Prevention Of Money Laundering And Terrorist Financing Act

(ZPPDFT-2)

SUMMARY DATA
Official Gazette of the Republic of Slovenia [Uradni list RS], No. 48/2022
Date of print: 20 April 2022
Valid clean copy – first release - Validity and/or application: 5 April 2022into the law of the Republic of Slovenia
Notes:
Later date of entry into force of individual provisions of the Act (see Article 193)
Link to the present document at IUS-INFO

CHAPTER I

GENERAL PROVISIONS

1.1 Subject of the Act

Article 1

(Subject of the Act, transposition of the Directives and implementation of the European Union Regulation)

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

This Act shall transpose into the law of the Republic of Slovenia Directive (EU) 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 purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5. 6. 2015, p. 73), last amended by Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to technical regulatory standards for minimum measures and a number of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries (OJ L 125, 14.5.2019, p. 4) (hereinafter: Directive 2015/849/EU).

(2) This Act shall transpose into the law of the Republic of Slovenia Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/PNZ (OJ L 186, 11.7.2019, p. 122; hereinafter: Directive 2019/1153/EU) regarding the exchange of financial analyses and financial information between the competent authorities referred to in Article 3(2) of Directive 019/1153/EU, financial intelligence units of other Member States, the Europol and the Office.

(3) This Act also regulates the implementation of Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls of cash entering or leaving the Union and repealing Regulation (EC) 1889/2005 (OJ L 284, 12.11.2019, p. 6; hereinafter: Regulation (EU) 2018/1672/EU as regards data records acquired pursuant to Articles 3 and 4, Article 5(3) and Article 6 of Regulation (EU) 2018/1672/EU, and the exchange of data between financial intelligence units pursuant to Article 9 of Regulation 2018/1672/EU.

1.2 Definitions and scope of application

Article 2

(Money laundering and terrorist financing)

For the purposes of this Act, the following definitions shall apply:

1. 'Money laundering' means any handling of money or property derived from a criminal offence and includes:

- the conversion or transfer of money or other proceeds of crime;

- the concealment or disguise of the true nature, origin, location, movement, disposition, rights with respect to or ownership of property derived from criminal activity.

2. 'Terrorist financing' means 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 for the carrying out of a terrorist act or other terrorist-related acts or by a terrorist or a terrorist organisation.

3. 'Terrorist act' means a criminal offence defined by **2.** Article of the International Convention for the Suppression of the Financing of Terrorism (Official Gazette of the Republic of Slovenia – International Treaties *[Uradni list RS – Mednarodne pogodbe],* No. 21/04), and terrorist or terrorism related offences as defined in the chapter of the Criminal Code that sets out crimes against humanity.

4. A 'terrorist' is a natural person who:

- commits or attempts to commit a terrorist act;

- is involved in the commission of a terrorist act as an accomplice, aider or abettor;

- arranges the commission of a terrorist act; or

- contributes to the commission of a terrorist act by an individual or a group of individuals operating to achieve a common goal, provided that this contribution is intentional and with the purpose of instigating or perpetuating the terrorist activity or provided that he/she understands the individual's or the group's intent to commit a terrorist act.

5. A 'terrorist organisation' means any group of terrorists that

- commits or attempts to commit a terrorist act;

- participates in committing a terrorist act;

- arranges the commission of a terrorist act; or

- contributes to the commission of a terrorist act by an individual or a group of individuals operating to achieve a common goal, provided that this contribution is intentional and with the purpose of instigating or perpetuating the terrorist activity or provided that he/she understands the individual's or the group's intent to commit a terrorist act.

Article 3
(Other definitions)

For the purposes of this Act, the following definitions shall apply:

1. 'Anonymous electronic money' referred to in Article 27 of this Act is a payment instrument that ensures the anonymity of the payer and prevents the tracking of payments by both electronic money issuers and payees;

2. 'Brokerage firm' means the same as in the Act governing the financial instruments market;

3. 'Tax identification number' means an identification mark assigned to the taxable person under the conditions laid down in the Act governing the tax procedure and the Act governing the financial administration and used in connection with all taxes or for the taxable person's tax purposes; the tax identification number is also considered to be the tax identification number used by non-residents in their country of residence;

4. 'Distribution channel' is a network of individuals or organisations involved in the supply of products or services to end users;

5. 'Other civil law entity' means an organised group of individuals who pool or will pool assets or other property resources for a particular purpose;

6. 'Asset management company' and a 'Member State asset management company' have the same meaning as in the Act governing investment funds and asset management companies;

7. 'Member State' means a Member State of the European Union (hereinafter: EU) or a party to the European Economic Area Agreement;

8. 'Electronic money' has the same meaning as in point 11 of paragraph one of Article 4 of the Payment Services, Services for Issuing Electronic Money and Payment Systems Act (Official Gazette of the Republic of Slovenia *[Uradni list RS],* Nos 7/18 and 9/18 - corrigendum and 102/20; hereinafter: ZPlaSSIED), except monetary value as defined in point 16 and 17 of paragraph one of Article 3 of the ZPlaSSIED;

9. The 'European Supervisory Authorities' include the European Banking Authority (EBA), established under Regulation (EU) 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Supervisory Authority (the European Banking Authority) and amending Decision No. 716/2009/EC (OJ L 331, 15.12.2010, p. 12), last amended by Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) 1093/2010 establishing the European Supervisory Authority (the European Banking Authority), Regulation (EU) 1094/2010 establishing the European Supervisory Authority (the European Insurance and Occupational Pensions Authority), Regulation (EU) 1095/2010 establishing the European Supervisory Authority (the European Securities and Markets Authority), Regulation (EU) 600/2014 on Markets in Financial Instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds (OJ L 334, 27.12.2019, p. 1); hereinafter: Regulation 2019/2175/EU), (hereinafter: Regulation 2020/1093/EU, the European Insurance and Occupational Pensions Authority (EIOPA), established under Regulation (EU) 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European

Supervisory Authority and amending Decision No. 716/2009/EC and repealing the Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48), last amended by Regulation 2019/2175/EU, and the European Securities and Markets Authority (ESMA), established under Regulation (EU) 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Supervisory Authority and amending Decision No. 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84), last amended by Regulation (EU) 2021/23 of the European Parliament and of the Council of 16 December 2020 on the framework for the recovery and resolution of central counterparties and amending Regulations (EU) 1095/2010, (EU) 648/2012, (EU) 600/2014, (EU) 806/2014 and (EU) 2015/2365 and Directives 2002/47/EC, 2004/25/EC, 2007/36/EC, 2014/59/EU and (EU) 2017/1132 (OJ L 22, 22.1.2021, p. 1);

10. 'The European Banking Authority' is the European Supervisory Authority (the European Banking Authority) established by Regulation 1093/2010/EU;

11. 'Factoring' means factoring with or without recourse;

12. 'Fiat currency' means cash funds (paper money, coins, deposit money and electronic money) that is recognised as means of exchange in the issuing country;

13. 'Financial analysis' is the result of an operational or strategic analysis already carried out by the financial intelligence unit in the performance of its tasks under Directive 2015/849/EU;

14. 'Financial institutions' means the obliged entities referred to in points 3, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 15 and sub-point (a) to (i) of paragraph one of Article 4 hereof and for institutions of Member States providing services equivalent to those provided by the persons liable referred to in the aforementioned points of paragraph one of Article 4 of this Act set out in this point;

15. 'Financial intelligence unit' is a central government body established in a Member State or third country for the purpose of monitoring and analysing suspicious transactions and other information on suspected money laundering, related criminal offences and suspected terrorist financing and for transmitting analysis results to competent authorities;

16. 'Financial information' is any information or data, such as data on financial assets, asset movements or financial business relationships, already available to the financial intelligence unit for the purposes of preventing, detecting and effectively combating money laundering and terrorist financing;

17. 'Forfeiting' means financing exports based on purchase with discount and without recourse of long-term outstanding receivables secured by a financial instrument;

18. 'Economic operator' is a company and a sole trader as defined by the Act governing companies, a cooperative as defined by the Act governing cooperatives, and an individual who independently carries out an activity as defined by this Act;

19. 'Cash' means notes or coins in circulation as a means of payment;

20. 'Cash transaction' means any receipt, delivery or exchange of cash in which the obliged entity physically receives cash from the customer or physically hands over cash to the customer for possession and disposal.

21. 'Major criminal offences' are a form of crime as listed in Annex I to Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and on substituting and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5. 2016, p. 53), last amended by Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (OJ L 236 of 19.9.2018, p. 72), (hereinafter: Regulation 2016/2012/EU);

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

23. 'Information about the activity of a customer who is a natural person' means data on a customer's private, professional or other similar engagement (employed, retired, student, unemployed, etc.) or data on a 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;

24. 'investment firm of a Member State' has the same meaning as in the Act governing the financial instruments market;

25. 'Third country investment firm' has the same meaning as in the Act governing the financial instruments market;

26. 'Correspondent relationship' means a correspondent banking relationship between a domestic and a respondent foreign credit (or other similar) institution established by opening the respondent's account with a domestic credit institution (opening a loro account);

27. 'Correspondent agreement" means an agreement concluded by a domestic credit or financial institution with a domestic or foreign credit, financial or similar institution, including for the purpose of conducting securities transactions or transfer of funds;

28. 'Credit institutions' means obliged entities referred to in points 1 and 2 of paragraph one of Article 4 of this Act and Member State entities providing the same kind of services as

the aforementioned obliged entities;

29. 'National risk assessment' is a comprehensive process of identifying and analysing the main risks of money laundering and terrorist financing in a given country, developing appropriate measures to prevent money laundering and terrorist financing based on identified risks and directing available resources as effectively as possible to control, mitigate or eliminate identified risks;

30. 'Senior responsible official holding a position on the management team' means a member of the management who is sufficiently familiar with the obliged entity's exposure to the risks of money laundering and terrorist financing and holds a high enough position to make decisions that affect the obliged entity's exposure to risk and is not necessarily is a management board member;

31. A 'shell bank' means a credit institution or an institution engaged in equivalent activities, registered in a jurisdiction in which it does not perform its services and which is unaffiliated with a supervised or otherwise regulated financial group.

32. 'Non-profit organisations' are societies, institutions, institutes, religious communities and other legal entities not established for the purpose of making profit;

33. 'Non-resident' has the same meaning as in the Act regulating foreign exchange operations;

34. 'Trust and company service provider' means 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 director or secretary of a company or partner, where the person concerned does not actually perform the management function or does not undertake business risks concerning capital contribution in the legal entity where he/she is a partner;

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

acting as or arranging for another person to act as 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;

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

35. 'Regulated market' has the same meaning as in the Act governing the financial instruments market;

36. 'Stock exchange' has the same meaning as in the Act governing the financial instruments market;

37. 'Personal name' consists of a first name and family name, of which each may be composed of several words that form a whole;

38. "34a) "remote payment transaction" as referred to in Article 22 hereof shall have the same meaning as in the act governing payment services, services for issuing electronic money and payment systems;"

39. 'Payment account' has the same meaning as in the act governing payment services, services for issuing electronic money and payment systems;

40. A 'self-employed person' is an individual independently engaged in a gainful occupation;

41. 'Business relationship' means any business or other contractual relationship which is related to the obliged entity's activity, established or entered into by the party with the obliged entity and is, at the time of its establishment, expected to be of a lasting nature, unless otherwise provided by this Act;

42. 'Management' as referred to in Article 42 hereof shall have the same meaning as in the act governing companies;

43. 'Property' means assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, and legal documents or instruments in any form, including electronic, evidencing title to or an interest in such assets;

44. 'Group' is a group of persons consisting of parent and subsidiary entities, its subsidiaries and persons in which the parent or its subsidiary has an equity interest. The group also means associated companies that meet the conditions for a parent company in accordance with the Act governing companies;

45. 'Assets' mean financial assets and economic benefits of every kind, including:

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

b) deposits with obliged entities referred to in Article 4 of this Act;

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

interest, dividends or other income from assets;

d) claims, loans and letters of credit;

e) other documents proving entitlement to assets or other financial sources;

46. 'Electronic identification means" have the same meaning as in Regulation (EU) No. 910/2014 of the European Parliament and Council of 23 July 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);

47. 'Permanent and temporary residence" is information about the street, street number, town, post office and state of permanent and temporary residence, if any;

48. 'Virtual currency services' are the following services provided to third parties by a natural person or legal entity as part of their business or professional activities:

a) exchange services between fiat currencies and virtual currencies;

b) exchange services between one or more types of virtual currencies;

c) transferring virtual currencies among various accounts or titles;

safekeeping or managing virtual currencies, including safeguarding private cryptographic keys on behalf of customers, safekeeping, for the purpose of storing and transferring virtual currencies;

d) services relating to the issuance or sale of virtual currencies;

49. 'Transaction' shall mean any receipt, handover, exchange, safekeeping, disposal or other handling of monies or other property by an obliged entity;

50. 'Third country means' a country other than an EU Member State;

51. 'Alternative investment fund manager' has the same meaning as in the Act regulating alternative investment funds;

52. 'Branch of a Member State AIF manager' has the same meaning as in the Act regulating alternative investment funds;

53. 'Branch of a third country AIF manager' has the same meaning as in the Act regulating alternative investment funds;

54. 'Office' means the Office for Money Laundering Prevention of the Republic of Slovenia;

55. 'Personal identification document' means any valid document bearing a photograph, which is issued by the competent authority of the Republic of Slovenia or other country and is considered to be an authentic instrument under the law of the issuing country;

56. 'Virtual currency' is a digital form of monetary value that is not issued and not guaranteed by a central bank or a state body and not necessarily linked to legally introduced currency and has no legal status of a currency or cash funds, yet is accepted by natural persons and legal entities as means of exchange that can be transferred, stored and exchanged electronically;

57. 'Life insurance' means insurance defined as life insurance by the Act governing insurance business.

