

ACT ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

UNOFFICIAL TRANSLATION

TEXT OF THE ARTICLES

CHAPTER I – GENERAL PROVISIONS

1.1 Contents of the Act

Article 1

(Contents of the Act and transposition of EU directives)

(1) This Act shall stipulate measures, competent authorities and procedures for detecting and preventing money laundering and terrorist financing and shall govern the inspection of the implementation of its provisions.

(2) This Act shall transpose Directive (EU) No 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, the amendment of the Regulation (EU) No 648/2012 of the European Parliament and of the Council and the repeal of Directive 2005/60/EC of the European Parliament and of the Council and the Directive of the Commission 2006/70/EC (OJ L No 141 of 5 June 2015, page 73; hereinafter referred to as: Directive 2015/849) into the legislation of the Republic of Slovenia.

1.2 Definitions and scope *Article 2*

(Money laundering and terrorist financing)

"(1) For the purposes of this Act, money laundering shall mean any conduct with money or property obtained by an offence and shall include:

1. conversion or any transfer of money or other property derived from criminal activity;
2. concealment or disguise of the true nature, origin, location, movement, disposition, ownership or rights with respect to money or other property derived from criminal activity."

(2) For the purposes of this Act, terrorist financing shall mean the direct or indirect provision or collection of funds or other property of legal or illegal origin, or attempted provision or collection of such funds or other property with the intent that they be used, or in the knowledge that they are to be used, in full or in part, to carry out a terrorist activity or other terrorist related activity, or by a terrorist or terrorist organisation.

(3) For the purposes of this Act, a terrorist act is a criminal offence as defined in Article 2 of the International Convention on the Suppression of the Financing of Terrorism (Act Ratifying the International Convention for the Suppression of the Financing of Terrorism, Official Gazette of the RS–MP, no. 21/04) and a terrorist crime and offences related to terrorism and determined in the Chapter of the Criminal Code, which defines crimes against humanity.

(4) For the purposes of this Act, a terrorist shall mean a natural person who:

- commits or intends to commit a terrorist act;
- is involved in the commission of a terrorist act as an accessory, instigator or aide;
- organises a terrorist act to be committed; or

- contributes to a terrorist act by an individual or group of people operating to achieve a common goal, provided such contribution is intentional and for the purpose of perpetuating the terrorist activity, or provided that he/she understands the group's intention to commit a terrorist act.

(5) For the purposes of this Act, a terrorist organisation shall mean any group of terrorists who:

- commits or intends to commit a terrorist act;
- participates in committing a terrorist act;
- organises a terrorist act to be committed; or
- contributes to a terrorist act by an individual or group of people operating to achieve a common goal, provided such contribution is intentional and for the purpose of perpetuating the terrorist activity, or provided that he/she understands the group's intention to commit a terrorist act.

Article 3 (Definition of other terms)

For the purposes of this Act:

1. "anonymous electronic money" as referred to in Article 22 of this Act shall mean a payment instrument that provides the anonymity of the payer and the inability of payment tracking to the both issuers of electronic money and receivers of payment.

2. "a brokerage company" shall have the same meaning as in the Act governing the financial instruments market;

3. "tax ID number" shall mean an identification mark assigned to a taxable person under the conditions stipulated in the Act governing tax procedures and the Act governing financial administration and used in relation to all taxes or tax-related purposes of a taxable person; the tax ID number shall also mean the identification number for tax purposes used by a non-resident in the country of residence;

4. "distribution channel" shall mean a network of individuals or organisations participating in the delivery of goods or services to an end user;

5. for the purposes of this Act, "other civil law entity" shall mean an organised group of individuals who pool, or will pool, assets or other property for a particular purpose;

6. "management company" and "Member State management company" shall have the same meaning as defined in the Act governing investment funds and management companies;

7. "Member State" shall mean a Member State of the European Union or a signatory state to the European Economic Area Agreement;

8. "electronic money" shall have the same meaning as in the Act governing payment transactions and systems;

9. "European supervisory authorities" shall mean the European Banking Authority (EBA) established under Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 on establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, the European Insurance and Occupational Pensions Authority (EIOPA) established under Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 on establishing a European Supervisory Authority, amending Decision No 716/2009/EC and repealing Commission Regulation 2009/79/EC, and the European Securities and Markets Authority (ESMA) established under Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 on establishing a European Supervisory Authority, amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC;

10. "factoring" shall mean factoring with or without recourse;

11. "financial institutions" shall mean obliged persons referred to in points 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16 and 20 (a) to (j) of paragraph 1 of Article 4 hereof and institutions of Member States providing equivalent services;

12. "financial intelligence unit" shall mean a central national authority established in the Member State or a third country to monitor and analyse suspicious transactions and other information on suspicions of money laundry, associated previous offences and suspicions of terrorist financing and to submit the results of analyses to the competent authorities;

13. "forfeiting" shall mean financing exports based on purchase with discount and without recourse to long-term outstanding receivables secured by a financial instrument;

14. "economic operator" as referred to in Article 35 of this Act shall mean a company and entrepreneur as defined in the Act governing companies, and a cooperative society as defined in the Act governing cooperative societies;

15. "cash" as referred to in Article 68 of this Act shall mean banknotes or coins in circulation as a means of payment;

16. "cash" as referred to in Article 120 of this Act shall have the same meaning as in the Regulation of the European Parliament and of the Council (EC) No 1889/2005 of 26 October 2005 on controlling cash when entering or leaving the Community (OJ L No 309 of 25 November 2005, p. 9);

17. "cash transaction" shall mean any receipt, handover or exchange of cash referred to in point 15 of this Article, whereby an obliged person receives physical cash from a customer or hands over physical cash to a customer in possession and disposition;

18. "games of chance" shall have the same meaning as in the Act governing games of chance;

19. "information about the activity of a customer (natural person)" shall mean data on a customer's private, professional or other similar engagement (employed, retired, student, unemployed, etc.) or data on customer's activities (in the field of sport, culture and art, scientific research, education or other similar areas) that provide an appropriate basis for establishing a business relationship;

20. "Member State investment company" and "third country investment company" shall have the same meaning as in the Act governing financial instruments market;

21. For the purposes of this Act, "correspondent relationship" shall mean a correspondent banking relationship between a domestic and a respondent foreign credit (or other similar) institution established by opening a domestic credit institution or a foreign or other similar credit institution account with a domestic credit institution (opening a loro account);

22. "correspondent relationship" shall also mean an agreement concluded by a domestic credit institution with a domestic or foreign credit or similar institution for the purpose of conducting business abroad through the respondent.

23. "credit institutions" shall mean obliged persons referred to in points 1 and 2 of paragraph 1 of Article 4 hereof and institutions of Member States providing equivalent services;

24. "network" as referred to in Article 124 hereof shall mean an extensive structure to which a person belongs and which has a joint owner, joint management or joint supervision of compliance with regulations;

25. "national risk assessment" shall mean an extensive process of identification and analysis of the major risks of money laundering and terrorist financing in a specific country, the development of suitable measures to prevent money laundering and terrorist financing on the basis of the established risks, and more efficient channelling of available resources to control, mitigate or eliminate the established risks;

26. "superior responsible person of senior management" as referred to in Articles 60, 61, 62 and 63 hereof shall mean a member of management who is sufficiently acquainted with the obliged person's exposure to the risk of money laundering and terrorist financing and who is in a position, not necessarily a member of the management board, to take decisions that affect the obliged person's exposure to risk;

27. "shell bank" shall mean a credit or financial institution or an institution engaged in equivalent activities and registered in a jurisdiction in which it does not perform its services and which is unaffiliated with a supervised or otherwise regulated financial group;

28. For the purposes of this Act, non-profit organisations shall mean societies, establishments, institutions and religious communities engaged in non-profit activities and established in accordance with the applicable legislation;

29. "non-resident" shall have the same meaning as in the Act governing foreign exchange;

30. "trust and company service provider" shall mean any natural person or legal entity which by way of business provides any of the following services to third parties:

a) forming legal entities;

b) acting as, or arranging for another person to act as, a director or secretary of a company or manager or partner, whereby the person concerned does not actually perform the management

function or does not undertake business risks concerning capital contribution in the legal entity of which he/she is formally a partner;

c) providing a head office, business, correspondence or administrative address and other related services for a legal entity;

d) acting as, or arranging for another person to act as, a trustee of an institution, trust or similar foreign law entity which receives, manages or distributes property funds for a particular purpose; the definition excludes the provision of trustee services for investment funds, mutual pension funds and pension companies;

e) acting as, or arranging for another person to act as, nominee shareholder for another person, other than a company whose securities are traded on a regulated market that is subject to disclosure requirements in conformity with European Union legislation or subject to equivalent international standards;

31. "regulated market and stock exchange" shall have the same meaning as in the Act governing the financial instruments market;

32. "personal name" shall consist of a first name and family name, of which each may be comprised of several words that form a whole;

33. "payment institution" shall have the same meaning as in the Act governing payment services and systems;

34. "payment account" shall have the same meaning as in the Act governing payment services and systems;

35. "individual performing an activity independently" shall be a natural person who is independently and continuously engaged in a revenue generating business in the free market;

36. "business relationship" shall mean a business or other contractual relationship linked with the operations of an obliged person concluded or established through the obliged person ;

37. "management" as referred to in Article 35 herein shall have the same meaning as in the Act governing companies;

38. "property" shall mean assets of any kind, whether corporeal or incorporeal, tangible or intangible, moveable or immoveable, and legal documents or instruments in any form, including electronic or digital, evidencing title to or interest in such assets;

39. "group" shall mean a group of people comprising superior and subordinate persons, its subsidiaries and persons in which the superior or its subsidiary participates, and also associated companies fulfilling the conditions for a managing company as per the Act governing companies;

40. "assets" shall mean financial assets and economic benefits of any kind, including:

a) cash, cheques, claims on money, drafts, money orders and other payment instruments;

b) deposits with organisations;

c) financial instruments stipulated by the Act governing financial instruments, namely publicly- and privately-traded securities, including shares and stocks, certificates, debt instruments, bonds, debentures, warrants and derivative financial instruments;

d) interest, dividends or other income from assets;

e) claims, loans and letters of credit;

f) other documents proving entitlement to assets or other financial sources.

41. "means of electronic identification" shall have the same meaning as in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 June 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L No 257 of 28 August 2014, p. 73)

42. "permanent and temporary residence" shall be information on the street, house number, post office and postcode and country of permanent and temporary residence if any;

43. "transaction" shall mean any receipt, handover, exchange, safekeeping, disposal or other handling of monies or other property by a person liable;

44. "third-country" shall mean a country that is not a Member State;

45. "manager of alternative investment funds", "subsidiary of a Member State manager" and "subsidiary of a manager of alternative investment fund manager of a third country" shall have the same meaning as in the Act governing alternative investment funds;

46. "office" shall mean the Office for Money Laundering Prevention of the Republic of Slovenia;

47. "official personal identification" shall mean any valid authentic instrument bearing a photograph and issued by the competent authority of the Member State or third country and which is deemed a public document as per the legislation of the issuing State;

48. "virtual currency" shall be a digital recording of value issued by a natural person or legal entity which is not a central bank or a public institution and which is used as means of exchange that may be electronically transferred, kept or exchanged and which is not necessarily related to traditional (fiat) currencies and may constitute a direct means of payment between entities that adopt it;

49. "life insurance" shall mean insurance defined as life insurance by the Act governing insurance business.

Article 4 (Obliged persons)

(1) The measures for detecting and preventing money laundering and terrorist financing stipulated by the present Act shall be carried out prior to or at the time of receiving, handing over, exchanging, safekeeping, disposing of or handling monies or other property and in concluding business relationships with:

1. banks, branches of banks from third countries and Member State banks which establish branches in the Republic of Slovenia or which are authorised to directly perform banking services in the Republic of Slovenia;

2. savings banks;

3. payment institutions, waived payment institutions, and payment institutions and waived payment institutions of the Member States which as per the Act governing payment services and systems establish a branch in the Republic of Slovenia or provide payment services in the Republic of Slovenia through a representative or directly;

4. post office if it provides services of money transfer (payments and disbursements) through a postal money order;

5. brokerage companies;

6. investment funds that sell their own units in the Republic of Slovenia; if an investment fund does not provide its own management, the provision of this Act that applies to an obliged person shall apply to a manager of the respective fund;

7. management companies and managers of alternative investment funds that provide portfolio management services and ancillary services set forth in the Act governing investment funds and management companies or the Act governing managers of alternative investment funds;

8. branches of an investment company of a Member State and branches of an investment company of a third country in the Republic of Slovenia;

9. branches of a management company in the Republic of Slovenia that provide portfolio management services and ancillary services set forth in the Act governing investment funds and management companies;

10. branches of a manager of a Member State and branches of a manager of alternative investment fund of a third country in the Republic of Slovenia that provide portfolio management services and ancillary services set forth in the Act governing managers of alternative investment funds;

11. managers of mutual pension funds;

12. managers of a bridging facility set forth in the Act governing bridging insurance for professional and top athletes;

13. founders and managers of pension companies;

14. insurance companies authorised to pursue life insurance business and branches of insurance companies from third countries with a permit to provide life insurance business and insurance companies from Member States which establish branches in the Republic of Slovenia or which are authorised to pursue life insurance business directly in the Republic of Slovenia;

15. issuers of electronic money, issuers of waived electronic money, branches of issuers of electronic money and issuers of waived electronic money from third countries and issuers of electronic money and issuers of waived electronic money from a Member State that establish a branch in the

Republic of Slovenia which are authorised to directly perform services of issuing electronic money in the Republic of Slovenia;

16. currency exchange offices;
17. auditing firms and independent auditors;
18. organisers and concessionaires organising games of chance;
19. pawnshops;
20. legal entities and natural persons conducting business relating to:
 - a) granting credit or loans, including consumer credit, mortgage credit, factoring and financing of commercial transactions, including forfeiting;
 - b) financial leasing;
 - c) issuing and managing other means of payment (e.g. bills of exchange and traveller's cheques), whereby it is not deemed a payment service as per the Act governing payment services and systems,
 - d) issuing and managing virtual currencies, including the service of exchanging virtual currencies to standard currencies and vice versa,
 - e) issuing of guarantees and other commitments;
 - f) portfolio management services for third parties and related advice, and investment management for the Republic of Slovenia in accordance with the law, governing the Slovenian Sovereign Holding;
 - g) safe custody services;
 - h) brokerage in concluding credit and loan business, except for those legal entities and natural persons whereby the brokerage activity is not their main activity and they do not do business on behalf of, and for the account of, a financial or credit institution (credit intermediaries in an ancillary capacity);
 - i) insurance agency services for the purpose of concluding life insurance contracts;
 - j) insurance intermediaries in concluding life insurance contracts; k) accounting services; l) tax advisory services; m) trust and company services;
 - n) trade in precious metals and precious stones or products made from these materials; o) trade in works of art; p) organisation and execution of auctions; and
 - r) real estate agency including real estate activities with own property, renting and operating of own or leased real estate and real estate agencies;
 - s) implementation of measures to strengthen the stability of banks of the Republic of Slovenia in accordance with the law, governing the measures of the Republic of Slovenia to strengthen the stability of banks.

(2) Measures for detecting and preventing money laundering and terrorist financing as determined in this Act, as per the provisions of Chapter 3 of this Act, shall also be implemented in lawyers, law firms, notaries, but only within the scope stipulated in Chapter 4 hereof.

(3) For the purposes of this Act, the term obliged person shall refer collectively to obliged persons referred to in paragraphs 1 and 2 of this Article.

Article 5 (Exceptions concerning games of chance)

(1) The Government of the Republic of Slovenia (hereinafter referred to as: Government) may stipulate with a regulation that organisers of games of chance as referred to in point 18 of paragraph 1 of the preceding Article with low risk of money laundering or terrorist financing shall be completely or partially exempt from implementing measures pursuant to this Act.

(2) The Government's decision referred to in the preceding paragraph is based on a report on the risk assessment conducted by the Financial Administration of the Republic of Slovenia in cooperation with the Office. In establishing the risk assessment, the following factors shall be considered:

- scope of the implementation of the games of chance service,
- level of vulnerability of the games of chance and transaction,
- methods of payment used, and
- findings of the national and transnational risk assessment referred to in Article 8 hereof.

(3) The provisions referred to in preceding paragraphs shall not apply to concessionaires organising special games of chance in casinos or gaming halls.

(4) All decisions on exemptions of organisers of games of chance from implementing provisions of this Act shall be reported to the European Commission by the Financial Administration of the Republic of Slovenia.

Article 6 **(Exceptions concerning the occasional performance of financial activity)**

(1) Legal entities, sole proprietors, and individuals that perform an activity individually and only occasionally or in a limited scope perform the financial activity referred to in points 16 and 20 (a) to 20 (h) of paragraph 1 of Article 4 of this Act and for which the risk of money laundering or terrorist financing is low may be exempt from implementing the provisions of this Act if the following conditions are met:

1. the financial activity is supplementary and directly related to the main activity;
2. annual net turnover from the financial activity does not exceed EUR 100,000 or 5% (five per cent) of the total annual net turnover of the obliged person;
3. their main activity is not:
 - auditing services,
 - organising games of chance,
 - accounting services,
 - tax advisory services,
 - real estate activities,
 - trust and company services, or
 - notary and attorney services;
4. the highest possible value of a transaction per customer and individual transaction – notwithstanding that it is executed in one or several transactions that seem related – must not exceed EUR 1,000 and
5. the financial activity is provided only to persons who are customers related to the performance of the main activity, and is not generally available to public.

(2) The preceding paragraph shall not apply to legal entities, sole proprietors or individuals performing an activity individually if they implement remittance as per the Act governing payment services and systems.

(3) The persons referred to in paragraph 1 of this Article shall lodge a request for suspension of the implementation of provisions of this Act at the Office. The request shall be submitted with documentation showing the fulfilment of the conditions referred to in paragraph 1 of this Article and documentation on an assessment of the risk of financial activity of money laundering and terrorist financing. In assessing the risk of money laundering or terrorist financing, special attention shall be paid to each financial activity which, due to its nature, may be used or abused for the purposes of money laundering or terrorist financing.

(4) Upon the request referred to in the preceding paragraph, the Office shall issue a decision in accordance with the Act governing general administrative procedures.

(5) The decision referred to in the preceding paragraph shall apply for two years from its issue. To be exempted from the implementation of provisions of this Act, a new request shall be lodged in accordance with paragraph 3 of this Article.

(6) If the circumstances on the basis of which the decision was issued change before the expiry of the order, the person referred to in paragraph 1 of this Article must inform the Office of these changes within fifteen days from their occurrence. On the basis of this notification or on the basis of other information, the Office ex officio issues a new decision by which it annuls the previous decision and decides anew on the permit to suspend the implementation of provisions of this Act in view of the changed circumstances.

(7) The Office shall notify the European Commission annually on decisions issued on the basis of this Article.

CHAPTER II – COOPERATION AND NATIONAL RISK ASSESSMENT

Article 7 (Cooperation of competent authorities)

The Office, supervisory bodies referred to in Article 139 of this Act and other authorities competent to detect and prevent money laundering and terrorist financing work together and harmonise the implementation of policies and activities of combating money laundering and terrorist financing. To attain strategic and operational objectives, these authorities may sign agreements on mutual cooperation and establish inter-ministerial working groups.

Article 8 (National risk assessment)

(1) To establish, assess, understand and mitigate the risks related to money laundering and terrorist financing, the Republic of Slovenia shall conduct a national risk assessment of money laundering and terrorist financing and update it at least every four years.

(2) To conduct the national risk assessment of money laundering and terrorist financing in the Republic of Slovenia, the Government shall establish a permanent inter-ministerial working group. The tasks of the inter-ministerial working group shall be as follows:

1. implementation of the national risk assessment of money laundering and terrorist financing in the Republic of Slovenia;
2. preparation of the report on identified national risks of money laundering and terrorist financing;
3. preparation of proposals for measures and an action plan to mitigate identified risks of money laundering and terrorist financing;
4. implementation of other analyses in the field of money laundering and terrorist financing which require cooperation and harmonisation between different institutions, and the preparation of reports on the analyses conducted.

(3) The work and tasks of the permanent inter-ministerial working group referred to in the preceding paragraph shall be directed and harmonised by the Office.

(4) When implementing the national risk assessment referred to in paragraph 1 of this Article, the findings of the report of the European Commission on the assessed risks of money laundering and terrorist financing (transnational risk assessment) shall be observed.

Article 9
(Report and purpose of the national risk assessment)

(1) Through the report on the findings of the national risk assessment of money laundering and terrorist financing referred to in point 2 of paragraph 2 of the preceding Article, the Office shall notify the Government.

(2) The findings of the report on the national risk assessment are intended to:

1. improve the national regulation of detecting and preventing money laundering and terrorist financing, in particular by defining sectors or activities where the obliged persons must take stricter measures related to customer due diligence and other liabilities set forth in this Act;

2. identify sectors or activities of little, or increased risk of, money laundering and terrorist financing;

3. define the priority arrangement of all resources and assets intended to prevent money laundering and terrorist financing;

4. prepare relevant regulations for individual sectors or activities according to the identified risks of money laundering and terrorist financing; and

5. assist obliged persons to implement their risk assessments of money laundering and terrorist financing.

(3) The activities referred to in the previous paragraph shall be directed and harmonised by the Office.

(4) With the regulation, the Government shall determine the sectors or activities of little or increased risk of money laundering or terrorist financing referred to in paragraph 2 of this Article.

Article 10
(Notifying Member States and European institutions)

The Office shall notify the European Commission, European supervisory authorities and other Member States with the title of the permanent inter-ministerial working group referred to in paragraph 2 of Article 8 of this Act and of summary of the report on the national risk assessment of money laundering and terrorist financing.

Article 11
(Recommendations of the European Commission)

(1) Within the scope of the arrangement for preventing money laundering and terrorist financing in the Republic of Slovenia, the recommendations of the European Commission on measures suitable to mitigate risks established in the national risk assessment may be observed.

(2) If the Republic of Slovenia decides not to observe the recommendations referred to in the preceding paragraph, it shall notify the European Commission thereof and state the reasons for its decision.

CHAPTER III – TASKS AND OBLIGATIONS OF OBLIGED PERSONS

3.1 General provision *Article 12*

(Tasks and obligations of obliged persons)

(1) For the purpose of detecting and preventing money laundering and terrorist financing, obliged persons shall carry out tasks stipulated by the present Act and regulations adopted on the basis thereof in the course of their business.

(2) The tasks referred to in the preceding paragraph shall comprise:

1. preparing a risk assessment of money laundering and terrorist financing;
2. establishing policies, controls and procedures to successfully mitigate and manage risks of money laundering and terrorist financing;
3. applying measures to acquire knowledge about the customer (hereinafter: customer due diligence) under the terms and conditions and in the manner provided by the present Act;
4. reporting prescribed and requisite data and submitting evidence to the Office in accordance with the provisions of the present Act;
5. appointing an authorised person and assistants of the authorised person and ensuring conditions for their work;
6. providing regular professional training for workers and ensuring regular internal control of the performance of tasks as per this Act;
7. preparing a list of indicators for identifying customers and transactions in respect of which reasonable grounds to suspect money laundering or terrorist financing exist;
8. ensuring protection and retention of data and management of records required by this Act;
9. implementing policies and procedures of a group and measures for detecting and preventing money laundering and terrorist financing in branches and majority-owned subsidiaries located in third countries;
10. implementing other tasks and obligations as per the provisions of this Act and regulations adopted on the basis thereof.

3.2 Risk assessment and management *Article 13*

(Risk assessment of money laundering and terrorist financing)

(1) Risk of money laundering or terrorist financing shall mean the risk that the customer would misuse the financial system to launder money or for terrorist financing or that a business relationship, transaction, product, service or distribution channel, taking into account the geographical factor (state or geographical area), would be used, directly or indirectly, for money laundering or terrorist financing.

(2) An obliged person shall prepare a risk assessment for individual groups or customers, business relationships, transactions, products, services or distribution channels and take into account factors of geographical risk with respect to their potential misuse of money laundering or terrorist financing.

(3) The risk assessment and procedure to determine the risk assessment referred to in the previous paragraph shall reflect the specific features of the obliged person and its operations.

(4) The risk assessment referred to in paragraph 2 of this Article shall be prepared by the obliged person according to the guidelines issued by the competent supervisory body referred to in Article 139 of this Act according to its powers and by observing the reports on the findings of national risk assessment and transnational risk assessment.

(5) The findings of risk assessment referred to in paragraph 2 of this Article shall be documented and updated by the obliged person at least every two years. Documented findings shall be available to the competent supervisory bodies referred to in Article 139 of this Act at their request.

(6) Upon all important changes in its business processes – such as the introduction of a new product, new business practice, including new distribution channels, introduction of new technology for new and existing products, or organisational changes – the obliged person shall perform a relevant assessment of how the changes affect the exposure of the obliged person to the risk of money laundering or terrorist financing.

(7) The obliged person shall perform the risk assessment referred to in the preceding paragraph before the introduction of a change and, according to findings, adopt measures to reduce risks of money laundering or terrorist financing.

Article 14

(Little or increased risk of money laundering and terrorist financing)

(1) If the obliged person assesses that a customer, business relationship, transaction, product, service, distribution channel, state or geographical area presents little risk of money laundering or terrorist financing, it may implement measures of simplified customer due diligence according to the provisions of this Act on simplified customer due diligence.

(2) If the obliged person assesses that a customer, business relationship, transaction, product, service, distribution channel, state or geographical area presents an increased risk of money laundering or terrorist financing, it must implement measures of enhanced customer due diligence according to the provisions of this Act on enhanced customer due diligence.

Article 15

(Risk management of money laundering and terrorist financing)

(1) To carry out efficient mitigation and management of risk of money laundering and terrorist financing identified on the basis of Article 14 of this Act, the obliged person shall establish efficient policies, controls and procedures that are proportional in terms of his/her activity and size (such as size and structure of the obliged person, scope and structure of business operations, types of customers with which the obliged person conducts business, types of products offered by the obliged person).

(2) The policies, controls and procedures referred to in the previous paragraph shall include: 1. development of internal policies, controls and procedures that refer to:

- models of risk management,
- customer due diligence,
- reporting of data to the Office,
- protection and retention of data and management of records,
- internal control of the performance of tasks in the field of detecting and preventing money laundering and terrorist financing,
- provision of compliance with regulations, and
- secure employment and, if required, security clearance of employees as per the Act governing classified information, and

2. establishment of an independent internal audit department verifying internal policies, controls and procedures referred to in the preceding point if the obliged person is a medium-sized or large company as per the Act governing companies.

(3) An obliged person that is a medium-sized or large company as per the Act governing companies shall appoint one of the members of Management Board or body who is responsible for implementing the tasks referred to in the preceding paragraph and providing compliance of the implementation of acts and other regulations in the field of detecting and preventing money laundering and terrorist financing.

(4) Prior to introducing policies, controls and procedures, obliged persons shall acquire the approval of the management, and according to the guidelines of supervisory bodies referred to in Article 139 of this Act, monitor and, if required, strengthen the measures adopted.

3.3 Customer due diligence 3.3.1 General provisions Article 16 (Elements of customer due diligence)

(1) If not otherwise provided by this Act, customer due diligence shall comprise:

1. establishing the customer's identity and verifying the customer's identity on the basis of authentic, independent and objective sources;
2. determining the beneficial owner of the customer;
3. obtaining data on the purpose and intended nature of the business relationship or transaction, as well as other data pursuant to this Act;
4. regular monitoring of business activities undertaken by the customer through the obliged person.

(2) In implementing the measures referred to in points 1 and 2 of the preceding paragraph of this Article, obliged persons shall verify that any person who acts on behalf of the customer has the right to representation or is authorised by the respective customer, and according to the provisions of this Act, establish and verify the identity of any person who acts on behalf of the customer.

(3) The obliged person shall implement all the measures of customer due diligence referred to in paragraphs 1 and 2 of this Article, whereby it may determine the scope of measures by taking into account the risk of money laundering and terrorist financing.

(4) In determining the scope of implementation of the measures referred to in paragraphs 1, 2 and 3 of this Article, the obliged person shall take into account at least:

- the purpose of concluding and nature of a business relationship;
- the amount of assets, value of property or scope of transactions;
- duration of a business relationship; and
- compliance of business with the purpose of concluding business relationship.

(5) The obliged person shall define procedures for implementing the measures referred to in paragraphs 1, 2, 3 and 4 of this Article in its internal regulations.

(6) The obliged person shall submit to the supervisory bodies referred to in Article 139 of this Act at their request respective analyses, documents and other information with which it proves the suitability of implemented measures in terms of established risks of money laundering and terrorist financing.

