

**ANTI MONEY-LAUNDERING AND COUNTER-TERRORISM FINANCING (AML/CTF)
POLICY OF HONOS OÜ OF 14/10/2019**

1. Obligated person, activity licenses

1. Obligated person: HONOS OÜ
2. Registry code: 14656968
3. Address: Lõõtsa str 2B, Tallinn, Republic of Estonia 11415
4. E-mail: info@honos.pro
5. Areas of activity and licenses:
 - 5.1. Virtual Currency Exchange Service, license FVR000714 issued by the Police and Border Guard Board of the Republic of Estonia on 15/02/2019
 - 5.2. Virtual Currency Wallet Service, License FRK000621, issued by the Police and Border Guard Board of the Republic of Estonia on 15/02/2019
 - 5.3. Currency Exchange Service, license FVR000714 issued by the Police and Border Guard Board of the Republic of Estonia on 20/02/2019

2. HONOS OÜ source documents for anti-money laundering and the prevention of terrorist financing and implementation of international financial sanctions

By decision of HONOS OÜ Management Board, on 07/02/2019, HONOS OÜ has established the “Internal Rules and Procedures for the Exchange of Virtual Currency and Virtual Currency Wallet Service Provider”.

3. Establishing a business relationship and verifying the customer

1. When establishing a business relationship, the identification (verification) of the customer by means of information technology tools is carried out on the Internet (online) in accordance with the “Technical Requirements and Procedures for Identifying and Verifying Identity through Information Technology Tools” and the requirements of §24 and §31 of the Money Laundering and Terrorist Financing Prevention Act valid in the Republic of Estonia;
2. Customer verification is carried out in cooperation with a contractual cooperation partner recognised in the Republic of Estonia and providing verification services (VERIFF OÜ, KCPASS OÜ, JUMIO CORPORATION etc);
3. When establishing a business relationship, it is checked whether the customer or the customer's country of origin is added to the list of international sanctions;
4. When establishing a business relationship, the customer's PEP status is checked (whether it is a politically exposed person, a family member of a politically exposed person, or a person considered close to him/her).

4. Data collected during the business relationship

1. Customer identification data (name, date of birth, personal identification code and other personal data, contact details, documents used for verification);
2. Customer location and tax residence details (citizenship, country of residence, address, tax identification number);
3. Customer's area of activity and business data;
4. The customer's PEP status (whether it is a politically exposed person, a family member of a politically exposed person, or a person considered close to him/her);
5. Transaction data (transactions, bank transfers, and card payments executed on the platform);
6. Data on the origin of funds and virtual currencies used in transactions (transaction counterparties and business partners, explanations of transactions);

7. Data collected during communication with the Counselling Centre (Customer Support);
8. Data collected from third parties (cooperation partners, registers, social media) used to fulfil statutory due diligence requirements.

5. Updating and amending customer data, monitoring and controlling customers and transactions

1. Customer data is updated at least once every two years, during which the customer is required to update and confirm his/her own data. Execution of transactions on the customer account is blocked before this requirement is fulfilled.
2. Under the terms of use of the HONOS.PRO platform, in case of change of personal data (personal data, contact details, residence data, PEP status, field of activity), the customer is obliged to immediately update the corresponding data in his/her own customer profile.
3. For transactions carried out on the HONOS.PRO platform, an automatic monitoring system (AML module) is applied. For transactions exceeding 32,000 euros (or the equivalent amount in other currencies, including virtual currencies) or that are more frequent than usual, as well as in case of the need for enhanced customer check, additional information is required from the customer (statement of transaction; certified statement of the customer's bank account; additional document identifying the person; other data).
4. Daily verification of the customer base is carried out with regards to the lists of international sanctions published on the website of the Financial Intelligence Unit at <https://www2.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/>
5. At least once a year, usually at the end of the financial year, the AML/CTF audit of the HONOS OÜ customer base is carried out.
6. Based on the results of the annual AML/CTF audit and the EU and national risk assessments, a monitoring plan for risky customer profiles and transactions is prepared for the following year, the risk assessment process is updated and updated by management, and new action plans are prepared. The Financial Intelligence Unit's contact person shall report (mark) the customer profiles with high risk category to all staff involved in customer management and financial transactions.

6. Risk categories, risk appetite and additional due diligence measures, service provision restrictions

1. Risk categories

- 1.1. The customers of HONOS OÜ are divided into three risk categories: low, normal and high risk. The determination of the risk category of a natural person customer is based primarily on his/her residency, PEP status and the nature of transactions. The legal person's risk category is determined based on the country of residence of the legal person, its field of activity, the structure and transparency of the governing bodies and owners of the legal person, and the nature of transactions.
- 1.2. In determining the risk category of the customer, the HONOS OÜ "Internal Rules and Procedures for the Exchange of Virtual Currency and Virtual Currency Wallet Service Provider. Annex 2" shall be applied, on the basis of which the risk category is determined as a sum of 7 sub risks, which is the risk related to the legal nature of the customer and the identification of its beneficial owners, the risk related to the national or regional areas or jurisdictions, the risk related to the customer's field of activity and products or services offered, the risk related to settlements and transactions, the risk related to a person with the PEP status, the

risk related to customer identity, and the risk related to the means of communication and transmission of information between HONOS OÜ and the customer.