Article 4 (Obliged entities)

(1) Measures for detecting and preventing money laundering and terrorist financing set out in this 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 shall be carried out by:

1. banks and their Member State branches, branches of banks from third countries and Member State banks which establish branches in the Republic of Slovenia;

2. savings banks;

3. national payment institutions and payment institutions benefiting from a waiver, and Member State payment institutions and Member State payment institutions which, in accordance with 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;

4. post office if it provides money transmission services (deposits and withdrawals) through postal money orders;

5. brokerage companies;

6. investment funds marketing own fund units in the Republic of Slovenia; if the fund does not manage itself the provisions of this Act that apply to the obliged entity shall apply to the fund's manager;

7. alternative investment fund managing companies and managers providing portfolio management services and non-core services in accordance with the act governing investment funds and management companies or the act governing alternative investment fund managers;

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

9. branches of an investment company in the Republic of Slovenia providing portfolio management services and non-core services in accordance with the act governing investment funds and management companies;

10. branches of a Member State managers or branches of third country alternative investment fund managers in the Republic of Slovenia providing portfolio management services and non-core services in accordance with the Act governing alternative investment fund managers

11. mutual pension fund managers except those in charge of compulsory supplementary pension insurance under the Act governing the system of compulsory supplementary pension and disability insurance, the system of compulsory supplementary pension insurance and the system of voluntary supplementary pension insurance;

12. pension companies;

13. insurance companies authorised to pursue 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 and establish a branch in the Republic of Slovenia;

14. electronic money undertakings, electronic money undertakings benefiting from a waiver, third country branches of electronic money undertakings , and Member State electronic money undertakings which establish branches in the Republic of Slovenia or distribute and realise electronic money in the Republic of Slovenia on their own behalf through a distributor;

15. foreign exchange offices;

16. auditing companies;

17. organisers and concessionaires organising games of chance;

18. pawnshops;

19. legal entities and natural persons in the performance of their business or professional activities;

a) granting credit or loans, including consumer credit, mortgage credit, factoring, and the financing of commercial transactions, including forfeiture;

b) financial leasing;

c) issuing and managing other payment instruments (e.g., bills and traveller's cheques), which are instruments of payment according to the Act governing payment services and systems;

č) virtual currency services or other transactions included in such services;

d) issuing of guarantees and other commitments;

e) portfolio management services to third parties and related advice and state-owned assets management pursuant to the Act governing the Slovenian Sovereign Holding;

f) safe custody services;

g) mediation in the conclusion of loan and credit transactions, except for those legal and natural persons for which brokering represents an ancillary function to their main activity and do not enter into transactions on behalf and for the account of a financial or credit institution (ancillary services credit intermediaries);

h) insurance agency services for the purpose of concluding life insurance contracts;

i) insurance intermediaries in concluding life insurance contracts;

j) accounting services;

k) tax advisory services, direct or indirect material aid, assistance or tax advisory services as main business or professional activity;

l) trust and company services;

m) trade in precious metals and precious stones and products made from these materials;

n) trade or intermediation in works of art, including when these services are performed by art galleries, auction houses and free-trade areas, storage of works of art when performed by free-trade areas;

o) organisation and execution of auctions;

p) real estate business, which includes business with own real estate, renting or operating of own or rented real estate and real estate brokerage;

r) implementation of measures to strengthen the stability of banks of the Republic of Slovenia pursuant to the Act governing Republic of Slovenia's measures to strengthen the stability of banks;

s) transactions in breeding horses;

(2) Pursuant to the provisions of Chapter III hereof, the measures for detecting and preventing money laundering and terrorist financing set out in this Act shall also be applied by lawyers, law firms and notaries; however, only to the extent defined in Chapter IV of this Act.

(3) For the purposes of this Act, the term 'obliged entity' shall refer collectively to the obliged entities referred to in paragraphs one and two of this Article.

(4) Where a natural person carrying out an activity as defined in points 16 and 17, sub-points j), k), l) or p) of point 19 of paragraph one of this Article, or an activity referred to in paragraph two of this Article, carries out this activity within the

framework of an employment relationship with a legal person, a sole trader or a self-employed person, the tasks and obligations under Article 17 of this Act shall apply to a legal person, a sole trader or a self-employed person and not to a natural person.

Article 5
(Register of virtual currency service providers)

(1) A register of virtual currency service providers shall be established for the purpose of supervision over providers of such services concerning the prevention of money laundering and terrorist financing. The register shall be maintained and controlled by the Office.

(2) The providers referred to in the preceding paragraph who have their registered office or a branch in the Republic of Slovenia shall be entered in the register referred to in the preceding paragraph before they start providing virtual currency services.

(3) The request for entry in the register of virtual currency service providers referred to in paragraph one of this Article shall be filed with the Office and shall be enclosed with following information and proof:

- for legal entities, sole traders or individuals performing an activity independently: company name, address, registered office, registration number and tax identification number;

. for their statutory representatives or sole trader activity holders or self-employed persons: full name, address of permanent and temporary residence, personal identification number or date and place of birth, tax identification number, citizenship;

- for their activity: standard classification of activities (SKD, NACE or other similar activity classification code) and the description of the method of providing virtual currency services;

- for their actual owners: full name, address of permanent and temporary residence, date of birth, citizenship, ownership interest or other method of supervision;

- for their statutory representatives or holders of sole trader activity or self-employed person and for their actual owners: extract from criminal records.

(4) The Office shall be notified of changes in information on virtual currency service providers referred to in the preceding paragraph within eight days of the occurrence of the change.

(5) (5) The Office shall dismiss the request for entry in the register if the statutory representative, general manager, sole trader activity holder or an individual performing an activity independently or the actual owner of the provider referred to in paragraph one of this Article have been convicted by a final judgment of a premeditated criminal offence prosecuted ex officio, or of one of the following negligent criminal offences: concealment, disclosure and undue obtaining of professional secrets, money laundering or disclosure of classified information, for as long as legal consequences of the final judgement apply.

(6) The Office shall obtain the information on the fulfilment of the conditions referred to in the preceding paragraph from the applicant who filed the request for entry in the register or from a person who is directly responsible for business operations of the applicant, or ex officio from the official records of competent authorities.

(7) The information referred to in indent one of paragraph three of this Article shall be publicly available.

(8) The Office's decision on entry in the register shall be governed by the provisions of the Act regulating the general administrative procedure.

(9) The minister responsible for finance shall lay down the rules on the establishment and maintenance of the register.

(10) The virtual currency service providers shall notify the Office in writing of the providers involved in their virtual currency services within 10 days of entry in the register referred to in paragraph one of this Article. If the cooperation between the virtual currency service providers and the providers involved in their virtual currency services starts after the entry in the register, the Office shall be notified of this cooperation within ten working days after the start of the cooperation.

Article 6
(Removal from the register of virtual currency service providers)

(1) The Office shall delete a provider from the register referred to in the preceding Article if:

1. the provider no longer meets the criteria for entry in the register referred to in the preceding Article;

2. the provider notifies the Office in writing on the termination of the provision virtual currency services;

3. the provider ceases to exist or bankruptcy proceedings or compulsory winding-up are initiated against the provider subject to the Act governing financial operations, insolvency proceedings and compulsory winding-up; or

4. In supervising the provider, the Bank of Slovenia or the Office establishes violations of the provisions of this Act which are more serious due to the amount of damage caused, the amount of direct or indirect unlawful material gain for the provider or repeated breaches by the provider, increased money laundering or terrorist financing risk.

(2) Virtual currency service providers shall be prohibited from entering into transactions concerning the performance of the

following activities:

1. in the case referred to in point 1 of the preceding paragraph: on the date of service of the decision on removal from the register;

2. in the case referred to in point 2 of the preceding paragraph: on the date of submission of a written notice on the termination of the provision of these services to the Office;

3. in the case referred to in point 3 of the preceding paragraph: on the date that the provider ceases to exist or the date that the initiation of bankruptcy proceedings or liquidation proceedings is officially published;

4. in the case referred to in point 4 of the preceding paragraph: on the date of service of the decision on the commencement of the procedure for removal from the register.

(3) The Office shall initiate the procedure for removal from the register on the grounds set out in point 4 of paragraph one of this Article ex officio or on the proposal of the Bank of Slovenia.

(4) The Office's decision on removal from the register shall be governed by the provisions of the Act regulating the general administrative procedure.

Article 7
(Obliged entities conducting real estate transactions)

The obliged entities referred to in sub-point p) of point 19 of paragraph one of Article4 hereof who rent own or leased property or act as agents in property renting or leasing activities shall implement the tasks referred to in Article 17 hereof if the monthly rent for an individual property amounts to EUR 10,000 or more.

Article 8
(Obliged entities relating to works of art)

The obliged entities referred to in sub-point n) of point19 of paragraph one of Article 4 hereof, who trade in works of art shall implement the measures referred to in Article 17 hereof if the value of a transaction or several linked transactions amounts to at least EUR 10,000.

Article 9
(Exceptions concerning games of chance)

(1) The Government of the Republic of Slovenia (hereinafter: the Government) may determine that the organisers of games of chance referred to in point 17 of paragraph one of Article 4 of this Act, which have a low risk of money laundering or terrorist financing, shall be fully or partly exempt from measures relating to the tasks and obligations referred to in paragraph two of Article 17 of this Act.

(2) The Government shall adopt the legal act referred to in the preceding paragraph after a risk assessment carried out by the Financial Administration of the Republic of Slovenia in cooperation with the Office. The risk assessment shall also take into consideration the following:

- the extent of organising games of chance;

- the vulnerability of individual games of chance and transactions;

- the method of payment used; and

- the findings of the national risk assessment referred to in paragraph one of Article 13 of this Act and the European Commission's report on assessed risks of money laundering and terrorist financing (hereinafter: transnational risk assessments).

(3) The provisions referred to in paragraphs one and two of this Article shall not apply to concessionaires organising special games of chance in casinos or gaming saloons.

(4) The Financial Administration of the Republic of Slovenia shall notify the European Commission of any decision to exempt organisers of games of chance from the implementation of the provisions of this Act.

Article 10
(Special provisions concerning games of chance)

(1) Taking into account the provisions of the Act governing games of chance, a member of the concessionaire's management board who organises special games of chance, persons performing managerial functions at the concessionaire, the actual owner of the concessionaire, a partner or shareholder with significant ownership share or number of shares and their actual owner, shall not be legally convicted by a final judgment to imprisonment for a crime against humanity, life and body, human health, property, the economy, legal transactions, official duty and public authority, or law and order.

(2) The concessionaire referred to in the preceding paragraph shall enclose an extract from criminal records of the ministry responsible for justice with the application for a concession for the operation of specific games of chance.

(3) Taking into account the provisions of the Act governing games of chance, a member of the concessionaire's management board who organises special games of chance, persons performing managerial functions at the concessionaire, the actual owner of the concessionaire, a partner or shareholder with significant ownership share or number of shares and their actual owner, shall not be legally convicted by a final judgment to imprisonment for a crime against humanity, life and body, human health, property, the economy, legal transactions, official duty and public authority, or law and order.

(4) In determining the duration of the prohibition on the activity, the supervisory authority shall take into account the concessionaire's attitude towards the commission of the criminal offence and the attitude towards the consequences of the criminal offence, including the benefit gained.

(5) Compliance with the conditions regarding impunity in accordance with paragraph one of this Article shall be supervised by an authorised person of the supervisory authority who, in accordance with the Act governing games of chance, performs supervisory tasks with the concessionaire.

Article 11
(Exceptions relating to the occasional pursuit of financial activities)

(1) Legal entities, sole traders and self-employed persons who only occasionally or to a limited extent carry out the financial activity referred to in points 15 and sub-points a) to g) of point 19 of paragraph one of Article 4 of this Act and for which there is a low risk of money laundering or terrorist financing, may be exempted from the implementation of the provisions of this Act if the following conditions are met:

1. the financial activity is ancillary and directly related to the main activity;

2. the net annual income of the ancillary financial activity does not exceed EUR 100,000 or does not exceed five percent of the obliged entity's total net annual income;

3. their main activity does thus not comprise the following:

- auditing services;

- organisation of games of chance;

- accounting services;

- tax advisory services;

- real estate activities;

- trust or company services; or

- notary and legal services;

4. the maximum threshold per customer and single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked, may not exceed EUR 1,000; and

5. the financial activity is provided only to the customers of the main activity and is not generally offered to the public.

(2) The preceding paragraph shall not apply to legal persons, sole traders and self-employed persons if they make money transfers in accordance with the Act governing payment services, electronic money issuance services and payment systems.

(3) The persons referred to in the paragraph one of this Article shall file to the Office an application for the permission to suspend the implementation of the provisions of this Act. The application shall be accompanied by documents on compliance with the conditions referred to in paragraph one of this Article and on the performed risk assessment of the financial activity regarding money laundering and terrorist financing. In assessing the risk of money laundering or terrorist financing, Member States shall pay special attention to any financial activity, which is regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

(4) The Office shall issue a decision on the application referred to in the preceding paragraph in accordance with the Act governing the general administrative procedure.

(5) The decision referred to in the preceding paragraph shall be issued for a period of two years. A new application for re-exemption from the implementation of the provisions of this Act shall be submitted in accordance with paragraph three of this Article.

(6) If the circumstances because of which the decision was issued change before the expiry of the decision, the person referred to in paragraph one of this Article shall notify the Office of the changes within fifteen days of their occurrence. On the basis of such notification or other information, the Office may ex officio issue a new decision revoking the previous decision and re-deciding on the permission to suspend the implementation of the provisions of this Act in the light of changed circumstances.

(7) The Office shall inform the European Commission once a year of decisions taken pursuant to this Article.

CHAPTER II
COOPERATION AND NATIONAL RISK ASSESSMENT

Article 12
(Cooperation of competent authorities)

The Office, the supervisory authorities referred to in paragraph one of Article 152 of this Act and other bodies responsible for the prevention and detection of money laundering and terrorist financing shall cooperate and coordinate the implementation of policies and activities to combat money laundering and terrorist financing. In order to achieve the strategic and operational objectives, the competent authorities may conclude cooperation agreements and set up interministerial working groups.

Article 13
(National risk assessment)

(1) In order to identify, assess, understand and mitigate the

risks of money laundering and terrorist financing, the Republic of Slovenia shall carry out a national risk assessment for money laundering and terrorist financing, which shall be updated at least every four years.

(2) The Government shall establish a permanent interministerial working group to carry out a national risk assessment of money laundering and terrorist financing in the Republic of Slovenia. The interministerial working group shall have the following tasks:

1. implementing the national risk assessment of money laundering and terrorist financing in the Republic of Slovenia;

2. drawing up a report on identified national risks of money laundering and terrorist financing;

3. preparing proposals for measures and an action plan to mitigate the identified money laundering and terrorist financing risks;

4. performing other analyses in the field of money laundering and terrorist financing, which require cooperation and coordination between different institutions, and drawing up reports on the analyses carried out.

(3) The activities and the tasks of the interministerial working group referred to in the preceding paragraph shall be directed and coordinated by the Office.

(4) On the basis of the proposal referred to in point 3 of paragraph two of this Article, the Government shall adopt an action plan to mitigate the identified money laundering and terrorist financing risks.

(5) The implementation of the national risk assessment referred to in paragraph one of this Article shall take into account the findings of the transnational risk assessment.

Article 14
(Report and purpose of the national risk assessment)

(1) The Office shall submit to the Government a report on the findings of the national money laundering and terrorist financing risk assessment referred to in point 2 of paragraph two of the preceding Article and shall publicly post an assessment summary and its updates omitting any confidential information.

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

1. improving the national regime for detecting and preventing of money laundering and terrorist financing, in particular by identifying sectors or activities in which obliged entities apply stricter measures regarding customer screening and other obligations under this Act;

2. identifying sectors or activities with a negligible or increased money laundering and terrorist financing risk;

3. prioritising all resources and assets aimed at preventing money laundering and terrorist financing;

4. drawing up suitable regulations for individual sectors or activities in line with the identified money laundering and terrorist financing risks;

5. obliged entities to assist them in the elaboration of their assessments of money laundering and terrorist financing risks (point;

6. reporting on institutional structure and general procedures of national rules on detecting and preventing money laundering and terrorist financing, including a financial intelligence unit, tax authorities and prosecution, and on human and financial resources allocated; and

7. reporting on national efforts as well as on human and financial resources dedicated to combating money laundering and terrorist financing.

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

(4) The government shall identify sectors or activities with a negligible or increased money laundering and terrorist financing risk referred to in point 2 of paragraph two of this Article.

Article 15
(Notifying the Member States and the European institutions)

The Office shall notify the European Commission, European Banking Authority and other Member States of the name of the permanent interministerial working group referred to in paragraph two of Article 13 hereof and of the summary report on the national money laundering and terrorist financing risk assessment referred to in paragraph one of the preceding Article and its updates.