Article 17 (Customer due diligence obligation)

(1) An obliged person shall perform customer due diligence in accordance with the terms and conditions provided by the present Act in the following cases:

1. when establishing a business relationship with a customer;
2. when carrying out a transaction amounting to EUR 15,000 or more, notwithstanding whether the transaction is carried out in a single or several operations which are evidently linked;

3. in organisers and concessionaires who offer games of chance upon payment of wins, bets or both when they are transactions in the value of EUR 2,000 or more, notwithstanding that a transaction is executed individually or with several transactions which are evidently linked;

4. when there are doubts about the veracity and adequacy of previously obtained data about a customer or beneficial owner;

5. whenever there is a suspicion of money laundering or terrorist financing in respect of a transaction or customer, assets or property regardless of the transaction amount.

(2) If the obliged person concludes an additional business relationship with the customer or on the basis of the existing business relationship performs transactions referred to in points 2 and 3 of the preceding paragraph, the obliged person shall obtain only the missing data referred to in paragraphs 1, 2, 3 and 4 of Article 48 of this Act, and that under the condition that it has already executed customer due diligence as per Article 16 of this Act and provided suitable verification and update of the preliminarily obtained documents and data on the customer within the scope of regular monitoring of business activities.

(3) In the transactions referred to in points 2 and 3 of paragraph 1 of this Article, an organiser or a concessionaire offering games of chance shall verify the identity of the customer carrying out the transaction and obtain the required information at the cashier's desk or other transaction points according to the type of game of chance and method of gaming.

(4) For the purposes of this Act, the customer's registration for participation in a system of organising games of chance with organisers and concessionaires who offer games of chance via the Internet or other telecommunications means shall be deemed an established business relationship.

(5) Pursuant to this Act, the customer's accession to the fund rules of a mutual fund managed by a management company shall be deemed as an established business relationship between the customer and the management company. Accession to the fund rules of another mutual fund managed by the same management company shall not be deemed as an established new business relationship between the customer and the management company.

(6) Pursuant to this Act, a customer's accession to the fund rules of an investment fund management or other document, on the basis of which the investor accesses the investment fund, shall be deemed as an established business relationship between the customer and the obliged person referred to in point 6 of paragraph 1 of Article 4 of this Act. Accession to the fund rules of another investment fund managed by the same management company or a manager of an alternative investment fund shall not be deemed as an established new business relationship as per this Act.

(7) The establishment of a business relationship as per this Act shall not include:

- implementation of payment transactions not exceeding EUR 1,000 on the basis of the UPN form with the providers of payment services with which the payer has no open payment account;
- implementation of minor business operations that do not exceed the value of EUR 1,000.

Article 18 **(Customer due diligence obligation in occasional transactions)**

(1) Notwithstanding the provisions of the preceding Article, the obliged person shall perform customer due diligence under the conditions stipulated by this Act at every occasional transaction, which means a transfer of assets and exceeds EUR 1,000.

(2) The occasional transaction referred to in the preceding paragraph shall mean a transaction implemented by a customer who is not in a business relationship with the obliged person.

(3) The transfer of means referred to in paragraph 1 of this Article shall mean any transaction which is at least partly implemented with electronic means on behalf of the payer through the provider of payment services for the purpose of making the assets available to the receiver of payment through the provider of payment services, regardless of whether the payer and receiver of payment are the same person and regardless of whether the provider of payment services and the receiver of payment are the same person, including the following payment services:

1. credit payments as defined in the Act governing payment services and systems;
2. direct debit as defined in the Act governing payment services and systems;
3. remittance of money as defined in the Act governing payment services and systems, regardless of whether it is a domestic or cross-border payment transaction; and
4. transfer performed with payment cards, electronic money, mobile phones or other digital or prepaid or subscription IT devices with similar characteristics.

Article 19 (Customer due diligence when establishing a business relationship)

(1) When establishing a business relationship referred to in point 1 of paragraph 1 of Article 17 of this Act, an obliged person shall execute the measures referred to in points 1, 2 and 3 of paragraph 16 of this Article before the business relationship is established.

(2) Notwithstanding the provisions of the preceding paragraph, an obliged person may exceptionally apply measures from points 1 and 2 of paragraph 1 of Article 16 also when establishing a business relationship with the customer if it is deemed necessary to preserve uninterrupted normal conduct of the obliged person's business and if, in accordance with Article 13 of this Act, there is little risk of money laundering or terrorist financing.

(3) Notwithstanding paragraph 1 of this Article, an obliged person referred to in points 1, 14, 20 (i) and 20 (j) of paragraph 1 of Article 4 of this Act, in addition to customer due diligence and as soon as the beneficiaries have been defined or determined, shall take measures of due diligence of beneficiaries of payments under the policy after the business relationship of life insurance and unit-linked life insurance have been established:

1. for beneficiaries who are defined as specific natural persons or legal entities or similar foreign law entities when establishing a business, an obliged person shall acquire information on their personal name and date of birth;
2. for beneficiaries who are defined according to their characteristics, categories or otherwise, an obliged person shall acquire sufficient data and information to establish and verify their identity at the time of payment.

(4) In the cases referred to in points 1 and 2 of the preceding paragraph, an obliged person shall determine and verify the identity of the beneficiary at the time of payment. In the case of a full or partial transfer of life insurance or unit-linked life insurance to a third party, an obliged person notified about the transfer shall define a new beneficiary at the time of transferring the insurance to a third party.

Article 20 (Customer due diligence when effecting transactions)

When effecting transactions referred to in points 2 and 3 of paragraph 1 of Articles 17 and 18 hereof, an obliged person shall apply the measures provided for in points 1, 2 and 3 of paragraph 1 of Article 16 hereof, taking into account paragraph 2 of Article 17 hereof, before the transaction is carried out.

Article 21
(Non-performance of customer due diligence obligation)

An obliged person who cannot apply the measures referred to in points 1, 2 and 3 of paragraph 1 of Article 16 hereof in accordance with the provisions of this Act shall not establish a business relationship or effect a transaction, or shall terminate the business relationship if already established, and shall consider the possibility of reporting the data on the customer or suspicious transaction to the Office in accordance with paragraph 3 of Article 69 hereof.

Article 22
(Exemption from certain measures of customer due diligence related to electronic money)

(1) The obliged persons referred to in point 15 of paragraph 1 of Article 4 of this Act need not apply customer due diligence referred to in points 1, 2, and 3 of paragraph 1 of Article 16 of this Act if, on the basis of a risk assessment, they establish that there is little risk of money laundering or terrorist financing, and the following conditions have been fulfilled:

1. on the payment instrument:
 - it is not possible to upload data or
 - the highest amount of monthly transactions does not exceed EUR 250, whereby the payment instrument can be used only in the Republic of Slovenia;
2. the highest amount of electronic money deposited on the payment instrument:
 - does not exceed EUR 250 or
 - does not exceed EUR 500, whereby the payment instrument can be used only in the Republic of Slovenia;
3. payment instrument may be used only to purchase goods or services;
4. payment instrument cannot be deposited with anonymous electronic money;
5. issuers of electronic money sufficiently monitor transactions or business relationship as referred to in point 4 of Article 16 of this Act to detect unusual or suspicious transactions.

(2) Notwithstanding the provisions of paragraph 1 of this Article, customer due diligence referred to in Article 16 of this Act shall be performed before redemption in cash or cash withdrawal of the monetary value of electronic money when the realised amount exceeds the value of EUR 100.

(3) The obliged persons referred to in paragraph 1 of this Article on the exemption from certain measures of customer due diligence shall notify the Office, namely before the product is placed on the market. The documentation on the fulfilment of conditions and risk assessment of money laundering and terrorist financing referred to in paragraph 1 of this Article shall be attached to the notification.

(4) Notwithstanding the provisions of paragraph 1 of this Article, the omission of certain measures of customer due diligence shall not be permitted when reasons to suspect money laundering or terrorist financing exist in connection with the customer, product, assets or transaction.

3.3.2 Application of customer due diligence measures

3.3. 2.1 Determining and verifying customer identity

Article 23
(Determining and verifying customer identity)

(1) For

- a customer who is a natural person or its legal representative, sole proprietor or individual performing an activity independently,
- statutory representative of the legal entity,

an obliged person shall determine and verify the customer's identity and obtain the data referred to in point 2 of paragraph 1 of Article 137 of this Act by examining the customer's official personal identification document in the customer's presence. If all the required data cannot be obtained from the aforementioned document, the requisite data shall be obtained from another authentic document submitted by the customer or directly from the customer.

(2) When the customer is a sole proprietor or self-employed person, an obliged person shall obtain the data referred to in point 1 of paragraph 1 of Article 137 hereof by applying Article 28 of this Act *mutatis mutandis*.

(3) If, in determining and verifying the identity of the customer pursuant to the provisions of this Article, the obliged person doubts the reliability or veracity of documents and other business records from which the data have been obtained, it shall also demand a written statement from the customer.

Article 24

(Determining and verifying the identity of a representative of natural person, sole proprietor, or individual performing an activity independently)

(1) An obliged person shall determine and verify the identity of an authorised person concluding a business relationship on behalf of a natural person, sole proprietor or individual performing an activity independently and shall obtain the data referred to in point 2 of paragraph 1 of Article 137 of this Act by examining the authorised person's official personal identification document in his/her presence. If all the required data cannot be obtained from the aforementioned document, the requisite data shall be obtained from another authentic document submitted by the authorised person or directly from the authorised person. When an authorised person acts on behalf of a natural person, sole proprietor or individual performing an activity individually, an obliged person shall obtain the data referred to in point 2 of paragraph 1 of Article 137 of this Act from the customer's written authorisation which is no older than three months

(2) If the customer referred to in the preceding paragraph performs the transaction referred to in point 2 or 3 of paragraph 1 of Article 17 and Article 18 of this Act, the obliged person shall obtain a statement from the customer on whether the customer is conducting business on its own behalf or on behalf of a third party. If the customer is conducting business on behalf of a third party, the obliged person shall act as per paragraph 3 of this Act. If the respective transaction is carried out on the basis of a previously established business relationship, information on whether the transaction was by the customer or its representative shall also be deemed sufficient data.

(3) If the transactions referred to in point 2 or 3 of paragraph 1 of Articles 17 and 18 hereof are carried out on behalf of the customer referred to in paragraph 1 of this Article by his/her authorised person, an obliged person shall determine and verify the authorised person's identity and obtain the required data on the customer and authorised person referred to in point 2 of paragraph 1 of Article 137 hereof, as set forth in paragraph 1 of this Article.

(4) If, in determining and verifying the identity of an authorised person, an obliged person doubts the reliability of the data received, it shall request the authorised person's written statement.

Article 25

(Determining and verifying the identity of an authorised person of a legal entity)

(1) An obliged person shall determine and verify the identity of an authorised person concluding a business relationship in place of a statutory representative on behalf of a customer who is a

legal entity and shall obtain the data referred to in point 2 of paragraph 1 of Article 137 of this Act by examining the authorised person's official personal identification document in his/her presence. If all the required data cannot be obtained from the aforementioned document, the requisite data shall be obtained from another authentic document submitted by the authorised person or directly from the authorised person. An obliged person shall obtain the data referred to in point 2 of paragraph 1 of Article 137 of this Act about a statutory representative, on whose behalf an authorised person acts, from the certified written authorisation issued by the statutory representative.

(2) If the customer referred to in the preceding paragraph performs the transaction referred to in point 2 or 3 of paragraph 1 of Articles 17 and 18 of this Act, the obliged person shall obtain a statement from the statutory representative on whether the customer is conducting business on its own behalf or on behalf of a third party. If the customer is conducting business on behalf of a third party, the obliged person shall act as per paragraph 3 of this Act. If the respective transaction is carried out on the basis of a previously established business relationship, information on whether the transaction was by the customer or its representative shall also be deemed sufficient data.

(3) If the transactions referred to in point 2 or 3 of paragraph 1 of Articles 17 and 18 hereof are carried out on behalf of the customer referred to in paragraph 18 of this Article by his/her authorised person, an obliged person shall determine and verify the authorised person's and statutory representative's identity and obtain the required data on the customer and authorised person referred to in point 2 of paragraph 1 of Article 137 hereof, as set forth in paragraph 1 of this Article.

(4) If, in determining and verifying the identity of an authorised person, an obliged person doubts the reliability of submitted data, it shall request the authorised person's written statement.

Article 26

(Determining and verifying the identity on the basis of means of electronic identification)

(1) Notwithstanding the provisions of Articles 23, 24 and 25 of this Act, an obliged person may also establish and verify the identity under the conditions defined by the minister responsible for finance through the Rules on the basis of:

1. means of electronic identification of such level of reliability, which requires the presence of the customer at the time of issuing and issued by an issuer of means of electronic identification with its registered office in the Republic of Slovenia as per regulations governing electronic identification,
2. means of electronic identification of such level of reliability that requires the presence of the customer at the time of issuing and issued by an issuer of means of electronic identification with its registered office in other Member State or a third country under the conditions defined by regulations governing electronic identification and provided that technological possibilities for such purpose are available.

(2) Determining and verifying identity on the basis of means of electronic identification referred to in paragraph 1 of this Article may be used for:

- a customer who is a natural person or its statutory representative, sole proprietor or individual performing an activity independently;
- an authorised person of the customer referred to in the preceding indent;
- a statutory representative or an authorised person of a legal entity.

(3) When determining and verifying the identity of a customer pursuant to the preceding paragraph, an obliged person shall obtain the required data on the customer referred to in point 2 of paragraph 1 of Article 137 hereof from the means of electronic identification referred to in paragraph 1 of this Article. Data not available on the means of electronic identification shall be obtained from the copy of the official personal document sent by the customer to the obliged person in paper or digital form. If all the required data cannot be obtained in the manner described above, the requisite data shall be obtained directly from the customer.

(4) The issuer of means of electronic identification referred to in paragraph 1 of this Article shall immediately forward to the obliged person, upon its request, data on the method by which it established and verified the identity of the customer who is the holder of the means of electronic identification referred to in paragraph 1 of this Article. The data obtained shall be kept by the obliged person in accordance with the provisions of the present Act and the Act regulating protection and retention of data.

(5) Notwithstanding paragraphs 1 and 2 of this Article, determining and verifying the identity of the client by using means of electronic identification shall not be permitted if there is a suspicion that the means of electronic identification has been misused, or if an obliged person establishes that circumstances substantially affecting the validity of the means of electronic identification have changed, but the issuer of the electronic identification has not yet revoked it.

(6) If, upon entering into a business relationship, the obliged person determines or verifies the identity of a customer on the basis of paragraph 1 of this Article, the obliged person shall adopt measures ensuring that, prior to effecting the customer's subsequent transaction through the obliged person, the first payment of the operation is carried out through a payment account opened by the customer in its name or a statutory representative or an authorised representative in its or customer's name or is opened with a credit institution.

(7) If an obliged person determines and verifies the identity as per this Article, the obliged person, in performing the risk assessment referred to in Article 13 hereof, shall take into account the higher risk of money laundering or terrorist financing which occurs if the customer has not been physically present.

Article 27
(Determining and verifying the identity of customers by using video-based electronic identification)

(1) Notwithstanding the provisions of Articles 23 and 24 hereof, an obliged person may exclusively establish and verify the identity of a customer who is a natural person without their presence by using video-based electronic identification, if the following conditions are fulfilled:

1. no increased risk of money laundering or terrorist financing as per Article 13 and paragraph 1 of Article 14 hereof is established in relation to products or services which are subject to the electronic video identification of a customer;
2. the identity of the customer shall be determined and verified exclusively on the basis of an official personal identification document equipped with a biometric photograph;
3. the customer is at least 18 years old;
4. the customer has a permanent residence in Member States or third countries that have established an efficient system for preventing and detecting money laundering and terrorist financing;
5. the customer does not have a permanent residence in countries included on the lists referred to in paragraph 3 of Article 50 hereof;
6. the obliged person shall compensate for the higher risk of money laundering and terrorist financing which occurs when the customer has not been physically present by using one or several measures of enhanced customer due diligence as per the provisions of this Act, whereby these measures must continue for at least one year; and
7. the obliged person shall adopt a measure to provide that, before implementing further transactions of a customer with the obliged person, the first payment of the operation is carried out through an account opened by the customer with the credit institution.

(2) When an individual transaction related to a product or a service exceeds EUR 15,000, the obliged person shall determine and verify the identity of the customer in the customer's presence as per the provisions of this Act on establishing and verifying the identity.

(3) When determining and verifying the identity of the customer pursuant to paragraph 1 of this Article, an obliged person shall obtain the data referred to in point 2 of paragraph 1 of Article 137 hereof.

(4) The data referred to in the preceding paragraph of this Article that cannot be obtained within the scope of determining and verifying the identity of the customer pursuant to paragraph 1 of this Article shall be obtained from the copy of the official personal identification document sent by the customer to the obliged person in paper or digital form. If all the required data cannot be obtained in the manner described above, the requisite data shall be obtained directly from the customer.

(5) The minister responsible for finance shall determine minimum technical conditions prescribed in the rules that must be fulfilled by means of video-based electronic identification.

Article 28 **(Determining and verifying the identity of a legal entity)**

(1) An obliged person shall determine and verify the identity of the customer (legal entity) and obtain the data referred to in point 1 of paragraph 1 of Article 137 hereof by inspecting original or certified documentation from the commercial, court register or other public register submitted to the obliged person by the statutory representative or his/her authorised person on behalf of the legal entity.

(2) The documentation referred to in the preceding paragraph shall not be older than three months.

(3) An obliged person may determine and verify the identity of a legal entity and obtain the data referred to in point 1 of paragraph 1 of Article 137 of this Act by inspecting a commercial, court or other public register. The extract from the register that is used shall bear a remark by the obliged person to indicate the date and time of access and the personal name of the person who inspected the register. The extract from the register shall be kept by the obliged person in accordance with the provisions of the present Act governing the protection and retention of data.

(4) An obliged person shall obtain other data referred to in paragraph 1 of Article 137 hereof, with the exception of data on a beneficial owner, by inspecting original or certified documents and other business documentation. If all the data referred to in paragraph 1 of Article 137 hereof cannot be obtained from such documents and documentation, the requisite data, with the exception of data on the beneficial owner, shall be obtained directly from the statutory representative or authorised person pursuant to the provisions of this Act on establishing the beneficial owner.

(5) If, in determining and verifying the identity of a legal entity, an obliged person doubts the reliability of submitted data or veracity of documents or other business records from which the data has been obtained, it shall require a written statement from the statutory representative or authorised person prior to entering into a business relationship or effecting a transaction.

(6) When determining and verifying the identity of the customer pursuant to paragraphs 1 and 3 of this Article, an obliged person shall examine beforehand the nature of the register from which data for the verification of identity shall be obtained.

(7) When the customer is a foreign legal entity pursuing an activity in the Republic of Slovenia through its branch, an obliged person shall determine and verify the identity of the foreign legal entity and its branch.

Article 29 **(Determining and verifying the identity of other civil law entities)**

When the customer is a civil law entity as referred to in point 5 of Article 3 hereof which is not a natural person or legal entity, the obliged person shall:

1. determine and verify the identity of the person with powers of representation (hereinafter: agent);
2. obtain certified written powers of representation;
3. obtain the data referred to in points 2 and 15 of paragraph 1 of Article 137 of this Act.

(2) The obliged person shall determine and verify the identity of the agent referred to in paragraph 1 of this Article and obtain the data referred to in point 2 of paragraph 1 of Article 137 of this Act by examining the agent's official personal identification document in the agent's presence. If all the required data cannot be obtained from the mentioned document, the requisite data shall be obtained from another authentic document submitted by the agent or directly from the agent.

(3) The obliged person shall obtain the data referred to in point 15 of paragraph 1 of Article 137 hereof about a person who is a member of a civil law entity as referred to in paragraph 1 of this Article from the certified written powers of representation submitted to the obliged person by the agent. If all the data referred to in point 15 of paragraph 1 of Article 137 hereof cannot be obtained from such document, the requisite data shall be obtained directly from the agent.

(4) Notwithstanding point 2 of paragraph 1 and paragraph 3 of this Article, the obliged person may obtain only written powers of representation if its customer is a group of secondary-school students, primary-school children or children in a nursery which is a part of the education system in the Republic of Slovenia, or a voluntary group of employees acting as a mutual assistance fund within the trade union of an individual employer.

(5) If, in determining and verifying the identity of a person referred to in paragraph 1 of this Article, the obliged person doubts the reliability of submitted data or veracity of documents from which the data has been obtained, it shall require a written statement from the agent prior to entering into a business relationship or effecting a transaction.

Article 30 **(Specific cases concerning determination of the identity of a customer)**

(1) Subject to the provisions of Article 17 of this Act, a customer's identity shall also be determined and/or verified in the following cases:

1. every time the customer enters the casino or gaming hall of the concessionaire offering games of chance;
2. every time the customer accesses a safe.

(2) In determining and verifying the identity of a customer pursuant to paragraph 1 of this Article, a concessionaire offering games of chance in a casino or gaming hall or an obliged person providing services related to the rental of safety-deposit boxes shall obtain the data required under points 3 and 5 of paragraph 1 of Article 137 of this Act.

(3) Notwithstanding the provisions of Articles 23, 24 and 25 hereof, the customer's identity may be determined and verified each time the customer accesses the safe by means of the electronic identification of a card, personal password for access or means of video-based electronic identification, or means that provide the identification of the customer on the basis of the customer's biometric characteristics.

(4) The provisions of this Act concerning the obligation to verify the identity of a customer when they access a safe shall apply to any natural person actually accessing the safe, regardless of whether or not the person concerned is a party to the safekeeping contract or only the party's statutory representative or authorised person, and shall apply only if the identity of all persons has been determined and verified in their presence when establishing a business relationship.

(5) The minister responsible for finance shall determine the minimum technical conditions prescribed in the conditions that must be met by safes and means of video-based electronic identification or means providing the identification of a customer on the basis of their biometric characteristics.

Article 31

(Special features in determining and verifying the identity of banks and other similar credit institutions, their statutory representatives and authorised representatives)

(1) The obliged persons referred to in points 1 and 2 of paragraph 1 of Article 4 hereof may determine and verify the identity of a bank or other similar credit institution and their statutory representatives by means of the careful collection and review of publicly available information on the bank or other similar credit institution, whereby:

1. notwithstanding Article 28 hereof, the identity of a legal entity shall be established by using sources normally applied in international banking relationships;

2. notwithstanding Articles 23 and 25 hereof, the identity of its statutory representatives and authorised representatives shall be established according to the method normally used in international banking relationships.

(2) The obliged person referred to in the preceding paragraph shall obtain data within the scope determined in paragraph 5 of Article 60 hereof.

(3) This Article shall not apply for the purposes of determining or verifying the identity of banks or other similar credit institutions when a bank or other similar credit institution has its registered office in a high-risk third country as referred to in paragraph 5 of Article 50 hereof.

Article 32

(Storage of copies of official personal identification documents in an electronic form)

Notwithstanding the provisions of other acts, obliged persons that are credit or financial institutions may store copies of official personal identification documents obtained within the scope of implementing measures to determine and verify the identity of a customer as per the provisions of this Act in electronic form if the documents are protected with organisational, logical and technical procedures and measures as per the Act governing personal data protection.

3.3.2.2 Beneficial owner

3.3.2.2.1 Determining the beneficial owner

Article 33 (Concept)

A beneficial owner shall be any natural person who ultimately owns or supervises or otherwise exercises oversight of a customer or a natural person on whose behalf a transaction is carried out.

Article 34
(Obligation to determine the beneficial owner)

(1) The obliged persons referred to in Article 4 hereof shall carry out a measure to determine a beneficial owner as an integral part of the customer due diligence referred to in Article 16 hereof, unless otherwise provided by this Act.

(2) Business entities shall determine the information on their beneficial owner, unless otherwise provided by this Act.

(3) Information and documentation obtained in relation to identifying a beneficial owner shall be stored by obliged persons referred to in Article 4 of this Act as per provisions of this Act on the storage of data.

Article 35
(Beneficial owner of a corporate entity)

(1) Pursuant to this Act, a beneficial owner of a corporate entity shall be:

1. any natural person who:

- is an indirect or direct owner of a sufficient business share, shares, voting or other rights based on which the person participates in the management of the corporate entity; or
- indirectly or directly participates in the capital of the corporate entity with a sufficient share; or
- has a controlling position in the management of the corporate entity's funds;

2. any natural person who indirectly provides or is providing funds to a corporate entity and on such grounds has the possibility of exercising control, guiding or otherwise substantially influencing the decisions of the management of the corporate entity concerning financing and business operations.

(2) The indication of direct ownership of a natural person or natural persons referred to in indents 1 and 2 of point 1 of the preceding paragraph in the corporate entity shall be ownership of at least 25% of the business share, voting or other rights on the basis of which the natural person participates in the management of the legal entity, or ownership of 25% and one share.

(3) The preceding paragraph shall apply, *mutatis mutandis*, when determining the indirect ownership of a legal entity in the corporate entity under control:

- one or several natural persons, or
- one or several legal entities under the control of the same one or several natural persons.

(4) A natural person who has controlling position in the management of a corporate entity's funds, or who in any other way exercises control, guiding or otherwise substantially influences the decisions of the management of the corporate entity as referred to in paragraph 1 of this Article, may be determined, *inter alia*, on the basis of conditions to be observed by a corporate entity that controls one or several subsidiaries in the preparation of the consolidated annual report as per the Act governing companies.

(5) If no natural person is determined as a beneficial owner as per the provisions of this Article – provided that all possible measures are taken to determine the beneficial owner and on the condition that there are no reasons to suspect money laundering or terrorist financing in relation to the transaction, person, property or assets – one or several persons in management positions shall be deemed as the beneficial owner(s) of the corporate entity.

(6) If doubt arises as to whether the determined natural person is the beneficial owner as per the provisions of this Article, one or several persons in management positions shall be deemed as the beneficial owner(s) of the corporate entity.

Article 36

(Beneficial owner of an entity with no business shares and beneficial owner of the institution)

(1) Pursuant to this Act, as a beneficial owner of a society, institute, political party, trade union, religious community or other business entity in which participation in management on the basis of a business share, share or participation in capital is not possible shall be deemed any natural person representing such an entity.

(2) Notwithstanding the preceding paragraph, a beneficial owner of the institution shall be deemed any natural person that is:

1. a founder of the institution if they have a controlling position in the management of the institution's assets
as per the Articles of Association or rules of the institution;
2. a trustee of the institution as per the Act governing institutions;
3. a representative of the institution if a founder of the institution cannot be deemed a beneficial owner.

Article 37

(Beneficial owner of a foreign trust, foreign institution or similar foreign law entity)

(1) For the purposes of this Act, the beneficial owner of a foreign trust, foreign institution or similar foreign law entity which accepts, administers or distributes funds for particular purposes shall mean:

- a) any natural person who is :
 - a founder of a foreign trust, foreign institution or similar foreign law entities;
 - a trustee of a foreign trust, foreign institution or similar foreign law entities;
 - a beneficiary of the proceeds of property under management, whereby the future beneficiaries have already been determined or can be determined;
 - a potential representative appointed to represent and protect the interests of recipients of proceeds;
- b) a category of persons with an interest in establishing a foreign trust, foreign institution or similar foreign law entity when the individuals that benefit from the foreign trust, foreign institution or similar foreign law entity have yet to be determined;
- c) any other natural person who in any other way indirectly or directly controls the property of a foreign trust, foreign institution or similar foreign law entity.

(2) Data and documentation on measures taken to determine a beneficial owner of a foreign trust, foreign institution or similar foreign law entities as per the previous paragraphs shall be kept by the obliged person as per the provisions of this Act on data storage.

3.3.2.2.2 Specific cases concerning determination of a beneficial owner

Article 38

(Beneficial owner of a sole proprietor or an individual performing an activity independently)

It shall be deemed that the beneficial owner of a customer who is a sole proprietor or an individual performing an activity independently is a natural person registered to pursue the activity of the customer and is at the same time a sole representative if it is not established otherwise by customer due diligence.

Article 39
(Beneficial owner of a single-member limited liability company)

It shall be deemed that the beneficial owner of a single-member limited liability company is a natural person who is a sole shareholder of this customer and at the same time its sole representative if it is not established otherwise by customer due diligence.

Article 40
(Exception related to indirect and direct budget users)

It shall be deemed that a beneficial owner of an indirect or direct budget user is a natural person who represents such an entity.

3.3.2.2.3 Obligations of business entities

Article 41
(Obligations of business entities related to identifying a beneficial owner)

(1) The business entities referred to in Articles 35 and 36 hereof entered in the Slovenian Business register must identify the data on their beneficial owner or owners according to the method defined in Articles 35 and 36 hereof.

(2) The business entities referred to in Article 37 must identify the data on their beneficial owner as per Article 37 hereof if their operations result in tax liabilities in the Republic of Slovenia.

(3) The business entities referred to in preceding paragraphs shall set up and manage precise records of data on their beneficial owners that are updated upon every change of data. The content of the records is prescribed in paragraph 16 of Article 137 hereof.

