passport of an Estonian citizen;
- 8.2.3. diplomatic passport;
- 8.2.4. the seafarer's passport;
- 8.2.5. the alien's passport;
- 8.2.6. temporary exit document;
- 8.2.7. refugee's exit document;
- 8.2.8. the seafarer's certificate;
- 8.2.9. certificate of return;
- 8.2.10. permission to return;
- 8.2.11. passport of a citizen of a foreign country;
- 8.2.12. ID card of a citizen of the European Union;
- 8.2.13. the driver's license if the name, photo or image of the person, signature or image of the signature and date of birth or personal identification number of the user are entered in the document.

8.3. TKNBX OÜ evaluates the document, submitted for identification of a person, as follows:
- 8.3.1. Verify the validity of the document by the validity period, the validity of the documents issued in Estonia is checked here: https://www.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/
- 8.3.2. The external similarity of the face and the compatibility of age with the appearance of the person indicated in the document are checked;
- 8.3.3. The conformity of the personal code / date of birth to the age of the person is checked;

8.3.4. In relation to information contained in codes issued to physical persons of a foreign country, in case of suspicion of the authenticity of the document or the identity of the person, it is necessary to consult with foreign missions or other competent institutions.

8.4. In addition to establishing the identity of the person, the address of the place of residence, the activity profile, the profession and the scope of activities of the person, the purpose and nature of the business relationship, if necessary, a real beneficiary and other similar important information for creating a business relationship, shall also be established. The obligated person shall register the address of the place of residence, activity profile, profession and sphere of activity of a physical person in the course of establishing identity and verification, on the basis of a person's testimony. In the case of a high-risk client, TKNBX OÜ asks the client to provide additional certificates / confirmations of the submitted data (request an account for their telephone or housing expenses).

8.5. Knowing the scope of activity, work or profession allows to assess whether business relations or transactions are consistent with the normal participation of the client in civil turnover, and whether the business relationship or transaction has a clear business rationale. In the appropriate case, TKNBX OÜ establishes the origin of the wealth of the person.

8.6. TKNBX OÜ keeps a copy of the document submitted for the identification of the person (.pdf, .jpg) in its CMR program, which shall be of such a quality that allows a clear reading of the data contained therein.

8.7. If the person to be identified has a valid document specified in clause 8.2 and their identity is established and it is verified on the basis of this document or by means of reliable e-identification services and e-transactions, and the document's effect is seen from this document or can be established using means of reliable e-identification services and e-transactions, additional data about the document need not be retained.

8.8. In addition to the address of the place of residence of the physical person, TKNBX OÜ asks the client to provide other contact details, including the e-mail address, telephone number and, if necessary (in case of suspicion) the social network account and other similar data.

8.9. When establishing a physical person, the following shall be investigated and checked:

8.9.1. Is the person a politically significant person or not: during the interview of the person and checked in public databases https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/

8.9.2. In the event that it is determined that there is a matter of dealing with a politically significant person, enhanced due diligence measures are applied to the person. The obligated person shall organize regular reinforced control in the business relationship established with the politically significant person.

8.9.3. Is the person subject to international sanctions or not: https://www2.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/ or https://www.sanctionsmap.eu/#/main. In the event that it is determined that there is a deal with a subject of international sanctions, TKNBX OÜ refuses to establish or continue business relations.

8.10. When establishing a physical person, an obligated person is obliged, if suspected, to establish also a real beneficiary of a physical person, that is, a person controlling a person's activities. The suspicion may be indicated by: the behavior of the person, the data presented, slurred speech, appearance, etc. When establishing a real beneficiary, one should also proceed from the risk of money laundering and terrorist financing, which depends on the type of client, country of origin, business relationship, product, service or transaction.

8.11. TKNBX OÜ generally establishes and verifies the identity of the client on the basis of documents and data provided through the electronic platform. In the case of a high-risk client, the client's identity is always established staying in the same place with the client or by applying other additional enhanced measures of thorough verification.