- 1.3. **Characteristics of a customer with low risk category (category “A”):** A natural person resident in the Republic of Estonia who is not a PEP; Government agencies, insurance companies, pension funds and publicly listed companies of the Republic of Estonia and the EU, Switzerland, Norway, Iceland, Australia, Brazil, Canada, Hong Kong, India, Japan, South Korea, Mexico, Singapore, South Africa and the US not active in the fishing industry; personal property management, construction and repair; wholesale and storage of fuel; retail sale of fuel; wholesale wood trade; private or personal banking, currency, virtual currency or payment exchange; gambling and games of chance or casino; buying and selling of gold, other precious metals or precious stones; providing online advertising; the establishment, sale and management of companies, the turnover of which does not exceed 40,000 euros per year, and the turnover of transactions in the HONOS account (sum of received and made payments) does not exceed 15,000 euros per year, and the accounts used for such payments are opened in such a credit or payment institution or its subsidiary whose place of registration or activity is in the Republic of Estonia or in a member state of the European Economic Community or in a country where requirements equivalent to those of Directive (EU) 2015/849 of the European Parliament and of the Council are applied.
- 1.4. **Characteristics of a customer with normal risk category (category “B”):** Resident natural person with PEP status; a non-resident natural person who does not have a PEP status; Companies registered in Estonia and publicly listed companies in the EU, Switzerland, Norway, Iceland, Australia, Brazil, Canada, Hong Kong, India, Japan, South Korea, Mexico, Singapore, South Africa and the US, whose area of activity is the fishing industry; personal property management, construction and repair; wholesale and storage of fuel; retail sale of fuel; wholesale wood trade; private or personal banking, currency, virtual currency or payment exchange; gambling and games of chance or casino; buying and selling of gold, other precious metals or precious stones; providing online advertising; the establishment, sale and management of companies; or the companies of those countries, the turnover of which exceeds 40,000 euros per year, or the turnover of transactions in the HONOS account (sum of received and made payments) exceeds 15,000 euros per year, and the accounts used for such payments are opened in such a credit or payment institution or its subsidiary whose place of registration or activity is in the Republic of Estonia or in a member state of the European Economic Community or in a country where requirements equivalent to those of Directive (EU) 2015/849 of the European Parliament and of the Council are applied.
- 1.5. **Characteristics of a customer with high risk category (category “C”):** A non-resident natural person with PEP status; companies that do not meet the requirements listed in Articles 5.1.2 and 5.1.3 of this document; persons with higher risk categorised by countries or geographical areas or jurisdictions on the basis of the personal risk assessment of HONOS OÜ or the EU and national risk assessment.

2. Risk appetite and additional due diligence measures.

- 2.1. Virtual currency transactions mean carrying out or intermediating a transaction that can promote anonymity, at the same time, everything

related to virtual currencies is considered to be innovative product and new business practice (including a new transmission mechanism and the use of new technology), and the business relationship is established and the transaction initiated in a manner that does not require being in the same room with the customer or his/her representative, which is why additional diligence measures are applied to all transactions involving virtual currencies.

- 2.2. For customers with PEP status and those belonging to the high risk category (risk category 3) as well as their transactions, additional due diligence measures are implemented in an enhanced manner to identify the origin of the financial resources and wealth used in the customer's transactions, including re-evaluating the customer's risk profile and deciding on the continuation of the business relationship 6 (six) months after the establishment of the business relationship.
- 2.3. An application for establishing a business relationship or continuing a business relationship with customers with PEP status and those belonging to the high-risk category (risk category 3) shall be reviewed and approved or rejected by the Management Board of HONOS OÜ.
- 2.4. Money (FIAT) contributions to the customer's HONOS account can be made without explanation only from the customer's own bank account or debit card. If the data of the person who made the payment without explanation does not match the customer's HONOS account data, then the transaction will be rejected.
- 2.5. Third-party (FIAT) contributions to the customer's HONOS account are not allowed.
- 2.6. A payment without an explanation from the customer's account (FIAT) is only granted to the customer's account in a bank or payment institution opened on behalf of the customer participating in the transaction in a credit or payment institution registered or established in a member state of the European Economic Area or in a country where requirements equivalent to those of Directive (EU) 2015/849 of the European Parliament and of the Council are applied, and which has been previously verified (a contribution or a verification payment to HONOS account has been made via the account).
- 2.7. Payments (FIAT) to a third party from the customer's HONOS account are not allowed.
- 2.8. Customers' payments received and made in virtual currencies are monitored automatically and continuously. In the case of a single transaction exceeding 32,000 euros or several successive transactions in one (1) year if the amount of transactions exceeds 32,000 euros, the customer is required to provide additional information on the origin of the funds used in the transaction and on the parties to the transactions. Also, the frequency of transactions with virtual currencies is monitored automatically and in case of more frequent transactions, additional explanations are required from the customer regarding the cause of the transactions. During the business relationship, the nature and deviations of transactions with virtual currencies are monitored.
- 2.9. Cash (FIAT) and virtual currency disbursements are subject to a two-step authentication requirement for the identification of customer and ensuring of security during the transaction.
- 2.10. During the business relationship, HONOS OÜ monitors the behaviour of its customers in their business operations and their financial transactions with a view to identifying the origin of the financial resources and funds used in the transactions, the customer's unusual transactions or operations and his/her economic activities to mitigate the money laundering and terrorist financing risks.