(4) Pursuant to this Act, the business entities referred to in paragraphs 1 and 2 of this Article shall keep the data on their beneficial owners for a period of five years from the day of termination of the beneficial owner's status.

(5) If the business entity referred to in paragraph 1 and 2 of this Article is terminated, a court or authority managing the termination proceedings or status change of the entity without a known successor must order that the data storage on beneficial owners be provided for the period referred to in the preceding paragraph prior to the termination of the business entity.

(6) The provision of this Article shall not apply to business entities that are:

- sole proprietors;
- individuals performing an activity independently;
- single-member limited liability companies; and
- direct or indirect budget users.

(7) The provisions of this Article shall not apply to business entities which are companies in an organised market in which they are obliged to comply with a disclosure requirement that provides suitable transparency of ownership information as per the legislation of the European Union or comparable international standards.

Article 42
(Submission of data)

The business entities referred to in the preceding Article shall immediately submit data on their beneficial owners at the request of:

- the obliged persons referred to in Article 4 hereof if the data is required in relation to implementing customer due diligence measures as per this Act; or
- law enforcement agencies, courts or supervisory bodies as referred to in Article 139 hereof.

3.3.2.2.4 Obligations of obliged persons

Article 43
(Obtaining data related to identifying a beneficial owner)

(1) An obliged person shall determine the beneficial owner of a customer by obtaining the data referred to in point 14 of paragraph 1 of Article 137 hereof. With regard to the risk of money laundering or terrorist financing to which the obliged person is exposed in conducting business with an individual customer, the obliged person shall verify the data to such an extent that the obliged person understands the ownership and control structure of its customer and certainly knows who the beneficial owner is.

(2) Notwithstanding the preceding paragraph, an obliged person shall not obtain data on the beneficial owner of the customer if the customer is a natural person not performing a gainful activity.

(3) The provisions of this Article shall not apply to business entities which are companies in an organised market in which they are obliged to comply with a disclosure requirement that provides suitable transparency of ownership information as per the legislation of the European Union or comparable international standards.

(4) The obliged person shall obtain the data referred to in paragraph 1 of this Article by inspecting the original or certified documentation from the business, court or other public register, which shall not be older than three months. The data may also be obtained by inspecting the business, court or other public register and by directly inspecting the register of beneficial owners, whereby the obliged person must not exclusively rely on data entered in the register of beneficial owners.

(5) If all the data on the beneficial owner of a customer cannot be obtained from the business, court or any other public register, the obliged person shall obtain the requisite data by inspecting the original or certified documents and business records submitted by the statutory representative or his/her authorised person.

(6) If, for objective reasons, the requisite data cannot be obtained in the manner described in this Article, the obliged person shall obtain it directly from the written statement of a statutory representative or his/her authorised person, whereby the obliged person is obliged to apply one or several measures of enhanced customer due diligence for this customer as prescribed in the provisions of this Act governing measures of enhanced customer due diligence. The same shall apply to the obliged person if they obtain all the data on the beneficial owner only from the register of beneficial owners.

(7) If, in determining the beneficial owner, the obliged person doubts the reliability of submitted data or veracity of documents or other business documentation from which the data were obtained, it must also require a written statement from the statutory representative or authorised representative prior to entering into a business relationship or effecting a transaction, whereby the obliged

person is obliged to apply one or several measures of enhanced customer due diligence for this customer as prescribed in the provisions of this Act governing measures of enhanced customer due diligence.

3.3.2.2.5 Register of beneficial owners

Article 44 (Register of beneficial owners)

(1) A register of beneficial owners (hereinafter referred to: register) in which accurate and updated data on beneficial owners is kept shall be set up for the purpose of providing transparency of ownership structures of business entities and thus prevent abuses of business entities for money laundering and terrorist financing. By setting up the aforementioned register, obliged persons are provided access to relevant data for the needs of implementing customer due diligence, and the law enforcement, courts and supervisory bodies referred to in Article 139 hereof are provided with respective access for the needs of implementing the duties and powers concerning the prevention and detection of money laundering and terrorist financing.

(2) The Agency of the Republic of Slovenia for Public Legal Records and Related Services (hereinafter referred to as: register administrator) shall maintain and manage the register.

(3) The business entities referred to in Articles 35, 36 and 37 hereof, except for:

- sole proprietors;
- individuals performing an activity independently;
- single-member limited liability companies; and
- direct or indirect budget users

shall enter the data on their beneficial owners and owners' changes in the register within eight days from the entry of the business entity in the Slovenian Business Register or Tax Register if they are not entered in the Slovenian Business Register, or within eight days from the change of data.

(4) The provisions of this Article shall not apply to business entities which are companies in an organised market in which they are obliged to comply with a disclosure requirement that provides suitable transparency of ownership information as per the legislation of the European Union or comparable international standards.

(5) Business entities shall be responsible for the accuracy of the data entered.

Article 45 (Entry of data)

(1) The following data shall be entered in the register:

a) data on the business entity;

- company, address, registered office, registration number and tax ID number, date of entry and deletion of a business entity – for business entities entered in the Slovenian Business Register.

- company, address, registered office, tax ID number, date of entry and deletion from the Tax Register – for business entities entered in the Slovenian Business Register.

b) data on the beneficial owner: personal name, address of the permanent and temporary residence, date of birth, tax ID number, citizenship, ownership share or other method of supervision, and date of entry and deletion of the beneficial owner from the register;

c) in the case referred to in point (b) of paragraph 1 of Article 37 hereof, the data on the category of persons with an interest in establishing a foreign trust, foreign institution or similar foreign law entity.

(2) The administrator shall maintain and manage the register so that:

- in addition to the last status of the data on beneficial owners, all previous entries, changes of data and deletions according to the time and types of event shall also be kept;
- the data in the register shall be available for five years after the deletion of a business entity from the Business Register or Tax Register; and
- notwithstanding the preceding indent, the data in the register shall be permanently available for the law enforcement, courts and supervisory authorities referred to in Article 139 hereof.

(3) The entry shall be carried out via the web portal of the register administrator.

(4) Upon entry, the data on business entities shall be automatically obtained on the basis of a registration number from the Slovenian Business Register, and the data on business entities not entered in the Slovenian Business register shall be obtained on the basis of a tax ID number from the Tax Register. The administrator shall obtain changes of data on business entities automatically from the Slovenian Business register or Tax Register.

(5) Upon entering the register, personal data on the beneficial owner shall be automatically obtained from the Central Population Register on the basis of the tax ID number. The administrator shall obtain changes of personal data on natural persons automatically from the Central Population register by using a tax ID number.

(6) Upon entering the register, the personal data on a beneficial owner who is a natural person not registered in the Central Population Register shall be automatically obtained from the Tax Register by using tax ID number. The administrator shall obtain changes of personal data on natural persons kept in the register of beneficial owners and not entered in the Central Population register automatically from the Tax Register by using a tax ID number.

(7) A business entity alone shall enter personal data and changes of personal data on a beneficial owner who is a natural person not registered in the Central Population register nor Tax Register

(8) By means of rules, the minister responsible for the economy, in agreement with the minister responsible for finance, shall determine the method of entering data entered in the register, a code list on a method of supervision of beneficial owners of a business entity, method of communicating public data on the internet and method of maintenance and administration as well as technical requirements for the establishment of the register.

Article 46 **(Access to data on beneficial owners)**

(1) Data on the personal name, permanent and temporary residence, ownership share or method of supervision of beneficiary owners and the date of entry and deletion of the beneficial owner from the register shall be public and accessed free of charge on the web site of the register administrator. The purpose of publishing data is to provide a higher level of legal protection when establishing business relationships, safety of legal transactions, integrity of the business environment and transparency of business relationships of individuals with business entities who operate in the business environment and legal transactions.

(2) No one except the obliged persons referred to in Article 4 and the law enforcement authorities, courts and supervisory bodies referred to in Article 139 of this Act shall have the right to access data from the register in a manner which would provide a finding on whether a certain person is a beneficial owner of a business entity or a beneficial owner of which entity it is.

(3) The obliged persons referred to in Article 4 when conducting customer due diligence as per the provisions of this Act shall have direct electronic access to all data on beneficial owners entered in the

register. The search of data on beneficial owners shall be also provided to the obliged persons referred to in Article 4 of this Act by using a combination of a personal name and tax ID number, personal name and date of birth or a combination of personal name and the address of permanent residence entered in the register.

(4) The law enforcement authorities, courts and supervisory authorities referred to in Article 139 of this Act shall have free direct electronic access to all data on beneficial owners entered in the register when they implement authorisations and tasks related to preventing and detecting money laundering and terrorist financing. The search of data on beneficial owners shall also be provided to the respective entities referred to in this paragraph by using a combination of a personal name and tax ID number, personal name and date of birth or a combination of personal name and the address of permanent residence entered in the register.

(5) The register administrator may charge costs as per the tariff to the obliged person referred to in Article 4 of this Act to access data from the register. The tariff shall be determined by the administrator in agreement with the minister responsible for finance.

(6) Notwithstanding the preceding paragraphs, state authorities shall have a free electronic access to all data on beneficial owners entered in the register when they make decisions on the rights of entities which have financial consequences for the state budget. The search of data on beneficial owners shall be also provided to state authorities by using a combination of a personal name and tax ID number, personal name and date of birth or a combination of personal name and the address of permanent residence entered in the register.

Article 47

(Access to data on beneficial owners on the basis of legitimate interest)

(1) Persons or organisations who show a legitimate interest in regard to money laundering, terrorist financing and related previous criminal offences shall, in addition to the right to access the data referred to in paragraph 1 of the preceding Article, also have the right to access data on the date of birth and citizenship of beneficial owners.

(2) The persons or organisations referred to in the preceding paragraph, shall lodge a request to access data on the date of birth and citizenship of beneficial owners with the Office. The request must clearly state in relation to which beneficial owner the request to access data on the date of birth and citizenship is made. The justification on which the eligibility of their interest in relation to the money laundering, terrorist financing and related previous criminal offences is based and is in the public interest must also be given.

(3) The justified interest referred to in the preceding paragraph is given when knowledge of the requested data affects the protection of direct benefit or right based on a law or other regulation of the respective person or organisation or its legal position.

(4) The procedure on the basis of the request referred to in paragraph 2 of this Article shall be managed and decided on by the Office at its discretion for the purpose to provide data on beneficial owners which would otherwise remain concealed from persons or organisations if their justified interest is shown as per the Act governing general administrative procedures.

(5) An administrative dispute, not a complaint, shall be permitted against the decision of the Office referred to in the preceding paragraph.

3.3.2.3 Acquisition of data on the purpose and intended nature of business relationships or transaction and other data as per this Act

Article 48 (Set of data)

(1) Within the customer due diligence referred to in point 1 of paragraph 1 of Article 17 of this Act, the obliged person shall obtain the data from points 1, 2, 4, 5 and 14 of paragraph 1 of Article 137 of this Act.

(2) Within the customer due diligence referred to in point 2 of paragraph 1 of Article 17 of this Act, the obliged person shall obtain the data from points 1, 2, 6, 7, 8, 9 and 14 of paragraph 1 of Article 137 of this Act.

(3) Within the customer due diligence referred to in point 3 of paragraph 1 of Article 17 of this Act, the obliged person shall obtain the data from points 3, 6, 7, 8 and 9 of paragraph 1 of Article 137 of this Act.

(4) Within the customer due diligence referred to in points 4 and 5 of paragraph 1 of Article 17 of this Act, the obliged person shall obtain the data from paragraph 1 of Article 137 of this Act.

(5) Within the customer due diligence referred to in Article 18 of this Act, the obliged person shall obtain the data from points 1, 2, 6, 7, 8, 9 and 14 of paragraph 1 of Article 137 of this Act.

3.3.2.4 Monitoring business activities

Article 49 (Due diligence in monitoring business activities)

(1) The obliged person shall monitor business activities undertaken by the customer through the obliged person with due diligence and thus ensure knowledge of the customer, including the origin of assets used in business operations. Monitoring business activities undertaken by the customer through the obliged person shall include:

- verifying the customer's business operation for the purpose and intended nature of the business relationship established by the customer through the obliged person;
- monitoring and verifying the customer's business operation's compliance with his/her regular scope of business;
- verifying and updating obtained documents and data on the customer.

(2) For a customer that is a legal entity, verifying and updating the obtained documents and data referred to in the preceding paragraph shall include:

1. verifying the data on the company, address and registered office of the legal entity;
2. verifying the data on the personal name and permanent or temporary residence of the legal entity's statutory representative;
3. verifying the data on the beneficial owner of the legal entity;
4. verifying the validity of the authorisation referred to in paragraph 3 of Article 24 of this Act;
5. determining whether the legal entity's statutory representative or authorised person or beneficial owner has become a politically exposed person during the business relationship.

(3) When the transactions referred to in paragraph 1 of Article 17 of this Act are carried out on behalf of, and for the account of, a foreign legal entity by its branch, the obliged person shall obtain, in

addition to the data referred to in the preceding paragraph, the following data within the verification and update of obtained documents on the customer:

1. data on the address and registered office of the foreign legal entity's branch;
2. data on personal name and permanent residence of the foreign legal entity's statutory representative.

(4) The obliged person shall ensure the scope and frequency of measures referred to in paragraph 1 of this Article appropriate to the risk of money laundering or terrorist financing to which it is exposed in carrying out individual transactions or in business operations with an individual customer. The obliged person shall determine the risk on the basis of Article 13 of this Act and by taking into account Article 9 of this Act. Notwithstanding the above stated, the obliged person must ensure that the obtained documents and data on the customer are updated at least after five years from the last customer due diligence if the customer has effected at least one transaction with the obliged person in the last twelve months.

Article 50 (Treatment of unusual transactions)

(1) In relation to complex or unusually high transactions or transactions which have an unusual structure or have no clearly evident commercially or legally justified purpose or do not comply or conform with the usual or expected business operation of the customer, the obliged person shall:

- examine the background and purpose of these transactions, including the origin of the proceeds and assets, namely to such an extent as the circumstances allow; and
- record and keep its findings.

(2) If the obliged person determines that an unusual transaction presents an increased risk of money laundering or terrorist financing, it shall use one or several measures of enhanced customer due diligence as prescribed in the provisions of this Act governing the measures of enhanced customer due diligence.

(3) When dealing with unusual transactions, the obliged person shall exercise due diligence of customers, business relationships or transactions related to countries:

1. included on the list of high-risk third countries with strategic deficiencies where no suitable measures of preventing or detecting money laundering or terrorist financing apply; or
2. with a great possibility of money laundering or terrorist financing.

(4) In the cases referred to in point 1 of the preceding paragraph, the obliged person must apply the measures of enhanced customer due diligence referred to in Article 59.

(5) For the purposes of point 1 of paragraph 3 of this Article, the obliged person shall observe the delegated act adopted by the European Commission as per Article 10 of Directive 2015/849/EU and which defines high-risk third countries where no suitable measures to prevent or detect money laundering and terrorist financing apply. The Office shall also publish the information on these countries on its web site.

(6) The list of countries referred to in point 2 of paragraph 3 of this Article shall be prepared by the Office, whereby it shall also take into account data from competent international organisations. The Office shall publish the information on these countries on its web site.

3.3.3 Customer due diligence via third parties

Article 51 (Due diligence relying on third parties)

(1) Under the conditions stipulated by this Act, an obliged person entering into a business relationship may rely on a third party to apply the measures referred to in points 1, 2 and 3 of paragraph 1 of Article 16 of this Act.

(2) The obliged person shall verify in advance whether the third party entrusted to carry out customer due diligence meets all the conditions stipulated by this Act.

(3) Customer due diligence performed for the obliged person by a third party may not be accepted as appropriate if, within this procedure, the third party has determined and verified the identity of a customer in the customer's absence.

(4) An obliged person who relies on a third party in respect of customer due diligence shall remain responsible for the correct customer due diligence procedure under this Act.

Article 52 (Third parties)

(1) The third parties referred to in the preceding paragraph may be:

1. the obliged persons referred to in points 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 of Article 4 of this Act;
2. a branch of a brokerage company established in a Member State;
3. an investment company of a Member State and its branches established in a Member State;
4. branches of investment companies of third countries established in other Member States;
5. a branch of a management company established in a Member State;
6. a management company of a Member State and its branches established in Member States;
7. a branch of a manager of alternative investment funds established in other Member State;
8. a manager of alternative investment funds of a Member State and its branches established in Member States;
9. branches of managers of alternative investment funds of third countries established in Member States;

(2) A third party may also be a bank, management company, investment company or insurance company with its registered office in a third country, namely under the condition that:

- it is subject to the implementation of equal or equivalent provisions on the implementation of customer due diligence and records management as stipulated by this Act, and
- it is, in terms of implementing these requirements, also supervised as per provisions which are equal or equivalent to the provisions stipulated by this Act.

(3) In taking into account the information obtained from the Office, the obliged persons shall verify whether the conditions referred to in the preceding paragraph of this Article are fulfilled.

(4) Notwithstanding the first paragraph of this Article, a consular representation of the Republic of Slovenia in another Member State or a third country shall also be considered a third party.

(5) Notwithstanding paragraph 1 of this Article, a notary public with its registered office in the Republic of Slovenia or other Member State or a third country where it is bound to implement equal or equivalent provisions regarding customer due diligence and records management as defined in this Act, and in terms of implementing these requirements is also supervised as per provisions which are equal or equivalent to the provisions of this Act, shall also be deemed a third party.

(6) Notwithstanding other provisions of this Article, a shell bank or other similar credit institution which does not or may not pursue its activities in the country of registration can in no case act as a third party.

(7) The following entities shall not be deemed third parties referred to in paragraph 1 of the preceding Article:

- outsourcing service providers or obliged persons' agents;
- entities established in third countries included on the list of high-risk third countries referred to in point 1 of paragraph 3 of Article 50 of this Act.

(8) Notwithstanding the preceding paragraph, an obliged person may entrust the implementation of customer due diligence to third parties that are branches or majority-owned subsidiaries established in high-risk third countries or countries with a high probability of money laundering and terrorist financing on the condition that:

- a founder of a branch or majority-owned subsidiary has its registered office in a Member State;
- and
- branches or majority-owned subsidiaries fully implement policies and procedures of a group that are equal or equivalent to provisions of Articles 71, 72 and 75 of this Act.

Article 53 **(Exceptions relating to customers)**

Notwithstanding paragraph 1 of Article 51 of this Act, an obliged person shall not entrust the implementation of customer due diligence to a third party if the customer is a foreign legal entity which is not or may not be engaged in trade, manufacturing or other activity in the country of registration.

Article 54 **(Obtaining data and documentation from a third party)**

(1) A third party applying customer a due diligence procedure instead of the obliged person shall make immediately available to the obliged person the data obtained on the customer which is required by the obliged person in order to enter into a business relationship under this Act.

(2) The third party shall immediately submit to the obliged person, upon request, copies of documents and other documentation used in the customer due diligence procedure. Obtained copies of documents and documentation shall be kept by the obliged person in accordance with the provisions of this Act and the Act governing protection and retention of data.

(3) After the data, copies of documents and documentation referred to in paragraph 1 and 2 of this Article are submitted to the obliged person, the third party shall not retain the data, documents and documentation on the customer obtained within the scope of customer due diligence.

(4) If the obliged person considers there is good reason to doubt the veracity of the performed customer due diligence or identification documentation or reliability of obtained data on the customer, the obliged person shall carry out due diligence.

(5) The obliged person shall not enter into a business relationship if:

1. the customer due diligence procedure has been applied by a person not considered a third party pursuant to Article 52 of this Act;
2. the third party relied on by the obliged person to apply customer the due diligence procedure determined and verified the identity of a customer in the customer's absence;

3. the obliged person failed to obtain in advance the data referred to in paragraph 1 of this Article from the third party which applied customer the due diligence procedure;

4. there is good reason to doubt the veracity of the applied customer due diligence or reliability of data obtained on the customer, and that the obliged person has failed to carry out due diligence.

Article 55 (Third parties and group programme)

Within the scope of its group policy, the obliged person may entrust the application of measures of customer due diligence referred to in points 1, 2 and 3 of paragraph 1 of Article 16 of this Act to a third party which is a part of the group, namely under the condition that:

1. this group applies measures of customer due diligence and observes the obligations related to the retention of data and has introduced appropriate programmes to prevent money laundering and terrorist financing which are equal or equivalent to the provisions of this Act or other regulations, and

2. the implementation of the obligations referred to in the preceding paragraph at the level of a group is supervised by the supervisory bodies referred to in Article 139 of this Act or the competent authorities of a Member State or a third country.

3.3.4 Special types of customer due diligence

Article 56 (General)

Customer due diligence procedure shall be applied in accordance with paragraph 1 of Article 16 of this Act; in some cases stipulated by this Act, simplified measures shall be allowed or particularly rigorous measures shall be required to carry out the customer identification and due diligence. Special types of customer due diligence shall be:

1. simplified due diligence;
2. enhanced due diligence.

3.3.4.1 Simplified customer due diligence

Article 57 (General)

(1) In the cases referred to in points 1, 2 and 3 of paragraph 1 of Article 17 and Article 18 of this Act, the obliged person may apply simplified customer due diligence if, according to paragraph 1 of Article 14 of this Act, it assesses that the customer, business relationship, transaction, product, service, distribution channel, country of geographic area presents little risk of money laundering or terrorist financing

(2) In making a decision on whether to apply simplified customer due diligence, the obliged person may also take into account whether little risk of money laundering or terrorist financing is established according to point 2 of paragraph 2 of Article 9 and regulation of paragraph 4 of Article 9 of this Act.

(3) In determining customers, business relationships, transactions, products, services, distribution channels, countries or geographic areas which it assesses as presenting little risk of money

laundering or terrorist financing, the obliged person may take into account the factors of low risk determined by the minister responsible for finance in the rules.

(4) In determining measures of simplified customer due diligence, obliged persons shall consider the guidelines of supervisory bodies referred to in Article 139 of this Act on the criteria of risk and measures that may be adopted in these cases.

(5) In determining measures of simplified customer due diligence, the Bank of Slovenia, Securities Market Agency and Insurance Supervisory Agency shall also consider the guidelines issued by European supervisory authorities.

(6) An auditing firm or independent auditor that establishes a business relationship of mandatory auditing pursuant to the Act governing customer's operations may apply a simplified due diligence procedure, except when reasons for suspecting money laundering or terrorist financing exist in connection with the customer or auditing circumstances.

(7) An obliged person shall sufficiently monitor the business activities of the customer and transactions so as to detect unusual and suspicious transactions. Simplified customer due diligence shall not be allowed if reasons exist to suspect money laundering or terrorist financing in relation to a customer, transaction, property or assets.

Article 58 **(Application of customer due diligence)**

(1) In the simplified customer due diligence referred to in paragraph 1 of the preceding Article, determining and verifying the identity of a customer shall be performed as per provisions of Articles 23 to 31 of this Act, and the data shall be acquired in the quantity stipulated in this Act.

(2) Determining the beneficial owner of the customer shall be performed as per provisions of Articles 33 to 40 of this Act.

(3) Obtaining data on the purpose, foreseen nature of a business relationship or transaction and other data shall be performed in the scope stipulated in this Article.

(4) Regular due diligence of business activities undertaken by the customer through the obliged person shall be performed as per the provisions of Article 49 of this Act.

(5) Within the scope of simplified due diligence of a customer who is a legal entity, sole proprietor or individual performing an activity independently, the obliged person shall obtain the following data:

1. in establishing a business relationship and monitoring and updating the data within the scope of due diligence of business activities:

- company, address and registered office of a legal entity, sole proprietor or individual performing an activity independently who establishes a business relationship or on whose behalf a business relationship is established;
- personal name of the statutory representative or authorised person who on behalf of the legal entity, sole proprietor or individual performing an activity independently establishes the business relationship; and
- purpose and foreseen nature of a business relationship, unless it is possible to determine the purpose and nature from the established business relationship, and the date of establishing the business relationship;

2. when conducting transactions under point 2 of paragraph 1 of Article 17 and Article 18 of this Act:

- company, address and registered office of the legal entity, sole proprietor or individual performing an activity independently for whom the transaction is conducted;
- personal name of the statutory representative or authorised person conducting the transaction for the legal entity sole proprietor or individual performing an activity independently;
- the date and time of the transaction;
- amount of the transaction and currency in which the transaction is being carried out;
- manner of executing the transaction and the country in which the transaction is being carried out; and
- purpose of the transaction, unless it is possible to determine the purpose from the type of transaction, and personal name and address of permanent and temporary residence, if any, or the company and the registered office of the person to whom the transaction is directed.

(6) The obliged person shall obtain the data referred to in the preceding paragraph of this Article by inspecting the original or certified documentation from the business, court or other public register submitted by the customer or by direct inspection of the court or other public register.

(7) When all the required data cannot be obtained in the manner stipulated in paragraph 6 of this Article, the obliged person shall obtain the requisite data from the original or certified documents and business records submitted by the customer. When, for objective reasons, the obliged person cannot obtain the requisite data even in the manner described, it shall obtain it directly from the written statement of the statutory representative or authorised person.

(8) The documentation referred to in paragraphs 6 and 7 of this Article submitted to the obliged person shall not be older than three months.

(9) Within the scope of simplified due diligence of a customer who is a natural person or its statutory representative or authorised person, the obliged person shall obtain the following data:

1. when establishing a business relationship:
 - personal name, address of permanent residence, date and place of birth and tax ID number or personal ID number of a person establishing a business relationship or for whom the business relationship is being established;
 - personal name, address of permanent residence, date and place of birth and tax ID number or personal ID number of a statutory representative or authorised person establishing a business relationship, and
 - purpose and foreseen nature of a business relationship, except if it is possible to determine the purpose and nature from the established business relationship, and the date of establishing the business relationship;
2. when conducting transactions under points 2 and 3 of paragraph 1 of Article 17 of this Act and Article 18 of this Act:
 - personal name, address of permanent or temporary residence, date and place of birth and tax ID number or personal ID number of a person performing a transaction;
 - personal name, address of permanent and temporary residence, date and place of birth and tax ID number or personal ID number of a statutory representative or authorised person establishing a business relationship for a natural person, and
 - the date and time of the transaction;
 - manner of executing the transaction;
 - the amount of the transaction, currency of transaction and manner of effecting the transaction; and
 - purpose of the transaction, unless it is possible to determine the purpose from the type of transaction, and personal name and address of permanent and temporary residence, or the company and the registered office of the person to whom the transaction is directed and the country in which the transaction is being carried out.

3.3.4.2 Enhanced customer due diligence

Article 59 (General)

(1) Enhanced customer due diligence shall, in addition to the measures referred to in paragraph 1 of Article 16 of this Act, include additional measures stipulated by this Act in the following cases:

1. entering into a correspondent banking relationship with a respondent bank or similar credit institution located in a third country;
2. entering into a business relationship or carrying out a transaction referred to in points 2 and 3 of paragraph 1 of Article 17 and Article 18 of this Act with a customer who is a politically exposed person as referred to in Article 61 of this Act;
3. when beneficiaries of life insurance or unit-linked life insurance and beneficial owners of the beneficiary are politically exposed persons as referred to in Article 62 of this Act;
4. when a customer or transaction is linked with a high-risk third country.

(2) The obliged person must apply enhanced customer due diligence procedure in all cases referred to in paragraph 1 of this Article and:

1. when as per paragraph 2 of Article 14 of this Act, it assesses that a customer, business relationship, transaction, product, service, country or geographic area present an increased risk of money laundering or terrorist financing;
2. when an increased risk of money laundering or terrorist financing is established as per point 3 of paragraph 2 of Article 9 and the regulation referred to in paragraph 4 of Article 9.

(3) In determining customers, business relationships, transactions, products, services, distribution channels, countries or geographic areas regarding which it assesses that they present an enhanced risk of money laundering or terrorist financing, the obliged person shall take into account factors of increased risk determined by the minister responsible for finance in the rules.

(4) In determining measures of enhanced customer due diligence, obliged persons shall consider the guidelines of supervisory bodies referred to in Article 139 of this Act on the risk factors and measures that may be adopted in these cases.

(5) In determining measures of enhanced customer due diligence, the Bank of Slovenia, Securities Market Agency and Insurance Supervisory Agency shall also consider the guidelines issued by European supervisory authorities.

Article 60 (Corresponding banking relationships with credit institutions of third countries)

(1) When entering into a corresponding banking relationship with a bank or similar credit institution located in a third country, the obliged person shall apply the measures referred to in paragraph 1 of Article 16 of this Act within enhanced the customer due diligence procedure and shall also obtain the following data, information and documentation:

1. date of issue of the authorisation to perform banking services, and name and registered office of the competent authority from the third country that issued the authorisation;
2. description of the performance of internal procedures relating to the detection and prevention of money laundering and terrorist financing, in particular to customer due diligence procedures, procedures for determining beneficial owners, for reporting data on suspicious transactions and customers to the competent authorities, for keeping records, internal control and other procedures adopted by the bank or other similar credit institution with respect to detecting and preventing money laundering and terrorist financing;

3. description of systemic arrangements in the field of detection and prevention of money laundering and terrorist financing applicable in the third country where the bank or other similar credit institution is established or registered;

4. a written statement that the bank or other similar credit institution does not operate as a shell bank;

5. a written statement that the bank or other similar credit institution has no established business relationships with shell banks and that it does not establish or conduct transactions with shell banks;

6. a written statement that the bank or similar credit institution is subject to administrative supervision in the country of its head office or registration and is, in accordance with the legislation of the country concerned, under the obligation to comply with laws and other respective regulations governing the detection and prevention of money laundering and terrorist financing.