8.12. TKNBX OÜ carries out digital verification of the identity of the person through a certificate allowing the digital setting (PIN 1). The function of the second source is performed by checking the provided data on the relevant web page of the Police and Border Guard Department https://www.politsei.ee/id-kaardi-kontroll/.

8.13. In a situation where, in the case of data provided to establish the person's identity, it is not possible to digitally verify the identity of the user of the document through a certificate allowing the digital setting (PIN 1), e.g.

persons who do not have an Estonian ID-card, digital ID, mobile ID, or who are not residents of Estonia can use the following data if there is a suspicion to establish a person's identity and verify the information provided:

8.13.1. to request an account, issued by the person providing communal services, communication service or other administrative services, from which these places of activity of the person are seen (the document to be submitted shall not be more than three months old);

8.13.2. to request from the state party of the agreement on the European Economic Area or the competent institution a confirmation or a certificate of early long-term relations with the person or about the activity (the document to be submitted shall not be more than three months old);

8.13.3. to request a control payment made from a personal account of a person who is in a credit institution or financial institution in a member state of the agreement on the European Economic Area or an account statement for the last month.

9. ESTABLISHMENT OF THE IDENTITY OF THE LEGAL ENTITY WHEN CREATING BUSINESS RELATIONS

9.1. TKNBX OÜ establishes the identity of a legal entity on the basis of the following documents:

9.1.1. registry card of the relevant register;

9.1.2. registration certificate of the relevant register;

9.1.3. or a document equivalent to the specified document.

9.2. TKNBX OÜ shall ensure that the information provided is accurate using information from a reliable and independent source, and if possible, TKNBX OÜ makes a request to the commercial register or the relevant register of a foreign state. If an obligated person has access to the data of the commercial register, the register of non-profit associations and foundations or the corresponding register of a foreign state through a computer network, it is not necessary to require the client to provide the documents specified in clause 9.1.

TKNBX OÜ establishes the identity of the legal entity registered in Estonia

and the branch of a foreign country's business association registered in Estonia, as well as the legal entity of a foreign state, and retains the following information about it:

9.2.1. the trade name or the name of the legal entity;

9.2.2. the registration code or the registration number and time of registration;

9.2.3. the name of the chairman of the management board or the names of members of the management board or members of another body substituting for it, and their authority when presenting the legal entity;

9.2.4. data of communication facilities of a legal entity;

9.2.5. data of real beneficiaries;

9.2.6. the scope of activity of the legal entity;

9.2.7. the purpose of the client relationship;

9.3. When establishing a legal entity, it is necessary to investigate and verify:

9.3.1. Are the persons who are politically significant persons in the management, real beneficiaries of the person or not: during the interview of the person and checked in public databases https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/.
In the event that it is determined that there is a matter of dealing with a politically significant person, enhanced due diligence measures shall be applied to the person. The obligated person shall organize regular reinforced control in the business relationship with the politically significant person.

9.3.2. Is the legal entity or management of a legal entity subject to international sanctions or not: https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/ or https://www.sanctionsmap.eu/#/main.
In the event that it is determined that there is a deal with a subject of international sanctions, TKNBX OÜ refuses to establish or continue business relations.

9.4. When establishing the identity of a representative of a legal entity, TKNBX OÜ proceeds from the rules set forth in clause 8. The representative of a legal entity of a foreign state shall, at the request of TKNBX OÜ, provide a document confirming their authority or a document certified in a manner equivalent to this procedure that is legalized or confirmed by a certificate

(apostille) substituting for legalization, unless otherwise established by an international treaty.

10. REAL BENEFICIARY

10.1. The real beneficiary is a physical person, who, using his influence, controls the transaction, operation or other person, and in the interests, in favor or at the expense of which the transaction or operation is made. In the case of a business association, the real beneficiary is a physical person, who ultimately owns or controls a legal entity by directly or indirectly owning a sufficient number of shares, equities, voting rights or ownership, including participation in the form of shares or bearer equities, or otherwise.