Article 16
(Recommendations of the European Commission)

(1) In the framework of its regulation of the money laundering and terrorist financing prevention, Slovenia may take into account the recommendations of the European Commission on suitable measures to be taken to mitigate the risks identified in the transnational risk assessment.

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

CHAPTER III

DUTIES AND OBLIGATIONS OF OBLIGED ENTITIES

3.1 General provision

Article 17

(Duties and obligations of obliged entities)

(1) For the purpose of detecting and preventing money laundering and terrorist financing, obliged entities shall carry out the tasks set out in this Act and regulations adopted on the basis thereof in the performance of their activities.

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

1. assessing the risk of money laundering and terrorist financing;

2. creating policies and setting up controls and procedures to effectively mitigate and manage the risks of money laundering and terrorist financing;

3. implementing measures to acquire knowledge about the customer (hereinafter: customer due diligence) under the terms and conditions and in the manner provided by this Act;

4. reporting to the Office the required and requested information and submitting documents pursuant to this Act;

5. appointing an authorised person and ensuring conditions for their work;

6. providing regular professional training for employees, and ensuring regular internal control over the performance of duties under this Act;

7. drawing up a list of indicators for the identifying clients 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. implementation of group policies and procedures and measures to detect and prevent money laundering and terrorist financing in own branches and majority-owned subsidiaries in third countries;

10. performing other tasks and duties under this Act and the ensuing regulations.

(3) Obliged entities may perform one or more tasks referred to in the preceding paragraph with the assistance of one or more contractors, except the tasks referred to in points 4, 5, 6, and 9 of the preceding paragraph. If the obliged entity is part of a group, one or more tasks referred to in the preceding paragraph, except for the appointment and performance of the tasks of the authorised person referred to in Article 83 of this Act, may be performed with the assistance of an external contractor who is part of the same group, provided that the conditions of Article 135 have been met.

(4) The obliged entities shall be responsible to ensure that all tasks are carried out by contractors under this Act and the regulations issued on the basis thereof. The responsibility for meeting the obligations under this Act shall lie with the obliged entity that performs individual tasks with the help of an external contractor.

(5) In the conclusion, throughout the duration and on the termination of the contract performed by an external contractor, the obliged entity shall act with due care and diligence and determine in writing the obligations that derive from the contract for the performance of individual tasks. In so doing, the obliged entity shall also consider the provisions concerning the requirements for the outsourcing of personal data processing as defined in Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation (OJ L 119, 4.5.2016, p. 1; hereinafter: the General Data Protection Regulation) in order to appropriately arrange the contractual processing of personal data.

(6) The fact that the obliged entity performs a particular task with the help of an external contractor shall not affect the quality of internal controls or obstruct the supervisory authorities in the performance thereof.

3.2 Risk assessment and risk management

Article 18

(Risk assessment of money laundering and terrorist financing

(1) The risk of money laundering or terrorist financing means 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 entity shall assess the risks associated with individual groups or customers, business relationships, transactions, products or distribution channels by taking into account geographical risk factors with respect to their potential misuse for money laundering or terrorist financing.

(3) On the basis of the risks identified in accordance with the preceding paragraph, the obliged entity shall assess the risk

of its operations (obliged entity risk assessment).

(4) Based on the risks identified in accordance with paragraphs two and three of this Article, the obliged entity shall make an assessment of individual customers' exposure to the risk of money laundering and terrorist financing (customer risk assessment).

(5) Obliged entities who have majority-owned branches and subsidiaries in Member States and third countries shall also carry out a group risk assessment taking into account the risks to which their branches and majority-owned subsidiaries and the group as a whole are exposed (group risk assessment).

(6) The risk assessment and the procedure for determining the assessment of the risk referred to in paragraphs two, three, four and five of this Article shall reflect the specificity of the obliged entity and its operations.

(7) The obliged entity shall make the risk assessment referred to in paragraphs two, three, four and five of this Article in accordance with guidelines issued by and within the powers of the competent supervisory authority referred to in Article 152 of this Act and by taking into account the report on the findings of the national risk assessment and of the transnational risk assessment.

(8) The obliged entity shall document and update the risk assessment findings referred to in paragraphs two, three, four and five of this Article at least every two years. Documented findings shall be made available to the competent supervisory authorities referred to in paragraph one of Article 152 of this Act upon their request.

(9) The obliged entity shall carry out an analysis of the impact of all major changes in its business processes, such as the introduction of a new product, new business practices including new distribution channels, introduction of a new technology or a change in organisation, on the obliged entity's exposure to the risk of money laundering or terrorist financing.

(10) The obliged entity shall carry out the risk assessment referred to in the preceding paragraph before introducing the change referred to in the preceding paragraph and shall adopt appropriate measures in order to reduce the risk of money laundering or terrorist financing in accordance with the findings of the analysis.

Article 19
Insignificant and increased risk of money laundering and terrorist financing

(1) If the obliged entity considers that a customer, business relationship, transaction, product, service, distribution channel, country or geographical area pose a negligible risk of money laundering or terrorist financing, it may implement simplified customer due diligence measures in accordance with the provisions of the Simplified Customer Due Diligence Act (Articles 62 and 63).

(2) If the obliged entity considers that a customer, business relationship, transaction, product, service, distribution channel, country or geographical area poses an increased risk of money laundering or terrorist financing, it shall implement customer due diligence measures in accordance with the provisions of the aforementioned Act on in-depth customer due diligence (Articles 64 to 70).

Article 20
(Management of money laundering and terrorist financing risk)

(1) In order to effectively mitigate and manage identified risks of money laundering and terrorist financing, obliged entities shall establish effective policies, controls and procedures that are in proportion to their activity and size (such as the obliged entity's size and structure, the volume and structure of its business, its customers and the types of products provided).

(2) The policies, controls and procedures referred to in the preceding paragraph shall include the following:

1. development of internal policies, controls and procedures relating to:

- risk management models;

- 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 detection and prevention of money laundering and terrorist financing;

- ensuring compliance with regulations;

- secure employment and, where appropriate, security clearance of employees in accordance with the Act governing classified information;

- staff education and training; and

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

(3) If the obliged entity is a medium-sized or a large company in accordance with the Act governing companies, it shall appoint one of the members of the administrative or management body responsible for carrying out the tasks referred to in the preceding paragraph and for ensuring compliance with the laws and other regulations in the field of

detecting and preventing money laundering and terrorist financing.

(4) In order to effectively mitigate and manage the risks, as set out in paragraph one of this Article, the obliged entities referred to in Article 4 of this Act, who have majority-owned branches or subsidiaries in Member States or third countries, shall establish effective policies, controls and procedures with regard to the risk exposure of the group as a whole. In this respect, the provisions of paragraph two of this Article and other provisions of this Act shall apply mutatis mutandis.

(5) Prior to the introduction of policies, controls and procedures, obliged entities shall obtain the approval of their own management and, in accordance with the guidelines of the supervisory authorities referred to in paragraph one of Article 152 of this Act, monitor and strengthen the adopted measures as necessary.

3.3 Customer due diligence

3.3.1 General provisions

Article 21

(Customer due diligence elements)

(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. determine 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 under this Act;

4. regular monitoring of business activities undertaken by the customer via the obliged entity.

(2) When implementing the measures referred to in points 1 and 2 of the preceding paragraph, the obliged entity shall verify that each person acting on behalf of the customer has the right to represent or has the authorisation of that customer, and in accordance with this Act establish and verify the identity of each person acting on behalf of customers.

(3) In carrying out the measures referred to in paragraph one of this Article, regardless of the form of the customer due diligence, the obliged entity shall also carry out the procedure to determines the political exposure of the customer or beneficial owner in accordance with Article 66 of this Act.

(4) The obliged entity shall implement all customer due diligence measures referred to in paragraphs one and two of this Article, determining the scope of implementation of the measures taking into account the risk of money laundering and terrorist financing.

(5) In determining the scope of implementation of the measures referred to in the preceding paragraph, the obliged entity shall take into account at least the following:

- the purpose of concluding and the nature of the business relationship;

- the amount of assets, the value of assets or the volume of transactions; - the duration of the business relationship; and

- business compliance with the purpose of entering into a business relationship.

(6) The obliged entity shall define procedures for the implementation of the measures referred to in paragraph one of this Article in its internal regulations.

(7) At the request of the supervisory authorities referred to in paragraph one of Article 152 of this Act, the obliged entity shall provide them with appropriate analyses, documents and other data proving the appropriateness of the implemented measures with regard to the identified risks of money laundering and terrorist financing.

Article 22
(Obligation to carry out customer due diligence)

(1) An obliged entity shall apply customer due diligence in accordance with the terms and conditions of this 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 operation or in several operations which are clearly linked;

3. upon the collection of winnings, the placing of a bet or both at organisers of games of chance and concessionaires, when they are transactions amounting to EUR 2,000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which are clearly linked;

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

5. whenever there are grounds for suspicion of money laundering or terrorist financing in respect of a transaction, customer, assets or property, irrespective of the transaction amount.

(2) If an obliged entity enters into an additional business relationship with the customer or performs transactions referred to in points 2 and 3 of the preceding paragraph, the obliged entity shall obtain only the missing data referred to in paragraphs two, paragraphs of Article 53 hereof, provided that it has previously performed due diligence of the customer in the manner specified in Article 21 of this Act, and that it has

ensured proper verification and updating of previously obtained documents and data on the customer as part of the regular monitoring of business activities performed by the customer.

(3) In respect to transactions set out in points 2 and 3 of paragraph one of this Article, the obliged entity shall verify the identity of the customer carrying out the transaction and obtain the required information when the transaction is effected at the checkout point or at other paying and receiving points, depending on the type of the game of chance or the method of playing.

(4) For the purposes of this Act, a customer's registration for participation in a system of organised games of chance with organisers and obliged entities who offer games of chance via the Internet or other telecommunications means, and the performance of transactions referred to in point 3 of paragraph one of this Article by organisers of games of chance and concessionaires shall be deemed as an established business relationship.

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

(6) Pursuant to point 6 of paragraph one of Article 4 of this Act, a customer's accession to the fund rules or other act of an investment fund shall also be deemed as an established business relationship between the customer and the obliged entity. Accession to the rules of another investment fund managed by the same management company or by an alternative investment fund manager shall not be deemed as an established new business relationship under this Act.

Article 23
(Obligation to carry out customer due diligence in occasional transactions)

(1) Notwithstanding the provisions of the preceding Article, an obliged entity shall, under the conditions laid down in this Act, also perform due diligence of a customer in the event of any occasional transaction involving the transfer of funds in excess of EUR 1,000.

(2) The occasional transaction referred to in the preceding paragraph is a transaction performed by a customer who has not entered into a business relationship with the obliged entity.

(3) The transfer of funds referred to in paragraph one of this Article shall mean any transaction, at least partially carried out by electronic means on behalf of the payer through a payment service provider, with a view to making funds available to the payee through the payment service provider. person, notwithstanding whether the payer's and the payee's payment service provider is the same entity, including the following payment services:

1. credit transfer as defined by the Act governing payment services, electronic money issuing services and payment systems;

2. direct debit as defined by the Act governing payment services, electronic money issuing services and payment systems;

3. cash remittance as defined by the Act governing payment services, electronic money issuing services and payment systems notwithstanding whether it relates to domestic or cross-border payments; and

4. transfer effected by means of debit cards, electronic money, mobile telephones or other digital or prepaid or subscription information technology devices with similar characteristics.

Article 24
(Customer due diligence on the establishment of a business relationship)

(1) (1) When establishing a business relationship referred to in point 1 of paragraph one of Article 22 of this Act, an obliged entity shall apply the measures provided for in points 1, 2 and 3 of paragraph one of Article 21 before the business relationship is established.

(2) Notwithstanding the preceding paragraph, an obliged entity may exceptionally implement measures
1. referred to in points 1 and 2 of paragraph one of Article 21 hereof during the establishment of a business relationship with the customer if this is necessary not to interrupt the normal conduct of the obliged entity's business and if, in accordance with Article 18 hereof, there is little risk of money laundering or terrorist financing. In such cases, these measures shall be implemented as soon as possible after the first contact between the obliged entity and the customer, its authorised person or statutory representative.

(3) Notwithstanding paragraph one of this Article, the obliged entity referred to in points 1 and 13 and sub-points h) and i) of point 19 of paragraph one of Article 4 of this Act shall, in addition to due diligence measures, carry out the following due diligence measures for the beneficiaries of payments under insurance policies when concluding life insurance transactions as soon as the beneficiaries are defined or identified:

1. for beneficiaries who, at the time of concluding the transaction, are defined as specific natural or legal entities or similar legal entities under foreign law, the obliged entity shall obtain information about their full name and date of birth;

2. for beneficiaries defined by characteristics, categories or otherwise, the obliged entity shall obtain sufficient information

and data to ensure that their identity can be established and verified at the time of payment.

(4) In instances referred to in points 1 and 2 of the preceding paragraph, the obliged entity shall establish and verify the identity of the beneficiary at the time of payment. In the case of full or partial transfer of life insurance or unit-linked life insurance to a third party, the obliged entity who is aware of the transfer shall identify the new beneficiary at the time of the transfer of insurance to a third party.

Article 25
(Customer due diligence in carrying out transactions)

In carrying out transactions referred to in points 2 and 3 of paragraph one of Article 22 and in Article 23 of this Act, obliged entities shall

3. implement the measures referred to in points 1, 2 and 3 of paragraph one of Article 21 of this Act before carrying out the transactions, taking into account the provisions of paragraph two of Article 22 of this Act.

Article 26
(Non-performance of customer due diligence obligation)

(1) An obliged entity that cannot apply the measures referred to in points 1, 2 and 3 of paragraph one of Article 21 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 reporting data on the customer or transaction to the Office in accordance with Article 76 hereof.

(2) In the cases referred to in the preceding paragraph, obliged entities shall document their conduct and keep the documents in accordance with the provisions of this Act.

Article 27
(Suspension of certain customer due diligence measures relating to electronic money)

(1) The obliged entities referred to in point 14 of paragraph one of Article 4 of this Act may suspend due diligence of the client referred to in points 1, 2 and 3 of paragraph one of Article 21 of this Act if on the basis of a risk assessment they establish that there is an insignificant risk of money laundering or terrorist financing, and provided that the following conditions are met at the same time:

1. regarding a payment instrument:

− data cannot be re-downloaded on it or

− the maximum total monthly payment transactions limit that is credited to or debited from the account does not exceed EUR 150, whereby the payment instrument may be used only in the Republic of Slovenia;

2. the maximum amount of electronic money stored on the payment instrument does not exceed EUR 150;

3. they can be used only to acquire a very limited range of goods or services;

4. anonymous electronic money cannot be used to fund the relevant payment instrument;

5. electronic money issuers sufficiently monitor transactions or business relationships, as provided for in point 4 of paragraph one of Article 21 of this Act to be able to detect unusual or suspicious transactions.

(2) Notwithstanding the preceding paragraph, the customer due diligence referred to in Article 21 hereof shall be conducted before the redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds EUR 50 and, in the case of remote payment transactions, where the amount paid exceeds EUR 50 per transaction.

(3) Remote payment transaction as referred to in the preceding paragraph hereof shall have the same meaning as in the Act governing payment services, services for issuing electronic money and payment systems.