(2) An employee of the obliged person establishing the correspondent relationship referred to in paragraph 1 of this Article and conducting the enhanced customer due diligence procedure shall obtain the written approval of his/her superior responsible person occupying a senior management position prior to entering into such relationship.

(3) The obliged person shall obtain the data referred to in paragraph 1 of this Article by inspecting public or other accessible data records, or by inspecting documents and business records submitted by the bank or other similar credit institution located in the third country.

(4) The obliged person shall document the implementation of measures referred to in the preceding paragraphs.

(5) The obliged person shall not enter into or continue a correspondent banking relationship with a respondent bank or other similar credit institution located in a third country if:

1. no data referred to in points 1, 2, 4, 5 and 6 of paragraph 1 of this Article have been obtained in advance;

2. the employee of the obliged person failed to obtain prior written approval of his/her superior responsible person for entering into the correspondent relationship;

3. the bank or other similar credit institution located in the third country does not have in place a system for detecting and preventing money laundering and terrorist financing, or is not, in accordance with the legislation of the third country where it is established or registered, under the obligation to comply with laws and other relevant regulations concerning the detection and prevention of money laundering and terrorist financing;

4. the bank or other similar credit institution located in the third country operates as a shell bank or enters into correspondent or other business relationships and effects transactions with shell banks.

Article 61 (Politically exposed persons)

(1) The obliged person shall establish a suitable system of risk management which also includes a procedure to determine whether a customer or its statutory representative or authorised person is a politically exposed person. This procedure based on the risk assessment referred to in Article 13 shall be defined in its internal act while taking account the guidelines of the competent supervisory body referred to in Article 139 of this Act. Political exposure is established also for beneficial owners of the customer.

(2) A politically exposed person referred to in the preceding paragraph shall be any person who is or has been entrusted with a prominent public function in a Member State or a third country in the previous year, including immediate family members and close associates.

(3) Natural persons who are, or have been, entrusted with prominent public function shall be the following:

a) heads of state, prime ministers, ministers and their deputies or assistants;

- b) elected representatives in legislative bodies;
- c) members of management bodies of political parties;
- d) members of supreme and constitutional courts and other high-level judicial authorities against whose decisions there is no ordinary or extraordinary legal remedy except in exceptional cases;
- e) members of courts of audit and boards of governors of central banks;
- f) heads of diplomatic missions and consulates and representations of international organisations, their deputies and high-ranking officers of armed forces;
- g) members of the management or supervisory bodies of undertakings in majority state ownership;
- h) representatives of bodies of international organisations (such as presidents, secretaries-general, directors, judges), their deputies and members of management bodies or holders of equivalent functions in international organisations.

(4) Immediate family members of the person referred to in paragraph 2 of this Article shall be the following: spouse, cohabitee, parents and children and their spouses or cohabitees.

(5) Close associates of the person referred to in paragraph 2 of this Article are all natural persons who are known to be joint beneficial owners or have any other close business relationships with a politically exposed person. A close associate is also a natural person who is the only beneficial owner of the business entity or similar foreign law entity which is known to have been established to the actual benefit of a politically exposed person.

(6) When a customer entering into a business relationship or effecting a transaction, or when a customer on whose behalf a business relationship is entered into or a transaction effected, or the customer's statutory representative, authorised person or beneficial owner is a politically exposed person, the obliged person shall take, in addition to the measures referred to in paragraph 1 of Article 16 of this Act within the enhanced customer due diligence procedure, the following measures:

1. obtain data on the customer's financial position and data on the source of funds and property that are, or will be, a subject of a business relationship or transaction, namely from the documents and other documentation submitted by the customer; if this data cannot be obtained in the manner described above, the obliged person shall obtain them directly from the written statement of the customer;

2. An employee of the obliged person who conducts the procedure for entering into a business relationship with a customer who is a politically exposed person shall obtain the written approval of his/her superior responsible person occupying a senior management position prior to entering into such relationship.

3. After a business relationship has been entered into, the obliged person shall monitor with due diligence the transactions and other business activities effected through the obliged person by a politically exposed person.

(7) When a politically exposed person as referred to in this Article ceases to be entrusted with a prominent public function, the obliged person shall continue to take appropriate measures for the period of 12 months. After this period, the obliged person shall re-assess the possible continued risk presented by this person and take appropriate measures by taking into account the risk until it considers that the respective person no longer presents a risk.

Article 62 **(Politically exposed persons and life insurance)**

(1) The obliged person shall establish suitable measures to determine whether beneficiaries of life insurance or unit-linked life insurance and beneficial owners of beneficiaries are politically exposed persons. The measures stated above shall be adopted at the time of payment of insurance policy, or full or partial transfer of the insurance policy at the latest. If an increased risk is found, the obliged person, in addition to the measures referred to in paragraph 1 of Article 16 of this Act, shall also take two additional measures, namely:

1. before the payment of the policy, the obliged person shall inform the responsible person occupying a senior management position about it;

2. it shall perform due diligence of the business relationship established with the holder of policy, and if there are reasons to suspect money laundering or terrorist financing, it shall notify the Office as per Article 69 of this Act regarding suspicious transactions.

(2) The measures referred to in the preceding paragraph shall be taken also with respect to immediate family members and close associates as referred to in paragraphs 4 and 5 of the preceding Article of this Act.

(3) When a politically exposed person as referred to in this Article ceases to be entrusted with a prominent public function, the obliged person shall continue to take appropriate measures for the period of 12 months. After this period, the obliged person shall re-assess the possible continued risk presented by this person and take appropriate measures by taking into account the risk until it considers that the respective person no longer presents a risk.

Article 63 (Due diligence of customers from high-risk third countries)

(1) if a customer or transaction is related to a high-risk third country referred to in paragraph 5 of Article 50 of this Act, the obliged person within the scope of enhanced customer due diligence and in addition to the measures referred to in paragraph 1 of Article 16 of this Act shall take at least the following measures:

1. obtain additional data on the activity of the customer and update the data on the identification of the customer and its beneficial owner more frequently;

2. obtain additional data on the purpose and foreseen nature of a business relationship and data on the reasons for the intended or effected transaction;

3. obtain data about the source of assets and property that is, or will be, the subject of the business relationship or transaction;

4. an employee of the obliged person who conducts the procedure for entering into a business relationship with a customer from a high-risk third country shall obtain the written approval of his/her superior responsible person occupying a senior management position prior to entering into such relationship.

5. after a business relationship has been entered into, the obliged person shall monitor the transactions and other business activities effected through the obliged person by a person from a high-risk third country with due diligence.

(2) The obliged person does not have to take the additional measures referred to in the preceding paragraph if the customer is a branch or majority-owned subsidiary with its registered office in the European Union established in a high-risk third country if the respective branch or subsidiary fully implements the policies and procedures of a group that are equal or equivalent to the provision of this Act. In these cases, the obliged person shall adjust the scope of measures to the risk assessment of money laundering and terrorist financing referred to in Article 13 of this Act.

3.3.5 Limitations on transactions with customers

Article 64 (Prohibition on using anonymous products)

The obliged person shall not open, issue or keep anonymous accounts, passbooks or bearer passbooks, or other products enabling, directly or indirectly, the concealment of the customer's identity.

Article 65
(Prohibition of establishing a business relationship)

The obliged person shall not establish a business relationship or effect transactions as referred to in Article 17 and 18 of this Act if the customer demonstrates ownership of a legal entity or similar foreign law entity on the basis of bearer shares, the traceability of which is not provided via the Central Clearing House and Depository or similar register or trading accounts and which cannot be determined on the basis of other business documentation.

Article 66
(Prohibition on conducting business with shell banks)

The obliged person shall not enter into or continue a correspondent banking relationship with a respondent bank that operates or may operate as a shell bank, or other similar credit or financial institution known to allow shell banks to use its accounts.

Article 67
(Limitations on cash operations)

(1) Persons pursuing the activity of selling goods or carry out services in the Republic of Slovenia shall not accept cash payments exceeding EUR 5,000 from their customers or third persons when selling individual goods or carrying out individual service.

(2) The limitation on accepting cash payments referred to in the preceding paragraph shall also apply when the payment is effected by several linked cash transactions exceeding a total amount of EUR 5,000.

(3) Persons pursuing the activity of selling goods or carrying out services shall receive payments referred to in paragraphs 1 and 2 of this Article from customers or third parties on their transaction accounts, unless otherwise provided by other act.

(4) The provisions referred to in the preceding paragraphs shall not apply to organisers and concessionaires organising games of chance.

3.4 Reporting information to the Office

Article 68
(The reporting obligation concerning cash transactions and remittances to risky countries and deadlines)

(1) The obliged person shall furnish the Office with the data referred to in points 1, 2, 6, 7, 8, 9 of paragraph 1 of Article 137 of this Act on any cash transaction exceeding EUR 15,000 immediately after the transaction is completed and not later than within three working days following its completion.

(2) The obliged person referred to in points 1, 2, 3, 4 and 18 of paragraph 1 of Article 4 of this Act shall furnish the Office with the data referred to in points 1, 2, 6, 7, 8 and 9 of paragraph 1 of Article 137 of this Act on any transaction exceeding EUR 15,000, and which at the request of a customer is deposited in the bank accounts of:

- the legal entities and natural persons of the countries referred to in points 1 and 2 of paragraph 3 of Article 50 of this Act;

- legal entities and natural persons with their registered office and permanent or temporary residence in the countries referred to in points 1 and 2 of paragraph 3 of Article 50 of this Act, immediately after the transaction is completed and not later than within three working days following its completion.

(3) The report referred to in paragraph 1 and 2 of this Article must be submitted to the Office via a protected electronic channel. If reporting via a protected electronic channel is hindered or prevented for technical reasons, this report may be exceptionally submitted to the Office in written form only.

(4) The reporting obligation concerning cash transactions referred to in paragraph 1 and transactions referred to in paragraph 2 of this Article shall not apply to auditing firms, independent auditors, legal entities or natural persons performing accounting or tax advisory services.

(5) The Office shall publish the data received as referred to in paragraph 2 of this Article on its web sites immediately, or no later than on the next working day. The data published comprises the data referred to in points 1, 7 and 8 of paragraph 1 of Article 137 of this Act, except for the information about the personal name and address of permanent and temporary residence referred to in point 8 of paragraph 1 of Article 137 of this Act.

(6) The minister responsible for finance shall issue rules setting the conditions under which the obliged person shall not be required to forward to the Office the data on certain customer transactions referred to in paragraph 1 of this Article.

Article 69 **(Reporting obligation concerning suspicious transactions and deadlines)**

(1) The obliged person shall furnish the Office with the data referred to in paragraph 1 of Article 137 of this Act and related documentation if reasons to suspect money laundering or terrorist financing exist in connection with the transaction, person, property or assets, prior to effecting the transaction, and shall state the time limit in which the transaction is to be carried out. The aforementioned report on suspicious transaction must be submitted to the Office via a protected electronic channel. Exceptionally, it may be submitted by telephone. In this case, it must be also submitted to the Office via a protected electronic channel by no later than the next working day.

(2) If the reporting of transactions referred to in the preceding paragraph via a protected electronic channel is significantly hindered or prevented due to technical reasons, this report may be exceptionally submitted to the Office in written form only.

(3) The reporting obligation concerning the transactions referred to in paragraph 1 of this Article shall also apply to an intended transaction, irrespective of whether it is effected at a later date or not.

(4) A suspicious transaction as referred to in paragraphs 1, 2 and 3 of this Article is any intended or effected transaction in respect of which the obliged person knows or has reasons to suspect that the property or assets originated from criminal offences that could constitute a prior act of money laundering or relate to terrorist financing or in terms of their characteristics correspond with indicators for detecting suspicious transactions as referred to in Article 85 of this Act that indicate grounds to suspect money laundering or terrorist financing.

(5) Auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services shall report all cases when a customer seeks advice on money laundering or terrorist financing purposes to the Office immediately or not later than within three business days from when such advice was sought.

(6) If, in the cases referred to in paragraphs 1, 2 and 3 of this Article, and due to the nature of the transaction or because the transaction has not been completed, or for other justified reasons, the

obliged person cannot conduct the described procedure, it shall furnish the data to the Office as soon as is practicable or immediately after the suspicion of money laundering or terrorist financing is raised. The obliged person shall explain in the report the reasons for not acting in accordance with the described procedure.

Article 70
(method of communication)

The obliged person shall forward to the Office the data referred to in paragraph 1 and 2 of Article 68 and the data referred to in paragraphs 1, 2 and 3 of Article 69 in the manner prescribed in the rules issued by the minister responsible for finance.

3.5 The implementation of group policy and measures for detecting and preventing money laundering and terrorist financing in branches and majority-owned subsidiaries located in Member States and third countries

Article 71
(Obligation to implement group policy)

(1) Obligated persons who are a part of a group shall implement the policies and procedures of this group that relate to the measures for detecting and preventing money laundering and terrorist financing stipulated by this Act, including the policies and procedures of data protection and information exchange within the group for the purposes of preventing money laundering and terrorist financing.

(2) The policies and procedures of the group referred to in the previous paragraph shall be implemented in branches and subsidiaries in which the obliged person has a controlling interest with their registered office in Member States and third countries.

(3) The exchange of information within a group shall be allowed, including the exchange of information about suspicious transactions referred to in Article 69 of this Act, unless the Office explicitly objects to the exchange of information about suspicious transactions.

(4) Before transferring personal data outside a third country, the obliged person shall obtain a written certificate of the receipt of data with its registered office in third countries stating that it provides the same level of personal data protection in its operations as the obliged person and that the third country provides a sufficient level of personal data protection.

Article 72
(Obligation to apply measures in Member States)

(1) An obliged person who directly performs business activity in other Member State or performs it via a branch or agents shall provide that branches and agents comply with the legislation of the respective Member State governing the field of detecting and preventing money laundering and terrorist financing.

(2) The supervision of the implementation of the preceding Article shall be carried out by the supervisory bodies of the Member State where the obliged person performs business activity via a branch, agents or directly, in cooperation with competent supervisory bodies referred to in Article 139 of this Act.

Article 73
(Central contact points)

(1) The Bank of Slovenia may request that issuers of electronic money or providers of payment services as defined in the Act governing payment services and payments appoint a central contact point in the territory of the Republic of Slovenia if the issuers of electronic money or providers of payment services:

1. are not branches or subsidiaries established in the territory of the Republic of Slovenia;
2. have their registered office in the territory of another Member State; and
3. they conduct business operations in the territory of the Republic of Slovenia through a network of several agents.

(2) The agents referred to in point 3 of the preceding paragraph shall be natural persons or legal entities who in conducting business operations related to issuing electronic money or payment services on the basis of the power of representation act on behalf of issuers of electronic money or providers of payment services.

(3) Notwithstanding paragraph 1 of this Article, issuers of electronic money or providers of payment services with their registered office in the territory of other Members State may upon their own initiative appoint a central contact point in the territory of the Republic of Slovenia. They shall notify the Bank of Slovenia of their intention to appoint a central contact point of issuers of electronic money or providers of payment services.

(4) Central contact points may be natural persons or legal entities with their permanent residence or registered office in the territory of the Republic of Slovenia.

(5) The Bank of Slovenia shall obtain the data referred to in paragraph 3 of Article 137 of this Act about the natural persons and legal entities that are central contact points.

(6) On behalf of the issuers of electronic money and providers of payment services, central contact points appointed in the territory of the Republic of Slovenia shall:

1. provide that networks of agents implement the measures to prevent and detect money laundering and terrorist financing stipulated by this Act;
2. submit data, information and documentation to the Bank of Slovenia or the Office at their request if the Bank of Slovenia or Office implements supervision as per the provisions of this Act.
3. provide assistance in cooperating and harmonising supervision of the network of agents between the Bank of Slovenia, the Office and competent supervisory bodies of Member States where the registered office of the issuers of electronic money or provider of payment services is located.

(7) In determining the conditions that have to be fulfilled to appoint a contact point, the Bank of Slovenia shall apply the technical standards issued by the European Commission in cooperation with European supervisory bodies.

Article 74
(Supervision of agents)

(1) If the Bank of Slovenia finds major deficiencies in implementing measures to prevent money laundering or terrorist financing in the operation of agents, it may adopt suitable and proportionate measures to eliminate deficiencies within its competencies. Such measures shall be temporary and shall be terminated when deficiencies are eliminated.

(2) In taking measures and eliminating deficiencies as referred to in the preceding paragraph, the Bank of Slovenia shall cooperate with the competent supervisory bodies of the Member State where a company issuing electronic money or provider of payment services has its registered office.

Article 75
(Obligation to apply measures in third countries)

(1) The obliged person shall ensure that the measures for detecting and preventing money laundering and terrorist financing as stipulated in this Act are also implemented at equal or higher level in its branches and its majority-owned subsidiaries established in third countries, namely within the scope stipulated by the law of the respective third countries.

(2) If the minimum standards of implementing the measures for detecting and preventing money laundering or terrorist financing in third countries referred to in the preceding paragraph are less strict than the measures prescribed in this Act, the obliged person shall ensure that its branches or its majority-owned subsidiaries adopt and implement suitable measures equivalent to the measures prescribed in this Act within the laws of the respective third country. Suitable measures also include measures for data protection.

(3) If the law of a third country does not allow the policies and procedures referred to in Article 71 of this Act and paragraphs 1 and 2 of this Article to be implemented, the Bank of Slovenia, Securities Market Agency and Insurance Supervision Agency shall notify European supervisory bodies and competent supervisory bodies of other Member States of this, namely for the purpose of harmonising activities in finding a suitable solution.

(4) If the law of a third country does not allow the implementation of policies and procedures referred to in Article 71 of this Act and paragraphs 1 and 2 of this Article, the obliged person shall provide that branches and majority-owned subsidiaries in the third country adopt and implement suitable additional measures through which they manage risks of money laundering and terrorist financing and notify the competent supervisory authorities referred to in Article 139 of this Act of this.

(5) If the additional measures referred to in the preceding paragraph do not suffice, the supervisory bodies referred to in Article 139 of this Act may order the obliged person to implement additional supervisory measures in the third country which may also include:

1. prohibition of establishing business relationships;
2. termination of a business relationship;
3. prohibition of conducting transactions; or
4. termination of operations in the respective third country.

(6) The obliged persons supervised by the Bank of Slovenia, Securities Market Agency and Insurance Supervision Agency shall take into account the minimum technical standards issued by the European Commission in cooperation with European supervisory bodies when adopting and implementing suitable equivalent measures as referred to in paragraph 2 of this Article and additional measures as referred to in paragraph 4 of this Article.

3.6 Authorised person, training and internal control

3.6.1 Authorised person

Article 76
(Appointment of authorised person and his/her deputy)

(1) Obligated persons shall appoint an authorised person and one or more deputies for the specific tasks of detecting and preventing money laundering and terrorist financing stipulated by this Act and the ensuing regulations.

(2) Notwithstanding the provisions of paragraph 1 of this Article, obliged persons, with fewer than four employees shall not be required to appoint an authorised person or conduct internal control pursuant to this Act.

Article 77
(Conditions for the authorised person)

(1) The obliged person shall ensure that the work of the authorised person referred to in the preceding Article is entrusted solely to a person meeting the following requirements:

1. holds a position as per the classification of posts by the obliged person that is high enough in rank to enable the rapid, quality and timely execution of tasks stipulated by this Act and ensuing regulations;

2. has not been convicted by a final judgement, and is not subject to criminal proceedings either for an intentionally committed criminal offence that is prosecuted ex officio or for one of the following criminal offences committed by negligence: negligent homicide, serious bodily harm, aggravated bodily harm, threatening work safety, concealment, disclosure and undue obtaining of professional secrets, money laundering, disclosure of classified information or causing general danger, and the penalty has not yet been expunged from the criminal record;

3. holds appropriate professional qualifications for the tasks of preventing and detecting money laundering and terrorist financing and has the characteristics and experience necessary to discharge the function of an authorised person;

4. is well acquainted with the nature of the obliged person's operations in the fields exposed to risks of money laundering or terrorist financing.

(2) The authorised person's deputy shall meet the requirements referred to in points 2, 3 and 4 of paragraph 1 of this Article.

Article 78
(Duties of authorised person and deputy)

(1) The authorised person referred to in Article 76 of this Act shall perform the following tasks:

1. provide for the setting up, functioning and development of a system for detecting and preventing money laundering and terrorist financing through the obliged person;

2. provide for correct and timely reporting to the Office in accordance with this Act and ensuing regulations;

3. participate in the drawing up and modification of the operative procedures and in the preparation of internal regulations concerning the prevention and detection of money laundering and terrorist financing;

4. participate in the elaboration of guidelines on the conduct of control related to the prevention and detection of money laundering and terrorist financing;

5. monitor and coordinate the activities of the obliged person in the field of detecting and preventing money laundering and terrorist financing;

6. participate in the setting up and development of information support for activities related to the detection and prevention of money laundering and terrorist financing through the obliged person;

7. suggest initiatives and make proposals to the management or other administrative body of the obliged person to improve the system for detecting and preventing money laundering and terrorist financing;

8. participate in preparing professional education and training programmes for employees in the field of prevention and detection of money laundering and terrorist financing.

(2) The deputy shall deputise for the authorised person in his/her absence with regard to the full scope of the tasks referred to paragraph 1 of this Article and carry out other tasks pursuant to this Act if so stipulated by the internal regulations of the obliged person.

Article 79
(Obligations of an obliged person)

To enable the authorised person to carry out tasks to detect and prevent money laundering and terrorist financing pursuant to this Act, the obliged person shall:

1. provide unlimited access to all data, information and documentation required to carry out those tasks;
2. give appropriate authorisations for the efficient performance of tasks referred to in paragraph 1 of the preceding Article;
3. provide appropriate staff, material and other working conditions;
4. ensure appropriate premises and technical capacities guaranteeing an adequate level of protection of classified information available to the authorised person pursuant to this Act;
5. provide appropriate information and technical support enabling the permanent and safe monitoring of activities in this field;
6. provide for regular professional training related to the detection and prevention of money laundering and terrorist financing; and
7. provide a replacement during the authorised person's absence.

(2) Internal organisational units, as well as the management or other administrative body of the obliged person, shall provide assistance and support to the authorised person in carrying out tasks pursuant to this Act and ensuing regulations, and supply updated information about any facts which are, or might be, linked to money laundering or terrorist financing. The obliged person shall lay down the method of cooperation between its internal organisational units and the authorised person in its internal regulation.

(3) The obliged person shall provide for the person acting as the authorised person pursuant to this Act to carry out his/her functions and duties as a sole full-time job, provided that due to the large number of employees, nature or scope of business or other justifiable reasons the workload concerning the detection and prevention of money laundering and terrorist financing is permanently increased.

(4) The authorised person referred to in the preceding paragraph shall carry out his/her tasks as an independent organisational unit directly responsible to the management or other administrative body and shall be functionally and organisationally separated from other organisational units of the obliged person.

(5) The obliged person shall forward to the Office the personal name and title of the position held by the authorised person and his/her deputy and any changes thereof immediately and in no case later than within fifteen days following the appointment or change of data.

3.6.2 Professional training

Article 80
(Obligation of regular training and education)

(1) The obliged person shall adopt measures to provide that the employees performing tasks of preventing and detecting money laundering and terrorist financing as per this Act are familiarised with provisions of this Act, including suitable measures relating to data protection. The adopted measures must be proportional with regard to the type and size of the obliged person and risk of money laundering and terrorist financing.

(2) The obliged person shall provide regular professional training for all employees carrying out tasks for the prevention and detection of money laundering and terrorist financing pursuant to this Act.

(3) The professional training and education referred to in the preceding paragraph shall relate to information about the provisions of the Act and ensuing regulations and internal regulations, about professional literature relating to the prevention and detection of money laundering and terrorist financing, and about lists of indicators for recognising customers and transactions in respect of which reasons to suspect money laundering or terrorist financing exist.

(4) The obliged person shall draw up an annual professional training programme for the prevention and detection of money laundering and terrorist financing not later than by the end of March for the current year.

3.6.3 Internal control and implementing regulations to carry out some duties

Article 81 (Regular internal control obligation)

The obliged persons shall ensure regular internal control of the performance of tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act.

Article 82 (Detailed regulations concerning the authorised person, method of executing internal control, retention and protection of data, keeping of records and professional training of employees)

The minister responsible for finance shall issue detailed rules concerning the authorised person, the method of executing internal control, retention and protection of data, the administration of records and professional training of employees within the obliged persons pursuant to this Act.

CHAPTER IV TASKS AND OBLIGATIONS OF LAWYERS, LAW FIRMS AND NOTARIES

Article 83 (Specific provisions concerning lawyers, law firms and notaries)

(1) A lawyer, law firm or notary shall implement measures for detecting and preventing money laundering and terrorist financing as per provisions of this Act only when:

1. assisting in planning or executing transactions for a client concerning:
 - a) buying or selling real property or a company;
 - b) managing client money, securities or other assets;
 - c) opening or managing bank, savings or securities accounts;
 - d) raising funds required to establish, operate or manage a company;
 - e) establishing, operating or managing foundations, trusts, companies or similar legal organisational forms; or
2. conducting a financial or real estate transaction on behalf of, and for the account of, the client.

(2) A lawyer, law firm or notary shall report all cases when a client seeks advice on money laundering or terrorist financing purposes to the office immediately or no more than three business days from when such advice was sought.

Article 84
(Exceptions)

(1) Article 21 shall not apply to a lawyer, law firm or notary when establishing a client's legal position or when acting as a client's legal representative in a judicial proceeding, including advice on instituting or avoiding such proceeding.

(2) The obligation to report referred to in Article 69 of this Act shall not apply to a lawyer, law firm or notary with regard to the data obtained from or about the client in the course of establishing the client's legal position or when acting as the client's legal representative in judicial proceedings, including advice on instituting or avoiding such proceedings, irrespective of whether such data is obtained before, during or after such proceedings.

(3) Subject to the conditions referred to in paragraph 2 of this Article, a lawyer, law firm or notary shall not be obliged to forward the data, information and documentation on the basis of a request from the Office referred to in paragraphs 1 and 2 of Article 92 of this Act. In such cases, they shall immediately, or not later than within 15 days of receiving the request, inform the Office in writing about the reasons for non-compliance with the Office's request.

CHAPTER V
LIST OF INDICATORS FOR THE IDENTIFICATION OF CUSTOMERS AND TRANSACTIONS IN
RESPECT OF WHICH REASONABLE GROUNDS TO SUSPECT MONEY LAUNDERING OR
TERRORIST FINANCING
EXIST

Article 85
(Obligation to compile and use the list of indicators)

(1) Obligated persons shall draw up a list of indicators for identifying customers and transactions in respect of which there are reasonable grounds to suspect money laundering or terrorist financing.

(2) In compiling the list of indicators referred to in paragraph 1 of this Article, obliged persons shall take into account in particular the complexity and scope of implementing the transactions, unusual patterns, value or relation of transactions which have no apparent economic or evident lawful purpose and/or are not in compliance or are disproportionate to the usual or expected business of a customer, as well as other circumstances related to the status and other characteristics of the customer.

(3) Obligated persons shall be obliged to use the list of indicators referred to in paragraph 1 of this Article when determining the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto.

(4) The minister responsible for finance may prescribe the obligatory inclusion of individual indicators on the list of indicators to identify customers and transactions in respect of which reasonable grounds to suspect money laundering or terrorist financing exist.

Article 86
(Participation in preparing the list of indicators)

The Office, Bank of Slovenia, Securities Market Agency, Insurance Supervision Agency, Financial Administration of the Republic of Slovenia, Agency for Public Oversight of Auditing, Slovenian Audit Institute, Chamber of Notaries of Slovenia, Bar Association of Slovenia, and associations and

societies whose members are bound by this Act shall also participate in drawing up a list of indicators as referred to in paragraph 1 of the preceding Article.

CHAPTER VI – DUTIES AND COMPETENCES OF THE OFFICE

6.1 General provisions

Article 87 (General)

(1) The Office shall perform duties relating to the prevention and detection of money laundering, previous criminal offences and terrorist financing, and other duties as stipulated by this Act.

(2) The Office shall be the central national body competent to adopt and analyse reports on suspicious transactions and other data, information and documentation on potential money laundering, related previous criminal offences or terrorist financing that are obtained as per the provisions of this and other Acts or directly applicable regulations of the European Union and for submitting the results of its analyses to the competent authorities.