10.2. Direct possession is a method of control, in which case a physical person owns 25 per cent plus one share in a business association, or over 25 per cent in ownership. Indirect possession is a method of exercising control, in which a business association has 25 percent plus one share in a business association or an ownership interest of more than 25 percent, a business association under the control of a physical person or several commercial associations under the control of the same physical person. If after the exhaustion of all possible methods of establishment it is impossible to establish the specified person and there is no suspicion that such person still exists, or if there is a suspicion that the established person is the real beneficiary, then the physical person, who is a member of the supreme governing body is considered to be the real beneficiary.

10.3. In the case of a limited partnership, a company, a union or another association that do not have the status of a legal entity, the real beneficiary is a physical person who, through direct or indirect ownership or in any other way, definitively controls the association and who is in such an association:

10.3.1. the founder or the person who transferred the property to the aggregate of property;

10.3.2. a trustee, a manager or a property owner;

10.3.3. the person providing and monitoring the safety, if such person is appointed, or

10.3.4. the beneficiary or, if the beneficiary or beneficiaries are appointed in the future, the circle of persons for whose benefit the association was primarily established or operates. In the case of a person or an

association not mentioned in this clause, a member of members of the board may be appointed as a real beneficiary.

10.4. TKNBX OÜ when creating a business relationship, establishes a real beneficiary, registers and saves information on all actions that have been taken to establish a real beneficiary.

10.5. TKNBX OÜ is forbidden to create a business relationship or allow the transaction to be made from time to time or to finish it if it cannot establish a real beneficiary or if there is a suspicion of money laundering or terrorist financing.

11. STRENGTHENED APPLICATION OF DUE DILIGENCE MEASURES

11.1. TKNBX OÜ applies a due diligence measure in a strengthened manner to properly manage and reduce the risk of money laundering and terrorist financing higher than the usual risk.

11.2. TKNBX OÜ applies due diligence measures if, based on the risk assessment, it is established that in the case of this economic or professional activity, scope or circumstances, there is a situation with a risk of money laundering and terrorist financing higher than usual.

11.3. Due diligence measures in a strengthened manner are always applied if:

11.3.1. when establishing the identity of a person or checking the information provided, there was a suspicion of the reliability of the information provided or the authenticity of the documents or the establishment of a real beneficiary;

11.3.2. a person who participates in a transaction or an official act in a business or professional activity, a person or a client using the service is a politically significant person, with the exception of a local politically significant person, a member of their family or a close colleague;

11.3.3. a person who participates in a transaction or an official act performed in an economic or professional activity, a person or a client using the service from a third person with a high risk or their place of residence or location, or the location of the person offering the payment service of the payee is in a third state with high risk;

11.3.4. the client or the person participating in the transaction or the person using the service from such state or territory, or their place of residence or location, or the location of the person offering the payment service of the payee is in the state or territory, according to reliable sources such as mutual assessments, reports or subsequent reports disclosed, there are no effective anti-money laundering and terrorist financing systems that are consistent with the Financial Measures Developing Group's revised recommendations to combat money laundering, or which are considered to be a territory with a low tax rate.

11.4. TKNBX OÜ selects additional due diligence measures to manage and reduce the established higher risk of money laundering and terrorist financing, and applies one or more of the following due diligence measures:

11.4.1. verification of additional information provided in the identification of a person on the basis of additional documents, data or information in a reliable and independent source;

11.4.2. collection of additional information on the purpose and content of business relations, transactions or actions, as well as verification of the information provided on the basis of additional documents, data or information in a reliable and independent source;

11.4.3. collection of additional information and documents on actual transactions in business relations, in order to exclude the imaginary nature of transactions;

11.4.4. collection of additional information and documents for establishing the source and origin of the funds used in the transaction performed in business relations, in order to exclude the imaginary nature of transactions;

11.4.5. execution of the first payment related to the transaction through an account opened in the name of the person or client participating in the transaction in a credit institution registered or located in a member state of the agreement on the European Economic Area or in a state where the requirements equivalent to the requirements of Directive of the European Parliament and Council (EL) 2015/849 apply;

11.4.6. application of due diligence measures in relation to a person or their representative staying with them in one place.