(4) Obliged entities referred to in paragraph one of this Article shall notify the Office of the suspension of certain customer inspection measures prior to the marketing of the product. The notification shall be accompanied by documents on compliance with the conditions and money laundering and terrorist financing risk referred to in paragraph one of this Article.

(5) Notwithstanding the provisions of paragraph one of this Article, the suspension of customer due diligence shall not be permitted when reasons for suspicion of money laundering or terrorist financing exist in connection with the customer, assets, product or transaction.

Article 28
(Prepaid cards issued in third countries)

Credit and financial institutions acting as acquirers may only accept payments carried out with anonymous prepaid cards issued in third countries where such cards meet requirements equivalent to those set out in the preceding Article.

3.3.2 Application of customer due diligence measures

3.3.2.1 Determining and verifying customer identity

Article 29
Determining and verifying customer identity

(1) In relation to

- a customer who is a natural person or their statutory representative, a sole trader, or a self-employed person;

- a statutory representative of a legal entity

obliged entities shall determine and verify their identity and obtain the information referred to in
2. point 10 of paragraph one of Article 150 of this Act by inspecting the customer's identity document in the customer's presence. When not all the required data can be obtained from this document, the missing data is obtained from another valid official document submitted by the customer, or directly from the customer.

(2) When the customer is a sole trader or self-employed person, an obliged entity shall obtain the data referred to in point 1 of paragraph one of Article 150 hereof by applying Article 36 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 entity doubts the reliability or veracity of documents and other business records from which the data has been obtained, it shall also demand a written statement from the customer.

Article 30
(Determining and verifying the identity of authorised representative of a natural person or sole trader or other self-employed person)

(1) When an obliged entity concludes a business relationship on behalf of a customer who is a natural person, sole trader or self-employed person, his or her authorised representative, the obliged entity shall establish and verify the identity of that authorised person and obtain the data referred to in point 2 of paragraph one of Article 150 of this Act by examining the authorised person's official personal identification document in his/her presence. When not all required data can be obtained from the aforementioned document, the missing data shall be obtained from another authentic document submitted by the authorised person or directly from the authorised person. The obliged entity shall obtain the data referred to in point 2 of paragraph one of Article 150 of this Act relating to a natural person, sole trader or self-employed person represented by an authorised representative from a certified letter of authorisation signed by an identified authorising person in the presence of the obliged entity's authorised person, or from a letter of authorisation in electronic form, if the authorising person's signature is certified by a qualified electronic signature in accordance with the regulations governing electronic identification and trust services, which may be considered authentic and appropriate in terms of the completeness of data, date of issue and validity and other circumstances.

(2) If the customer referred to in the preceding paragraph carries out the transaction referred to in point 2 of paragraph one of Article 22 and Article 23 of this Act, the obliged entity shall obtain from the customer a declaration on whether the customer operates on his own behalf or on behalf of a third party. If the customer operates on behalf of a third party, the obliged entity shall act in accordance with paragraph three of this Article. If this transaction is carried out on the basis of a previously established business relationship, the obliged entity shall not be required to obtain the statement referred in the first sentence of this paragraph, but shall only indicate whether the transaction was carried out by the customer or his or her authorised person.

(3) If the transactions referred to in point 2 or 3 of paragraph one of Article 22 hereof is effected on behalf of the customer by his or her authorised person, the obliged entity shall determine and verify the authorised person's identity and obtain the required customer's and the authorised person's data referred to in point 2 of paragraph one of Article 150 hereof as set forth in paragraph one of this Article.

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

Article 31
(Determining and verifying the identity of a legal entity's authorised representative)

(1) An obliged entity shall determine and verify the identity of an authorised person concluding a business relationship in place of a statutory representative on behalf of a legal entity and shall obtain the data referred to in point 2 of paragraph one of Article 150 of this Act by examining the authorised person's official personal identification document in his or her presence. When not all required data can be obtained from the aforementioned document, the missing data shall be obtained from another authentic document submitted by the authorised person or directly from the authorised person. Obliged entities shall obtain the data referred to in point 2 of paragraph one of Article 150 of this Act relating to the statutory representative represented by the authorised person from a certified letter of authorisation issued by the statutory representative whose identity has been established and

verified, signed in the presence of the obliged entity's authorised person, or from a letter of authorisation in electronic form, if the statutory representative's signature is certified by a qualified electronic signature in accordance with the regulations governing electronic identification and trust services, which may be considered authentic and appropriate in terms of the completeness of data, date of issue and validity and other circumstances.

(2) If the customer referred to in the preceding paragraph carries out the transaction referred to in point 2 of paragraph one of Article 22 and Article 23 of this Act, the obliged entity shall obtain from the customer a declaration on whether the customer operates on his own behalf or on behalf of a third party. If the customer operates on behalf of a third party, the obliged entity shall act in accordance with paragraph three of this Article. If this transaction is carried out on the basis of a previously established business relationship, the obliged entity shall not be required to obtain the statement referred in the first sentence of this paragraph, but shall only indicate whether the transaction was carried out by the customer or his or her authorised person.

(3) If the transactions referred to in point 2 or 3 of paragraph one of Article 22 hereof is effected on behalf of the customer by his or her authorised person, the obliged entity shall determine and verify the authorised person's identity and obtain the required statutory representative's and the authorised person's data referred to in point 2 of paragraph one of Article 150 hereof as set forth in paragraph one of this Article.

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

Article 32
(Exception to determining and verifying identity with minimal risk)

(1) Notwithstanding the provisions of Articles 29, 30 and 31 of this Act, the obliged entity may also establish and verify the identity of a customer, statutory representative or authorised person in a way that the customer, statutory representative or authorised person is not present in person if the existence of a minimal risk of money laundering or terrorist financing has been established.

(2) When determining and verifying the identity of the customer, the statutory representative or the authorised person pursuant to the preceding paragraph of this Article, an obliged entity shall obtain the required data on the customer, the statutory representative or the authorised person referred to in point 2 of paragraph one of Article 150 hereof from the copy of the official identification document that is sent by the aforementioned persons to the obliged entity in paper or digital form. When not all the data required can be obtained in the manner described above, the missing data is obtained from the customer directly.

(3) The obliged entity may establish and verify the identity of the customer, the statutory representative or the authorised person in accordance with the provisions of this Article if the obliged entity adopts and implements measures to manage the risks arising from their absence.

Article 33
(Determining and verifying identity using an electronic identification means)

(1) Notwithstanding the provisions of Articles 29, 30 and 31 hereof, the obliged entity may also establish and verify the identity of a natural person on the basis of means of electronic identification of high reliability or on the basis of other methods of electronic identification for accessing electronic services of high reliability in accordance with regulations governing electronic identification and trust services.

(2) Identity may be determined and verified pursuant to the preceding paragraph for

- a customer who is a natural person or their statutory representative, a sole trader, or a self-employed person;

- an authorised person of the customer referred to in the preceding indent;

- a statutory representative and authorised person of a legal entity.

(3) When determining and verifying the identity of the customer pursuant to paragraph two of this Article, an obliged entity shall obtain the required data on the customer referred to in point 2 of paragraph one of Article 150 hereof from the electronic identification means referred to in paragraph one of this Article. Data not available on this certificate shall be obtained from a copy of the official personal identification document sent by the customer to the obliged entity in paper or digital form. When not all the data required can be obtained in the manner described above, the missing data shall be obtained from the customer directly.

(4) Notwithstanding the provisions of paragraphs one and two of this Article, establishing and verifying the identity of a customer using electronic means of identification shall not be permitted if there is a suspicion that the means of electronic identification has been misused or if the obliged entity establishes that circumstances substantially affecting the validity of a certificate have changed but the issuing certification authority has not yet revoked it.

Article 34
Identifying customers and verifying their identity by using video-based electronic identification)

(1) Notwithstanding the provisions of Articles 29, 30 and 31

of this Act, obliged entities may establish and verify the identity of a customer who is a natural person, sole proprietor or self-employed person, statutory representative or authorised person of the customer by using video-based electronic identification, provided the following conditions are met:

1. no increased risk of money laundering or terrorist financing has been identified under Article 18 and paragraph two of Article 19 of this Act;

2. the identity of the customer, statutory representative or authorised person has been established and verified solely on the basis of an official identity document containing a photograph, which shows a clear image of the customer face, and contains at least the customer's full name and date of birth;

3. the customer or his or her statutory representative or authorised person has a permanent place of residence or establishment in a Member State or in a third country that has an effective system in place to prevent and detect money laundering and terrorist financing, and

4. The customer, the customer's statutory representative has no permanent place of residence or establishment in the countries listed in paragraph three of Article 55 of this Act.

(2) The obliged entity shall monitor the customer with due diligence for at least six months after the establishment and verification of identity under this Article.

(3) When determining and verifying the identity of the customer, the statutory representative or the authorised person pursuant to paragraph one of this Article, an obliged entity shall obtain the required data on the customer, the statutory representative or the authorised person referred to in point 2 of paragraph one of Article 150 of this Act.

(4) Data on the customer, statutory representative or authorised person that cannot be obtained during identification and verification of identity of the aforementioned persons pursuant to paragraph one of this Article shall be obtained from the copy of the official identity document that is sent by the aforementioned persons to the obliged entity in paper or digital form. When not all the data required can be obtained in the manner described above, the missing data shall be obtained from the aforementioned persons directly.

(5) The Minister shall determine the minimum technical requirements for video-based electronic identification used in establishing and verifying the identity of the persons referred to in paragraph one of this Article.

Article 35
(Other methods of identifying customers)

In addition to the methods of establishing and verifying the identity of the customers set out in Articles 32, 33 and 34 of this Act, the obliged entity may establish and verify the identity of a customer who is a natural person, sole proprietor or self-employed person, statutory representative or authorised person of the customer including by using other appropriately secure remote controlled or electronic procedures and identification methods, provided that the following conditions are met at the same time:

(1)

1. no increased risk of money laundering or terrorist financing has been identified under Article 18 and paragraph two of Article 19 of this Act;

2. the identity of the customer, statutory representative or authorised person has been established and verified solely on the basis of an official identity document containing a photograph, which shows a clear image of the customer face, and contains at least the customer's full name and date of birth;

3. the customer or his or her statutory representative or authorised person has a permanent place of residence or establishment in a Member State or in a third country that has an effective system in place to prevent and detect money laundering and terrorist financing, and

4. the customer, the customer's statutory representative has no permanent place of residence or establishment in the countries listed in paragraph three of Article 55 of this Act.

(2) The obliged entity shall monitor the customer with due diligence for at least six months after the establishment and verification of identity under this Article.

(3) When determining and verifying the identity of the customer, the statutory representative or the authorised person pursuant to paragraph one of this Article, an obliged entity shall obtain the required data on the customer, the statutory representative or the authorised person referred to in point 2 of paragraph one of Article 150 of this Act.

(4) Data on the customer, statutory representative or authorised person that cannot be obtained during identification and verification of identity of the aforementioned persons pursuant to paragraph one of this Article shall be obtained from the copy of the official identity document that is sent by the aforementioned persons to the obliged entity in paper or digital form. When not all the data required can be obtained in the manner described above, the missing data shall be obtained from the aforementioned persons directly.

(5) The Minister, in agreement with the minister responsible

for information society, shall determine in greater detail the minimum technical requirements for video-based electronic identification used in establishing and verifying the identity of the persons referred to in paragraph one of this Article.

Article 36
(Determining and verifying the identity of a legal entity)

(1) An obliged entity shall determine and verify the identity of the customer (legal entity) and obtain the data referred to in point 1 of paragraph one of Article 150 hereof by inspecting the original or certified documents from the court register or other public register submitted to the organisation by the statutory representative or his/her authorised person on behalf of the legal entity.

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

(3) An obliged entity may determine and verify the identity of a legal entity and obtain the data referred to in point 1 of paragraph one of Article 150 of this Act by inspecting a court or other public register. The obliged entity shall keep information on the date and time of the inspection and the identity of the person who performed the inspection. The extract from the register shall be kept by the obliged entity in accordance with the provisions of this Act and the Act governing the protection and retention of data.

(4) Obliged entities shall obtain other data referred to in paragraph one of Article 150 hereof, with the exception of data on a beneficial owner, by inspecting original or certified documents and other business documents. When all the data referred to in paragraph one of Article 150 hereof cannot be obtained from such documents, the missing data, with the exception of data on the beneficial owner, shall be obtained from the statutory representative or authorised person.

(5) If, in determining and verifying the identity of a legal entity, an obliged entity doubts the reliability of submitted data or veracity of documents and other business records from which the data have 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 one and three of this Article, an obliged entity shall beforehand examine 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 entity shall determine and verify the identity of the foreign legal entity and its branch.

Article 37
(Determining and verifying the identity of other civil law entities)

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

1. determine and verify the identity of the person with powers of representation (hereinafter: the agent);

2. obtain a certified letter of authorisation issued by the agent whose identity has been established and verified, signed in the presence of the obliged entity's representative, or from a letter of authorisation in electronic form, if the agent's signature is certified by a qualified electronic signature in accordance with the regulations governing electronic identification and trust services;

3. obtain the data referred to in points 2 and 15 of paragraph one of Article 150 of this Act.

(2) The obliged entity shall determine and verify the identity of the agent referred to in paragraph one of this Article and obtain the data referred to in point 2 of paragraph one of Article 150 of this Act by examining the agent's official personal identification document in the agent's presence. When not all required data can be obtained from the aforementioned document, the missing data shall be obtained from another authentic document submitted by the agent or directly from the agent.

(3) The obliged entity shall obtain data referred to in point 15 of paragraph one of Article 150 hereof on each natural person that is a member of the civil law entity referred to in paragraph one of this Article from a certified power of attorney for representation issued to the obliged entity by the agent whose identity has been established and verified, signed in the presence of the obliged entity's representative, or from a power of attorney in electronic form, if the agent's signature is certified by a qualified electronic signature in accordance with the regulations governing electronic identification and trust services. When not all the data referred to in point 15 of paragraph one of Article 150 hereof can be obtained from such document, the missing data shall be obtained directly from the agent.

(4) Notwithstanding the provision of point 2 of paragraphs one and three of this Article, when the obliged entity's customer is a community of students, pupils or nursery school children, which forms a part of the education system of the Republic of Slovenia, or a voluntary community of employees operating as a mutual assistance fund of a legal entity's trade union, the obliged entity may only obtain a written power of attorney for representation.

(5) If, in determining and verifying the identity of a person referred to in paragraph one of this Article, the obliged entity

doubts the reliability of submitted data or veracity of documents from which the data have been obtained, it shall require a written statement from the agent prior to entering into a business relationship or effecting a transaction.

Article 38
(Specific cases concerning determination and verification of the identity of a customer)

(1) Pursuant to Article 22 of this Act, a customer's identity shall also be determined or verified in the following cases:

1. upon the customer's entry into a casino or gaming hall run by a concessionaire offering games of chance;

2. each time the customer accesses the safe.

(2) In determining and verifying the identity of the customer pursuant to paragraph one of this Article, a concessionaire offering games of chance in a casino or gaming hall or an obliged entity providing safekeeping services shall obtain the data required under points 3 and 5 of paragraph one of Article 150 of this Act.

(3) Notwithstanding the provisions of Articles 29, 30 and 31 of this Act, the identity of the customer may be established and verified on the basis of an electronic identification card, personal access password and means of video-based electronic identification or means allowing customer identification by way of biometric authentication.