(3) In conducting its duties referred to in the preceding paragraph, the Office shall be fully autonomous, independent and functionally independent, including in making decisions on adopting and analysing data, information and documentation and on submitting the results of its analyses to the competent authorities.

(4) To implement its duties, the Office shall have timely, direct or indirect access to data, information and documentation which are at the disposal of obliged persons, state authorities and holders of public authorisations, including information relating to the detection and prosecution of criminal offences.

(5) As per this Act, all data, information and documentation shall be forwarded to the Office free of charge.

Article 88 (Training)

(1) The Office's own activities shall include carrying out training for obliged persons with regard to the provisions of this Act, referring to the prevention and discovery of money laundering, predicate offences and terrorist financing.

(2) The Office shall issue a detailed internal general legal document concerning how it conducts its activity, the pricing method, disclosing revenues and expenses, and other elements of its activity.

6.2 Detection of money laundering and terrorist financing

Article 89 (Receiving and analysing data and information)

The Office shall be competent to receive and analyse the following data and information types: 1. notifications concerning suspicious transactions received from obliged persons, based on paragraphs one, two, and four of Article 69 of this Act;

2. notifications concerning cash transactions and bank transfers received from obliged persons, based on paragraphs one and two of Article 68 of this Act;
3. initiatives received on the basis of paragraphs one and two of Article 99 of this Act;
4. initiatives received on the basis of Article 100 of this Act;
5. data received from the Financial Administration of the Republic of Slovenia based on Article 120 of this Act;
6. facts received on the basis of Article 140 of this Act;
7. requests, notifications, data, information and documentation acquired on the basis of the provisions of this Act concerning international cooperation;
8. data, information, and documentation collected on the basis of Articles 91, 92, 93, and 94 of this Act;
9. data and information acquired in any other way regarding which the Office deems that they contain grounds for suspected money laundering or terrorist financing.

Article 90 (Analytical function of the Office)

Within its analytical function, the Office uses data, information, and documentation received and collected based on the preceding Article and Article 115 of this Act to perform:

1. operative analyses focusing on analysing:
 - individual or selected notifications concerning suspicious transactions, persons, property, or assets referred to in point 1 of paragraph one of the preceding Article, and
 - other messages, notifications, data, and information from the preceding paragraph, for the purpose of determining whether a transaction, person, property, or assets are grounds for suspecting the criminal offence of money laundering, predicate offences and terrorist financing, and
2. strategic analyses focusing on determining the typologies and trends with regard to money laundering and terrorist financing.

Article 91 (Request to an obliged person for the submission of data on suspicious transactions, persons, assets, or funds)

(1) If the Office deems that there are grounds for suspecting money laundering, related predicate criminal offences, or terrorist financing in relation to a particular transaction, person, property, or assets, or in events referred to in Article 100 of this Act, the Office may request the obliged person to submit:

1. data from records of customers and transactions, which shall be kept by obliged persons pursuant to paragraph one of Article 137 hereof;
2. data on the assets and other property of said person with the obliged person;
3. data on transactions with assets, individual transactions, and the property of said person with the obliged person;
4. data on other business relationships of the obliged person;
5. all other data and information obtained or retained by the obliged person under this Act which are required for detecting and proving money laundering and terrorist financing.

(2) In the request referred to in the preceding paragraph, the Office shall specify the data required, as well as the legal basis for submission, purpose of processing, and the time limit within which the required data should be submitted to the Office.

(3) The data referred to in paragraph one of this Article may be required by the Office from the obliged person also for a person in respect of whom there are grounds to believe that he/she has

participated or been engaged in the transactions or business of a person in respect of whom there are grounds to suspect money laundering or terrorist financing.

(4) In the cases referred to in paragraphs one and three of this Article, the obliged person shall additionally be obliged to forward to the Office upon its request all other necessary documentation.

(5) The obliged person shall forward the data, information and documentation referred to in the preceding paragraphs to the Office without delay and at the latest within 15 days of receiving the request. Exceptionally, the Office may set a shorter time limit for the request if this is necessary to determine circumstances relevant to issuing an order temporarily suspending a transaction, or to forward the data to foreign authorities and international organisations, and in other urgent cases when it is necessary to prevent the occurrence of property damage.

(6) In cases of extensive documentation or for other justified reasons, the Office may, by written notification, extend to the obliged person, upon its written and reasoned initiative, the time limit determined in paragraph five of this Article and it may, in such cases, inspect the documentation in the obliged person.

Article 92

(Request to a lawyer, law firm or notary for the submission of data on suspicious transactions, persons, property, or assets)

(1) If the Office considers that there are grounds to suspect money laundering or terrorist financing in connection with a transaction or a certain person, property, or assets, or in events referred to in Article 100 of this Article, it may require from the lawyer, law firm or notary the data, information and documentation relating to the transactions referred to in Article 83 hereof, which are needed for detecting and proving money laundering, predicate criminal offences, and terrorist financing. In the request, the Office shall specify the data required, as well as the legal basis for submission, purpose of processing, and the time limit within which the required data should be submitted to the Office.

(2) The data referred to in the preceding paragraph may be requested by the Office from the lawyer, law firm or notary also for the person in respect of whom there are grounds to believe that he/she has participated or has been engaged in the transactions or business of the person in respect of whom there are grounds to suspect money laundering, related predicate criminal offences, or terrorist financing.

(3) Regarding the time limit for forwarding the data, information and documentation referred to in paragraphs one and two of this Article, the provisions of paragraphs five and six of the preceding Article of this Act shall apply *mutatis mutandis*.

Article 93

(Request to a state authority or holders of public authority to submit data on suspicious transactions, persons, property, or assets)

(1) If the Office considers that there are grounds to suspect money laundering, related predicate criminal offences, or terrorist financing in connection with a transaction, a certain person, property, or assets, or in events referred to in Article 100 hereof, it may require from state authorities and holders of public authority the data, information and documentation needed for detecting and proving money laundering, predicate criminal offences, and terrorist financing. In the request, the Office shall specify the data required, as well as the legal basis for submission, purpose of processing, and the time limit within which the required data should be submitted to the Office.

(2) The data referred to in the preceding paragraph may be requested by the Office from state authorities and holders of public authority also for a person in respect of whom there are grounds to believe

that he/she has participated or has been engaged in the transactions or business of a person in respect of whom there are grounds to suspect money laundering, predicate criminal offences, or terrorist financing.

(3) State authorities and holders of public authority shall forward to the Office the data, information and documentation referred to in the preceding paragraphs without delay and at the latest within 15 days of receipt of the request, or shall allow the Office, without compensation, direct electronic access to certain data and information.

(4) Notwithstanding paragraph three of this Article, the Office may exceptionally set a shorter deadline for the request if this is necessary to determine circumstances relevant to issuing an order temporarily suspending a transaction, or to forward the data to foreign authorities and international organisations, and in other urgent cases when it is necessary to prevent the occurrence of property damage.

Article 94

(Request to other persons governed by public or private law for the submission of data on suspicious transactions, persons, property, or assets)

(1) If the Office considers that there are grounds to suspect money laundering, related predicate criminal offences, or terrorist financing, or in events referred to in Article 100 hereof, in connection with a transaction, a certain person, property, or assets, it may also require from other persons governed by public or private law the data, information and documentation needed for detecting and proving money laundering, predicate criminal offences, and terrorist financing. In the request, the Office shall specify the data required, as well as the legal basis for submission, purpose of processing, and the time limit within which the required data should be submitted to the Office.

(2) The data referred to in the preceding paragraph may be requested by the Office from other persons governed by public or private law also for a person in respect of whom there are grounds to believe that he/she has participated or has been engaged in the transactions or business of the person in respect of whom there are grounds to suspect money laundering, predicate criminal offences, or terrorist financing.

(3) Other persons governed by public or private law shall forward to the Office the data, information and documentation referred to in the preceding paragraphs without delay and at the latest within 15 days of receipt of the request, or shall allow the Office, without compensation, direct electronic access to certain data and information.

(4) Notwithstanding paragraph three of this Article, the Office may exceptionally set a shorter deadline for the request if this is necessary to determine circumstances relevant to issuing an order temporarily suspending a transaction, or to forward the data to foreign authorities and international organisations, and in other urgent cases when it is necessary to prevent the occurrence of property damage.

Article 95

(Verifying data accuracy)

Notwithstanding any other provisions hereunder, the Office may acquire from a competent state authority the unique identification code of the person to whom the submitted data refers in order to verify the accuracy of the data forwarded to the Office pursuant to Articles 68 and 69 of this Act.

Article 96
(Order temporarily suspending a transaction)

(1) The Office may issue a written order temporarily suspending a transaction for a maximum of three working days if the Office considers that there are reasonable grounds to suspect money laundering or terrorist financing, and it shall inform the competent authorities thereof.

(2) The purpose of the temporary suspension is to give the Office the necessary time to analyse suspicious transactions, other data, and information and to forward its findings to competent authorities.

(3) If, due to the nature or manner of executing the transaction or accompanying circumstances, no delay is possible, as well as in other urgent cases, the order may exceptionally be issued orally, but the Office shall be obliged to submit a written order to the obliged person as soon as possible and/or on the same day that the order was issued. The responsible person in the obliged person shall make a note of the receipt of oral order and keep the note in its records in accordance with the provisions of the present Act regulating protection and retention of data.

(4) In respect of issuing an order and if additional information needs to be obtained during pre-criminal or criminal proceedings, or due to other justified reasons, the Office may give the obliged person instructions on the procedure regarding the persons to whom the temporary suspension refers, including information that may be disclosed to the party.

(5) The competent authorities referred to in paragraphs one and two of this Article shall be obliged to act very quickly after receiving the notification concerning the order or the Office's findings, and within three working days of the temporary suspension of the transaction, shall take measures in accordance with their competencies.

Article 97
(Termination of a temporary suspension of a transaction)

(1) If the Office finds within three working days of the time the order on temporary suspension of a transaction was issued that there are no longer reasonable grounds to suspect money laundering or terrorist financing, it shall inform the competent authorities and the obliged person thereof, which may then execute the transaction immediately.

(2) If the Office does not act within the time provided in the preceding paragraph, the obliged person may proceed with the transaction immediately

Article 98
(Request for ongoing monitoring of a customer's financial transactions)

(3) The Office may request in writing from the obliged person the ongoing monitoring of the financial transactions of a person in respect of whom there are reasonable grounds to suspect money laundering or terrorist financing, or of another person in respect of whom there are reasonable grounds to believe that he/she has participated or has been engaged in the transactions or business of said person, and it may request continuous data reporting on the transactions or business undertaken by the persons concerned within the obliged person. In its request, the Office shall be obliged to set a time limit within which obliged persons must forward the data requested.

(4) The obliged person shall forward the data referred to in the preceding paragraph to the Office before the transaction or business has been effected, and shall state the time limit in which the transaction is expected to be executed.

(5) If, due to the nature of the transaction or business, or due to other justified reasons, the obliged person cannot act as provided for in paragraph two of this Article, it shall be obliged to forward the data to the Office as soon as possible or on the following working day at the latest. The obliged person shall be obliged to explain in the report the reasons for not acting in accordance with the provisions of paragraph two of this Article.

(4) The application of the measure referred to in paragraph one of this Article may continue for no longer than three months; however, for substantiated reasons the duration may be extended each time by one month, but for no more than six months in total.

Article 99 (Initiators)

(1) If, with regard to a transaction, a person, property, or assets, there are reasons to suspect money laundering, related predicate criminal offences, or terrorist financing, the Office may begin to collect and analyse data, information, and documentation by written notification of the court, state prosecutor, the police, the Slovenian Intelligence and Security Agency, the Intelligence and Security Service of the Ministry of Defence, the Court of Audit, the Commission for the Prevention of Corruption, the Budget Supervision Office of the Republic of Slovenia, the Financial Administration of the Republic of Slovenia, and the Public Payments Administration of the Republic of Slovenia. The initiative must contain the information referred to in paragraph seven of Article 137 hereof.

(2) When there are grounds to suspect money laundering, related predicate criminal offences, or terrorist financing in connection with the operation of a non-profit obliged person, its members or persons associated with them, the Office may collect and analyse data, information and documentation on the basis of a reasoned written initiative by the inspectorate responsible for internal affairs, as well as other inspection authorities responsible for supervising the operation of non-profit organisations.

(3) The Office shall refuse the initiative referred to in paragraphs one and two of this Article if the initiative fails to state substantiated grounds for suspecting money laundering, related predicate criminal offences, or terrorist financing. The Office shall inform the initiator of the refusal in writing, stating the reasons for which the initiative was not tabled for discussion.

Article 100 (State prosecutor's initiative with regard to the procedure for confiscating the proceeds of criminal offences)

(1) When the State Prosecutor's Office manages a financial investigation procedure pursuant to the Act regulating the confiscation of the proceeds of criminal offences, the Office may begin collecting and analysing data, information, and documentation at the written and reasoned initiative of the State Prosecutor's Office, which must contain the data referred to in paragraph seven of Article 137 hereof.

(2) When collecting data, the Office shall, *mutatis mutandis*, apply the authorisations set forth in Articles from 91 to 94 and the chapter on international cooperation contained herein.

Article 101 (Notification of suspicious transactions)

(1) If the Office considers, on the basis of data, information and documentation acquired under this Act, that there are grounds to suspect money laundering, related predicate criminal offences, or terrorist financing in connection with a transaction or a certain person, property or assets, or in events

referred to in Article 100 herein, it shall notify the competent authorities in writing and submit the necessary documentation.

(2) In the notification referred to in the preceding paragraph, the Office shall not state information about the employee or his/her respective obliged person which first forwarded the information on the basis of Article 69 hereof unless there are reasons to suspect that the obliged person or its employee committed the criminal offence of money laundering or terrorist financing, or if such data are necessary in order to establish facts during criminal proceedings and if the submission of said data is requested in writing by the competent court.

Article 102 (Information on other criminal offences)

Notwithstanding the provision of paragraph one of the preceding Article hereof, the Office shall forward a written notification including the necessary documentation to the competent authorities also in cases whereby the Office considers, on the basis of data, information and documentation obtained under this Act, that in connection with a transaction or a certain person, property or assets, there are grounds to suspect criminal offences which are set forth in the Criminal Code, prosecuted ex officio and punishable by imprisonment have been committed.

Article 103 (Feedback)

The Office shall inform in writing the obliged person referred to in Article 69 hereof, the initiator referred to in Articles 99 and 100 hereof, and the supervisory authority referred to in Article 153 hereof concerning the completed collection and analysis of data, information, and documentation concerning a transaction, a person, property or assets regarding which there are grounds to suspect that money laundering, predicate criminal offences, or terrorist financing have been committed, or if facts have been discovered that are, or could be, related to money laundering, predicate criminal offences, or terrorist financing, unless it assesses that this could harm an ensuing procedure.

The Office shall inform the obliged persons which notify the Office of suspicious transactions based on the provisions hereof, concerning the usefulness and helpfulness of the notified suspicious transactions.

6.3 International participation

Article 104 (General provisions)

(1) The provisions of this Act concerning international cooperation shall apply unless otherwise stipulated by international agreement or a directly applicable EU regulation.

(2) The provisions of this Act concerning international cooperation refer to cooperation between the Office and foreign financial intelligence units, regardless of their organisational status, and cooperation with the European Commission.

(3) Cooperation between the Office and foreign financial intelligence units refers to the exchange of data, information, and documentation concerning clients, transactions, assets, and property

regarding which there are grounds to suspect money laundering, predicate criminal offences, or terrorist financing. Cooperation encompasses:

1. a request submitted by the Office to foreign financial intelligence units,
2. a request submitted by foreign financial intelligence units to the Office,
3. exchange based on a spontaneous initiative by the Office or foreign financial intelligence units.

(4) The office shall cooperate with the European Commission and other competent EU authorities when this is required in order to more easily coordinate and exchange information between the financial intelligence units of Member States regarding important issues in their field of work and cooperation that refers to:

- the discovery of suspicious transactions with cross-border dimensions,
- the standardisation of data and information exchange through a protected, decentralised computer network intended for data and information exchange regarding money laundering and terrorist financing among financial intelligence units;
- joint analyses of cross-border issues,
- defining trends and factors relevant to assessing the risk of money laundering and terrorist financing at the national level and at the level of the European Union.

(5) For the purpose of data, information, and documentation exchange referred to in paragraph three of this Article, the Office may enter into a cooperation agreement with foreign financial intelligence units.

(6) Prior to sending personal data to a foreign financial intelligence unit, the Office shall obtain guarantees that the financial intelligence unit from the country to which data is being sent has a suitable level of personal data protection and that it will use these data only for the purposes set forth herein.

(7) The varying definitions of tax-related criminal offences in individual Member States or in third states shall not hinder data and information exchange among the financial intelligence units from Member States or third states, as provided by national legislation.

Article 105 **(A request to a foreign financial intelligence unit to submit data)**

(1) In the course of performing its tasks for discovering and preventing money laundering, predicate criminal offences, and terrorist financing, the Office may request in writing that a foreign financial intelligence unit submit data, information, and documentation concerning clients, transactions, assets, and property required in order to process, analyse, discover, and prevent money laundering, predicate criminal offences, or terrorist financing.

(2) If the Office requires data, information, and documentation from an obliged person from a different Member State, it shall send a request to the financial intelligence unit of such Member State.

(3) The request of the Office referred to in the preceding paragraphs shall contain relevant facts and circumstances concerning reasons to suspect money laundering or terrorist financing, as well as a definition of the purpose for the use of requested data. It may also request the data if a predicate criminal offence related to money laundering is not known at the time that the request is made.

(4) The Office may use the data, information and documentation acquired pursuant to the preceding paragraph solely for the purposes stipulated by this Act. The Office may not, without the prior consent of the foreign financial intelligence unit, forward or allow insight into the acquired data, information and documentation to a third person or use them in contravention of conditions and restrictions stipulated by the authority to whom the request was made.

Article 106

(Submitting data and information at the request of a foreign financial intelligence unit)

(1) The Office shall submit the data, information, and documentation concerning clients, transactions, assets, and property regarding which there are reasons to suspect money laundering or terrorist financing acquired or managed pursuant to the provisions of this Act, and which could be relevant to processing or analysing information on money laundering, predicate criminal offences, or terrorist financing in a different Member State or third state, to a foreign financial intelligence unit at its request, provided that de facto reciprocity applies.

(2) When a foreign financial intelligence unit requests that the Office submit data, information, and documentation referring to an obliged person with registered offices in the Republic of Slovenia, the Office shall apply all authorisations available to it pursuant to the provisions of this Act when acquiring data, information, and documentation.

(3) The request of a foreign financial intelligence unit referred to in preceding paragraphs shall contain relevant facts and circumstances concerning reasons to suspect money laundering or terrorist financing, and the purpose for the use of requested data shall also be evident. The Office may respond to the request of the foreign financial intelligence unit even if a predicate criminal offence regarding money laundering is not known at the time that the request is submitted.

(4) The Office may exceptionally reject the fulfilment of a request submitted by a foreign financial intelligence unit in the following cases:

1. if no guarantee concerning personal data protection and the purpose of its use referred to in paragraph six of Article 104 of this act is given;
2. if the submission of data and information is contrary to the principles of the *acquis* of the Republic of Slovenia.

The Office shall inform the foreign financial intelligence unit concerning the rejection of the request in writing and the notification shall state and clarify the grounds for rejection.

(5) The data, information, and documentation submitted on the basis of the preceding paragraphs of this Article may be used by foreign financial intelligence units exclusively for the purposes for which they are submitted. The foreign financial intelligence unit may not, without prior consent of the Office, forward or allow viewing of the acquired data, information and documentation to a third person or use them in contravention of the conditions and restrictions stipulated by the Office.

(6) The Office shall give consent to the forwarding of data to third persons referred to in the preceding paragraph as soon as possible and to the greatest extent possible. The Office may refuse to provide third persons with data only in the following cases:

1. if the submission of data exceeds the application of the provisions of this Act;
2. if the submission of data jeopardises or may jeopardise the course of criminal proceedings in the Republic of Slovenia, or may in any other way prejudice the interests of these proceedings;
3. if the submission of data was disproportionate to the legitimate interests of a natural or legal person or of the Republic of Slovenia;
4. if the submission of data was not in accordance with the basic principles of the *acquis* of the Republic of Slovenia;
5. if no guarantee concerning personal data protection and the purpose of its use referred to in paragraph six of Article 104 of this act is given.

Each refusal to issue a consent shall be suitably clarified.

(7) The Office may set forth additional conditions and restrictions which must be taken into account by a foreign financial intelligence unit in order to use the data referred to in paragraph one of this Article.

Article 107

(Submission of data and information concerning beneficial owners at the request of a foreign financial intelligence unit from a Member State)

(1) The Office shall submit data, information, and documentation concerning beneficial owners to a foreign financial intelligence unit from a Member State at its request.

(2) The Office may set forth additional conditions and restrictions which must be taken into account by a foreign financial intelligence unit in order to use the data referred to in the preceding paragraph.

Article 108

(Spontaneous submission of data to a foreign financial intelligence unit)

(1) The Office shall forward the data, information, and documentation concerning clients, transactions, assets, and property regarding which there are reasons to suspect money laundering or terrorist financing, acquired or managed pursuant to the provisions of this Act and which could be relevant to processing or analysing information on money laundering, predicate criminal offences, or terrorist financing in a different Member State or third state, to a financial intelligence unit of this Member State or a third state at its own initiative, provided that de facto reciprocity applies.

(2) If it is evident from the notification concerning suspicious transactions received by the Office based on Article 69 of this Act that persons, transactions, property, or assets are related to a different Member State, the Office shall send to a financial intelligence unit of this Member State the data referred to in points 1, 2, 8, 11, 12, and 13 of paragraph one of Article 137 of this Act.

(3) In order to exchange data based on this Article, the provisions of this Act contained in the chapter on international cooperation shall apply mutatis mutandis.

Article 109

(Feedback)

(1) The Office shall provide a foreign financial intelligence unit, at its request and provided that de facto reciprocity exists, feedback concerning the usefulness and helpfulness of the received data referred to in paragraph one of Article 105 of this Act and the information concerning the results of analyses drafted on the basis of the data received from the foreign financial intelligence unit.

(2) The Office may request feedback from a foreign financial intelligence unit concerning the usefulness and helpfulness of the submitted data referred to in paragraph one of Article 106 of this Act and the information concerning the results of analyses obtained on the basis of the submitted data.

Article 110

(Transaction suspension at the initiative of a foreign financial intelligence unit)

(1) The Office may, under the conditions stipulated by this Act and subject to effective reciprocity, issue a written order temporarily suspending a transaction for a maximum of three working days also on the basis of a reasoned and written request by a foreign financial intelligence unit, and inform the competent authorities thereof.

(2) The Office may refuse an initiative given by a foreign financial intelligence unit if, based on facts and circumstances stated in the initiative referred to in the preceding paragraph of this Article, the

Office finds that no reasonable grounds have been given to suspect that money laundering or terrorist financing have been committed. The Office shall inform the initiator of the refusal in writing, stating the reasons for the refusal of the initiative.

(3) With respect to the order on the temporary suspension of a transaction under this Article, the provisions of Articles 96 and 97 herein shall apply mutatis mutandis.

Article 111
(An initiative provided to a foreign financial intelligence unit to suspend a transaction)

In conducting its tasks of discovering and preventing money laundering and terrorist financing, the Office may send to foreign financial intelligence units a written initiative to suspend a transaction if it discovers reasonable grounds to suspect that money laundering or terrorist financing have been committed.

Article 112
(Safe communications systems)

The exchange of data, information, and documentation between the Office and foreign financial intelligence units based on Articles from 104 to 111 of this Act shall be carried out by means of secure communications systems.

Article 113
(Diagonal exchange)

(1) The Office may also indirectly ask foreign authorities of a Member State or a third state competent for discovering and preventing money laundering and terrorist financing to provide data, information, and documentation, but such data, information, and documentation exchange must be carried out only through a financial intelligence unit of such state by means of secure communications systems.

(2) The Office may also, indirectly and upon request, provide foreign authorities of a Member State or a third state competent for discovering and preventing money laundering and terrorist financing with data, information, and documentation, but such data, information, and documentation exchange must be carried out only through a financial intelligence unit of such state by means of secure communications systems.

(3) In order to exchange data based on this Article, the provisions of this Act contained in the chapter on international cooperation shall apply mutatis mutandis.

6.4 Prevention of money laundering and terrorist financing

Article 114
(Prevention of money laundering and terrorist financing)

The Office shall perform duties related to the prevention of money laundering and terrorist financing in such a manner that it shall:

1. propose to the competent authorities changes and amendments to regulations concerning the prevention and detection of money laundering and terrorist financing;

2. participate in drawing up a list of indicators for the purpose of identifying customers and transactions in respect of which there are reasonable grounds to suspect money laundering or terrorist financing;

3. draw up and issue recommendations or guidelines for the uniform implementation of the provisions of this Act and regulations issued on the basis hereof, for persons under obligation referred to in Article 4 of this Act;

4. cooperate with regard to the professional training of employees working for the obliged person, state authorities, and holders of public authority;

5. collect and publish statistical data on money laundering and terrorist financing;

6. inform the public, in any other appropriate manner, of the various forms of money laundering and terrorist financing.

Article 115 **(Submitting data to the Office)**

(1) The Office may require the following data from the obliged persons referred to in Article 4 of this Act, supervisory bodies referred to in Article 139 of this Act, and other state authorities and organisations with public authority:

1. from all records that they are obliged to keep based on this Act;

2. concerning all business relationships entered into with their clients, regardless of their type or form;

3. concerning all transactions between them and their clients;

4. concerning all transactions of their clients performed within the Republic of Slovenia;

5. concerning all transactions performed by their clients for Member States or third states;

6. concerning all transactions performed in Member States or third states for their clients in the Republic of Slovenia;

7. other available data and documentation kept on the basis of other regulations and required by the Office for purposes referred to in this Article.

(2) In the request, the Office shall specify the data required, as well as the legal basis for submission, the purpose of processing, and the time limit within which the required data should be submitted to the Office.

(3) The data, information, documentation, and other available data referred to in paragraph one of this Article shall be used by the Office for the purpose of carrying out operational and strategic analysis, determining exposure and carrying out risk assessments for the financial and non-financial system of the Republic of Slovenia for money laundering and terrorist financing and for determining the forms of money laundering and terrorist financing and their trends.

(4) The obliged persons referred to in Article 4 of this Act shall submit the data, information, documentation, and other available data referred to in paragraph one of this Article to the Office free of charge and within fifteen days of receiving the request.

(5) Furthermore, the supervisors referred to in Article 139 of this Act and other state authorities and obliged persons with public authority shall also submit the required data to the Office free of charge and within the time limit specified in the preceding paragraph.

(6) Notwithstanding the time limit referred to in paragraphs four and five of this Article, the Office may, due to the scope of the documentation or other reasonable grounds, extend the time limit for the entities referred to in paragraphs four and five of this Article at their reasoned written initiative by means of a written notification.

(7) The Office shall publish the results of strategic analyses, determined risk assessments, forms, and trends in money laundering on its website, and it may also inform the Government by means of a special or regular annual report on the work of the Office.

6.5 Other tasks

Article 116 (Submission of data to the court, prosecutor's office or police)

(1) The Office shall submit to the court, the State Prosecutor's Office, or the police, at their reasoned written request, the data from its records referred to in points 1 to 5 and 9 to 12 of paragraph four of Article 136 of this Act, which the court, the State Prosecutor's Office or the police require:

1. when researching circumstances relevant to the discovery, prosecution or trial of criminal cases regarding money laundering, predicate criminal offences, or terrorist financing, pursuant to the provisions of the Act regulating criminal proceedings;
2. when researching the circumstances vital for the protection or forfeiture of proceeds, in accordance with the provisions of the Act regulating criminal proceedings or of the Act regulating the forfeiture of assets of illegal origin.

(2) Notwithstanding the provision of the preceding paragraph, the Office shall not submit data from the records referred to in points 4 and 5 of paragraph four of Article 136 of this Act to the court, the State Prosecutor's Office or the police if a foreign financial intelligence unit has not consented to such submission.

(3) It shall be evident from the reasoned written request referred to in paragraph one that discovery, prosecution, or investigation procedures concerning money laundering, predicate criminal offences, or terrorist financing or procedures concerning the forfeiture of assets of illegal origin are being carried out with regard to persons, transactions, assets, and property of illegal origin.

(4) The Office may refuse the request referred to in paragraphs one and two if it deems:

1. that there are actual reasons to assume that providing such information would inhibit or prevent the operation and performance of tasks by the Office, or
2. in exceptional cases, that the submission of data is evidently disproportionate to the legitimate interests of a natural or legal person or irrelevant to the purposes for which it was submitted.