11.5. TKNBX OÜ shall, when applying due diligence measures in a strengthened manner, more often than usual monitor business relations, including no later than six months after the establishment of a business relationship, reassess the client's risk profile.

11.6. If TKNBX OÜ collides with a **third high-risk country** through a business transaction or a participating transaction of a person using the service of a person or client, TKNBX OÜ shall apply the following due diligence measures:

11.6.1. obtaining additional information about the client and their real beneficiary;

11.6.2. obtaining additional information about the planned content of business relations;

11.6.3. obtaining information about the origin of funds and the wealth of the client and their real beneficiary;

11.6.4. obtaining information on the reasons for planned or completed transactions;

11.6.5. obtaining permission from senior management to establish or continue business relations;

11.6.6. intensification of monitoring of business relations, increasing the number and frequency of verification measures applied, and selecting indicators of transactions that are additionally verified.

11.7. In addition to the foregoing, TKNBX OÜ may require the client to make a payment from the client's personal account located in the credit institution of the state party to the agreement on the European Economic Area or a third state where the requirements equivalent to the requirements of the European Parliament and Council Directive (EL) 2015 / 849 apply.

11.8. The board shall decide on rendering of services, establishment and continuation of business relations with a high-risk client.

12. MEASURES IN A SIMPLIFIED MANNER CAN BE APPLIED IF THE FOLLOWING CONDITIONS ARE FOLLOWED:

12.1. The measures in a simplified manner can be applied if the following conditions are met:

12.1.1. a long-term contract has been concluded with the person;

12.1.2. entries occur only through an account located in a commercial institution registered in a commercial register of Estonia or a branch of

a credit institution of a foreign state or in a credit institution that is established or whose place of business is located in a member state of an agreement on the European Economic Area or state where equivalent requirements apply;

12.1.3. the total value of the incoming and outgoing payments made in business relations does not exceed EUR 15,000 per year.

12.2. When creating a business relationship or attempting to create one, simplified due diligence measures can be applied, if the person participating in a business transaction or an operation performed in an economic or professional activity is:

12.2.1. a public legal entity established in Estonia;

12.2.2. a government agency or other public institution in Estonia;

12.2.3. a credit institution or financial institution registered in Estonia, over which state supervision is exercised;

12.2.4. a notary or a bailiff of Estonia;

12.2.5. a credit institution operating in its own name or a financing institution located in a member state of the agreement on the European Economic Area or a State where equivalent requirements apply;

12.2.6. a person, who is a resident of a member state of the agreement on the European Economic Area or an equivalent state.

12.3. TKNBX OÜ is prohibited to apply simplified measures in case any suspicion of money laundering or terrorist financing arose at any stage of the service provision, in relation to the client or their activity.

13. PROCEDURES FOR THE EVALUATION AND MANAGEMENT OF RISKS COVERED BY TECHNOLOGY

13.1. **Definitions**

Information system is a technical system for processing, storing or transferring data, together with the resources and processes necessary for normal operation.

Risk analysis of the information system is the analysis that identifies the potential dangers and shortcomings for a critical information system,

assesses the likelihood of hazards and associated losses, and selects appropriate security measures to reduce the impact of the implementation of threats.

Information assets are basic and information technologies and technical equipment necessary for their processing.

Confidentiality is access to information resources only for authorized users (physical persons or technical systems) and inaccessibility for all others.

Availability is timely and convenient accessibility of data for authorized users. Timely and easy availability of the information resources used in the required time (that is, in the required time and within the required time period) for authorized users (persons or technical means).