(4) The provisions of this Act concerning the obligation to verify the identity of the customer when accessing the safe shall apply to each natural person actually accessing the safe, notwithstanding whether the person concerned is a party to the safekeeping contract or the party's statutory representative or authorised person and shall be in force only if the identity of all persons has been established and verified in their presence on entering the business transaction.

(5) The Minister shall lay down the minimum technical requirement to be met by safe deposit boxes and video-based means of identification or means allowing the identification of a customer by way of biometric authentication.

Article 39
(Specificities in determining and verifying identity of banks and other credit institutions, their statutory representatives and authorised persons)

(1) The obliged entities referred to in points 1 and 2 of paragraph one of Article 4 of this Act may establish and verify the identity of banks or other credit institutions and their statutory representatives by consistently collecting and evaluating publicly available information about banks or other credit institutions, whereby

1. notwithstanding the provisions of Article 36 of this Act, the identity of a legal entity is established by using sources of information that are common to international banking relations;

2. notwithstanding the provisions of Articles 29 and 31 of this Act, the identity of a legal entity is determined in a manner that is common to international banking relations.

(2) Notwithstanding the provisions of Article 47 of this Act, the obliged entities referred to in the preceding paragraph shall determine the actual owner of a bank of other credit institution in a manner that is common to international banking relations.

(3) This Article shall not apply to establishing and verifying the identity of banks and other similar credit institutions when the bank or other similar credit institution is established in a high-risk third country referred to in paragraph six of Article 55 of this Act.

3.3.2.2 Beneficial owner

3.3.2.2.1 Determining the beneficial owner

Article 40
(Definition)

The beneficial owner is any natural person who is the ultimate owner of the customer, or who supervises or otherwise controls the customer, or the natural person on whose behalf the transaction is carried out.

Article 41
(Obligation to identify the beneficial owner)

(1) The obliged entities referred to in Article 4 of this Act shall identify the customer's beneficial owner as an integral part of due diligence of the customer as set out in Article 21 of this Act, unless this Act provides otherwise.

(2) Business entities shall be required to establish information about their beneficial owners unless otherwise provided by this Act.

(3) Business entities shall retain data and documents obtained in connection with the identification of the beneficial owner in accordance with the provisions of this Act on data retention.

Article 42
(Beneficial owner of a business entity)

(1) Pursuant to this Act, the beneficial owner of a company shall be deemed to be:

1. any natural person that

- directly or indirectly owns a sufficient amount of equity, shares or voting or other rights, shares, voting or other rights

by virtue of which he or she participates in the management of a business entity, or

- has a sufficient direct or indirect participating interest in a business entity, or

- has the controlling position in the management of the business entity's assets;

2. any natural person who indirectly provides funds to an economic operator and, on that basis, has the power to control, direct or otherwise significantly influence the decisions of the economic operator's management when deciding on financing and operations.

(2) An indicator of direct or indirect ownership is the ownership of more than 25% of equity interest, voting or other rights on the basis of which natural persons referred to in the first and second indent of point 1 of the preceding paragraph participate in the management of the legal entity, or ownership of 25% plus one share.

(3) This provisions of the preceding paragraph shall apply mutatis mutandis the determining indirect ownership of a business entity's assets held by a legal entity controlled by

- one or two natural persons or

- one or more legal entities controlled by one or more of the same natural persons.

(4) A natural person that has the controlling position in the management of a business entity or in any other way controls, directs or materially influences the decision-making of the business entity's management board may, inter alia, be determined on the basis of the conditions to be taken into account by a business entity controlling one or more subsidiaries when drawing up the consolidated annual report in accordance with the Act governing companies.

(5) If no natural person is identified as beneficial owner pursuant to this Article, provided that all possible measures have been taken to identify the beneficial owner and provided that there are no grounds for the suspicion of money laundering or terrorist financing in relation to the transaction, person, assets or funds, one or more persons occupying management positions in that business entity shall be considered to be the beneficial owner of that business entity.

(6) If there is any doubt that a natural person is identified as the beneficial owner pursuant to this Article, one or more persons occupying a management position in the aforementioned business entity shall deemed to be the beneficial owner thereof.

Article 43
(Beneficial owner of an entity having no equity interest and beneficial owner of an institution)

(1) Under this Act, any natural person representing such an entity is considered to be the beneficial owner of a society or an association, institution, political party, trade union, religious community or other business entity in which there is no possibility of participating in its management on the basis of a an equity holding, share ownership or a participating interest in its capital unless otherwise determined during due diligence of the customer.

(2) The following shall not be considered as other business entity referred to in the preceding paragraph:

- the Republic of Slovenia;

- self-governing local communities and sub-units thereof

- the government, ministries, bodies within ministries, government agencies, administrative units and other state bodies;

- the Bank of Slovenia;

- public agencies;

- public institutes not co-founded by natural persons or legal entities governed by private law;

- public funds.

(3) Unless determined otherwise during due diligence of a customer, the beneficial owner of an institution under this Act shall, notwithstanding paragraph one of this Article, be considered to be any natural person who is:

1. a founder of the institution if control is exercised on the basis of the act governing institutions and the founder has a controlling position in the management of the institution's assets;

2. a trustee of the institution as defined by the Act governing institutions;

3. a representative of the institution if the founder of the institution cannot be deemed a beneficial owner.

Article 44
(Beneficial owner of a foreign fund, foreign institution or similar foreign law entity)

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

a) any natural person who is

- the founder of a foreign fund, foreign institution or similar foreign law entities;

- the trustee of a foreign fund, foreign institution or similar foreign law entities;

- the beneficiary of the proceeds of the property under management,
provided that future beneficiaries have already been determined or can be determined;

- the potential protector appointed to represent and protect interests of the beneficiaries of the proceeds of property;

b) a category of persons in whose interest the foreign trust, foreign institution or similar foreign law entity has been established and operates, where 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 through direct or indirect ownership or other type of control exercises ultimate control over a foreign trust, foreign institution or similar business entity established under foreign law.

(2) Data and documents on measures taken to identify the beneficial owner of a foreign fund, foreign institution or similar foreign law legal entities pursuant to the preceding paragraph shall be kept by the obliged entity in accordance with the provisions of the Data Retention Act.

3.3.2.2.2 Obligations of business entities

Article 45
Obligations of business entities to identify the beneficial owner)

(1) The business entities referred to in Articles 42 and 43 hereof entered in the Slovenian Business Register, including branches of foreign entities referred to in this paragraph, shall obtain data on their beneficial ownership according to the method defined in Articles 42 and 43 hereof.

(2) In accordance with Article 44 of this Act, business entities referred to in Article 44 of this Act shall establish data on their beneficial owner if: - the trustee of a trust or a person with an equivalent position has its registered office or residence in the Republic of Slovenia;

– the trustee of a trust or a person in equivalent position has its registered office or residence in a third country and enters into a business relationship or acquires real estate on behalf of a business entity;

– the trustee of a trust or a person in equivalent position has its registered office or residence in different Member States and enters into a business relationship or acquires real estate on behalf of a business entity in different Member States, whereby they have not yet fulfilled the obligation of being entered in the register of beneficial owners kept by an individual Member State;

(3) If the trustee of a trust or a person in equivalent position has its registered office or residence in different Member States and enters into a business relationship or acquires real estate on behalf of a business entity in different Member States, a certificate of proof of registration or an extract of the beneficial ownership information held in a register kept by one Member State may be considered as sufficient to consider the obligation of being entered in the register of beneficial owners fulfilled.

(4) (Legal entities referred to in paragraphs one and two of this Article shall set up and keep accurate records of data on their beneficial owners in accordance with paragraph eighteen of Article 150 hereof, which shall be updated at every data modification.

(5) Beneficial owners of business entities referred to in paragraphs one and two of this Article are bound to provide these business entities with all the data required for the fulfilment of obligations referred to in paragraphs one, two, four and six of this Article.

(6) Legal entities referred to in paragraphs one and two shall retain the data on their beneficial owners for a period of five years from the date of termination of the beneficial owner's status hereunder. This information must be available at the business entity's head office.

(7) In the event of winding up of the business entity referred to in paragraphs one and two of this Article, a court or authority conducting the winding up proceedings or status change of the entity without a known successor shall order that the data storage on beneficial owners be provided for the period referred to in the preceding paragraph prior to the winding up of the business entity.

(8) The provisions of this Article shall not apply to business entities, which are companies on a regulated market that is subject to disclosure requirements that provide suitable transparency of ownership information in conformity with European Union legislation or subject to the equivalent international standards.

Article 46
(Provision of data)

(1) The business entities referred to in the preceding Article shall without delay provide information on their beneficial owners upon request of:

- the obliged entities referred to in Article 4 of this Act when the information is required for the purpose of implementing customer due diligence measures under this Act; or

- law enforcement bodies and supervisory authorities referred to in paragraph one of Article 152 of this Act.

(2) The trustee or a person in equivalent position who enters

into a business relationship or conducts a transaction for the entity referred to in Article 44 hereof shall be bound to reveal their status to the obliged entity and provide all data on their beneficial owners in a timely manner.

3.3.2.2.3 (Obligations of obliged entities)

Article 47
(Acquisition of information in relation to identifying the beneficial owner)

(1) An obliged entity shall determine the beneficial owner of a customer by obtaining the data referred to in point 14 of paragraph one of Article 150 hereof and a certificate of proof of registration or an extract from the register of beneficial owners. With regard to the risk of money laundering or terrorist financing to which the obliged entity is exposed in conducting business with an individual customer, the obliged entity shall verify the data to such an extent that the obliged entity understands the ownership and control structure of its customer and certainly knows who the customer's beneficial owner is.

(2) When the obliged entity identifies the beneficial owner under paragraph five of Article 42 hereof, in accordance with their risk assessment, the obliged entity shall adopt suitable measures for verifying the identity of the beneficial owner. The implementation of these measures and any potential issues arising in the process of verification shall be documented.

(3) In the case of establishing the beneficial owner of a foreign trust, foreign institution or similar foreign law entity referred to in point b) of paragraph one of Article 44 hereof, in establishing a business relationship, an obliged entity shall acquire sufficient data on the category of persons with an interest in establishing a foreign trust, foreign institution or similar foreign law entity that it is able to determine the identity of the beneficiary at the time of payment or at the time when the beneficiary of the proceeds exercises the acquired rights.

(4) Notwithstanding paragraph one of this Article, an obliged entity shall not obtain data on the beneficial owner of the customer if the customer is a natural person not performing a gainful activity, but shall, during the customer due diligence in accordance with paragraph two of Article 30 of this Act, verify whether the customer is acting on its own behalf or on behalf of a third party.

(5) Notwithstanding the provision of paragraph one of Article 21 of this Act, it is not necessary to determine the beneficial owner for business entities referred to in paragraph two of Article 43 of this Act and for business entities that are companies on a regulated market that is subject to disclosure requirements that provide suitable transparency of ownership information in conformity with European Union legislation or subject to the equivalent international standards.

(6) The obliged entity shall obtain the data referred to in paragraph one of this Article by inspecting the original or certified documents from the business, court or other public register, which shall not be older than three months. The obliged entity may also obtain such data by direct inspection of the business, court or other public register and by direct inspection of the register of beneficial owners, whereby the obliged entity shall not rely exclusively on the data entered in the beneficial owners register.

(7) When not all the required data can be obtained from the business, court or other public register, the obliged entity shall obtain the missing data by inspecting the original or certified copies of documents and other business records submitted by the customer's statutory representative or authorised person.

(8) If, for objective reasons, the missing data cannot be obtained in the manner described in this Article, the obliged entity shall obtain it directly from the written statement of a statutory representative or their authorised person, whereby the obliged entity shall 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 Article 64 to Article 70). The same shall apply to the obliged entity if they obtain all data on the beneficial owner only from the register of beneficial owners.

(9) If, in determining the beneficial owner, the obliged entity doubts the reliability of the submitted data or veracity of documents or other business documents from which the data were obtained, it shall also require a written statement from the statutory representative or authorised representative prior to entering into a business relationship or conducting a transaction, whereby the obliged entity shall be bound 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 (Article 64 to Article 70).

(10) If the obliged entity establishes that the data on the beneficial owner entered in the register is inconsistent with the data that the obliged entity obtained by themselves, the obliged entity shall submit a written notice thereof to the Office within 15 days of detecting the inconsistency.

3.3.2.2.4 Beneficial owners register

Article 48

(Beneficial owners register)

(1) The register of beneficial owners (hereinafter: register) in which accurate and updated data on beneficial owners is kept shall be set up to ensure the transparency of ownership structures of business entities, thereby preventing the abuse of business entities for money laundering and terrorist financing. By setting up the aforementioned register, obliged entities are provided access to the relevant data for the needs of implementing customer due diligence, and the law

enforcement, courts and supervisory authorities referred to in paragraph one of Article 152 hereof are provided with respective access for the needs of performing the powers and duties 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: register administrator) shall maintain and manage the register.

(3) The business entities referred to in Articles 42, 43 and 44 hereof shall enter the data on their beneficial owners, including on branches of the business entities referred to in this paragraph, 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 trustee of a trust or a person in an equivalent position at the entity referred to in Article 44 hereof with its registered office or permanent residence in the Republic of Slovenia shall enter the data on the beneficial owners of the entity referred to in Article 44 hereof or within eight days from the entry of the business entity who is a trustee of a trust or a person in equivalent position in the Slovenian Business Register or within eight days from the registration of permanent residence in the Republic of Slovenia, or within weight days of the occurrence of the change of data.

(5) The trustee of a trust or a person in an equivalent position at the entity referred to in Article 44 hereof with its registered office or permanent residence in a third country shall enter the data on the beneficial owners of the entity referred to in Article 44 hereof within eight days from the entry into a business relationship or the entry of the acquisition of the property right to a real estate into the land register, or within eight days of the occurrence of the change of data.

(6) Where the trustee of a trust or a person in equivalent position at the entity referred to in Article 44 hereof has its registered office or permanent residence in different Member States or enters into several business relationships in different Member States, the obligation of being entered in the register of beneficial owners is deemed fulfilled if the trustee submits a certificate of proof of registration or an excerpt of the beneficial ownership information held in a register kept by a Member State.

(7) Notwithstanding paragraph three of this Article, the register administrator shall automatically carry out the first entry of data on beneficial owners by transferring the data on a business entity and tax identification numbers of persons who are considered beneficial owners pursuant to the provisions hereof in the register within eight days from the entry of data in the Slovenian Business Register for the following business entities:

– the entities referred to in paragraph one of Article 43 of this Act, having no ownership interest that are specified in the rules referred to in Article 50 hereof;

– sole traders;

– self-employed persons; and

– single-member limited liability companies in which the only shareholder is a natural person.

(8) Personal data on the beneficial owner for the entry in the register in accordance with the preceding paragraph shall be obtained by the register administrator in the manner prescribed in paragraphs six and seven of Article 50 hereof. The following persons shall be entered automatically as beneficial owners of the entity: for the entities referred to in indents one of the preceding paragraph: all natural persons representing the entity; for the entities referred to in indents two and three of the preceding paragraph: all persons registered to perform an activity; for the entities referred to in indent four of the preceding paragraph: the shareholder. The register administrator shall also automatically transfer all subsequent changes of data on beneficial owners of the business entity referred to in this paragraph from the Slovenian Business Register in the register.