(5) The court, the State Prosecutor's Office and the police shall, at least once a year and at the latest by the end of January of the current year for the previous year, inform the Office concerning any measures that were adopted on the basis of the received data referred to in this Article and concerning the results of investigations or inspections carried out on the basis of such data.

Article 117 (Submitting data to the Financial Administration of the Republic of Slovenia)

(1) The Office shall submit to the Financial Administration of the Republic of Slovenia the data from the records referred to in point 1 of paragraph four of Article 136 referring to the persons and transactions referred to in Article 68 of this Act which the Financial Administration of the Republic of Slovenia requires for the purposes of carrying out the following tasks within its competencies:

1. financial supervision;
2. financial investigation;
3. supervision of the obliged person of gambling;
4. supervision of the registration of transferring cash in and out of the area of the European Union;
5. carrying out tasks in the field of customs based on EU regulations which regulate mutual legal assistance among administrative authorities of Member States.

(2) The data referred to in the preceding paragraph may be requested by the Financial Administration of the Republic of Slovenia only on the basis of a reasoned written request, which must show that it is performing the tasks referred to in the preceding paragraph pursuant to its competencies.

(3) The Office may refuse the request referred to in paragraphs one and two if it deems:

1. that there are actual reasons to assume that providing such information would inhibit or prevent the operation and performance of tasks by the Office, or

2. in exceptional cases, that the submission of data is evidently disproportionate to the legitimate interests of a natural or legal person or irrelevant to the purposes for which it was submitted.

(4) The Financial Administration of the Republic of Slovenia shall be obliged to inform the Office, once per year and at the latest by the end of January of the current year for the previous year, of its findings made on the basis of the received data referred to in this Article, and other measures taken on the basis hereof.

Article 118

(Submitting data to the permanent coordination group established pursuant to the Act regulating restrictive measures)

(1) The Office shall submit the data from its records referred to in points 1 to 5 and 9 to 12 of paragraph four of Article 136 of this Act to a permanent coordination group established pursuant to the Act regulating restrictive measures; this data is required by this group to carry out its competencies pursuant to the regulations regulating restrictive measures.

(2) Notwithstanding the provision of the preceding paragraph, the Office shall not submit data from the records referred to in points 4 and 5 of paragraph four of Article 136 of this Act to the permanent coordination group established pursuant to the Act regulating restrictive measures if a foreign competent body has not consented to such submission.

(3) The data referred to in the preceding paragraph may be requested by the permanent coordination group only on the basis of a reasoned written request which must show that it is performing the tasks referred to in the preceding paragraph relating to persons or transactions pursuant to its competencies.

(4) The Office may refuse the request referred to in paragraphs one and two if it deems:

1. that there are actual reasons to assume that providing such information would inhibit or prevent the operation and performance of tasks by the Office, or

2. in exceptional cases, that the submission of data is evidently disproportionate to the legitimate interests of a natural or legal person or irrelevant to the purposes for which it was submitted.

(5) The permanent coordination group referred to in paragraph one of this Article shall be obliged to inform the Office, once per year and at the latest by the end of January of the current year for the previous year, of its findings made on the basis of the received data referred to in this Article, and other measures taken on the basis thereof.

Article 119

(Reporting to the Government)

The Office shall submit to the Government a report on its work at least once annually.

CHAPTER VII
DUTIES OF STATE AUTHORITIES AND HOLDERS OF PUBLIC AUTHORITY

Article 120
(Financial Administration of the Republic of Slovenia)

(1) The Financial Administration of the Republic of Slovenia shall be obliged to forward to the Office, at the latest within three days, the data referred to in paragraph four of Article 137 of this Act on any declared import or export of cash amounting to or exceeding €10,000 upon entering or leaving the European Union.

(2) The Financial Administration of the Republic of Slovenia shall be obliged to forward to the Office the data referred to in paragraph four of Article 137 of this Act, even if the import or export of cash when entering or leaving the European Union referred to in paragraph one of this Article was not declared to the Financial Administration of the Republic of Slovenia.

(3) The Financial Administration of the Republic of Slovenia shall forward to the Office the data referred to in paragraph five of Article 137 of this Act also in the event of the import and/or export of cash, or attempted import and/or export of cash, in an amount of less than €10,000 when entering or leaving the European Union if, in connection with the person carrying the cash, the manner in which it carried or other circumstances thereof, there are grounds to suspect money laundering or terrorist financing.

Article 121
(Courts, prosecutors' offices and other national authorities)

(1) To enable the centralisation and analysis of all data related to money laundering and terrorist financing, the courts, prosecutors' offices and other state authorities shall forward to the Office data on criminal offences of money laundering and terrorist financing activities, and on offences under this Act.

(2) The competent state authorities shall forward the following data to the Office on an ongoing basis if such data are available to them:

1. date of filing the criminal charge;
2. the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) or the company name, address, registered office, registration no., and tax number of the denounced person;
3. statutory definition of the criminal offence and the place, time and manner of committing an action which has signs of a criminal offence;
4. statutory definition of the predicate offence and the place, time and manner of committing the action which has signs of a predicate offence.

(3) State prosecutor's offices and courts shall send the following data to the Office once a year, but at the latest by the end of January of the current year for the previous year, if such data are available to them:

1. the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) or company name, address, registered office, registration no., and tax number of the person against whom a complaint has been filed, or a charged person or a person who has filed a request for judicial protection within the offence proceedings;
2. case file number, procedure phase, and their last decision in each phase;
3. statutory definition of the criminal offence or minor offence;
4. the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) or company name, address, registered office, registration no., and tax number of the person with regard to whom temporary security of the claim for the confiscation of proceeds or a temporary confiscation has been ordered;

5. date of issue and duration of the order to temporarily secure the claim for forfeiture of proceeds or temporary seizure;

6. amount of assets or value of property which is the subject of the order on temporary protection of the request for forfeiture of proceeds or temporary seizure;

7. date of issue of the order concerning the confiscation of assets or property;

8. the amount of confiscated assets or the value of the confiscated property.

(4) The competent state authorities shall be obliged to report to the Office, once per year and at the latest by the end of January of the current year for the previous year, on its findings made on the basis of notifications of suspicious transactions as referred to in Article 103 of this Act, or information on other criminal offences referred to in Article 104 of this Act, and other measures taken on the basis thereof.

CHAPTER VIII PROTECTION AND SAFEKEEPING OF DATA AND STATISTICAL DATA, AND KEEPING OF RECORDS

8.1 Data protection

Article 122 (Disclosure ban)

(1) Obligated persons and their employees, including members of the management, supervisory or other executive bodies, or other persons having any access to data on the below facts shall not disclose to a customer, a third person, or any other supervisory body referred to in points b) to i) of paragraph one of Article 139, unless set forth otherwise herein, that:

1. the piece of data, information, or documentation concerning a customer or a transaction referred to in Article 69 of this Act has been forwarded to the Office;

2. the Office requested that the data referred to in Articles 91, 92, 93, and 94 of this Act be submitted;

3. on the basis of Article 96 of this Act, the Office temporarily suspended the transaction and/or gave the obliged persons instructions with regard to this, unless the disclosure is pursuant to paragraph four of Article 96 of this Act;

4. the Office, pursuant to Article 98 of this Act, required ongoing monitoring of the customer's business operations;

5. the Office is carrying out, or will carry out, the operational analysis referred to in point 1 of Article 90 against the customer or third person;

6. a pre-trial investigation or criminal proceedings have been, or are likely to be, launched against the customer or a third person on grounds of money laundering or terrorist financing.

(2) The facts referred to in paragraph one of this Article and notification of suspicious transactions, and/or information on other criminal offences referred to in Articles 101 and 102 of this Act and the data referred to in Articles 116, 117 and 118 of this Act shall be classified and treated according to their level of classification, in accordance with the Act regulating classified information.

(3) The director of the Office shall decide on the lifting of the classification referred to in the preceding paragraph.

(4) The ban on the disclosure of the facts referred to in paragraph one of this Article shall not be in effect if the data, information and documentation obtained and retained in accordance with this Act by

an obliged person are necessary to establish facts in criminal proceedings, and if the submission of said data is required or imposed in writing by the competent court.

(5) The ban on disclosing the facts referred to in point 1 of paragraph one of this Article shall not be in effect if the data referred to in that point are required by the supervisory body referred to in Article 139 of this Act to supervise the implementation of the provisions of this Act and the ensuing regulations conducted within its competencies.

The existence of the facts referred to in points 2 to 6 of paragraph one of this Article shall be verified by the supervisory bodies directly at the Office.

(6) When a lawyer, law firm, notary, audit company, independent auditor, legal entity or natural person performing accountancy services or tax advisory services seeks to dissuade a client from engaging in illegal activity, this does not constitute disclosure within the meaning of paragraph one of this Article.

Article 123 (Data disclosure within a group)

(1) The ban on disclosing the data referred to in point 1 of paragraph one of the preceding paragraph shall not be in effect if this is a disclosure of data carried out among credit institutions and financial institutions from Member States which are a part of the same group, and if the policies and procedures of the group are equal to the provisions of this Act.

(2) The data disclosure ban referred to in point 1 of paragraph one of the preceding Article shall also not be in effect if this is a disclosure of data carried out among credit or financial institutions from Member States and their subsidiaries and affiliates, the majority share of which they own, established in third states, provided that the following conditions have been met:

1. the subsidiaries or affiliates, the majority share of which they own, which are located in third states, shall carry out the policies and procedures of the group, including the procedures for inter-group information exchange equal to the provisions referred to in Articles 71, 72, and 75 of this Act, and
2. the policies and procedures of the group shall be equal to the provisions of this Act.

(3) For the purpose of carrying out this Article, an obliged person shall keep records of the data, to which the disclosure ban does not apply and which have been disclosed within the group, in which the following data are processed:

- the name of the legal entity, sole trader, or individual who independently performs activities regarding which a transaction is carried out;
- the personal name, surname, and date of birth of the legal representative or authorised person who carries out a transaction on behalf of a legal entity, sole trader, or individual who carries out activities independently;
- the personal name, surname, and date of birth of the natural person carrying out a transaction;
- the personal name and surname, and date of birth of the legal representative or authorised person conducting the transaction for the legal entity;
- date and time of the transaction; and
- amount of the transaction and currency in which the transaction is being carried out.

(4) The obliged person shall forward the records referred to in the preceding paragraph to the Office at its request without undue delay.

(5) Prior to exporting the personal data referred to in paragraph three of this Article to third states, the obliged person shall acquire a written guarantee from the recipient of the data which has registered offices in third states, stating that it provides an equal level of personal data protection within the

scope of its operations as an obliged person, and that the third state provides a suitable level of personal data protection.

Article 124
(Data disclosure within a network)

(1) The data disclosure ban referred to in point 1 of paragraph one of Article 122 of this Act shall not apply in the event of a disclosure among lawyers, law firms, notaries, audit companies, independent auditors, legal entities or natural persons performing accountancy services or tax advisory services, provided that they perform their professional activities at the same legal entity or in the same network, and that their registered offices are in Member States.

(2) The provision referred to in the preceding paragraph shall also apply, *mutatis mutandis*, if the persons or entities referred to in the preceding paragraph have registered offices in third states, provided that measures for discovering and preventing money laundering and terrorist financing that are equal to the provisions of this Act are carried out in third states.

(3) For the purpose of carrying out complying with this Article, an obliged person shall keep records of the data, to which the disclosure ban does not apply and which have been disclosed within the network, in which the following data are processed:

- the name of the legal entity, sole trader, or individual who independently performs activities regarding which a transaction is carried out;
- the personal name, surname, and date of birth of the legal representative or authorised person who carries out a transaction on behalf of a legal entity, sole trader, or individual who carries out activities independently;
- the personal name, surname, and date of birth of the natural person carrying out a transaction;
- the personal name and surname, and date of birth of the legal representative or authorised person conducting the transaction for the legal entity;
- date and time of the transaction; and
- amount of the transaction and currency in which the transaction is being carried out.

(4) The obliged person shall forward the records referred to in the preceding paragraph to the Office at its request without undue delay.

(5) Prior to exporting the personal data referred to in paragraph three of this Article to third states, the obliged person shall acquire a written guarantee from the recipient of the data which has registered offices in third states, stating that it provides an equal level of personal data protection within the scope of its operations as an obliged person, and that the third state provides a suitable level of personal data protection.

Article 125
(Data disclosure within the same categories)

(1) The data disclosure ban referred to in point 1 of paragraph one of Article 122 of this Act shall not apply if this is a disclosure among persons or entities that are credit or financial institutions, lawyers, law firms, notaries, audit companies, independent auditors, legal entities or natural persons performing accountancy services or tax advisory services if the following conditions have been met:

1. the transaction refers to two or more of the aforementioned persons or entities,
2. the transaction refers to the same customer,

3. the said persons or entities have registered offices in a Member State or a third state that takes measures to discover or prevent money laundering and terrorist financing that are equivalent to the provisions of this Act,

4. the said persons or entities carry out the same type of activity or are in the same category of professions

5. and obligations regarding the protection of professional and trade secrets and personal data apply to them.

(2) For the purpose of complying with this Article, an obliged person shall keep records of data to which the disclosure ban does not apply and which have been disclosed within the same categories in which the following data are processed:

- the name of the legal entity, sole trader, or individual who independently performs the activities regarding which a transaction is carried out;
- the personal name, surname, and date of birth of the legal representative or authorised person who carries out a transaction on behalf of a legal entity, sole trader, or individual who carries out activities independently;
- the personal name, surname, and date of birth of the natural person carrying out a transaction;
- the personal name and surname, and date of birth of the legal representative or authorised person conducting the transaction for the legal entity;
- date and time of the transaction; and
- amount of the transaction and currency in which the transaction is being carried out.

(3) The obliged person shall forward the records referred to in the preceding paragraph to the Office at its request without undue delay.

(4) Prior to exporting the personal data referred to in paragraph two of this Article to third states, the obliged person shall acquire a written guarantee from the recipient of the data which has registered offices in third states stating that it provides an equal level of personal data protection within the scope of its operations as the obliged person.

Article 126 (Exemptions from the principle of confidentiality protection)

(1) When forwarding data, information or documentation to the Office under this Act, the obligation to protect classified data, trade secrets, professional secrets, and confidential bank information shall not apply to an obliged person, state authority or any other holder of public authority, court, prosecutor's office, or its employees.

(2) Obligated persons and their employees shall not be held liable for any damage caused to customers of third parties if, in accordance with the provisions of this Act, they:

1. submit to the Office data, information and documentation on their customers;
2. obtain and process data, information and documentation on their customers;
3. implement an order to temporarily suspend a transaction or instruction issued in connection with the said order;
4. implement a request by the Office to continue monitoring the customer's financial transactions.

(3) An employee of an obliged person may not be held liable for disciplinary or criminal action for violating the obligation to protect classified data, business secrets, and confidential bank data if:

1. they submit data, information and documentation to the Office in accordance with the provisions of this Act;
2. they process data, information and documentation obtained in accordance with this Act for the purpose of verifying customers and transactions in respect of which there are grounds to suspect money laundering or terrorist financing.

Article 127

(Use of acquired data)

(1) The Office, state authorities and other holders of public authority, obliged persons and their employees may use the data, information and documentation obtained under this Act solely for the purposes stipulated herein.

(2) The bodies referred to in Articles 116, 117, and 118 of this Act may use the data acquired on the basis of the said Articles only for the purposes for which they have been obtained.

(4) The processing of data, information, and documentation acquired under this Act for any other purposes, such as commercial purposes, shall be prohibited.

Article 128

(Notifying individuals concerning personal data processing)

Obliged persons which collect personal data based on the provisions of this Act directly from individuals shall notify such individuals concerning personal data processing prior to entering into a business relationship or prior to carrying out a transaction as referred to in paragraph one of Articles 17 and 18 of this Act, and in accordance with the Act regulating personal data protection.

8.2 Data retention

Article 129

(Retention period of data within the obliged person)

(1) An obliged person shall keep data obtained on the basis of Articles 16, 17, 18, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 43, 48, 49, 50, 54, 58, 59, 60, 61, 62, 63, 68, 69, 96, 97 and 98 of this Act and the corresponding documentation referring to customer or individual transaction due diligence for 10 years after the termination of a business relationship, the completion of a transaction, a customer's admission to a casino or gaming hall, or a customer's access to a safe, unless a longer period for retention is determined by another act.

(2) The corresponding documentation referred to in the preceding paragraph shall include copies, records, or originals of the following documentation:

- official documents for discovering and verifying the identity of a customer,
- documentation of business relationships and accounts,
- documentation on business correspondence,
- transcripts and records required to recognise and trace domestic or cross-border transactions,
- documentation related to discovering the background and purpose of unusual transactions, and
- other corresponding documentation that has been acquired or drafted during customer due diligence or during an individual transaction.

(3) Obliged persons shall keep the data and the corresponding documentation concerning the authorised person and their deputy, the professional training of employees, the performance of internal control and risk management referred to in Articles 13, 76, 77, and 80 of this Act for four years after appointing the authorised person and their deputy, the completed professional training, and performed internal control and the analysis of effects due to changes in the obliged person's business processes related to the risk of money laundering or terrorist financing.

(4) After the expiry of the periods referred to in the preceding paragraphs of this Article, personal data shall be erased, unless determined otherwise by another Act.

(5) In the event of the liquidation of an obliged person, the authority performing the liquidation procedure or carrying out a status change of an obliged person without a known successor shall inform the Office prior to the liquidation of the obliged person and ensure that data and corresponding documentation are retained for the periods set forth herein.

Article 130
(Period for data retention at the Financial Administration of the Republic of Slovenia)

The Financial Administration of the Republic of Slovenia shall keep data from the records referred to in paragraphs four and five of Article 137 of this Act for a period of 12 years from the date it acquires them. These data and information shall be destroyed upon the expiry of this period.

Article 131
(Retention period of data by the Bank of Slovenia)

The Bank of Slovenia shall retain the data from the records referred to in paragraph two of Article 136 of this Act for a period of ten years from the date when a natural person or a legal entity ceases to act as the central contact point. The data shall be destroyed upon the expiry of this period.

Article 132
(Retention period of data within the Office)

(1) The Office shall keep the data and information from the records maintained by it under this Act for a period of 12 years from the date when the Office acquired them, unless another Act determines a longer period. These data and information shall be destroyed upon the expiry of this period.

(2) The Office shall not inform the person concerned that data and information about him/her have been compiled, nor shall such information be disclosed to a third person.

(3) The person to whom the data and information refer shall have the right to inspect his/her personal data and/or to obtain their original, print-out or copy:

- for the records referred to in points 1, 2, 3, 4, 5, and 12 of paragraph four of Article 136 of this Act, eight years after the data were collected;
- for the records referred to in points 6, 7, 8, 9, 10, and 11 of paragraph four of Article 136 of this Act, after the final verdict or any other decision on criminal offence or other offence, and/or after the limitation of criminal prosecution, and/or immediately after the final decision of the competent authority that no measures shall be taken against the person to whom the data and information refer.

8.3 Statistical data

Article 133
(Collecting the Office's statistical data)

For the purpose of drafting a national risk assessment and verifying the effectiveness of the money laundering and terrorist financing discovery and prevention system, the Office shall collect, on an annual basis, statistical data concerning:

- the number, size, and significance of particular groups of obliged persons,
- the number of notified suspicious transactions sent to the Office pursuant to this Act,
- the number of notifications concerning suspicious transactions that the Office forwarded to competent authorities,
- the number and portion of suspicious transaction on the basis of which measures were taken by the police, a state prosecutor's office, or a court,
- the number of received, rejected, and answered requests from foreign financial intelligence units.

Article 134
(Collection of statistical data by other state authorities)

(1) For the purpose of drafting a national risk assessment and verifying the effectiveness of the money laundering and terrorist financing discovery and prevention system, courts, state prosecutor's offices, and other state authorities shall collect, on an annual basis, statistical data concerning:

1. the number of persons concerning whom a criminal investigation related to money laundering or terrorist financing is being carried out,
2. the number of persons concerning whom a criminal complaint related to money laundering or terrorist financing has been filed,
3. the number of persons concerning whom an investigation has been launched,
4. the number of persons charged with money laundering or terrorist financing,
5. the number of persons convicted of money laundering or terrorist financing,
6. the type of predicate criminal offence related to money laundering or terrorist financing, provided that this piece of data is available,
7. the value of secured, confiscated, or seized illegal assets in euros.

(2) Once a year, courts, state prosecutor's offices, and other state authorities shall forward to the Office the data referred to in the preceding paragraph at the latest by the end of January of the current year for the previous year.

Article 135
(Publication of statistical data)

At least once a year, the Office shall publish and forward to the European Commission the statistical data related to money laundering and terrorist financing referred to in Articles 133 and 134.

8.4 Managing records

Article 136
(Managing records)

(1) Obligated persons shall manage the following data records:

1. records of data on all customers, business relationships and transactions referred to in Articles 17 and 18 of this Act;
2. records of data reported to the Office as referred to in Articles 68 and 69 of this Act.

(2) The Bank of Slovenia shall manage the records concerning contact points referred to in Article 72 of this Act.

(3) The Financial Administration of the Republic of Slovenia shall manage the following data records:

1. records on declared and undeclared imports or exports of cash in the amount of €10,000 or more when entering or leaving the European Union referred to in paragraphs one and two of Article 120 of this Act;

2. records on imports or exports of cash, or attempted imports or exports of cash in an amount less than €10,000 when entering or leaving the European Union if there are grounds to suspect money laundering or terrorist financing, as referred to in paragraph three of Article 120 of this Act.

(4) The Office shall manage the following data records:

1. records of data on persons and transactions referred to in Articles 68 and 69 of this Act;
2. records of initiatives received, as referred to in Articles 99 and 100 of this Act;
3. records of notifications and the information referred to in Articles 101 and 102 of this Act;
4. records of international requests referred to in Articles 105 and 106 of this Act;
5. records on personal data exported from the country, as referred to in Articles 105, 106, 107, and 108 of this Act;
6. records of data access referred to in Article 116 of this Act;
7. records of data access referred to in Article 117 of this Act;
8. records of data access referred to in Article 118 of this Act;
9. records of criminal offences referred to in Article 121 of this Act;
10. records of minor offences referred to in Article 121 of this Act;
11. records of controls performed, violations discovered, and decisions issued and other control measures referred to in Article 152 of this Act;
12. records of facts reported, as referred to in Article 153 of this Act.

(5) Business entities shall manage the data records concerning their beneficial owners referred to in Articles 35, 36, and 37 of this Act.

(6) For the purpose of implementing Article 87 of this Act, the Office may, free of charge, acquire, use, and process data, including personal data, from databases kept by duly authorised bodies and organisations in the Republic of Slovenia, namely from the data collections of the following data managers:

1. the Ministry of the Interior:
 - data from the Central Population Register (name and surname, unique personal ID-no. (EMŠO), nationality, tax number, permanent or temporary residence, state of residence, address for service, marital status, father, mother, spouse, child, change of personal name, withdrawal and reinstatement of full legal capacity, date of death, data of residency permit issued to foreigners,
 - data on the household from the Household Register (name and surname and the unique personal ID-number (EMŠO) of persons in a common household, data on the head of the household and the relationship with the head of the household);
2. the Ministry of Infrastructure:
 - data on the ownership of a vehicle and on a vehicle from the Motor Vehicle and Trailer Records (the date of the first registration of a vehicle, data on the owner, data on the person in whose name the vehicle is registered but who is not the owner of the vehicle, data on the vehicle);
3. the Pension and Disability Insurance Institute of the Republic of Slovenia:
 - data on insured persons included in the pension and disability insurance (the basis for insurance, date of registration and de-registration for pension and disability insurance and data concerning the insurance period) and data on the beneficiaries of the pension and disability insurance paid by the Pension and Disability Insurance Institute (concerning the type, amount, payment date, and the date of eligibility to claim particular rights);
4. the Health Insurance Institute of Slovenia:
 - data on the insured persons included in the compulsory health insurance (the basis for insurance, date of registration and de-registration for compulsory health insurance) and data on the insured persons included in the pension and disability insurance;

5. the Financial Administration of the Republic of Slovenia:

- data on income declared in the annual income tax return
- data on the assessment of value added tax arising from monthly value added tax returns,
- data on corporate income tax assessment arising from the corporate income tax returns,
- data arising from the income tax prepayment calculation and the personal income tax prepayment for income from self-employment,
- data on real estate transfer tax return,
- data on the management of fiscal control procedures,
- data on the management of tax investigation procedures,
- data on the bank account numbers of persons abroad
- data from the tax register (an entity entered in the court register, natural persons with permanent or temporary residence in the Republic of Slovenia, sole traders, other legal entities or natural persons performing an activity and entered in another register or other prescribed records in the territory of the Republic of Slovenia; a legal entity or natural person who does not have registered offices or other registered entities in the Republic of Slovenia and performs activities in the territory of the Republic of Slovenia, an association of persons under foreign law that are without legal personality, a direct user of the national or municipal budget, other persons entered in the tax register);

6. the Surveying and Mapping Authority of the Republic of Slovenia:

- data on the value of real estate (generalised market value according to the mass valuation of real estate from the real estate register),
- data on the type of real estate (the actual use of the land plot from the land cadastre and the use of buildings and their parts from the building cadastre),
- data on the area of apartments;

7. the Slovenian Maritime Administration:

- data on the ownership of water vessels of a particular person and on the water vessel itself;

8. local courts:

- data on the ownership of real estate and other real rights related to the real estate of a particular person;

9. central securities clearing companies:

- a computer print-out of data entered in the central register of dematerialised securities referring to individual holders of dematerialised securities;

10. SISBON Credit Bureau:

- data on the type of transaction (personal accounts with approved extraordinary limits, extraordinary limit, credit cards, sureties for others, other receivables), date of transaction, currency sign, amount upon approval, annuity or instalment amount, type of annuity or instalment, repayment period in months, data on the moratorium (grace period), data on business events affecting the course of the transaction (repayment of debt, early repayment, modification of the repayment period, modification of the instalment), data on business events that are not in accordance with an agreement (termination of a transaction due to the failure to repay debt, unpaid due debt, blocking, de-blocking);

11. the Agency of the Republic of Slovenia for Public Legal Records and Related Services:

- data on business entities, their founders and representatives, including all modifications (date of entry and deletion, registration number, tax number, company name, registered office, personal or business name, registered office or the address of the permanent or temporary residence, unique personal ID number (EMŠO) or registration number, tax number),
- data on the value of ownership interest (registration number of a private undertaking or a legal entity, date of entry into or deletion from the Slovenian Business Register, legal form of obliged person, the tax number of a private undertaking or a legal entity, the amount of share capital, the ownership share of a person in a corporation or a cooperative),
- data on the amount of profit earned by private undertakings and legal entities,
- data on the bank account number,
- data on bank account status (opened, closed),
- date of bank account closure.

(7) The Office shall access written and graphic data from the databases referred to in the preceding paragraph by means of a direct computer connection, provided that this is enabled by technical means.

(8) For the purpose of carrying out paragraph two of Article 87 of this Act, the records referred to in paragraphs three and four of this Article may be integrated with each other and with the records referred to in paragraph six of this Article.

(9) In order to perform the integration of the records referred to in paragraphs three and four of this Article with each other, a tax number or a unique personal ID number (EMŠO), registration number and similar number defined by the Office marking the records may be used.

(10) In order to integrate the records referred to in paragraphs three and four of this Article with the records referred to in paragraph six of this Article, a tax number or unique personal ID number (EMŠO) or registration number of a business entity shall be used concerning personal data.