Weakness is vulnerability for information assets, through which one or more risks can be implemented.

Danger is an event or circumstance that can lead to an interruption or damage to the information resource by any other means.

Risk is indefinite assessment of circumstances that may impede the ability of an institution or enterprise to provide a vital service in a timely manner in an established capacity or at a planned level. Information security is often expressed as a combination of the consequences of an information security event and its occurrence.

13.2. **Identification of technological risks**

Risk identification is carried out through risk analysis. The assessment of probabilities and consequences is based on the methodology of qualitative risk analysis.

Conducting a qualitative risk analysis is based on the analysis of various risk scenarios, taking into account the importance of threats and the value of protected assets and their potential shortcomings. Estimates are based on experience, and decisions are made primarily on the basis of past

experience and knowledge of appraisers. The qualitative risk analysis uses step scales to estimate the frequency of occurrence of potential risks and incidents. Scale of qualitative risk assessment. Definitions are interpreted by the Office of the State Information System.

13.3. **Management of technological risks**

Risk management is the process of selecting a method for identifying risks and implementing a risk reduction approach in accordance with the risk tolerance. The reduction in risks is primarily associated with the introduction of controls. Perhaps it was decided to reduce the risk or weakness associated with a specific risk.

14. RESPONSIBILITY OF COMMUNICATION IN CASE OF SUSPICION OF MONEY LAUNDERING AND TERRORIST FINANCING

14.1. If TKNBX OÜ establishes in the course of economic or professional activities, official activity or service, activities or circumstances, the signs of which indicate the use of income derived from criminal activities, terrorist financing, or the commission of an associated crime or attempt on such activities, or in case of which it has a suspicion or knows that there is money laundering or terrorist financing or the commission of an associated crime, it is obliged to inform the Money Laundering Data Office immediately through the X-tee service, but not later than within two business days after the establishment of the activity or circumstances, or the occurrence of suspicion.

14.2. Clause 14.1 applies also in the event that the creation of a business relationship, a transaction, an action or a provision of services remains unimplemented, and in the presence of circumstances specified in Articles 42 and 43 of the RahaPTS.

14.3. TKNBX OÜ is prohibited from notifying the person, the real beneficiary, the representative of that person or a third person, of the information on the message provided to the Money Laundering Data Office about them, the plans for providing such a message or the granting of information, as well as of the order issued by the Money Laundering Data Office based on articles 57 and 58 of the RahaPTS, or the commencement of criminal proceedings.

15. TRACKING OF UNUSUAL AND SUSPICIOUS TRANSACTIONS

15.1. All transactions and actions of clients, who lack a clear economic or legal reason, and which cannot be considered ordinary business activities of clients shall be considered unusual. TKNBX OÜ decides whether the transaction is different from the ordinary, on the basis of the set of circumstances known about the client and the transaction, considering that the client can, in view of an unreasonable suspicion, get damage. When evaluating a transaction or action, it shall be ascertained whether there is a different, but explained circumstance or change, taking into account the current behavior of the client, or there is a transaction with signs of money laundering or terrorist financing.

15.2. In the event of an unusual transaction, action or circumstance, TKNBX OÜ is obliged to analyze and compare the circumstances of the transaction with the signs of transactions suspected of money laundering. It is also obliged to verify the legal origin of the property before the transaction, at least in the event that the transaction, taking into account the current client relationship, is unusual, with suspicion of money laundering or terrorist financing.

15.3. The instruction of Money Laundering Data Office on the characteristics of transactions suspected of money laundering is part of these rules[19]. The employee evaluates the activities of the client according to the indicators specified in the instructions of the Money Laundering Data Office.

15.4. The instruction of the Money Laundering Data Office on the Signs of Transactions with Suspicion of Terrorist Financing is part of these rules[20]. The employee evaluates the activities of the client according to the indicators specified in the instructions of the Money Laundering Data Office.

15.5. If there is a suspicion of money laundering and terrorist financing, TKNBX OÜ is required to notify the Money Laundering Data Office.