(9) The register administrator shall use a special label for marking business entities for which the entry of the beneficial owner is conducted automatically.

(10) If the beneficial owner of the business entity referred to in paragraph seven hereof is not a natural person who would be automatically entered in the register in accordance with paragraph seven of this Article or if not all its beneficial owners were included in the automatic entry in accordance with paragraph seven of this Article, the aforementioned business entity shall enter the data on its beneficial owner or owners and owners' changes in the register within 15 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 15 days from the change of data. If data is entered by the business entity itself, the register administrator shall automatically remove the special label for the automatic entry of data referred to in the preceding paragraph from the register.

(11) The business entity referred to in paragraph seven of this Article, who registered the data on their beneficial owner(s) on their own, may submit to the register administrator a request for subsequent automatic transfer of data on the beneficial owner in accordance with paragraph eight of this Article.

(12) Notwithstanding paragraph seven of this Article, the register administrator shall not automatically make the first entry of data on beneficial owners for business entities referred to in the second and third indents of paragraph seven of this Article if in the Central Population Register there is a note "deceased" for a natural person registered for carrying out activities with a business entity.

(13) Notwithstanding paragraph seven of this Article, the register administrator shall not automatically make the first entry of data on beneficial owners for business entities referred to in paragraph seven of this Article if not all data required for registering a business entity and its beneficial owner in the Central Population Register or in the Tax Register.

(14) At the request of a supervisory authority referred to in paragraph one of Article 152 of this Act, the register administrator shall use a special label for marking business entities for which an inconsistency of data on the beneficial owner is detected. After being notified by the supervisory authority referred to in paragraph one of Article 152 of this Act that the inconsistency of data on the beneficial owner in the register has been resolved, the register administrator shall remove the special label.

(15) The provisions of this Article shall not apply to business entities, which are companies on a regulated market that is subject to disclosure requirements that provide suitable transparency of ownership information in conformity with European Union legislation or subject to the equivalent international standards.

(16) The responsibility for the correctness of the registered data lies with individual business entities.

Article 49
(Interconnecting the register via European platform)

(1) The register shall be interconnected via the European central platform established by paragraph one of Article 22 of Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (OJ L 169, 30.6.2017, p. 46), as last amended by Directive (EU) 2021/23 of the European Parliament and of the Council of 16 December 2020 on a framework for the recovery and resolution of central counterparties and amending Regulations (EU) No 1095/2010, (EU) No 648/2012, (EU) No 600/2014, (EU) No 806/2014 and (EU) 2015/2365 and Directives 2002/47/EC, 2004/25/EC, 2007/36/EC, 2014/59/EU and (EU) 2017/1132 (OJ L 22, 22.1.2021, p. 1) in accordance with the technical specifications and procedures established by implementing acts adopted by the European Commission.

(2) Through the system of interconnection of registers, the register administrator shall ensure that the data on beneficial ownership referred to in Article 50 hereof is available at least five years after the business or other legal entity has been deleted from the register.

Article 50
(Entry of data)

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

a) data on the business entity:

− company name, address, registered office, registration number and tax identification number, date of entry and deletion of a business entity – for business entities entered in the Slovenian Business Register;

− company name, address, registered office, tax identification number, date of entry and deletion of a business entity from the Tax Register – for business entities not entered in the Slovenian Business Register;

b) data on the beneficial owner: personal name, address of permanent and temporary residence, date of birth, tax identification 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 item b) of paragraph one of Article 44 hereof: the data on the category of persons with an interest in establishing a foreign trust, foreign institution or similar foreign law entity;

č) label on the automatic entry of the beneficial owner of a business entity;

d) label on the detected inconsistency of data on the beneficial owner of a business entity.

(2) In the case of a non-resident without a registration number or tax identification number, the information on the foreign identifier of the entity, on the country that allocated the identifier and on the register in which the entity is entered in the foreign country shall be entered in the register instead of the registration number or tax identification number.

(3) The register administrator shall maintain and control 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 type 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 to the law enforcement authorities, courts and supervisory authorities referred to in Article 152 hereof for 30 years after they have been deleted from the Business Register or Tax register.

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

(5) Upon entry, the data on business entities shall be automatically obtained based on a registration number from the Slovenian Business Register, and the data on business entities not entered in the Slovenian Business register shall be obtained based on a tax identification number from the Tax

Register. The register administrator shall obtain the changes of the data on business entities automatically from the Slovenian Business register or Tax Register. In the case of a non-resident referred to in paragraph two of this Article, the first entry in the register and all changes of data shall be entered manually.

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

(7) Upon entry, the personal data on the beneficial owner who is a natural person not entered in the Central Population Register shall be automatically obtained from the Tax Register on the basis of the tax identification number. The register 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 identification number.

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

(9) The Minister shall determine in greater detail the following:

– the method of entering data entered in the register;

– the code list on the method of supervision of beneficial owners of a business entity;

– the code list on the business entities referred to in paragraph one of Article 43 of this Act, having no ownership interest;

– the method of communicating public data on the internet;

– the method of maintenance and administration as well as technical requirements for the establishment of the register;

– the method of register information exchange between Member States via the European platform.

Article 51
(Access to beneficial ownership data)

(1) (1) The data on the personal name, month and year of birth, country of permanent and temporary residence, citizenship, ownership share or method of supervision of beneficiary owners, date of entry and deletion of the beneficial owner from the register, label for the automatic entry of the beneficial owner and label for marking the inconsistency of data on the beneficial owner 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 entities referred to in Article 4 of this Act and the law enforcement authorities, courts and supervisory authorities referred to in paragraph one of Article 152 of this Act, shall have the right to access data from the register in a way that would allow to determine whether a person is the beneficial owner of a business entity and of which entity the person is the beneficial owner of the business entity and with respect to which business entity a person is entered as a beneficial owner.

(3) The obliged entities referred to in Article 4 of this Article shall have direct electronic access to all beneficial ownership data entered in the register while performing due diligence of a customer under the provisions of this Act. The search for beneficial ownership information shall also be facilitated by using a combination of full name and tax identification number, full name and date of birth or a combination of full name and address of permanent residence entered in the register.

(4) The law enforcement authorities, the courts and supervisory authorities referred to in paragraph one of Article 152 of this Act shall have free direct electronic access to all actual ownership data entered in the register when they carry out their powers and tasks in connection with the prevention and detection of money laundering and terrorist financing and detecting other crimes. The entities referred in this paragraph shall also be allowed to look for beneficial ownership information by using a combination of full name and tax identification number, full name and date of birth or a combination of full name and address of permanent residence entered in the register.

(5) The register administrator may not disclose information on access to data to the beneficial owner and business entity pursuant to the preceding paragraph. The register administrator may not disclose such information for eight years after each access.

(6) The register administrator may charge an obliged entity referred to in Article 4 of this Act a fee for accessing data in accordance with its rates. The rates shall be determined in agreement with the minister responsible for finance.

(7) Notwithstanding the provisions of this Article, state bodies shall have direct free electronic access to all data on beneficial ownership entered in the register when deciding on the rights of entities that have a financial impact on the state budget. State bodies shall also be allowed to search for beneficial ownership information by using a combination of full name and tax identification number, full name and date of birth or a combination of full name and address of permanent residence entered in the register.

(8) For the purposes of performing the tasks referred to in

this Act, the Office shall obtain the entire database from the register.

Article 52
(Submission of data and information on beneficial owners at request of competent authorities of a Member State)

The supervisory authorities referred to in Article 152 hereof shall submit data, information and documentation on the beneficial owners free of charge and in due time to the foreign financial intelligence unit and supervisory authorities of a Member State for the needs of implementing the powers and duties concerning the prevention and detection of money laundering and terrorist financing.

3.3.2.3 Obtaining data on the purpose and the intended nature of the business relationship or transaction, as well as other data pursuant to this Act

Article 53
(The purpose and the intended nature of the business relationship or transaction and dataset)

(1) As part of the customer review, an obliged entity evaluates and, if necessary, additionally obtains information about the purpose and intended nature of the business relationship or transaction in a way to make its purpose and intended nature clearly understandable.

(2) In the framework of customer due diligence referred to in point 1 of paragraph one of Article 22 of this Act, an obliged entity shall obtain the data referred to in points 1, 2, 4 and 14 of paragraph one of Article 150 of this Act.
5. .

(3) In the framework of customer due diligence referred to in point 2 of paragraph one of Article 22 of this Act, an obliged entity shall obtain the data referred to in points 1, 2, 6, 7, 8, 9 and 14 of paragraph one of Article 150 of this Act..

(4) In the framework of customer due diligence referred to in point 3 of paragraph one of Article 22 of this Act, an obliged entity shall obtain the data referred to in points 3, 6, 7, 8 and 9 of paragraph one of Article 150 of this Act..

(5) In the framework of customer due diligence referred to in point 4 of paragraph one of Article 22 of this Act, an obliged entity shall obtain the data referred to in paragraph one of Article 150 of this Act.

(6) In the framework of customer due diligence referred to in Article 23 of this Act, an obliged entity shall obtain the data referred to in points 1, 2, 6, 7, 8, 9 and 14 of paragraph one of Article 150 of this Act.

3.3.2.4 (Monitoring of business activities)

Article 54

(Due diligence in monitoring of business activities)

(1) Obliged entities shall monitor with due diligence business activities carried out by their customers in order to acquire knowledge of the customer, including knowledge of the source of customer's assets. Regular monitoring of business activities undertaken by the customer via the obliged entity shall include:

- verifying the customer's business operations compliance with the purpose and intended nature of the business relationship established between the customer and the obliged entity;

- monitoring and verifying the customer's business operations compliance with the customer’s regular scope of business;

- verifying and updating obtained documents and data on the customer.

(2) An obliged entity shall meet the obligation referred to in the first and second indents of the preceding paragraph in such a way that they can conform the compliance of the client's operations throughout the duration of the business relationship.

(3) For a customer who is a legal entity, verification and updating of obtained documents and data referred to in the preceding paragraph shall include the following:

1. verifying data on full name, permanent and temporary residence, citizenship and the number, type and name of issuer, date of issue and expiry date of the customer’s official identity document or his or her statutory representative or authorised person;

2. verification of the adequacy of the letter of authorisation referred to in Article 30 of this Act;

3. determining whether the customer has become a foreign politically exposed person during the period of business relationship.

(4) For a customer who is a legal entity, verification and updating of obtained documents and data referred to in the preceding paragraph shall include the following:

1. verification of the data about the company, address and registered office of the legal entity;

2. verification of the data on the full name and permanent or temporary residence of the legal entity’s statutory representative;

3. verification of the data on the legal entity’s beneficial

owner;

4. verification of the adequacy of the letter of authorisation referred to in Article 31 of this Act;

5. determining whether the legal entity's beneficial owner has become a foreign politically exposed person during the period of business relationship.

(5) When the transactions referred to in paragraph one of Article 22 of this Act are carried out on behalf and for the account of a foreign legal entity by its branch, the obliged entity shall obtain, in addition to the data referred to in paragraph two of this Article, the following data within the annual review of a foreign legal entity:

1. data on the address and head office of the foreign legal entity's branch;

2. data on full name and permanent residence of the foreign legal entity's statutory representative.

(6) The obliged entity shall ensure the scope and frequency of measures referred to in paragraph one 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 entity shall determine the risk pursuant to Article 18 in conjunction with Article 14 of this Act. Notwithstanding the above, the obliged entity shall ensure that the obtained documents and customer data are updated when significant changes in the customer's circumstances are identified, if the obliged entity has a legal obligation to contact the customer for the purpose of establishing the beneficial owner and at least after the expiry of five years from the date of the last customer due diligence if the customer carries out at least one transaction with the obliged entity in the past twelve months.

Article 55
(Treatment of unusual transactions)

(1) In relation to complex or unusually high transactions or transactions which have an unusual structure or pattern 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 entity 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;

– record and keep its findings; and

– enhance the monitoring of the customer's business activities to ascertain whether these transactions or activities seem suspicious.

(2) If the obliged entity considers that a transaction poses an increased risk of money laundering or terrorist financing, it shall implement one or more customer due diligence measures in accordance with the provisions of this Act regulating in-depth customer due diligence (Articles 64 to 70).

(3) When dealing with unusual transactions, the obliged entity shall pay special care, as defined in paragraph one of this Article, to customers, business relationships or transactions related to the following countries:

1. countries on the list of high-risk third countries with strategic shortcomings where suitable measures for the prevention and detection of money laundering or terrorist financing are not in force; or

2. countries in which there is a higher probability of risk of money laundering and terrorist financing.

(4) The obliged entity shall establish the connectedness of business relations or transactions with the countries referred to in the preceding paragraph based on the information obtained during the implementation of measures to know their customer and the risk of money laundering and terrorist financing represented by the customer, business relationship or transaction.

(5) In the case referred to in point 1 of paragraph three of this Article, obliged entities shall be required to apply the measures set out in Article 69 of this Act.

(6) For the purposes of point 1 of paragraph three of this Article, an obliged entity shall comply with the delegated act adopted by the European Commission in accordance with Article 9 of Directive 2015/849/EU, which defines high-risk third countries that do not apply to appropriate measures to detect and prevent money laundering and terrorist financing. The office shall publish the information about the aforementioned countries on its web pages.

(7) The list of countries referred to in point 2 of paragraph three of this Article shall be prepared by the Office, taking into account the data obtained from competent international organisations. The office shall publish the information about the aforementioned countries on its web pages.

3.3.3 Customer due diligence via third parties

Article 56

(Due diligence relying on third parties)

(1) Under the conditions stipulated by this Act, an obliged entity 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 one of Article 21 of this Act.

(2) The obliged entity shall verify in advance whether the third party entrusted to carry out customer due diligence

meets all the conditions provided by this Act.

(3) Customer due diligence performed for the obliged entity 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, unless customer due diligence was performed by means of electronic identification of high reliability or on the basis of other methods of electronic identification for accessing electronic services of high reliability in accordance with regulations governing electronic identification and trust services.

(4) The obliged entity which relies on a third party in respect of customer due diligence shall remain responsible for the proper customer due diligence procedure under this Act.

Article 57
(Third parties)

(1) Third parties referred to in the preceding Article may be the following:

1. obliged entities referred to in points 1 to 14 and in point 16 of paragraph one of Article 4 of this Act;

2. banks established in an EU Member State and their branches in EU Member States;

3. auditing firms established in an EU Member State;

4. insurance companies established in an EU Member State and their branches in EU Member States;

5. branches of brokerage companies established in an EU Member State;

6. investment firms of an EU Member State and their branches established in an EU Member State;

7. branches of third-country investment firms established in other EU Member States;

8. branches of management companies established in an EU Member State;

9. EU Member State management companies and their branches established in EU Member States;

10. branches of an alternative investment fund manager established in another Member State;

11. alternative investment funds manager established in an EU Member State and their branches established in EU Member States;

12. branches of third-country alternative investment fund managers established in EU Member States;

13. payment institutions of EU Member States and their branches established in an EU Member State;

14. electronic money institutions of an EU Member State and their branches established in an EU Member State.

(2) Third parties may also include banks, management companies, investment firms or insurance companies established in a third country, provided that:

- they are obliged to implement the same or equivalent rules on the performance of customer due diligence and record management as determined by this Act; and

- with regard to the implementation of these rules they are subject to supervision in accordance with rules that are equal to or equivalent to the provisions of this Act.

