Taurus Pay s.r.o
Anti-Money Laundering Policy Statement & Program Procedures
Compliance and Supervisory Procedures
For
Taurus Pay s.r.o
Cimburkova 916/8, 130 00, Prague 3 - Žižkov

Taurus Pay s.r.o - Anti-Money Laundering Program Overview

1. General Framework

1.1. Taurus Pay s.r.o (the "Company") has no tolerance for money laundering, financing of terrorism or any other form of illicit activity, and is committed to implementing appropriate policies, procedures, and controls to prevent those activities. Our policies are shaped by industry best practices, a risk-based approach and the effective anti-money laundering standards applied in the Czech Republic and worldwide. These policies apply, without exception, to all employees of the Company, its Board Members and Directors, as well as to its subsidiaries.

1.2. The purpose of this text is to provide to the Company's clients, providers, partners, vendors, contractors, employees, law enforcement and other concerned stakeholders a high-level and summarized overview of the Company's main anti-money laundering ("AML") policy and procedures. By no means is this content to be considered as the whole set of all policies, procedures and controls that are implemented and in place by the Company for prevention of money laundering, financing of terrorism and other forms of illicit activity. This document and all underlying policies, processes and procedures are prepared in line with provisions, requirements, and recommendations as applicable to the Company.

1.3. The Company operates from, and under the laws of the Czech Republic and is incorporated as [appropriate legal status]. The Company is required to comply with the Anti-Money Laundering Regulations 2020, which require the Company to identify and verify its clients' identities appropriately, conduct ongoing monitoring of their activity (including transaction monitoring), maintain records of clients' activity and related documents for at least five years and report suspicious transactions to authorities.

1.4. The Company understands money laundering as:
Process by which the direct or indirect benefit of crime is channeled through the economy/financial system to conceal the true origin and ownership of the proceeds of criminal activities. Generally, to launder criminal proceeds, a money launderer places the funds/proceeds in the financial system without arousing any suspicion, moves it in a series of complex transactions to disguise its original (criminal) source and finally, if successful, integrates it into the economy to make the funds appear to be derived legitimately.

1.5. The Company understands terrorist financing as:
Providing funds for terrorist activity, meaning as the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of the law. This activity is done by intentionally causing substantial property damage that is likely to seriously harm people or by seriously interfering with or disrupting essential services, facilities or systems.

2. Risk-Based Approach

2.1. The Company takes a risk-based approach ("RBA") towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with clients and uses all available data when reviewing client activity.

2.2. The Company performs a risk-based due diligence and collects necessary information and documentation on each prospective client in order to assess the risk profile. Before entering into a client relationship, necessary checks are conducted in line with the RBA so as to ensure that the identity of the clients does not match with an entity with a known criminal background or with banned entities, such as terrorist organizations. Enhanced due diligence is required for clients who are deemed to be of high risk, especially those for whom the business activities (sources of funds) are not clear, or for transactions of higher value and frequency, which can be determined by the Company at its sole and absolute discretion.

2.3. The Company's employees exercise care, due diligence and good judgement in determining the overall profile and business nature of its clients. The Company conducts its business in accordance with the highest ethical standards and may decide not to enter a client relationship that can adversely affect the Company's reputation.

3. Client Due Diligence

3.1. The Company requires all business clients to undergo proper due diligence before using our services. This includes, without limitation:

3.1.1.identification of a customer, whether a customer in an established business relationship or a one-off transaction, and whether natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information.

3.1.2.verify that a person purporting to act on behalf of a customer is properly authorised and identify and verify the identity of the person.

3.1.3.identify a beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from reliable

sources, so as to be satisfied that the person knows the identity of the beneficial Owner.

3.1.4. understand and obtain information on, the purpose and intended nature of a business relationship; and

3.1.5. conduct ongoing due diligence on a business relationship including —

- scrutinising transactions undertaken throughout the course of the business relationship to ensure that transactions being conducted are consistent with the person's knowledge of the customer, the customer's business and risk profile, including where necessary, the customer's source of funds; and
- ensuring that documents, data or information collected under the customer due diligence process is kept current and relevant to customer due diligence, by reviewing existing records at appropriate times, taking into account whether and when customer due diligence measures have been previously undertaken, particularly for higher risk categories of customers.

3.2. In addition to the requirements of paragraph (3.1.1), for customers that are legal persons or legal arrangements, the Company shall —

3.2.1. understand the ownership and control structure of the customer and the nature of the customer's business.

3.2.2. identify the customer and verify its identity by means of the following information-

- name, legal form and proof of existence.
- the constitutional documents that regulate and bind the legal person or arrangement, as well as satisfactory evidence of the identity of the director, manager, general partner, president, chief executive officer or such other person who is in an equivalent senior management position in the legal person or arrangement; and
- the address of the registered office and, if different, a principal place of Business.

3.3. For the purpose of paragraph (3.1.3), for customers that are legal persons, the Company shall —

3.3.1. identify and verify the identity of the natural person, if any, who is the beneficial Owner.