---

[19] The instruction of the Money Laundering Data Office on the Signs of Money Laundering Transactions, which can be found on the published website of the Police and Border Guard Service: https://www.politsei.ee/dotAsset/258252.pdf.

[20] The instruction of the Money Laundering Data Office on the Signs of Money Laundering Transactions, which can be found on the published website of the Police and Border Guard Service: https://www.politsei.ee/dotAsset/258252.pdf.

16. SCREENING

16.1. According to the tracking of transactions in real time, TKNBX OÜ verifies the behavior and transactions of the client, in order to establish unusual or suspicious, or those exceeding the prescribed limits of the transaction.

16.2. TKNBX OÜ when tracking transactions in real time selects information technology tools based on the parameters provided:

16.2.1. whether the counterparty is a client of TKNBX OÜ;

16.2.2. transactions with persons, name, date of birth, and similar data of which coincide with the data published in the list of persons who are subjects of international sanctions;

16.2.3. transactions with persons whose country of business and origin is in the list of countries with a higher risk (terrorism).

17. MONITORING

17.1. In order to facilitate the disclosure of suspicious transactions, TKNBX OÜ applies measures to disclose the lack of information related to the payer in the payment instruction.

17.2. With the help of monitoring systems, TKNBX OÜ determines from the number of payments whether the notice used for the transaction is submitted, according to the service offer, with the correct entry.

17.3. For the subsequent monitoring, it is possible to analyze transactions that, based on the presence of the provided parameters, are separated from the mass of transactions. In addition, with subsequent monitoring of transactions, larger transactions are analyzed for a certain period under consideration, for different virtual currencies.

17.4. Scenarios for monitoring transactions are as follows:

17.4.1. transactions of a larger volume of the period under review (transactions exceeding EUR 15,000), including in various virtual currencies;

17.4.2. single, unusually large (i.e. one transaction is over EUR 15,000), inconsistent with turnover and / or quite unreasonable transaction;

17.4.3. a sharp increase in the volume of transactions of the client with a small turnover (i.e. transactions exceeding EUR 15,000);

17.4.4. an account from which no transactions were made within three months, becomes active;
17.4.5. transactions, for which TKNBX OÜ is known to be associated with PEP;
17.4.6. transactions, for which TKNBX OÜ is aware of the relationship with the risk state (e.g. in the case of a legal entity, a real beneficiary).

17.5. If TKNBX OÜ finds that the information required is missing or incomplete in the instruction, then TKNBX OÜ refuses to complete the transaction or asks the client for full information. If the client is not able to provide the required information on a regular basis during the provision of the service, TKNBX OÜ applies measures that include setting deadlines for obtaining information and issuing warnings about the termination of business relations. If the person does not respond to the terms indicated in the letter, TKNBX OÜ refuses to make any transactions with this client and terminates the business relationship. TKNBX OÜ reports such termination of the business relationship to the Money Laundering Data Office.

18. KLIENDISUHTE LÕPETAMINE JA LEPINGU ÜLESÜTLEMINE

18.1. TKNBX OÜ is obliged to refuse from the service agreement with the client exceptionally without observing the terms of the notification, if the person does not provide, in spite of the relevant requirement, documents and information necessary for applying the due diligence measures, or if the provided documents and data do not eliminate the suspicion of TKNBX OÜ that the purpose of the transaction or business relationship may be money laundering or terrorist financing.
18.2. In case of termination of business relations, prior to the performance of instructions given in connection with the service, TKNBX OÜ transfers the client's funds back to the account where the payment instruction came from.
18.3. If a person, with whom previous business relations on the initiative of TKNBX OÜ has been terminated on the basis of suspicion of money laundering and terrorist financing, appeals to TKNBX OÜ to re-establish business relations, a contact person shall be involved in making a decision on the establishment of a business relationship.