(3) Taking into account the information obtained from the Office, obliged entities shall check whether the conditions referred to in the preceding paragraph are met.

(4) (2) Notwithstanding paragraph one of this Article, a third party shall also be deemed to be a notary established in the Republic of Slovenia or another Member State or third country in which he or she is obliged to implement the same or equivalent customer due diligence and record management rules as those provided for by this Act and shall, with regard to the implementation of these rules, also be subject to supervision in accordance with the provisions that are equal to or equivalent to the provisions of this Act.

(5) 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.

(6) Third parties referred to in paragraph one of the preceding Article shall not include:

- obliged entities' external contractors and agents;

- persons established in a third country listed as high-risk third countries set out in point 1 of paragraph three of Article 55 of this Act.

(7) Notwithstanding the preceding paragraph, an obliged entity may entrust the performance of the customer review to third parties who are majority-owned branches or subsidiaries established in high-risk third countries or countries where money laundering and terrorist financing are more likely to occur, provided that:

- the founder who has majority ownership of a branch or a subsidiary is established in an EU Member State; and

- majority-owned branches or subsidiaries fully implement group policies and procedures equal to or equivalent to the provisions of Articles 78, 79 and 82 of this Act.

Article 58
(Exceptions relating to customers)

Notwithstanding paragraph one of Article 56 of this Act, an

obliged entity shall not entrust the performance of customer due diligence to a third party when 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 59
(Obtaining data and documents from a third party)

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

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

(3) After sending the data, copies of documents and documentation referred to in paragraphs one and two of this Article, the third party may not keep the data, documents and documentation on the customer obtained in due diligence process.

(4) When the obliged entity considers that there is good reason to doubt the veracity of the customer due diligence carried out or identification documents or the reliability of obtained data on the customer, it shall perform due diligence on its own.

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

1. customer due diligence procedure was applied by a person not considered a third party pursuant to Article 57 of this Act;

2. if the third party relied on by the obliged entity to apply the customer the due diligence procedure established and verified the identity of a customer contrary to paragraph three of Article 56 hereof;

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

4. there is good reason to doubt the veracity of the performed customer due diligence procedure or reliability of obtained data on the customer, and the obliged entity fails to perform due diligence on its own.

Article 60
(Third parties and the group programme)

In the framework of its group policy, an obliged entity may entrust the implementation of customer due diligence measures referred to in points 1, 2 and 3 of paragraph one of Article 21 of this Act to a third party who is part of this group, provided that:

1. this group implements customer review measures and complies with data retention obligations and has in place appropriate anti-money laundering and anti-terrorist financing programmes that 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 point at group level shall be supervised by the supervisory authorities referred to in paragraph one of Article 152 of this Act or by the competent supervisory authorities of a Member State or a third country.

3.3.4 Special types of customer due diligence

Article 61
(General)

Customer due diligence procedure shall be applied in accordance with paragraph one of Article 21 of this Act; in some cases determined by this Act, simplified or particularly rigorous due diligence measures shall be required. Special types of customer due diligence shall be

1. simplified customer due diligence procedure and

2. enhanced customer due diligence procedure.

3.3.4.1 Simplified customer due diligence procedure

Article 62
(General)

(1) In the cases referred to in points 1 and 3 od paragraph one of Article 22 and Article 23 of this Act, an obliged entity shall apply simplified customer due diligence measures if, according to paragraph one of Article 19 of this Act they deem that a customer, a business relationship, a transaction, a product, a service, a distribution channel, a country or a geographical area present a minor risk of money laundering or terrorist financing.

(2) In deciding whether simplified customer due diligence is to be applied, the obliged entity may take into consideration the fact that a minor risk of money laundering and terrorist financing has been identified in accordance with point 2 of paragraph two of Article 14 and the regulation referred to in paragraph four of Article 14 of the same Act.

(3) In determining customers, business relationships, transactions, products, services, distribution channels, countries or geographical areas deemed to pose a minor risk of money laundering or terrorist financing, an obliged entity shall take into account insignificant risk factors determined by

the Minister.

(4) In determining simplified customer due diligence measures, obliged entities shall comply with the guidelines provided by the supervisory authorities referred to in paragraph one of Article 152 of this Act on the risk criteria and measures to be taken by obliged entities in such cases.

(5) Obliged entities shall monitors the customer's business activities and transactions to a sufficient extent to be able to identify unusual and suspicious transactions. Simplified customer due diligence shall not be permitted where there are grounds for suspecting money laundering or terrorist financing in relation to the customer, transaction, property or assets.

Article 63
(Performance of simplified customer due diligence)

(1) In the simplified customer due diligence referred to in paragraph one of the preceding Article, a customer's identity shall be determined and verified in accordance with Articles 29 to 39 of this Act, and data shall be obtained to the extent set out in paragraph five of this Article.

(2) The beneficial owner of the customer shall be identified pursuant to the provisions of Articles 40 to 44 of this Act, while data on the beneficial owner shall be obtained to the extent set out in paragraph five of this Article.

(3) Data on the purpose and the intended nature of the business relationship or transaction, as well as other data pursuant to this Act shall be obtained to the extent set out in paragraph five of this Article.

(4) Regular due diligence of business activities undertaken by the customer via the obliged entity shall be performed in accordance with Article 54 of this Act.

(5) Obliged entities shall obtain the following information in the framework of the simplified due diligence of a customer who is a legal entity, sole proprietor or self-employed person:

1. when entering into a business relationship and verifying and updating data in the context of monitoring business activities:

– company name, address and registered office of the legal entity, sole trader or self-employed person establishing the business relationship or on whose behalf the business relationship is established;

– full name of a statutory representative or authorised person that establishes the business relationship on behalf of a legal entity, sole trader or self-employed person;

– the purpose and intended nature of the business relationship, unless the purpose and the nature may be inferred from the established business relationship, and the date of establishment of the business relationship; and

- the full name and the state of permanent residence of the beneficial owner;

2. when carrying out transactions referred to in points 2 and 3 of paragraph one of Article 22 and in Article 23 of this Act, obliged entities:

– company name, address and registered office of the legal entity, sole trader or self-employed person establishing the business relationship or on whose behalf the business relationship is established;

– full name of a statutory representative or authorised person carrying out a transaction on behalf of a legal entity, sole trader or self-employed person;

- the date and time of the transaction;

- the amount of the transaction and the currency in which the transaction is carried out;

- the method of carrying out the transaction and the state in which the transaction is carried out;

- the purpose of the transaction, the full name, address of permanent and temporary residence, or company name and registered office of the person to whom the transaction is directed, and

- the full name and the state of permanent residence of the beneficial owner.

(6) The obliged entity shall acquires the information referred to in the preceding paragraph by inspecting the original or certified copies of the court register or any other public register submitted by the customer or by accessing the court register or any other public register.

(7) When information requested cannot be obtained in such a manner, the obliged entity shall acquire information from the originals or certified copies and other business documents submitted by the customer. When due to objective reasons an obliged entity cannot obtain the missing information even in the manner described, it shall obtain it directly from the written statement of a statutory representative or authorised person.

(8) The submitted documents referred to in the preceding paragraph shall not be older than three months.

(9) In the framework of the simplified due diligence of a customer who is a legal entity, sole proprietor or self-employed person, obliged entities shall obtain the following information:

1. when establishing a business relationship

- full name, address of permanent residence, date and place of birth, and tax identification number or personal identification number of a person establishing the business relationship or on whose behalf the business relationship is established;

- full name, address of permanent residence, date and place of birth, and tax identification number or personal identification number of the statutory representative or authorised person establishing the business relationship; and

– the purpose and intended nature of the business relationship, unless the purpose and the nature may be inferred from the established business relationship, and the date of establishment of the business relationship;

2. when carrying out the transaction referred to in points 2 and 3 of paragraph one of Article 22 and in Article 23 of this Act:

- full name, address of permanent or temporary residence, and date and place of birth, and tax identification number or personal identification number of the person carrying out the transaction;

- full name, address of permanent residence, date and place of birth, and tax identification number or personal identification number of the statutory representative or authorised person carrying out the transaction on behalf of a natural person;

- the date and time of the transaction;

– manner of executing the transaction;

- the amount of the transaction, the currency of the transaction and the manner of carrying out the transaction; and

- the purpose of the transaction, unless its purpose may be inferred from the type of the transaction, and the full name, address of permanent and temporary residence, or company name and registered office of the person to whom the transaction is directed, and the state in which the transaction is carried out.

3.3.4.2 Enhanced customer due diligence

Article 64 (General)

(1) Enhanced customer due diligence shall, in addition to the measures referred to in paragraph one of Article 21 of this Act, include additional measures determined by this Act in the following cases:

1. entering into a correspondent banking relationship with a respondent bank or similar credit institution established in a third country;

2. entering into a business relationship or carrying out a transaction referred to in points 2 and 3 of paragraph one of Article 22 and Article 23 of this Act with a customer who is a politically exposed person referred to in Article 66 of this Act;

3. when beneficiaries of life insurance policies or unit-linked life insurance policies and the beneficial owners of beneficiaries are politically exposed persons referred to in Article 68 of this Act;

4. when a customer or transaction is related to a high-risk third country.

(2) Obliged entities shall perform an enhanced customer due diligence in the cases set out in the preceding paragraph when:

1. in accordance with paragraph two of Article 19 of this Act, they deem that a customer, business relationship, transaction, product, service, state or geographical area presents an increased risk of money laundering or terrorist financing;

2. an enhanced risk of money laundering and terrorist financing has been identified in accordance with point 2 of paragraph two of Article 14 of this Act and the regulation referred to in paragraph four of Article 14 of the same Act.

(3) In determining customers, business relationships, transactions, products, services, distribution channels, countries or geographical areas deemed to pose an enhanced risk of money laundering or terrorist financing, an obliged entity shall take into account enhanced risk factors determined by the Minister.

(4) In determining enhanced customer due diligence measures, obliged entities shall comply with the guidelines provided by the supervisory authorities referred to in paragraph one of Article 152 of this Act on the risk factors and measures to be taken by obliged entities in such cases.

Article 65 (Corresponding banking relationships between credit and financial institutions)

(1) When entering into a corresponding banking relationship with a credit or financial institution with its registered office in a Member State or a third country, the obliged entity shall, to fully understand the nature of a customer's business operation, verify the customer's reputation and evaluate the quality of its supervision, apply the measures referred to in paragraph one of Article 21 hereof within the enhanced customer due diligence procedure and shall also obtain the following data, information and documents:

1. the date of issue of the authorisation to perform banking services, and name and registered office of the competent authority from the Member State or third country that issued the authorisation;

2. the 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 credit or financial institution with respect to detecting and preventing money laundering and terrorist financing in order to assess the adequacy of internal controls;

3. the description of systemic arrangements in the field of detection and prevention of money laundering and terrorist financing applicable in the Member State or the third country where the credit or financial institution is established or registered in order to understand the responsibility of individual institutions and to establish whether the credit, financial or other similar institution is subject to adequate supervision in terms of preventing money laundering and terrorist financing;

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

5. a written statement that the credit or financial institution does not enter into and has no business relationships with shell banks and that it does not establish or conduct transactions with shell banks;

6. a written statement that the credit or financial 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 entity establishing the correspondent relationship referred to in the preceding paragraph and conducting the enhanced customer due diligence procedure shall obtain a written approval of their superior responsible person holding a senior management position prior to entering into such relationship.

(3) The obliged entity shall obtain the data referred to in paragraph one of this Article by inspecting public or other accessible data records, or by inspecting documents and business records submitted by the credit or financial institution.

(4) The obliged entity shall document the implementation of measures referred to in paragraphs one, two and three of this Article.

(5) The obliged entity shall not enter into or continue a correspondent banking relationship with a credit or financial institution with its registered office in a Member State or a third country if:

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

2. the employee of the obliged entity failed to obtain the written approval of their superior responsible person prior to entering into the correspondent relationship;

3. the credit or financial institution with its registered office in a Member State or a 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 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 credit or financial institution with its registered office in a Member State or a third country operates as a shell bank or enters into correspondent or other business relationships and conducts transactions with shell banks;

5. in the case of correspondent accounts directly used by third persons to conduct transactions on their own behalf (suspense accounts), the credit or financial institution with its registered office in a Member State or a third country failed to implement the measures to acquire knowledge about the customer concerning third persons who have direct access to correspondent bank accounts and, at the request of the correspondent bank, cannot provide the required data, information and documentation on customer due diligence.

Article 66
Politically exposed persons

(1) The obliged entity shall establish a suitable system of risk management that also includes a procedure to determine whether a customer or its statutory representative, beneficial owner or authorised person is a politically exposed person. This procedure based on the risk assessment referred to in Article 18 hereof shall be defined in its internal act while taking account of the guidelines of the competent supervisory authority referred to in Article 152 hereof.

(2) The politically exposed person referred to in the preceding paragraph shall mean any natural person who is or has been entrusted with prominent public function in the previous year and resides in any other country, including its immediate family members and close associates.

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

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

b) elected representatives in legislative bodies;

c) members of the official bodies of political parties;

members of supreme and constitutional courts and other high-level judicial authorities against whose decisions there is no ordinary or extraordinary legal remedy, save in exceptional cases;

d) members of courts of audit and boards of governors of central banks;

e) heads of diplomatic missions and heads of consular posts and representative offices of international organisations and high-ranking officers of armed forces;

f) members of the administrative, management or supervisory authorities of state-owned enterprises;

g) heads of bodies of international organisations (such as presidents, secretaries-general, directors, and judges), their deputies and members of governing bodies or holders of equivalent functions in international organisations.

(4) state-owned enterprises referred to in point f) of the preceding paragraph shall by any enterprise that meets one of the following conditions:

1. the majority of voting rights in it are held by the State;

2. the State owns the majority of its holdings or shares;

3. the State has the right to appoint or dismiss a majority of the members of the management or supervisory board of that enterprise and is at the same time its partner or shareholder;

4. the State is a shareholder or partner and controls most of the voting rights in that enterprise on the basis of a contract with other shareholders or members of that enterprise;

5. the State has the right to exercise a dominant influence or control.

(5) The immediate family members of the person referred to in the second paragraph of this Article are: spouse or common-law partner, formal or non-formal civil union partner, parents and children and their spouses or common-law partners.

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

(7) When a customer entering into a business relationship or conducting a transaction, or when a customer on whose behalf a business relationship is entered into or a transaction conducted, or its beneficial owner is a politically exposed person, the obliged entity shall take the following measures in addition to those referred to in paragraph one of Article 21 hereof within the enhanced customer due diligence procedure:

1. in accordance with the scope of the risk assessment of the business relationship, transaction, product, service or distribution channel, obtain on behalf of the customer or its beneficial owner data on the origin of assets that are, or will be, the subject of a business relationship or transaction, namely from the documents and other documentation submitted to the obliged entity by the customer; if this data cannot be obtained in the manner described above or if the procedure of obtaining this data is in accordance with the scope of the risk assessment of the business relationship, product, service or distribution channel, the obliged entity shall obtain them directly from the written statement of the customer;

2. an employee of the obliged entity who conducts the procedure for entering into a business relationship with a customer shall obtain the written approval of their superior responsible person holding a senior management position prior to entering into such relationship; the approval of the continuation of the business relationship shall also be obtained if political exposure is determined after the establishment of the business relationship;

3. after the business relationship has been established, the obliged entity shall monitor with due diligence the transactions and other business activities conducted through the obliged entity by the politically exposed person.