Article 137 (Contents of records)

(1) In the records on customers, business relationships and transactions managed by obliged persons, the following data shall be processed for the purpose of implementing the provisions of Article 16 of this Act:

1. company name, address, registered offices, registration number, and tax number of:
 - legal entities,
 - sole traders, or
 - self-employed personsentering into a business relationship or performing a transaction, or on behalf of which a business relationship is being entered into or a transaction is being performed;
2. personal name, permanent or temporary address, date and place of birth, tax number or unique personal ID-no. (EMŠO), nationality, and the number, type and name of the authority that issued the official personal document:
 - of a natural person or their legal representative, sole trader or self-employed person entering into a business relationship or performing a transaction, or a natural person on behalf of whom a business relationship is being entered into or a transaction is being performed;
 - of a legal representative of a legal entity entering into a business relationship or performing a transaction,
 - of an authorised person of a natural person, sole trader, or a self-employed person entering into a business relationship or performing a transaction,
 - of an authorised person entering into a business relationship or performing a transaction on behalf of a legal entity or other civil law entity referred to in point 5 of Article 3 of this Act;
3. the personal name, address of the permanent or temporary residence, and date and place of birth of the natural person entering a casino or gaming hall to whom profit has been paid or who places a bet as referred to in point 3 of paragraph one of Article 17, or of a natural person approaching a safe;
4. the purpose and intended nature of the business relationship, including information about the activity of the customer;
5. the date of entering into the business relationship or the date and time of entering a casino or gaming hall or approaching a safe;
6. the date and time of the transaction;
7. the amount of the transaction and currency in which the transaction is being carried out;
8. the purpose of the transaction and the personal name and permanent and temporary residence or name and registered office of the person/entity to whom the transaction is intended, and the state, to which the transaction was sent;
9. the manner of executing the transaction;
10. information about the source of assets or property that is, or will be, the subject of a business relationship or transaction;

11. the personal name, permanent or temporary address, date and place of birth, and tax number or unique personal ID no. (EMŠO), nationality and number, type and name of the authority that issued the official personal document or name of the company, address and registered office and registration number of the person in respect of whom there are grounds to suspect money laundering or terrorist financing;

12. data on the transaction, assets, and property in respect of which there are grounds to suspect money laundering or terrorist financing (amount, currency, type of assets and property, value of assets and property, date or period of execution of transaction);

13. grounds to suspect money laundering or terrorist financing;

14. For beneficial owners referred to in Articles 35, 36, 37, 38, 39, and 40 of this Act:

a) personal name, permanent or temporary address, date of birth, nationality, and the amount of ownership interest or any other type of control;

b) in the case referred to in point b of paragraph one of Article 37 of this Act, provide data on the category of persons who benefit from the foundation and operation of a foreign fund, a foreign institution, or a similar legal entity under foreign law;

15. the name of the other civil law entity referred to in point 5 of Article 3 of this Act and the personal name, permanent or temporary address, date and place of birth and tax number or unique personal ID-no. (EMŠO) of the member.

(2) In the records managed by obliged persons concerning the data reported to the Office, the data referred to in paragraph one of this Article shall be processed for the purpose of implementing the provisions of Articles 68 and 69 of this Act.

(3) In the records managed by the Bank of Slovenia concerning contact points, the following data shall be processed for the purpose of implementing the provisions of Article 73 of this Act:

1. the personal name, permanent or temporary address, date and the place of birth, tax number or unique personal ID-no. (EMŠO), nationality, and the number, type and name of the authority that issued the official personal document of the natural person who was appointed as the central contact point;

2. the company name, address, registered office, registration number and tax number of the legal entity appointed as the central contact point.

(4) In records managed by the Financial Administration of the Republic of Slovenia concerning declared and undeclared importation or export of cash in the amount of €10,000 or more when entering or leaving the European Union, the following data shall be processed for the purpose of implementing paragraphs one and two of Article 120 of this Act:

1. the personal name, permanent or temporary address, date and place of birth, tax number or unique personal ID-no. (EMŠO), nationality, and the number, type and name of the authority that issued the official personal document of the natural person who imports or exports cash across European Union borders;

2. the company name, address, registered office, registration number and tax number of a legal entity, or the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) and nationality of a natural person on whose behalf cash is being imported or exported across the border of the European Union;

3. the company name, address, registered office, registration number and tax number of a legal entity, or the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) and nationality of a natural person who is the intended recipient of the cash;

4. amount, currency and type of cash being imported or exported across the border of the European Union;

5. source and intended use of cash being imported or exported across the border of the European Union;

6. date, place and time of crossing the border of the European Union;

7. information on whether the importation or export of cash has been reported to the Financial Administration of the Republic of Slovenia.

(5) In the records managed by the Financial Administration of the Republic of Slovenia concerning the importation or export of cash, or the attempted importation or export of cash in an amount less than €10,000 when entering or leaving the European Union if there are grounds to suspect money laundering or terrorist financing, the following data shall be processed for the purpose of implementing paragraph three of Article 120 of this Act:

1. the personal name, permanent or temporary address, date and place of birth, tax number or unique personal ID-no. (EMŠO), nationality, and the number, type and name of the authority that issued the official personal document of the natural person who imports or exports or attempts to import or export cash across European Union borders;

2. the company name, address, registered office, registration number and tax number of a legal entity, or the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) and nationality of a natural person on whose behalf cash is being imported or exported across the border of the European Union;

3. the company name, address, registered office, registration number and tax number of a legal entity, or the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) and nationality of a natural person who is the intended recipient of the cash;

4. the amount, currency and type of cash being imported or exported across the border of the European Union;

5. the source and intended use of cash being imported or exported across the border of the European Union;

6. the place, date and time of crossing or attempting to cross the European Union border;

7. the grounds for suspecting money laundering or terrorist financing.

(6) In the records managed by the Office of the data on persons and transactions acquired pursuant to Articles 68 and 69 of this Act, the data referred to in paragraph one of this Article shall be processed for the purpose of implementing the provisions of Article 87 hereof.

(7) In the records managed by the Office of the initiatives received under Articles 99 and 100 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 87 and 113 of this Act:

1. the personal name, permanent or temporary address, date and place of birth, and tax number or unique personal ID no. (EMŠO), and number, type and name of the authority that issued the official personal document or name of the company, address and registered office and registration number and tax number of the person in respect of whom there are grounds to suspect money laundering or terrorist financing;

2. data on the transaction in respect of which there are grounds to suspect money laundering or terrorist financing (amount, currency, date or period of execution of transaction);

3. the grounds for suspecting money laundering or terrorist financing or grounds for initiating the procedure to confiscate assets of unlawful origin.

(8) In the records managed by the Office of the notifications and information referred to in Articles 101 and 102 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 87 and 113 of this Act:

1. the personal name, permanent or temporary address, date and place of birth, and tax number or unique personal ID no. (EMŠO), and number, type and name of the authority that issued the official personal document or name of the company, address and registered office and registration number and tax number of the person in respect of whom the Office sent the notification or information;

2. data on the transaction in respect of which there are grounds for suspecting money laundering (amount, currency, date or period of execution of transaction);

3. data on previous criminal offence(s);

4. data on the authority to which the notification or information was sent.

(9) In the records managed by the Office of international requests under Articles 105 and 106 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 87 and 113 of this Act:

1. the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) and number, type and name of the authority that issued the official personal document or name of the company, address and registered office and registration number and tax number of the person to which the request refers;

2. the name of the country and the name of the authority to whom the request was sent, or of the authority issuing the request.

(10) In the records managed by the Office of personal data sent abroad referred to in Articles 105, 106, 107, and 108 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 87 and 113 of this Act:

1. the personal name, permanent or temporary address, date and place of birth, and tax number or unique personal ID no. (EMŠO), and number, type and name of the authority that issued the official personal document or name of the company, address and registered office and registration number of the person whose data is sent from the country;

2. the name of the country and name of the authority to whom the data are being sent.

(11) In the records managed by the Office of criminal offences under Article 121 of this Act, the following data shall be processed for the purpose of centralising and analysing all data on money laundering and terrorist financing:

1. the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) or the company name, address, registered office, registration no., and tax number of the person against whom a complaint is filed, or a charged person or a person with regard to whom the temporary security of the claim for the confiscation of proceeds of unlawful activities was ordered;

2. the place, time and manner with respect to which the action which has signs of a criminal offence was committed;

3. the phase of the procedure in which the matter is currently processed, and the legal classification of the offence of money laundering, predicate criminal offence, and terrorist financing;

4. the amount of money seized or the value of unlawfully acquired assets and the date of forfeiture.

(12) In the records managed by the Office of criminal offences under Article 121 of this Act, the following data shall be processed for the purposes defined by the Act governing minor offences and for the purpose of centralising and analysing all data on money laundering and terrorist financing:

1. the name and surname, address of permanent and temporary residence, date and place of birth, tax number or unique personal ID-no. (EMŠO) or the company name, address, registered office, registration no., and tax number of the person, against whom minor offence proceedings related to a minor offence under this Act are taken before minor offence authorities or the court;

2. the place, time and manner of committing the action which has signs of a minor offence;

3. the phase of the process in which the matter is being processed, and the legal classification of the minor offence;

4. the amount of money seized or the value of unlawfully acquired assets and the date of forfeiture.

(13) In the records managed by the Office of completed supervisions, violations discovered, issued decisions and other measures taken with respect to noted offences by the supervisory bodies referred to in Article 139 of this Act, the following data shall be processed for the purpose of implementing the provisions of Article 152 of this Act:

1. data on the obliged person – natural person (personal name, unique personal ID no. (EMŠO) if the natural person is a foreigner, and the date and place of birth and permanent or temporary address);

2. data on the obliged person – legal entity (name, registered office and registration number);

3. the place and time of supervision;

4. the subject of supervision;
5. findings;
6. data on the supervisory measures imposed;
7. data on the offender – natural person (personal name, unique personal identification number (EMŠO) or, if a foreigner, date and place of birth, citizenship and permanent or temporary address of the natural person, and for the responsible person of a legal entity, also employment and tasks and duties performed by him/her);
8. data on the offender – legal entity (name, registered office and registration number);
9. case reference number and the date of issue of a decision concerning a minor offence;
10. date of the finality of the decision concerning a minor offence;
11. legal classification of a minor offence;
12. description of the offence.

(14) In the records managed by the Office of the notified facts referred to in Article 153 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 87 and 113 of this Act:

1. personal name, permanent or temporary address, date and place of birth, and tax number or unique personal ID no. (EMŠO), nationality, and number, type and name of the authority that issued the official personal document or name of the company, address and registered office, registration number and tax number of the person in respect of whom there are facts that might be related to money laundering or terrorist financing;
2. data on the transaction in respect of which there are facts that are or may be associated with money laundering or terrorist financing (amount, currency, date or period of executing the transaction);
3. description of facts that are associated with or may be associated with money laundering or terrorist financing.

(15) In the records managed by the Office of the submission of data referred to in Articles 116, 117 and 118 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 87 and 113 of this Act:

1. personal name, permanent or temporary address, date and place of birth, tax number or unique personal ID no. (EMŠO), and nationality, and number, type and name of the authority that issued the official personal document or name of the company, address and registered office, registration number, and tax number of the entity in respect of which the court, state prosecutor's office, the police, the Financial Administration of the Republic of Slovenia, or an authority competent for introducing or implementing restrictive measures accessed the data of the Office;
2. data on the transaction in respect of which the court, state prosecutor's office, the police, the Financial Administration of the Republic of Slovenia, or an authority competent for introducing or implementing restrictive measures accessed the data of the Office (amount, currency, date, or period of executing transactions);
3. the description of the circumstances and grounds for submitting the data of the Office and of the purpose for the use of the requested data.

(16) In the records managed by business entities concerning beneficial owners, the following data shall be processed for the purpose of implementing the provisions of Articles 35, 36, and 37 of this Act:

1. personal name, permanent or temporary address, date of birth, nationality, and the amount of the ownership interest or any other type of control;
2. in the case referred to in point b of paragraph one of Article 37 of this Act, provide data concerning the category of persons who benefit from the foundation and operation of a foreign fund, a foreign institution, or a similar legal entity under foreign law.

(17) Notwithstanding the provisions of the preceding paragraphs, the records referred to in Article 136 of this Act shall not include the registration number and/or tax number in the case of non-residents and if a registration number has not been provided to a non-resident.

Article 138

(Records of access to data, information and documentation by supervisory bodies)

(1) The obliged person shall keep separate records of access to data, information and documentation referred to in paragraph one of Article 122 hereof by the supervisory bodies referred to in Article 139.

(2) The records referred to in paragraph one of this Article shall contain the following information:

1. name of the supervisory body;
2. personal name of the official person authorised by the supervisory body who inspected the data;
3. date and time of inspecting the data;
4. the data, information, and documentation which were accessed by the supervisory body.

(3) Any access to the data referred to in paragraph one of this Article by the supervisory bodies referred to in Article 139 hereof shall be reported to the Office by the obliged person in writing and at the latest within three working days following the inspection of said data.

CHAPTER IX SUPERVISION

9.1 Supervisory bodies

Article 139 (Supervisory bodies and their activity)

(1) Supervision of the implementation of the provisions of this Act and the ensuing regulations shall be exercised within their competencies by:

- a) the Office,
- b) Bank of Slovenia,
- c) Securities Market Agency
- d) Insurance Supervision Agency,
- e) Financial Administration of the Republic of Slovenia
- f) Market Inspectorate of the Republic of Slovenia,
- g) Agency for Public Oversight of Auditing, and the Slovenian Institute of Auditors,
- h) Bar Association of Slovenia, and
- i) Chamber of Notaries of Slovenia

(2) If, in exercising supervision, the supervisory body referred to in paragraph 1 of this Article establishes offences referred to in Articles 91, 163, 164, 165, 166, 167, 168, 169 and 170 hereof, it shall have the right and duty to:

1. order measures to remedy the irregularities and deficiencies within a time limit that it specifies;
2. carry out proceedings in accordance with the law regulating offences;
3. propose the adoption of appropriate measures to the competent authority;
4. order other measures and perform acts for which it is authorised by law or any other regulation.

(3) Offence proceedings shall be led and decided on by an official person authorised by the supervisory body referred to in paragraph one of this Article that meets the conditions stipulated by the stated Act and the regulations adopted on the basis therein.

Article 140 (Supervision and risk assessment)

(1) With regard to the supervision of the obliged persons referred to in Article 4 of this Act, an approach based on money laundering and terrorist financing risks shall be used.

(2) When planning the frequency, scope, intensity, and implementation of supervision, the supervisory bodies referred to in the preceding Article shall take into account:

- data concerning discovered risks of money laundering or terrorist financing from the national risk assessment,
- data concerning specific national or international risks related to clients, products, and services,
- data concerning the risk of individual obliged persons, and other available data and
- important events or modifications related to the management of the obliged person, and any change of activities.

(3) When planning and carrying out inspections, the Bank of Slovenia, the Securities Market Agency, and the Insurance Supervision Agency shall also take into account the guidelines provided by European supervisory bodies.

(4) The Office shall suggest to the other supervisory bodies referred to in the preceding paragraph that they implement supervision of a particular obliged person or type of obliged persons, depending on the information and data available to the Office and depending on the performed strategic and operational analyses.

Article 141
(General competencies of the Office)

(1) The Office shall perform supervision of the implementation of the provisions of this Act by the obliged persons referred to in Article 4 of this Act.

(2) The Office shall supervise the implementation of the provisions of this Act by collecting and verifying data, information and documentation obtained on the basis of the provisions of this Act.

(3) The obliged persons shall submit to the Office in writing the data, information and documentation on the performance of their duties as provided by this Act, as well as other information which the Office requires for conduct supervision, without delay and at the latest within eight days of receiving the request.

(4) The Office may also demand from state authorities and from holders of public authority all data, information and documentation required for exercising supervision under this Act and for conducting offence proceedings.

9.2 Inspection performed by the Office

Article 142
(Competencies of the Office concerning inspection)

(1) In addition to the supervision carried out by supervisory bodies pursuant to Articles 140 and 141 of this Act, inspection of the implementation of this Act and other regulations in the field of the discovery and prevention of money laundering and terrorist financing shall be performed by the Office on- and off-site.

(2) Within the scope of the report referred to in Article 119 of this Act, the Office shall also report to the Government on its work in the field of inspection control.

Article 143
(Inspector for the prevention of money laundering)

The tasks of inspection control provided by the Office are carried out by officials. Officials under this Act shall be inspectors for the prevention of money laundering.

Article 144
(The application of the Act)

The inspector for the prevention of money laundering shall independently perform supervisory tasks under this Act, manage procedures, and issue decisions in administrative and minor offence proceedings.

Article 145
(Service ID card)

(1) The inspector shall prove their authorisation to perform inspection-related tasks by showing the service ID card issued by the minister competent for finances.

(2) The form of the card and the procedure for issuing it shall be decided by the minister competent for finances, unless set forth otherwise by a special Act.

Article 146
(Authorisations of the inspector)

(1) In addition to the authorisations set forth by the Act governing inspection control, the inspector for the prevention of money laundering shall also be authorised to the following when performing inspection control tasks related to a natural person or legal entity:

- to enter and inspect premises, land, and means of transport (hereinafter: premises) at the registered offices of the obliged persons and elsewhere;
- to inspect the internal acts, books of account, business correspondence, records, and other data and documentation referring to the operation of the obliged person and the implementation of measures to discover and prevent money laundering and terrorist financing, regardless of the storage media in which the data is recorded or stored (hereinafter: books of account and other documentation);
- to confiscate or obtain copies, forensic copies or extracts from books of account and other documentation in any format by using the photocopying devices and computer equipment of the obliged person or the Office; if copies cannot be made by using the photocopying devices and computer equipment of the obliged person or the Office due to technical reasons, the inspector may take the books of account and other documentation and keep them as long as is necessary to make copies; an official note concerning this shall be made;
- to seal all business premises and books of account and other documentation for the period and to extent required to perform supervision;
- to confiscate items and books of account and other documentation for a maximum of 20 working days;
- to require from any representative of the obliged person (hereinafter: representative) or person employed at the obliged person to provide an oral or written clarification concerning facts or documents referring to the object or purpose of supervision, and to draft minutes on this; if the inspector requires a written clarification, a deadline for submitting such clarification shall be fixed;
- to inspect documents by means of which the identity of persons may be verified;
- to perform other actions in accordance with the purpose of supervision.

(2) The obliged person shall enable the inspector access to its premises and its books of account and other documentation, and it shall not interrupt the performance of inspection control in any way, unless attorney-client privileges are being enforced. At the request of the inspector, the obliged person shall enable working conditions at its premises.

(3) In exercising the authorisations of the inspector for preventing money laundering referred to in paragraph one of this Article, the principle of proportionality shall be observed. When exercising the authorisations and imposing measures relating to the obliged person, the inspector shall not exceed that which is necessary to fulfil the objectives of this Act. When selecting from multiple authorisations and measures, the inspector shall select those that are the most favourable for the obliged person if this fulfils the purpose of the Act. When doubt arises, the matter shall be decided to the benefit of the obliged person.

(4) The inspector for preventing money laundering shall inform the Bar Association of Slovenia beforehand concerning the tentative time and location of the planned inspection control in order to secure the presence of their representative during inspection control.

(5) The attorney in whose office the inspection control is being carried out and the law firm where the inspection control is being carried out shall be entitled to require that the inspection control be carried out in the presence of a representative of the Bar Association of Slovenia. All actions related to inspection control shall be suspended pending the arrival of the representative, but not for longer than two hours from the times when the attorney or the law firm request their presence. After this period expires, the supervision shall continue without their presence.

(6) When carrying out inspection control tasks at an attorney's office or at a law firm, the inspector for preventing money laundering shall be entitled to exercise the authorisations referred to in paragraph one of this Article, unless the exercise of these authorisations would violate attorney-client privileges.

(7) In the inspection control procedure, the attorney, the law firm, or the representative of the Bar Association of Slovenia, if present, shall be entitled to object to the inspection of data and documents or their confiscation in order to protect attorney-client privileges. In the event of an objection, the procedure shall continue by applying, *mutatis mutandis*, the provisions of the Act governing criminal proceedings.

Article 147 (Interfering with supervision)

If an obliged person fails to allow entry to their premises or interferes with such entry, or fails to allow access to books of account and other documentation or interferes with such access, or if it interferes with the performance of inspection control in any other way, or if there are grounds to expect this, the inspector may enter the premises or access books of account or other documentation against the will of the obliged person with the assistance of the police, unless the obliged person is an attorney or a law firm. The costs of entry or access and any damages shall be borne by the obliged person.

Article 148 (Minutes)

(1) Minutes shall be drafted on the performed inspection control, which must include the following information in particular:

- on the beginning and end or the duration of the inspection control,
- information on the obliged person,
- the actual state of affairs discovered,
- the statements given by persons present at the inspection control,
- the confiscation of documentation,
- the authorised official carrying out the inspection and any other persons present during the inspection.

(2) For the needs of the management of the minor offence procedure, the minutes referred to in the preceding paragraph shall also include data pursuant to the Act governing minor offences, in particular:

- data on the perpetrator of the minor offence: name and surname, unique personal ID number (EMŠO), date and place of birth, nationality, residence, or the name, registered offices, and registration number of the legal entity, employment of the responsible person,
- place and time of the minor offence,
- legal classification of the minor offence.

**Article 149
(Decision)**

(1) Following an inspection, the inspector shall be competent to issue a decision to the obliged person to ensure that an action is taken or omitted, or an act is issued securing the enforcement of laws and other regulations in the inspector's jurisdiction within a deadline determined by the inspector.

(2) An appeal against the decision referred to in the preceding paragraph shall be permitted within fifteen days from the date of receipt. An appeal shall not stay the implementation of the decision.

(3) The obliged person shall report to the inspector concerning the execution of the decision within eight days after the expiry of a particular deadline for its execution.

**Article 150
(Appeal body)**

Appeals against a decision referred to in paragraph one of the preceding Article shall be decided on by the ministry competent for finances.

9.3 The competencies of other supervisory bodies

**Article 151
(Other supervisory bodies)**

(1) The Bank of Slovenia, in accordance with its competencies stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by the obliged persons referred to in points 1, 2, 3, 15, 16 and 20 d) of paragraph 1 of Article 4 hereof and by other entities.

(2) The Securities Market Agency, in accordance with its competences stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by the obliged persons referred to in points 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 of paragraph one of Article 4 hereof and by other entities. It shall only perform supervision of the obliged persons referred to in points 1, 2, and 3 of paragraph one of Article 4 hereof with regard to the services and activities of the obliged person's investment banking activities and regarding matters to which the provisions of the Act governing the financial instruments market apply. It may perform supervision independently or in cooperation with the Bank of Slovenia.

(3) The Insurance Supervision Agency, in accordance with its competencies stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by the obliged persons referred to in points 11, 12, 13, 14, 20 i), and 20(j) of paragraph one of Article 4 hereof and by other entities.

(4) The Financial Administration of the Republic of Slovenia, in accordance with its competencies stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by the obliged persons referred to in point 18 of paragraph one of Article 4 hereof and by other entities.

(5) The Financial Administration of the Republic of Slovenia, in accordance with its competencies, shall exercise supervision of the implementation of prohibitions against the acceptance of payments for goods and performed services in cash in an amount exceeding €5,000 by legal entities and natural persons referred to in Article 67 of this Act.

(6) The Market Inspectorate of the Republic of Slovenia, in accordance with its competencies stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by the obliged persons referred to in points 19, 20(a), 20(b), 20(h), 20(n), and 20(r) of paragraph one of Article 4 hereof and by other persons.

(7) The Agency for Public Oversight of Auditing and the Slovenian Institute of Auditors, in accordance with its competencies stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by the obliged persons referred to in point 17 of paragraph one of Article 4 hereof and by other persons or entities.

(8) The Bar Association of Slovenia, in accordance with its competencies stipulated herein and in other acts, exercise shall supervision of the implementation of the provisions of this Act by lawyers, law firms and other persons.

(9) The Chamber of Notaries of Slovenia, in accordance with its competencies stipulated herein and in other acts, shall exercise supervision of the implementation of the provisions of this Act by notaries and other persons.

(10) The supervisory bodies referred to in this Article shall forward to any other supervisory body, upon its request, all necessary information required by that supervisory body to conduct its supervisory tasks.

9.4 Reporting data on supervision

Article 152 (Notification of violations and measures)

(1) The supervisory bodies referred to in Article 139 herein shall immediately notify the Office in writing concerning supervisions performed, violations discovered, decisions issued and other supervisory measures, and other significant findings.

(2) The notification referred to in the preceding paragraph shall contain all the data referred to in paragraph thirteen of Article 137 of this Act.

(3) A supervisory body which detects a violation shall also inform other supervisory bodies of its findings and/or any irregularities if relevant to their work.

(4) To enable the centralisation and analysis of all data related to money laundering and terrorist financing, supervisory bodies shall also forward to the Office a copy of any decision issued concerning a violation, as well as any decisions or orders by means of which other measures have been imposed.

Article 153 (Notifying facts)

(1) The supervisory bodies referred to in Article 139 hereof shall immediately notify the Office in writing if, during supervision under this Act or during the performance of their activities or business operations in accordance with the competencies stipulated in other acts, they establish or discover facts that indicate or may indicate money laundering or terrorist financing.

(2) On the basis of the notified facts referred to in paragraph one of this Article, the Office, if it deems appropriate, may start collecting and analysing data, information and documentation in compliance with its authorisations stipulated by this Act.

9.5 Issuing recommendations and guidelines

Article 154 (Issuing recommendations and guidelines)

With a view to ensuring uniform implementation of the provisions of this Act and the ensuing regulations by obliged persons, the supervisory bodies referred to in Article 139 hereof shall independently, or in cooperation with other supervisory bodies, issue recommendations and guidelines on the implementation of individual provisions of this Act by the obliged persons referred to in Article 4 hereof.

Article 155 (National cooperation)

(1) The Office and other supervisory bodies referred to in Article 139 of this Act shall cooperate in the performance of their tasks and authorisations when carrying out supervision, and they shall make efforts to ensure the effectiveness of measures and supervision in combating money laundering and terrorist financing.

(2) The Office and other supervisory bodies referred to in Article 139 of this Act shall, to the greatest extent possible, endeavour to unify supervisory practices and, in this context, also to ensure the comparability of the methodological approach when carrying out measures and supervision.

9.6 Cooperation with competent supervisory bodies of Member States, third states, and European supervisory bodies

Article 156 (Cooperation with the competent supervisory authorities of Member States)

(1) The Office and other supervisory bodies referred to in Article 139 of this Act shall cooperate with bodies of Member States which are competent for supervision in the field of preventing money laundering and terrorist financing, specifically with regard to the supervision of obliged persons that mainly operate through subsidiaries and affiliates in the Republic of Slovenia and other Member States in which they do not have registered offices.

(2) The Office and other supervisory bodies referred to in Article 139 of this Act shall cooperate with competent supervisory bodies from other Member States, particularly by exchanging all information that could help facilitate the supervision of obliged persons.

Article 157 (Cooperation with the competent supervisory authorities of third countries)

(1) The Office and other supervisory bodies referred to in Article 139 of this Act shall cooperate with bodies of third states which are competent for supervision in the field of preventing money laundering and terrorist financing, specifically with regard to the supervision of obliged persons that mainly operate

through subsidiaries and affiliates in the Republic of Slovenia and in third states, in which they do not have registered offices.

(2) The Office and other supervisory bodies referred to in Article 139 of this Act shall cooperate with competent supervisory bodies from third states, particularly by exchanging all information that could help facilitate the supervision of obliged persons.

(3) Cooperation with competent supervisory bodies from third states shall be possible if, in these third states, there are established standards for preventing money laundering and terrorist financing, which are equivalent to the provisions of this Act, of international standards, or other regulations.

Article 158 (Cooperation with European supervisory bodies)

(1) The Bank of Slovenia, the Securities Market Agency, and the Insurance Supervision Agency shall provide European supervisory bodies with all information that is required to enable the performance of their tasks related to preventing money laundering and terrorist financing.

9.7 Violation notification system

Article 159 (Internal violation notification system)

(1) An obliged person shall establish a violation notification system, which enables employees and persons in comparable positions to internally report violations of the provisions of this Act through independent and anonymous reporting channels.

(2) The system referred to in the preceding paragraph shall include clearly defined procedures for receiving and processing reports which are proportionate to the nature and size of the obliged person.

(3) When the identity of a person filing the report is disclosed despite the provision referred to in paragraph one of this Article, the obliged person shall ensure that all data on the persons who filed a report concerning violations are processed as confidential, pursuant to the Act governing the protection of personal data. The obliged person shall not disclose this information without the prior consent of the person filing the report, unless the disclosure of the identity of the person filing the report is needed to carry out a pre-trial investigation of criminal proceedings.

Article 160 (A system for notifying supervisory bodies concerning violations)

(1) The supervisory bodies referred to in Article 139 of this Act shall establish an effective and reliable notification system which enables employees and persons in comparable positions working for obliged persons to file reports concerning possible or actual violations of the provisions of this Act.

(2) With regard to the notification system referred to in the preceding paragraph, the supervisory bodies referred to in Article 139 of this Act shall ensure the following:

a simple and easily accessible method for filing reports on violations,
internal procedures for accepting and processing reports,

suitable protection of the personal data of persons who filed a report against an obliged person, and of persons who are allegedly responsible for a violation, pursuant to the provisions of the Act governing the protection of personal data.

(3) It shall not be permitted to disclose the data referred to in point 3 of the preceding paragraph without the prior consent of both the person filing the report and the person allegedly committing a violation, unless the disclosure of their identity is needed to carry out a pre-trial investigation and criminal proceedings in accordance with the Act. The supervisory bodies referred to in Article 139 of this Act shall not disclose the data on the person filing the report or the person allegedly committing the violation to the obliged person against which a report has been filed. The supervisory bodies referred to in Article 139 of this Act shall endeavour to prevent the disclosure of the identity of the person filing the report and the person allegedly committing the violation when discovering and processing violations which are the object of the report.

9.8 Disclosures related to supervision

Article 161

(Disclosure of information on measures imposed)

(1) For the purpose of preventing and discouraging actions that are considered to be violations of this Act, the supervisory bodies referred to in Article 139 of this Act shall publicly publish information on supervisory measures and sanctions imposed due to violations of this Act.