19. DATA COLLECTION AND STORAGE

19.1. TKNBX OÜ registers:

19.1.1. the date or period of the transaction and the description of the contents of the transaction;

19.1.2. information on the creation by the obligated person of a business relationship or circumstances of refusal to enter into a transaction from time to time;

19.1.3. on the establishment of business relations on the initiative of the person participating in the transaction or service, the person or client using the service, or the circumstances of the refusal to conclude the transaction, including the transaction from time to time, if the refusal is related to the application by the obligated person of the due diligence measures;

19.1.4. information if through the information technology means it is impossible to apply the due diligence measures specified in part 1 of article 20 of the RahaPTS;

19.1.5. information on the circumstances of the termination of business relations due to the inability to apply due diligence measures;

19.1.6. information, which is the basis of the obligation of communication, which arises from Article 49 of the RahaPTS;

19.1.7. making transactions with the representative of the company, union or other association that does not have the status of a legal entity or with a trusted fund or with a trustee, the circumstance that the person has such status, as well as the extract from the registry card from the register or a certificate from the holder of such register, where the association without the status of a legal entity is registered.

19.2. TKNBX OÜ is required to keep the originals or copies of documents that are the basis for establishing the identity of the person and verification of the information provided, and documents that are the basis for establishing business relations, for five years after the termination of business relations.

19.3. TKNBX OÜ shall keep the documents prepared for the transaction on any data carrier, as well as the documents and data that are the basis for the obligation to communicate, for at least five years after the transaction or the performance of communication obligation.

19.4. TKNBX OÜ shall keep the above documents and data in a manner that allows exhaustive and immediate response to the requests of the Money Laundering Data Office or, in accordance with the legal acts of other supervisory institutions, investigative institutions and courts, including whether or not the obligated person is or was in business relations with the person specified in the request during the previous five years, as well as the kind of the essence of these relations.

19.5. TKNBX OÜ applies all rules for the protection of personal data when applying the requirements of this law. TKNBX OÜ processes collected personal data only to counter money laundering and terrorist financing.

20. TRANSFER OF ACTIVITIES

20.1. The transfer of activities established by the rules, in general due diligence measures (for example, identification of a person) to third parties may arise from the need to fulfill their duties related to economic activities more effectively. When transferring activities to third parties, TKNBX OÜ is fully responsible for violation of the requirements.

20.2. TKNBX OÜ in the transfer of activities concludes a written contract with the cooperation partner. The transfer of activities is permissible only if:

20.2.1. this does not prejudice the justified interest of TKNBX OÜ;

20.2.2. this does not preclude the activities of TKNBX OÜ and the performance of duties related to combating money laundering and terrorist financing;

20.2.3. this does not preclude the exercise of state supervision over TKNBX OÜ;

20.2.4. the third person to whom the activity is transferred has the necessary knowledge and skills, and also is able to perform all requirements related to countering money laundering and terrorist financing (must be an obligated person);

20.2.5. TKNBX OÜ has the right and the ability to monitor compliance by a third party with anti-money laundering and terrorist financing requirements;

20.2.6. it is ensured that documents and data that are collected to perform the anti-money-laundering and terrorist financing related requirements will be stored in accordance with the established procedure.

20.3. TKNBX OÜ undertakes to notify the heads of the cooperation partners about the requirements for combating money laundering and terrorist financing, as well as to train their employees in the field of combating money laundering and terrorist financing. TKNBX OÜ also undertakes to inform the employees of the cooperation partners at least once a year after the training, of the nature of the risks of combating money laundering and terrorist financing and new directions in this area. First of all, employees shall be aware of the requirements that regulate the counteraction to money laundering and terrorist financing, with regard to the application of due diligence measures and identification of money laundering and reporting on it.

20.4. TKNBX OÜ reports the transfer of its activities immediately to the Money Laundering Data Office.

21. INTERNATIONAL SANCTIONS

21.1. When establishing business relations and during business relations, special attention should be paid to the person's activities and circumstances that indicate the possibility that a person is subject to an international financial sanction and the establishment of an entity of an international financial sanction, a contact person shall be immediately informed of the relevant suspicion and measures taken.