- 2.11. In the performance of additional due diligence obligation in the course of the business relationship, the employees of HONOS OÜ shall be guided by the “Internal Rules and Procedures for the Exchange of Virtual Currency and Virtual Currency Wallet Service Provider”.
- 2.12. Communication with the customer takes place only via verified means of communication (e-mail, contact phone).
- 2.13. Service provision restrictions

3. Service provision restrictions

- 3.1. As of 07/05/2019, HONOS OÜ has excluded the establishment of a business relationship with the following high-risk third-country residents: Afganistan; American Samoa; Aruba; Bahamas; Barbados; Belize; Bermuda; Bosnia and Herzegovina; Botswana; Cambodia; Democratic People's Republic of Korea (DPRK; North Korea); Democratic People's Republic of Laos; Dominica; Ethiopia; Fiji; Ghana; Guam; Guyana; Iran; Iraq; Marshall Islands; Oman; Pakistan; Samoa; Serbia; Sri Lanka; Syria; Trinidad and Tobago; Tunisia; Uganda; United Arab Emirates; US Virgin Islands; Vanuatu; Yemen and individuals carried to the list of international sanctions with whom the establishment of a business relationship is excluded due to the type of sanction. Upon deletion of countries or persons from the list, restrictions on the establishment of a business relationship shall be lifted, or if such customers are added to the list with whom a business relationship was established earlier, the business relationship shall be terminated.
- 3.2. Business relations are not established with companies registered outside the Republic of Estonia and the EU, Switzerland, Norway, Iceland, Australia, Brazil, Canada, Hong Kong, India, Japan, South Korea, Mexico, Singapore, South Africa, and the US (third countries) whose shares are not publicly listed.
- 3.3. No business relationship is established, or the established business relationship is terminated in the following cases:
 - 3.3.1. The customer has provided false personal data (including foreign or forged documents used for the identification of the person);
 - 3.3.2. The customer refuses to disclose the actual beneficiaries' data or transaction statements or knowingly provides false information;
 - 3.3.3. It has become evident during verification of the customer's transactions that it is related to money laundering or terrorist financing;
 - 3.3.4. Upon the complex assessment of the risks of the customer and his/her transactions, the risk of money laundering or terrorist financing or the commission of criminal offences is higher than acceptable;
 - 3.3.5. If it turns out that a customer or business partner is a shell bank, that is, an institution carrying out equivalent activities to a credit institution or a credit.

4. Contact person of the Financial Intelligence Unit

- 4.1. The phone number of HONOS OÜ's contact person of the Financial Intelligence Unit is +372 5685 3318 and the e-mail is: AML@honos.pro
- 4.2. The contact person organises the compliance of HONOS OÜ employees with AML/CTF requirements in accordance with the instructions established by the FIU and the laws and directives of the Republic of Estonia and the European Union and performs or ensures the corresponding training of employees.
- 4.3. All employees of HONOS OÜ are obliged to inform the contact person of any suspicions of money laundering or terrorist financing or unusual

cases, refusals to establish a business relationship under the Money Laundering and Terrorist Financing Prevention Act, or extraordinary cancellation (termination) of a business relationship and identification of a person subject to a financial sanction.

- 4.4. The contact person shall inform the management board of HONOS OÜ of any suspicion of AML/CTF cases and of the identification of a person subject to a financial sanction.
- 4.5. In case of reasonable doubt, the contact person shall forward a notification of any suspicion of AML/CTF case and identification of a person subject to a financial sanction to the Financial Intelligence Unit at <https://www2.politsei.ee/et/organisatsioon/rahapesu/saada-teade.dot>
- 4.6. It is forbidden to notify the customer and other employees of HONOS OÜ (except the contact person and the Management Board) of the transmission of a case report with suspicion of AML / CTF to the Financial Intelligence Unit before receiving instructions from the Financial Intelligence Unit.