3.3.2. to the extent that there is doubt under paragraph (3.1.1) as to whether the person with the controlling ownershi interest is the beneficial owner or where no natural person exerts control through ownership interests, identify the natural person exercising control of the legal person or arrangement customer through other means; or

3.3.3. where no natural person is identified under (3.1.1) or (3.1.2), identify the relevant natural person who is the senior managing official.

3.4. In addition to the above requirements for customers that are legal arrangements, the

Company, where applicable, shall identify and take reasonable measures to verify the identity of beneficial owners by means of the following information —

3.4.1.for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control or ownership); or

3.4.2.for other types of legal arrangements, the identity of persons in equivalent or similar positions.

3.5. Information collected and held shall be kept accurate and up to date and shall be updated on a timely basis.

4. Compliance Officer

4.1. The management board of Taurus Pay s.r.o appointed a Money Laundering Reporting Officer, who performs the AML duties and obligations of the Company. A Money Laundering Reporting Officer reports directly to the management board and has the competence, means and access to relevant information across all the structural units of the Company.

4.2. Taurus Pay s.r.o ensures that a Money Laundering Reporting Officer is a natural, independent and autonomous person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties, has and shall have access to all relevant material in order to make an assessment as to whether the activity is or is not suspicious; and can dedicate sufficient time for the efficient discharge of the function.

5. Internal Controls

5.1. Taurus Pay s.r.o has developed and implemented rules of procedure that allow for effective mitigation and management of risks relating to money laundering and terrorist financing, which are identified in the risk assessment performed in accordance with the Company's risk-based approach.

5.2. Internal reporting procedures maintained by Taurus Pay s.r.o includes the following provisions —

5.2.1.identifying the Money Laundering Reporting Officer and specifying that the Money Laundering Reporting Officer is the person to whom a report is to be made of any information or other matter which comes to the attention of a person carrying out relevant financial business and which, in the opinion of the person, gives rise to —

- a knowledge or suspicion or reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist financing; or
- a knowledge or suspicion or reasonable grounds for knowing or suspecting that the transaction or attempted transaction relates to money laundering or

terrorist financing.

5.2.2. requiring that a report under subparagraph (5.2.1) be considered in light of all other relevant information by the Money Laundering Reporting Officer for the purpose of determining whether or not the information or other matter contained in the report gives rise to such a knowledge or suspicion.

5.2.3. for a person charged with considering a report in accordance with subparagraph (5.2.2) to have access to other information which may be of assistance to the person, and which is available to the person who is responsible for maintaining the internal reporting procedures concerned; and

5.2.4. for ensuring that any information or other matter contained in a report is disclosed to the Financial Reporting Authority where the person who has considered the report under subparagraph (5.2.2) —

- knows or has reasonable cause to suspect that another person is engaged in money laundering other than terrorist financing; or
- knows, suspects or has reasonable cause to suspect that another person is engaged in terrorist financing.

6. Simplified Due Diligence

6.1. Taurus Pay s.r.o may apply simplified due diligence (“SDD”) measures where a risk assessment prepared on the basis of these rules of procedure identifies that, in the case of the jurisdiction, economic sector of activity or amounts transacted the risk of money laundering or terrorist financing is lower than usual.

6.2. Before the application of SDD measures to a client, an employee of Taurus Pay s.r.o establishes that the business relationship, transaction or act is of a lower risk and the Company attributes to the transaction, act or client a lower degree of risk.

6.3. The application of SDD measures is permitted to the extent that Taurus Pay s.r.o ensures sufficient monitoring of transactions, acts and business relationships, so that it would be possible to identify unusual transactions and allow for notifying of suspicious transactions in accordance with these rules of procedure

7. Enhanced Due Diligence

7.1. Taurus Pay s.r.o applies enhanced due diligence (“EDD”) measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing. EDD measures are applied always when:

7.1.1. where a higher risk of money laundering or terrorist financing has been identified.

7.1.2. where through supervisory guidance a high risk of money laundering or terrorist financing has been identified.

7.1.3. where a customer or an applicant for business is from a foreign country that has been identified by credible sources as having serious deficiencies in its anti-money laundering or counter terrorist financing regime or a prevalence of corruption.

7.1.4.in relation to correspondent banking relationships.
7.1.5.where the customer or the applicant for business is a politically exposed person.
7.1.6.in the event of any unusual or suspicious activity; or
7.1.7.in relation to business relationships and transactions with persons, including financial institutions, from countries for which this is requested by the Financial Action Task Force, and in each case, the enhanced customer due diligence shall be proportionate to the risk.

7.2. Taurus Pay s.r.o also applies EDD measures whereas the assessment of risk is assessed as higher, in accordance to its internal policies and procedures.

8. Politically Exposed Persons

8.1. Politically Exposed Persons ("PEP") includes —
8.1.1. a person who is or has been entrusted with prominent public functions by a foreign country, for example a Head of State or of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, and important political party official.
8.1.2. a person who is or has been entrusted domestically with prominent public functions, for example a Head of State or of government, senior politician, senior government, judicial or military official, senior executives of a state-owned corporation and important political party official; and
8.1.3. a person who is or has been entrusted with a prominent function by an international organisation like a member of senior management, such as a director, a deputy director and a member of the board or equivalent functions.