21.2. If TKNBX OÜ suspects that a person wishing to conclude a service contract or an existing client is subject to an international sanction, additional information shall be requested from the client to determine whether the person is such or not. If a person refuses to provide additional information or with its help it is impossible to establish whether a person is an entity of international sanction, it is not allowed to start a business relationship with the person and make a deal with the client, the measures prescribed by the international sanction shall be applied and the Money Laundering Data Office shall be informed.

21.3. Subjects of international sanction are checked by TKNBX OÜ on the website of the Money Laundering Data Office https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/ by entering the name of the audited person. TKNBX OÜ undertakes to ensure that when establishing a

business relationship and providing a single service, it is ascertained that no international sanctions have been applied to the persons involved in the transaction. The verification of persons from the sanctions list is carried out manually and the following data is stored in the CRM program for 5 years:

- verification time;
- name of the person who carried out the verification;
- results of the verification;
- measures taken.

21.4. The contact person shall immediately inform the Money Laundering Data Office if it turns out that a person who wishes to enter into business relations with TKNBX OÜ or has already entered into a business relationship will be subject to an international sanction or if it is suspected that the person concerned is subject to an international sanction. The client immediately loses access to services and undergoes an international sanction taking into account its content and scope.

22. EMPLOYEES' TRAINING

22.1. The contact person regularly and necessarily conducts training to clarify the requirements and duties fixed in the rules, and also provides information on modern methods of money laundering and terrorist financing and related risks.

22.2. The first training in the field of money laundering is carried out with the recruitment of employees and for employees directly engaged in servicing clients, training is conducted once a year.

22.3. During the training, the contact person shall proceed from the following circumstances:

22.3.1. The opportunity for an employee to face unusual transactions that may be related to money laundering and terrorist financing;

22.3.2. Typical cases of suspicious and unusual transactions, possibly observed in the sphere of the employee's activity, and the applied prevention mechanisms;

22.3.3. The application of sanctions against employees who do not fulfill the requirements of the law or the legal acts established on the basis of it for combating money laundering and terrorist financing.

22.4. The contact person keeps records of trained workers, noting the subject of training, the exact time and the name of the participating employee.

23. ACTIONS FOR INTERNAL CONTROL

23.1. The internal control system of TKNBX OÜ is structured in such a way that the contact person directly supervises the performance of the rules by the employees.

23.2. The contact person shall draw up, as a result of the control, a monitoring report containing at least the following information:

- purpose of control;
- time of control;
- name and position of the person who carried out the control;
- description of the control performed;
- analysis of control results and general conclusions of the control performed.

23.3. If there are any deficiencies in applying the rules revealed in the course of the control, the contact person shall include a description of the deficiencies in the report, together with the associated risks. As a result of the control, the time to eliminate the shortcomings, the measures preferably used to eliminate the shortcomings and the time for the subsequent control, are appointed.

23.4. When implementing the follow-up control, the control report shall be accompanied by an analysis of the results of the follow-up control and a list of measures used to eliminate the shortcomings, indicating the actual time spent to eliminate the shortcomings.

23.5. The contact person, in connection with the control over the implementation of measures to combat money laundering and terrorist financing, has the following duties:

- to monitor compliance with the requirements of combating money laundering and terrorist financing;
- to assess the need for employee training;
- to analyze the results of monitoring compliance with requirements.

23.6. The contact person, in connection with the control over the implementation of measures to combat money laundering and terrorist financing, has the following rights:

- to monitor the work of employees and obtain the necessary technical means for this;
- to demand an immediate termination of the violation of the requirements for combating money laundering and terrorist financing;
- to make proposals for the elimination of deficiencies identified during the control, including for the introduction of amendments and additions to the rules.

23.7. The contact person conducts internal control at least once a year.