(2) The information referred to in the preceding paragraph shall include the following data:

1. on the person committing the violation and the obliged person against which a measure is taken:
 - the name and registered office of a legal entity or
 - the personal name of a natural person;
2. on the violation or the nature of the measure imposed:
 - a description of the circumstances and actions that are considered to be a violation of this Act or necessitate the imposition of the measure concerned,
 - the nature of the violations discovered or the type of deficiencies due to which a measure was imposed:
3. the operative part of the decision by means of which the proceedings were finally concluded;
4. on the possible elimination of the violation or the performance of the measure that has been ordered.

(3) Once the decision by means of which a violation has been discovered, a measure imposed, or a minor offence declared becomes final and the obliged person against which the measure is to be imposed is informed of such decision, the information referred to in paragraph two of this Article shall be published on the websites of the supervisory bodies referred to in Article 139, and it shall be accessible on the websites for five years following the publication. The purpose of the publication of the information referred to in the preceding paragraph is to prevent the violation of statutory provisions and, as a result, to provide greater legal security when persons enter into business relationships and improve the integrity of the business environment, and to inform the interested public on the operation of businesses which operate in the business environment and with legal transactions in the field of regulations concerning the prevention of money laundering and terrorist financing.

(4) The Bank of Slovenia, the Securities Market Agency, and the Insurance Supervision Agency shall forward the information referred to in paragraph two of this Article to competent European supervisory bodies.

Article 162
(Disclosure of the identity of the person committing a violation)

(1) Notwithstanding paragraphs one and two of the preceding Article, the supervisory bodies referred to in Article 139 of this Act shall not publish the information on the identity of the person committing the violation and the obliged person against which measures will be imposed if:

1. the supervisory measure or sanction has been imposed due to minor violations as referred to in Article 165 of this Act, or

2. the publication of information on the identity of the person committing a violation or the obliged person against which a measure is to be imposed could inhibit the conduct of a pre-trial investigation or criminal proceedings.

(2) If the supervisory bodies referred to in Article 139 of this Act find upon issuing a decision that, relating to the publication of the identity of the person committing a violation, there are grounds as referred to in the preceding paragraph whereby, in addition to issuing a decision by means of which they impose supervisory measures, they shall also decide:

- not to publish the identity of the person committing a violation, or
- to suspend publication of the identity of the person committing a violation and to state a time limit on the suspension of publication if it is deemed that the grounds for suspending publication will cease to exist during this period.

CHAPTER X – PENAL PROVISIONS

Article 163
(The gravest violations)

(1) A fine of €12,000 to €120,000 shall be imposed for an infringement on a legal entity:

1. if they fail to draft a risk assessment or determine a risk assessment of a particular group or type of client, business relationship, transaction, product, service, or distribution path, and take into account geographic risk factors, or fail to carry out a suitable assessment of the impact on risk exposure of changes in business processes (paragraphs two and six of Article 13 of this Act);
2. if they fail to carry out measures related to in-depth client due diligence, even though it is deemed that the client, business relationship, transaction, product, service, distribution path, country, or geographic area may pose an increased risk (paragraph two of Article 14 of this Act);
3. if they fail to establish effective policies, controls, and procedures for effective risk mitigation and management (paragraph one of Article 15 of this Act);
4. if they fail to carry out customer due diligence (paragraph one of Article 17 and paragraph four of Article 22 hereof);
5. if they establish a business relationship with a customer without prior application of the prescribed measures (paragraph one of Article 19 hereof);
6. if they effect a transaction without prior application of the prescribed measures (Article 20 hereof);
7. if, prior to marketing a product (paragraph three of Article 22 hereof), they fail to inform the Office concerning a planned partial omission of customer due diligence, and if they fail to attach documentation on the fulfilment of conditions and risk assessment referred to in paragraph one of Article 22 to the notification;
8. if they fail to determine and verify the identity of a customer which is a natural person or his/her statutory representative, a sole trader or self-employed person of a statutory representative of a legal entity, authorised person of a natural person, sole trader or self employed person, legal entity, an agent of other civil law entities or a beneficial owner, or fail to obtain the prescribed data, or failure to obtain them in the prescribed manner, or fail to obtain the certified written authorisation or a written authorisation for representation (Articles 23, 24, 25, 28, 29, 35, 36, 37 and 43 hereof);

9. if they determine and verify the identity of a customer by using electronic identification means in a prohibited manner (paragraph five of Article 26 hereof);
10. if they determine and verify the identity of a customer by using video-electronic identification in a prohibited manner (Article 27 hereof);
11. if they fail to determine or verify the identity of a customer upon the customer's entry to a casino or gaming hall of a concessionaire who organises games of chance, or each time the customer accesses a safe, or if they fail to acquire the prescribed data or if they fail to acquire them in a prescribed manner (Article 30 hereof);
12. if, contrary to the provisions of the Act, they determine and verify the identity of banks and similar credit institutions which have registered offices in a high-risk third state as referred to in paragraph five of Article 50 (paragraph three of Article 31);
13. if they fail to keep data and documentation acquired with regard to determining the beneficial owner, pursuant to the provisions of this Act (paragraph three of Article 34);
14. if they fail to obtain data on the purpose and intended nature of the business relationship or transaction, as well as other data pursuant to this Act, or fail to obtain all the required data (Article 48 hereof);
15. if the obliged person entered into a business relationship in contravention of the provisions of this Act (paragraph five of Article 54 hereof);
16. if they carry out simplified customer due diligence even though they fail to assess, pursuant to paragraph one of Article 14 of this Act, that the customer, the business relationship, transaction, product, service, distribution path, country, or geographic area pose a negligible threat (paragraph one of Article 57 hereof);
17. if they fail to obtain by simplified customer due diligence the prescribed data on a customer, business relationship or transaction, or if they fail to obtain the data in the prescribed manner (Article 58 hereof);
18. if they fail to apply the prescribed measures and, in addition, obtain data, information and documentation in accordance with paragraph one of Article 60 when entering a correspondent banking relationship with a bank or other similar credit institution located in a third state, or fail to obtain the data in the prescribed manner (paragraphs one and three of Article 60 hereof);
19. if they enter into or continue, contrary to law, a correspondent banking relationship with a respondent bank or other similar credit institution located in a third state (paragraph five of Article 60 hereof);
20. if it fails to obtain data on the source of funds and property that are, or will be, the subject of a business relationship or transaction when entering into a business relationship or effecting a transaction on behalf a customer who is a politically exposed person, or for failure to obtain the data in the prescribed manner (point 1, paragraph six of Article 61 hereof);
21. if it fails to establish and carry out measures with regard to politically exposed persons in life insurance transactions and life insurance linked to units of investment funds (Article 62 hereof);
22. if it fails to carry out measures by means of in-depth customer due diligence when the customer is from a high-risk third state (Article 63 hereof);
23. if they open, issue or keep for a customer anonymous accounts, passbooks or bearer passbooks, or other products enabling, directly or indirectly, concealment of the customer's identity (Article 64 hereof);
24. if they enter into a business relationship or carry out a transaction referred to in Articles 17 and 18 of this Act, even though the customer reports the ownership of a legal entity or a similar entity under foreign law based on bearer shares the traceability of which is not enabled through a central securities clearing corporation or a similar register (Article 65 hereof);
25. if they enter into or continue a correspondent banking relationship with a bank that operates or may operate as a shell bank, or other similar credit institution known to allow shell banks to use its accounts (Article 64 hereof);
26. if they accept cash payment from a customer or third person when selling goods or performing individual services exceeding the amount of €5,000, or accepting payment effected by several linked cash transactions exceeding in total the amount of €5,000 (paragraphs one and two of Article 67 hereof);

27. they fail to furnish the Office with the prescribed data within a statutory time limit, when grounds to suspect money laundering or terrorist financing exist in connection with a customer or transaction or an intended transaction (Article 69 hereof);
28. if they fail to submit to the Office, within the prescribed time limit, the required data, information and documentation, if in respect of a transaction, a person, or property or assets there are grounds to suspect money laundering or terrorist financing (Article 91 hereof);
29. if they fail to comply with the Office's order temporarily suspending a transaction or the Office's instructions issued in this regard (Article 96 and paragraphs one and three of Article 110 hereof);
30. if they fail to comply with the Office's written order for continuous monitoring of a particular customer's financial transactions (paragraphs one, two and three of Article 98 hereof);
31. if they disclose to a customer or a third person the facts referred to in paragraph one of Article 122 hereof;
32. if they fail to remedy irregularities and deficiencies within the time limit as specified by an official authorised person (point 1 of paragraph two of Article 139 hereof);
33. if they fail to submit to the Office, within the prescribed time limit and in the prescribed manner, data, information and documentation on the performance of duties as provided by this Act, as well as other information which the Office requires to conduct supervision (paragraph three of Article 141 hereof);
34. if they fail to enable access to premises and books of account and other documentation to the inspector for preventing money laundering, or hinders the inspector in any other way in the exercise of his authorisations (paragraph two of Article 146 hereof);

(2) A fine from €4,000 to €40,000 shall be imposed on a sole trader or self-employed person for the offence referred to in the preceding paragraph.

(3) A fine from €800 to €4,000 shall be imposed on the responsible person of a legal entity, the responsible person of a sole trader or a self-employed person for the offence referred to in paragraph one of this Article.

(4) If the nature of the offence referred to in points 1 to 22 of paragraph one is particularly grave due to the amount of the damage caused or the amount of unlawfully acquired proceeds, due to the perpetrator's intent or their intention to gain self-interest, due to the recurrent or systematic nature of the offence, the legal entity shall receive a fine in an amount up to:

1. €1,000,000, or
2. an amount that is double the proceeds acquired by means of the offence if such proceeds can be determined and if this amount exceeds the amount referred to in the preceding point.

(5) If the nature of the offence referred to in points 1 to 22 of paragraph one is particularly grave due to the amount of damage caused or the amount of unlawfully acquired proceeds, due to the perpetrator's intent or their intention to gain self-interest, due to the recurrent or systematic nature of the offence, a sole trader or a self-employed person shall receive a fine in an amount up to:

1. €500,000, or
2. an amount that is double the proceeds acquired by means of the offence if such proceeds can be determined and if this amount exceeds the amount referred to in the preceding point.

(6) A responsible person of the legal entity referred to in paragraph four of this Article and a responsible person of a sole trader or a self-employed person as referred to in paragraph five of this Article shall be fined an amount up to €250,000.

(7) A legal entity as referred to in paragraph four of this Article which is a credit or financial institution shall be fined in the amount of:

1. €5,000,000, or
2. 10% of the total annual turnover in the preceding business year, provided that this amount exceeds the amount referred to in the preceding point.

(8) If the legal entity referred to in the preceding paragraph is an entity, a credit or financial institution that controls one or more controlled companies, or that is an affiliate, the consolidated annual report shall be taken into account with regard to the data on the total annual turnover in the preceding business year, pursuant to the Act governing companies.

(9) A sole trader or self-employed person as referred to in paragraph five of this Article which is a credit or financial institution shall be fined in the amount of:

1. €2,500,000, or
2. 10% of the total annual turnover in the preceding business year, provided that this amount exceeds the amount referred to in the preceding point.

(10) A responsible person of a legal entity referred to in paragraph seven of this Article and a responsible person of a sole trader or self-employed person referred to in paragraph nine of this Article shall be fined an amount up to €500,000.

(11) In addition to the fine, a permanent or temporary suspension of the permission to perform activities shall also be ordered against the legal entity referred to in paragraphs four and seven of this Article and against the sole trader or self-employed person referred to in paragraphs five and nine of this Article if the legal entity, sole trader, or self-employed person requires such permission to perform their activities.

(12) The order to permanently or temporarily suspend the permission to perform activities referred in the preceding paragraph shall be issued by the body which issued such permission in proceedings instituted by the body itself or upon the proposal of the Office.

(13) In addition to a fine, a temporary ban on the performance of leadership tasks shall also be imposed against a responsible person as referred to in paragraphs six and ten of this Article.

(14) The order to temporarily ban the performance of leadership tasks referred to in the preceding paragraph shall be issued by the body which allowed the performance of leadership tasks in proceedings instituted by the body itself or upon the proposal of the Office.

Article 164 (Grave violations)

(1) A fine of €6,000 to €60,000 shall be imposed for an infringement on a legal entity:

1. if they fail to carry out customer due diligence to the prescribed extent (paragraph one of Article 16 hereof);
2. if they fail to define procedures for implementing the measures referred to in paragraph one of Article 16 in its internal regulations (paragraph five of Article 16 hereof);
3. if they fail to demand a written statement from a customer, legal representative, authorised person or agent of other civil law entities (paragraph three of Article 23, paragraph four of Article 24, paragraph four of Article 25, paragraph five of Article 28 and paragraph five of Article 29 hereof);
4. if they fail to carefully monitor business activities undertaken by a customer through the obliged person (paragraph one of Article 49 hereof);
5. if they fail to acquire the prescribed data when verifying and updating data (paragraphs two and three of Article 49 hereof);
6. if they entrust a third party with the performance of customer due diligence without having verified whether this third party meets all the conditions stipulated by this Act (paragraph two of Article 51 hereof);
7. if they accept customer due diligence as appropriate in which a third party determined and verified the identity of a customer in the customer's absence (paragraph three of Article 51 hereof);

8. if they entrust customer due diligence to a third party which is a shell bank or other similar credit institution which does not or may not pursue its activities in the country of registration (paragraph six of Article 52 hereof);
9. if they entrust customer due diligence to a third party, whereby the customer is a foreign legal entity which is not or may not be engaged in trade, manufacturing or other activity in the country of registration (Article 53 hereof);
10. if the obliged person fails to define the procedure for determining foreign politically exposed persons in its internal act (paragraph one of Article 61 hereof);
11. if they enter into a business relationship with a customer who is a foreign politically exposed person, but does not monitor with due diligence the transactions and other business activities carried out by that person (point 3, paragraph six of Article 61 hereof);
12. if they fail to furnish the Office, within the prescribed time limit, with the prescribed data on any cash transaction exceeding €15,000 (paragraph one of Article 68 hereof);
13. if they fail to furnish the Office, within the prescribed time limit, with the prescribed data on any cash transaction exceeding €15,000 and executed on the accounts referred to in paragraph two of Article 68 (paragraph two of Article 68 hereof);
14. if they fail to ensure the implementation of the policies and procedures of the group to which they belong regarding measures for discovering and preventing money laundering and terrorist financing (paragraph one of Article 71 hereof);
15. if they fail to ensure that its branches and majority-owned subsidiaries with head offices in third countries apply the measures for detecting and preventing money laundering and terrorist financing stipulated by this Act (paragraph one of Article 75 hereof);
16. if they fail to appoint an authorised person and one or more deputies for particular tasks of detecting and preventing money laundering and terrorist financing stipulated by this Act and the ensuing regulations (Article 76 hereof);
17. if they fail to provide an authorised person with appropriate authorisations, conditions and support to perform his/her duties and tasks (Article 79 hereof);
18. if they fail to draw up a list of indicators for identifying customers and transactions in respect of which there are reasonable grounds to suspect money laundering or terrorist financing, or if they fail to draw up the said list in the prescribed manner and time limit (Article 85 hereof);
19. if they fail to keep data and documentation for five years after the termination of a business relationship, completion of a transaction, or the customer's entry to a casino or gaming hall or access to a safe (paragraph one of Article 129 hereof).

(2) A fine from €2,000 to €20,000 shall be imposed on a sole trader or a self-employed person for the offence referred to in the preceding paragraph.

(3) A fine from €400 to €2,000 shall be imposed on a responsible person of a legal entity, sole proprietor or self-employed person for the offence referred to in paragraph one of this Article.

Article 165 **(Minor violations)**

(1) A fine of no less than €3,000 to €30,000 shall be imposed for an infringement on a legal person:

1. if they fail to examine in advance, when verifying the identity of a customer, the nature of the register from which data on the customer is to be obtained (paragraph six of Article 28 hereof);
2. if they fail to ensure that the scope and frequency of measures referred to in paragraph one of Article 49 are appropriate to the risk of money laundering or terrorist financing to which the obliged person is exposed when carrying out individual transactions or in business operations with individual customers (paragraph four of Article 49 hereof);

3. if they fail to inform the competent supervisory bodies referred to in Article 139 of this Act and take appropriate measures to eliminate the risk of money laundering or terrorist financing (paragraph four of Article 75 hereof);
4. if they fail to ensure that the work of an authorised person or his/her deputy is entrusted solely to a person meeting the prescribed requirements (paragraphs one and two of Article 77 hereof);
5. if they fail to forward to the Office, within the prescribed time limit, the personal name and title of the position held by the authorised person and his/her deputy and any changes thereof (paragraph five of Article 79 hereof);
6. if they fail to provide regular professional training to all employees carrying out tasks for the prevention and detection of money laundering and terrorist financing pursuant to this Act (paragraph two of Article 80 hereof);
7. if they fail to draw up, within the prescribed time limit, the annual professional training and education programme for the prevention and detection of money laundering and terrorist financing (paragraph four of Article 80 hereof);
8. if they fail to ensure regular internal control of the performance of tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act (Article 81 hereof);
9. if they fail to use the list of indicators referred to in paragraph one of Article 85 when determining the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto (paragraph three of Article 85 hereof);
10. if they fail to keep the data and corresponding documentation concerning the authorised person and their deputy, the professional training of employees, the performance of internal control and risk management referred to in Articles 13, 76, 77, and 80 of this Act for four years after appointing the authorised person and their deputy, the completed professional training, and performed internal control and the analysis of impacts due to changes in the obliged person's business processes related to the risk of money laundering or terrorist financing (paragraph three of Article 129 of this Act).
11. if they fail to keep separate records of access to data, information and documentation referred to in paragraph one of Article 122 hereof which was held by the supervisory bodies referred to in Article 139, or for keeping incomplete records (paragraphs one and two of Article 138 hereof);
12. if they fail to inform the Office within the prescribed time limit and in the prescribed manner of any access by the supervisory bodies referred to in Article 139 hereof to the data, information, and documentation referred to in paragraph one of Article 122 (paragraph three of Article 138 hereof).

(3) A fine in the amount of €1000 to €10,000 shall be imposed on a sole trader or a self-employed person who commits the offence referred to the preceding paragraph.

(2) A fine of no less than €200 to €1,000 shall be imposed on the responsible person of a legal entity, the responsible person of a sole trader or the responsible person of a self-employed person, for an offence referred to in paragraph one of this Article.

Article 166 **(Offences committed by issuers of electronic mean of identification)**

(1) A fine from €12,000 to €120,000 shall be imposed for the offence of an issuer of electronic means of identification if they fail to submit to the obliged person, upon its request, data on the manner of determining and verifying the identity of the customer that is the holder of the electronic means of identification (paragraph four of Article 26 hereof).

(2) A fine from €800 to €4,000 shall be imposed on the responsible person of an issuer of electronic means of identification for the offence referred to in paragraph one of this Article.

Article 167 **(Offences committed by business entities related to data on the beneficial owner)**

(1) A fine of €6,000 to €60,000 shall be imposed for an infringement on a legal entity:

1. if they fail to discover data or if they discover false data on their beneficial owner or owners; if they fail to establish and manage precise records of data concerning their beneficial owners, or if they fail to update such records upon each modification of data, or if they fail to keep the data on their beneficial owners for five years following the date of the termination of beneficial owner status (paragraphs one, two, three, and four of Article 41 of this Act);
2. if they fail to furnish, without undue delay, any data concerning their beneficial owners, or if they furnish false data upon the request of obliged persons or bodies for detecting and prosecuting criminal offences, courts, and the supervisory bodies referred to in Article 130 of this Act (Article 42 hereof);
3. if they fail to enter into the register any data concerning their beneficial owner and their modifications, or if they enter false data within eight days following their entry in the Slovenian Business Register or following their entry in the tax register, if they have not been entered in the Slovenian Business Register, or within eight days following any modification of data (paragraph three of Article 44 of this Act).

(2) A fine between €400 and €2,000 shall be imposed for an offence on a responsible person of a legal entity who commits the offence referred to in the preceding paragraph.

Article 168 (Offences committed by employees working for an obliged person)

(1) A fine from €200 to €1,000 shall be imposed for an offence committed by an employee working for an obliged person establishing the correspondent relationship referred to in paragraph one of Article 60 and carrying out the enhanced customer due diligence procedure if he/she fails to obtain the written consent of his/her superior responsible person in the obliged person holding a senior leadership position prior to entering into such a relationship (paragraph two of Article 60 hereof).

(2) A fine from €200 to €1,000 shall be imposed for an offence by an employee working for an obliged person who carries out the procedure for entering into a business relationship with a customer who is a foreign politically exposed person if he/she fails to obtain the written consent of his/her superior responsible person holding a senior leadership position prior to entering into such a relationship (point 2 of paragraph six of Article 61 hereof).

Article 169 (Specific offences by auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services)

(3) A fine from €12,000 to €120,000 shall be imposed for an offence by an auditing firm for carrying out simplified due diligence procedure despite the fact that in respect of the customer or auditing circumstances, grounds to suspect money laundering or terrorist financing exist (paragraph six of Article 57 hereof).

(4) A fine from €4,000 to €40,000 shall be imposed for an offence by an independent auditor for carrying out simplified due diligence procedure despite the fact that in respect of the customer or auditing circumstances, grounds to suspect money laundering or terrorist financing exist (paragraph six of Article 57 hereof).

(5) A fine from €12,000 to €120,000 shall be imposed for an offence by an auditing firm or a legal entity performing accounting or tax advisory services if they fail to report to the Office, within the prescribed time limit, data concerning all cases in which a customer has sought advice on money laundering or terrorist financing (paragraph five of Article 69 hereof).

(6) A fine from €4,000 to €40,000 shall be imposed for an offence by an independent auditor or a self-employed person performing accounting or tax advisory services if they fail to report to the Office, within the prescribed time limit, data concerning all cases in which a customer has sought advice on money laundering or terrorist financing (paragraph five of Article 69 hereof).

(7) A fine from €400 to €2,000 shall be imposed on the responsible person of a legal entity, of a sole trader, or of self-employed person for the offence referred to in paragraphs one, two, three, or four of this Article.

Article 170
(Offences by lawyers, law firms and notaries)

(1) A fine from €12,000 to €120,000 shall be imposed for an offence by a law firm if it fails to report to the Office, within the prescribed time limit, that a client has sought advice on money laundering or terrorist financing (paragraph two of Article 83 hereof).

(2) A fine from €4,000 to €40,000 shall be imposed for an offence by a lawyer or notary for failing to inform the Office, within the prescribed time period, that a client sought advice on money laundering or terrorist financing (paragraph two of Article 83 hereof).

(3) A fine from €12,000 to €120,000 shall be imposed for an offence by a law firm for failing to submit to the Office, within the prescribed time limit, the required data, information and documentation, if in respect of a transaction, person, property, or assets there are grounds to suspect money laundering or terrorist financing (paragraphs one, two and three of Article 92 hereof).

(4) A fine from €4,000 to €40,000 shall be imposed for an offence by a lawyer or notary for failing to submit to the Office, within the prescribed time limit, the required data, information and documentation, where in respect of a transaction, person, property, or assets there are grounds to suspect money laundering or terrorist financing (paragraphs one, two and three of Article 92 hereof).

(5) A fine of €800 to €4,000 shall be imposed on a responsible person of a law firm, lawyer, or notary if they commit the offence referred to in paragraphs one, two, three, or four of this Article.

Article 171
(Imposing fines in fast-track proceedings for minor offences)

A fine in an amount which is higher than the lowest prescribed amount specified by this Act may be imposed in a fast-track procedure for offences referred to in this Act.

Article 172
(Application of provisions concerning minor offences)

Until amendments to the provisions concerning the amounts and ranges of fees stipulated by the Act governing minor offences are introduced, the amounts and ranges of fees determined in Article 163 hereof shall be applied regardless of the provisions of the Act governing minor offences.

CHAPTER XI TRANSITIONAL AND FINAL PROVISIONS

Article 173 (Implementing regulations)

(1) The Government shall adopt the decree referred to in paragraph five of this Act at the latest within six months after becoming familiar with the report on the risk assessment carried out by the Financial Administration of the Republic of Slovenia in cooperation with the Office.

(2) Until the decree referred to in the preceding paragraph is adopted, the obliged persons determined in points 12, 13, and 14 of paragraph one of Article 4 of the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia [Uradni list RS], Nos. 60/2007, 19/2010, 77/2011, 108/2012 and 19/2014) shall be deemed the obliged persons referred to in point 18 of paragraph one of Article 4 of this Act.

(3) The Government shall adopt the decree referred to in paragraph four of Article 9 of this Act at the latest within six months after becoming familiar with the report on the findings of the national risk assessment which will be carried out pursuant to this Act.

(4) The minister competent for finance shall adopt the rules referred to in:

- paragraph one of Article 26,
- paragraph five of Article 27,
- paragraph five of Article 30,
- paragraph three of Article 57,
- paragraph three of Article 59,
- paragraph six of Article 68,
- Article 70,
- Article 82, and
- paragraph two of Article 145

of this Act at the latest within six months following its entry into force.

(5) At the latest within six months of the entry into force of this Act, the minister responsible for the economy shall issue, in agreement with the minister responsible for finance, the rules referred to in paragraph eight of Article 45 of this Act.

Article 174 (Issuing guidelines)

Within one year following the entry into force of this Act, the supervisory bodies referred to in Article 139 of this Act shall issue the guidelines referred to in Article 154 of this Act.

Article 175 (Performance of a risk assessment)

Within six months following the issue of the guidelines referred to in the preceding Article, obliged persons shall draft a risk assessment pursuant to Article 13 of this Act concerning individual groups or types of customers, business relationships, transactions, products, services, or distribution paths, taking into account geographic risk factors relating to possible abuse for the purpose of money laundering or terrorist financing.

Article 176

(Discovering and entering data concerning beneficial owners into the Register of beneficial owners)

(1) Within one year following the entry into force of this Act, business entities shall discover the data concerning their beneficial owner or owners pursuant to Article 41 hereof.

(2) Within fourteen months following the entry into force of this Act, business entities shall enter the data concerning beneficial owners pursuant to Article 44 hereof into the register of beneficial owners.

Article 177

(Discovering beneficial owners)

Within two years following the entry into force of this Act, obliged persons shall, pursuant to the provisions of this Act, discover the beneficial owner of existing customers.

Article 178

(Determining politically exposed persons)

(1) Within two years following the entry into force of this Act, obliged persons shall discover whether existing customers, their legal representatives, authorised persons, or beneficial owners are politically exposed persons as referred to in Article 61 hereof.

(2) The obligation arising from the preceding paragraph shall apply to those customers, their legal representatives, authorised persons, or beneficial owners, regarding whom there was no obligation to discover whether they are politically exposed persons prior to the entry into force of this Act.

Article 179

(Compliance for anonymous products)

Notwithstanding the provision of Article 64 of this Act, the obliged person shall carry out, in respect of anonymous products existing on the day this Act enters into force, and for which it is impossible to identify the owner, due diligence regarding customer or other user of the product, in accordance with Article 16 of this Act, upon the first transaction effected by the customer or other user on the basis of such a product.

Article 180 (Repealing regulations)

(1) On the day that this Act enters into force, the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia [Uradni list RS] Nos 60/2007, 19/2010, 77/2011, 108/2012, and 19/2014) shall cease to be in force.

(2) On the day of entry into force of this Act, the following implementing regulations shall cease to apply:

1. Rules on the determination of the list of equivalent third countries (Official Gazette of the Republic of Slovenia [Uradni list RS], Nos. 10/08, 102/11, and 84/12)
2. Rules laying down conditions for identifying a customer and verifying the customer's identity on the basis of the customer's qualified digital certificate (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 10/08);
3. Rules on the performance of internal control, authorised person, retention and protection of data, and the administration of records within organisations, lawyers, law firms and notaries (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 10/08);
4. Rules laying down conditions under which information on cash transactions executed by certain clients need not be reported (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 10/08);
5. Rules laying down conditions that must be met by a person in order to be allowed to act as a third party (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 10/08);

6. Rules laying down the conditions under which a person may be considered as a customer presenting a low risk of money laundering or terrorist financing (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 10/08);
7. Rules on the Method of Forwarding Information by Lawyer, Law Firm or Notary to the Office for Prevention of Money Laundering of the Republic of Slovenia (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 10/08);
8. Rules on the Method of Forwarding Information to the Office for Prevention of Money Laundering of the Republic of Slovenia (Official Gazette of the Republic of Slovenia [Uradni list RS], no. 90/11).

(3) The implementing regulation referred to in paragraph two of this Article shall apply until new regulations are issued, provided that they are not contrary to this Act.

Article 181

(Entry into force and commencement of application)

This Act shall enter into force on the fifteenth day following its publication in the Official Gazette of the Republic of Slovenia.