8.2. Taurus Pay s.r.o shall in addition to satisfying customer due diligence requirements, shall
8.2.1. put in place risk management systems to determine whether a person or beneficial owner with whom that person has a business relationship is a politically exposed person, family member or close associate; and
8.2.2. ensure that the risk management procedures under subparagraph (8.2.1) —
• contain as a component, procedures for requiring that senior management approval be obtained before establishing or continuing a business relationship with a politically exposed person or a family member or close associate.
• take reasonable measures to establish the source of wealth and the source of funds of a person involved in a business relationship and a beneficial owner identified as a politically exposed person or a family member or close associate; And
• contain as a component, monitoring of the business relationship with the politically exposed person or a family member or close associate.

9. Sanctions

9.1. Taurus Pay s.r.o shall make its sanctions an integral part of its all-compliance programme

and accordingly shall have policies, procedures, systems and controls in relation to sanctions compliance. Taurus Pay s.r.o shall provide adequate sanctions related training to their staff.

9.2. Taurus Pay s.r.o shall screen applicants, customers, beneficial owners, transactions, service providers and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country.

9.3. Where there is a true match or suspicion, Taurus Pay s.r.o shall take steps that are required to comply with the sanction obligations including reporting pursuant to the laws, rules and regulations. Taurus Pay s.r.o shall document and record all the actions that were taken to comply with the sanction regime, and the rationale for each such action. Taurus Pay s.r.o shall keep track of all the applicable sanctions, and where the sanction lists are updated, ensure that existing customers are not listed. These sanctions apply to all individuals and entities in the Czech Republic.

10. Suspicious Activity Monitoring and Reporting

10.1.Taurus Pay s.r.o shall examine, as far as reasonably possible, the background and purpose
of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. The frequency of ongoing monitoring for any customer would be determined by the level of risk associated with the business relationship. In case the risks are high, Taurus Pay s.r.o shall apply enhanced monitoring, increasing the frequency and intensity.

11. Termination of Services

11.1.Taurus Pay s.r.o reserves the right to deny or terminate servicing a client or account at any time in line if suspicion arises that a client is involved with or connected with money laundering, criminal activity, terrorist financing or any other predicate offense to money laundering or terrorist financing.

11.2.In case Taurus Pay s.r.o is unable to complete and comply with Customer Due Diligence requirements as specified in the regulations, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, Taurus Pay s.r.o shall terminate the relationship.

12. Data Retention

12.1.Taurus Pay s.r.o is obligated to retain all documents and information which served for identification and verification of the client, for a period of no less than 5 (five) years after termination of the business relationship. This includes records pertaining to enquiries

about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records shall be made available to domestic competent authorities upon request.

12.2.Taurus Pay s.r.o shall implement necessary rules for the protection of personal data upon application of the requirements arising from its obligations.

12.3.Where there has been a report of a suspicious activity or Taurus Pay s.r.o is aware of a continuing investigation relating to a customer or a transaction, records relating to the transaction, or the customer shall be retained until confirmation is received that the matter has been concluded.

13. Training

13.1.The Compliance Officer shall ensure that Taurus Pay s.r.o's employees are fully aware of their legal obligations under this policy, by introducing a complete employees' education and training program.

13.2.Regular employee training shall be provided for the identification of persons or entities and assets subject to terrorist financing sanctions as well as the processes to be followed where such persons or entities are identified. Taurus Pay s.r.o shall provide training to employees to ensure proper and efficient recognition and treatment of transactions carried out by, or on behalf of, any person or entity who is or appears to be engaged in terrorist and/or proliferation financing, or whose funds or other assets are subject to terrorist financing sanctions. Ongoing training and assessments of employees shall be conducted to ensure that they obtain and maintain adequate knowledge of matters related to terrorist financing sanctions, sanctions obligations and compliance standards.

14. Sector and Jurisdiction Restrictions

14.1. Taurus Pay s.r.o shall consider jurisdictions it is exposed to, either through its own activities or the activities of clients, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient anti-money laundering controls and listed by Financial Action Task Force.

14.2.While it's beyond Taurus Pay s.r.o's scope to set policies for the client's own business dealings, Taurus Pay s.r.o reserves the right to not serve clients who themselves have business activities, clients or otherwise accept purchases originating from certain Jurisdictions.

14.3.It goes without saying that Taurus Pay s.r.o can't provide services to any client that isn't legally established or is offering illegal goods or services in their operating jurisdiction(s).

14.4.Clients incorporated in non-serviced jurisdictions and from restricted sectors cannot access or be on boarded to use Taurus Pay s.r.o’s services. Attempts to circumvent this policy, by providing false, forged or modified documents meant to deceive or mislead will be considered fraud and treated as such with law enforcement.

14.5.Taurus Pay s.r.o shall ensure that the group entities apply anti-money laundering measures consistent with the requirements of this jurisdiction."