(8) When the politically exposed person referred to in this Article ceases to act in a visible public position, the obliged entity shall continue to implement appropriate measures for another 12 months. After this period, it shall assess the subsequent risk posed by that person and take appropriate risk-based measures until it determines that the person no longer poses a risk.

Article 67
(List of functions qualifying as prominent public functions)

(1) A list indicating the exact functions referred to in paragraph three of the preceding Article that qualify as prominent public functions in the Republic of Slovenia shall be compiled by the Government. This list shall be updated promptly.

(2) The ministry responsible for internal affairs shall, based on a written proposal from the ministry responsible for finance, request international organisations with their registered office in the Republic of Slovenia to issue and keep up to date the list of prominent public functions at that international organisation and submit it to the European Commission.

Article 68
(Politically exposed persons and life insurance)

(1) An obliged entity shall take appropriate measures to determine whether beneficiaries of life insurance policies or unit-linked life insurance policies and the beneficial owners of beneficiaries are politically exposed persons. The aforementioned measures shall be taken no later than at the time of payment or full or partial transfer of the policy. In the event of an established increased risk, the obliged entity shall,

in addition to the measures referred to in paragraph one of Article 21 of this Act, take the following measures:

1. notify the superior responsible person holding a senior management position of the intended policy payment;

2. examine with special care the business relationship entered into with the policyholder and, in the event of grounds for suspicion of money laundering or terrorist financing, submit to the Office a report on suspicious transactions in accordance with Article 76 of this Act.

(2) The measures referred to in the preceding paragraph shall also be implemented for close family members and close associates referred to in paragraphs five and six of Article 66 of this Act.

(3) When the politically exposed person referred to in this Article ceases to act in a visible public position, the obliged entity shall continue to implement appropriate measures for another 12 months. After this period, it shall assess the subsequent risk posed by that person and take appropriate risk-based measures until it determines that the person no longer poses a risk.

Article 69
(Due diligence of high-risk third-country customers)

(1) When a customer or transaction is related to a high-risk third country referred to in paragraph five of Article 55 hereof, within the scope of the enhanced customer due diligence and in addition to the measures referred to in paragraph one of Article 21 hereof, the obliged entity 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 the business relationship and data on the reasons for the intended or conducted transaction;

3. obtain data about the origin of assets and property of the customer and beneficial owner, especially the data on the origin of assets and property that is, or will be, the subject of the business relationship or transaction;

4. an employee of the obliged entity who conducts the procedure for entering into a business relationship with a customer related to a high-risk third country shall obtain the written approval of their superior responsible person holding a senior management position prior to entering into such relationship; the approval of the continuation of the business relationship shall also be obtained if a relationship with a high-risk third country is determined after the establishment of the business relationship;

5. after the business relationship has been established, the obliged entity shall monitor the transactions and other business activities conducted through the obliged entity by a person from a high-risk third country with due diligence by ensuring the more frequent and extended monitoring of business operations, including the determination of transaction patterns that shall be continuously examined.

(2) In the cases referred to in the preceding paragraph and where appropriate, the obliged entity shall, in addition to the measures set out in the preceding paragraph at the request of the supervisory authority referred to in the first paragraph of Article 152 of the Act:

– use additional elements of the enhanced customer due diligence;

– introduce enhanced relevant reporting mechanisms or systematic reporting of data to the Office;

– limit the conduct of the business relationship or transactions.

(3) The obliged entity shall not have to take the additional measures referred to in paragraph one of this Article 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 provisions of this Act. In such cases, the obliged entity shall adjust the scope of measures to the risk assessment of money laundering and terrorist financing referred to in Article 18 hereof.

Article 70
(Other cases of increased risk)

In the cases referred to in paragraph two of Article 64 of this Act, an obliged entity shall take one or more additional measures in addition to those referred to in paragraph one of Article 21 of this Act which include, for instance, the following:

1. obtaining additional data on the activity of the customer and updating of data about the identification of the customer and its beneficial owner more frequently;

2. obtaining additional data on the purpose and foreseen nature of the business relationship and data on the reasons for the intended or conducted transaction;

3. obtaining data about the origin of assets and property of the customer and beneficial owner, especially the data on the origin of assets and property that is, or will be, the subject of the business relationship or transaction;

4. obtaining a written approval of their superior responsible person holding a senior management position prior to entering into such relationship; the approval of the continuation of the business relationship if political exposure is determined after the establishment of the business relationship;

5. due diligence monitoring of transactions and other

business activities undertaken by the customer through the obliged entity;

6. verifying the authenticity of obtained data and documents with outside sources.

3.3.5 Limitations on transactions with customers

Article 71
(Prohibition on using anonymous products)

The obliged entity shall not open, issue or keep anonymous accounts, password-protected passbook accounts or bearer passbook accounts, anonymous safe deposit boxes or other products on behalf of customers enabling, directly or indirectly, the concealment of the customer's identity.

Article 72
(Prohibition on establishing a business relationship)

(1) An obliged entity shall not establish a business relationship or effect transactions referred to in Articles 22 and 23 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 Securities Depository or similar register or trading accounts and which cannot be determined on the basis of other business documents.

(2) For the purposes of implementing the provision of the preceding paragraph, obliged entities shall obtain data on the holders of bearer shares for a specific client from the Central Securities Depository.

Article 73
(Prohibition on conducting business with shell banks)

An obliged entity 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 74
(Limitations on cash operations)

(1) Persons pursuing the activity of selling goods 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 providing individual services. They may also not pay cash to a customer or a third party in the course of their business if this payment exceeds EUR 5,000.

(2) The limitation of cash payments referred to in the preceding paragraph shall also apply where the payment is effected by several linked cash transactions for the sale of goods or the provision of services exceeding in total EUR 5,000.

(3) Persons pursuing the activity of selling goods or providing services shall receive payments referred to in paragraphs one and two of this Article from the customer or some other person on their payment accounts, unless otherwise provided by other Act.

(4) The provisions of the preceding paragraphs shall not apply to the obliged entities referred to in points 1 to 15 and in point 17 of paragraph one of Article 4 of this Act.

3.4 Reporting data to the Office

Article 75
(Obligation to report cash transactions and remittances tohigh-risk countries and deadlines)

An obliged entity shall provide the Office with the data referred to in points 1, 1, 2, 6, 7, 8, 10, 11 and 9 of paragraph one of Article 150 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.

An obliged entity shall provide the Office with the data referred to in points 1, 1, 2, 6, 7, 8 and 9 of paragraph one of Article 150 of this Act;
4. on any cash or cashless transaction which exceeds EUR 15,000 and which, at the request of a customer, is deposited in the bank accounts of:

- legal and natural persons from the countries set out in points 1 and 2 of paragraph three of Article 55 of this Act;

- legal and natural persons having their registered office and permanent or temporary residence in the countries set out in points 1 and 2 of paragraph three of Article 55 of this Act immediately upon completion of the transaction, but no later than three business days after its completion.

(3) The report referred to paragraphs one and two of this Article shall be submitted to the Office via secure electronic means. If reporting via secure electronic means is substantially difficult or impossible for technical reasons, it shall be exceptionally sent to the Office only in writing.

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

(5) The Office shall publish on its website immediately, but no later than the next business day after receiving the data referred to in paragraph two of this Article, the data referred to in items 1, 7 and 8 of paragraph one of Article 150 of this Act, except for full name and address of permanent and temporary residence.

(6) The Minister shall specify in detail the conditions under which an obliged entity is not required to report data on transactions referred to in paragraph one of this Article to the Office if the customer's activity or activity poses a minor risk of money laundering and terrorist financing and if such reporting of data on the transactions referred to in paragraph one of this Article could represent an excessive administrative burden for the obliged entity.

Article 76
(obligation to report on suspicious transactions and deadlines)

(1) The obliged entity shall report to the Office information set out in paragraph one of Article 150 of this Act whenever there is a suspicion of money laundering or terrorist financing associated with a transaction, person, property or assets; this information shall be submitted before executing the transaction[2] and shall specify the time limit in which the transaction is to be executed. Such suspicious transaction report shall be submitted to the Office via secure electronic means. Exceptionally it may be submitted by telephone; in such an event it must be submitted to the Office by secure electronic means no later than the next business day. Where there are grounds for suspecting money laundering or terrorist financing only after a transaction has taken place, the obliged entity shall communicate the data to the Office immediately or no later than five working days after having identified the grounds for suspicion or having sufficient information to be able to identify the grounds for such suspicion.

(2) If the reporting of the transactions referred to in the preceding paragraph via secure electronic means is substantially difficult or impossible for technical reasons, the report shall be exceptionally sent to the Office only in writing.

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

(4) A suspicious transaction referred to in paragraphs one, two and three of this Article shall be any intended or executed transaction in respect of which the obliged entity knows or has reason to suspect that the property or assets originate from criminal offences that could constitute a predicate crime of money laundering or relate to terrorist financing, or in terms of their characteristics correspond with indicators for identifying suspicious transactions as referred to in Article 92 of this Act that point to the grounds to suspect money laundering or terrorist financing.

(5) Auditing firms, legal entities and natural persons who perform accounting or tax advisory services shall report all cases where the customer seeks advice for money laundering or terrorist financing purposes to the Office without delay or not later than within three business days of seeking such advice.

(6) If in cases referred to in paragraphs three and four of this Article and due to the nature of the transaction or because the transaction has not been completed, or due to other justified reasons, an obliged entity cannot follow the prescribed procedure, it shall submit 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 entity shall explain in the report the reasons for not acting in accordance with the prescribed procedure.

Article 77
(The method and form of reporting)

The data and documents referred to in paragraph ten of Article 47 of this Act, the data referred to in paragraphs one and two of Article 75 of this Act, first, paragraphs two and three of Article 76 of this Act, paragraph five of Article 86 of this Act and paragraph three of Article 151 of this Act of the Act and annual reports on the implementation of internal control measures and measures based on the request of the Office referred to in paragraph one of Article 126 or paragraph three of Article 154 of this Act shall be submitted to the Office shall be submitted by obliged entities in the manner and form prescribed by the Minister.

3.5 Implementation of group policy and measures for detecting and preventing money laundering and terrorist financing in branches and majority-owned subsidiaries established in the Member States and third countries

Article 78
(Obligation to implement group policy)

(1) Obliged entities that are part of the group shall implement group policies and procedures concerning the measures for detecting and preventing money laundering and terrorist financing, including data protection policies and procedures and intra-group information exchange aimed at preventing money laundering and terrorist financing.

(2) Obliged entities that have branches and majority-owned subsidiaries established in the Member States and third countries shall establish and implement policies and procedures of the group referred to in the preceding paragraph and implement them in their branches and subsidiaries. Upon the establishment of policies and procedures of the group, the obliged entity shall comply with the requirements referred to in Article 18 hereof.

(3) The exchange of information within the group, including the exchange of information on suspicious transactions referred to in Article 77 of this Act shall be permitted unless the Office explicitly opposes the exchange of information on suspicious transactions.

(4) In the framework of the exchange of information referred to in the preceding paragraph, the exchange of data referred

to in paragraph one of Article 150 of this Act shall also be permitted for ensuring knowledge of the customer.

(5) The transmission of data to third countries shall permitted if the conditions set out in Chapter V of the General Data Protection Regulation are met.

Article 79
(Obligation to apply measures in the Member States)

(1) An obliged entity that directly carries out its business activity in another Member State of through a branch or agents shall ensure the compliance of itself or its branches and agents with the laws of another Member State concerning prevention of money laundering and terrorist financing.

(2) Supervision over the implementation of the preceding paragraph shall be performed by the competent supervisory authorities of the Member State in which the obliged entity carries out its business activity through a branch, agents or directly, in cooperation with the competent supervisory authorities referred to in paragraph one of Article of this Act.

Article 80
(Central contact points)

(1) The Bank of Slovenia may require electronic money issuers or payment service providers, as defined in the law governing payment services, electronic money issuing services and payment systems, to designate a central contact point in the territory of the Republic of Slovenia in cases where electronic money issuers or payment service providers:

1. are not branches or subsidiaries established in the territory of the Republic of Slovenia;

2. are established in the territory of another Member State; and

3. carry out their business in the territory of the Republic of Slovenia through a network of several agents or electronic money distributors.

(2) Agents and electronic money distributors referred to in 3. point 3 of the preceding paragraph shall be natural persons or legal entities acting on behalf of electronic money issuers or payment service providers in the performance of transactions involving the issuance of electronic money or payment services based on a power of attorney.

(3) Notwithstanding paragraph one of this Article, issuers of electronic money or payment service providers established in the territory of another Member State may, on their own initiative, designate a central contact point in the territory of the Republic of Slovenia. They shall inform the Bank of Slovenia of their intention to appoint a central contact point for electronic money issuers or payment service providers.

(4) The central contact points may be natural persons or legal entities who have a permanent residence or registered office in the territory of the Republic of Slovenia.

(5) The Bank of Slovenia shall obtain the data on natural and legal persons who are the central contact points referred to in paragraph three of Article 150 of this Act.

(6) Central contact points designated in the territory of the Republic of Slovenia on behalf of electronic money issuers and payment service providers:

1. shall ensure that networks of agents implement measures to prevent and detect money laundering and terrorist financing provided for in this Act;

2. submit data, information and documents to the Bank of Slovenia or to the Office at their request as they carry out supervision in accordance with the provisions of this Act;

3. provide assistance in cooperating and coordinating the supervision of the network of agents between the Bank of Slovenia, the Office and the competent supervisory authorities of the Member States in which the electronic money issuers or payment service providers are established.

Article 81
(Control over the agents)

(1) If the Bank of Slovenia finds serious deficiencies in the operations of electronic money agents or distributors referred to in paragraph two of the preceding paragraph relating to the implementation of measures to prevent money laundering or terrorist financing, it may take appropriate and proportionate measures to remedy the deficiencies. The measures shall be temporary and shall cease to apply once the deficiencies have been remedied.

(2) In adopting the measures and remedying the deficiencies referred to in the preceding paragraph, the Bank of Slovenia shall cooperate with the competent supervisory authorities of the Member State in which the electronic money institution or payment service provider is established.

Article 82
(Obligation to apply measures in third countries)

(1) An obliged entity shall implement the group policies and procedures referred to in paragraph two of Article 78 of this Act aimed at ensuring that money laundering prevention and terrorist financing measures under this Act are carried out to the same extent in its branches and majority-owned subsidiaries established in third countries, within the scope provided by the law of the respective third countries.

(2) If in third countries referred to in the preceding paragraph the minimal standards governing measures to detect and prevent money laundering and terrorist financing are less rigorous than those provided by this Act, obliged entities shall ensure that their branches and majority-owned subsidiaries

adopt and apply suitable measures that are equivalent to the measures laid down by this Act, within the scope provided by the law of a third country. Suitable measures shall also include data protection measures.

(3) Where the law of a third country does not allow the implementation of policies and procedures referred to in Article 78 of this Act and paragraphs one and two of this Article, the Bank of Slovenia, the Securities Market Agency and the Insurance Supervision Agency shall inform thereof the European Banking Authority and the competent supervisory authorities of other Member States in order to coordinate activities for reaching an appropriate solution.

(4) If the law of a third country does not allow the implementation of the policies and procedures referred to in Article 78 hereof and paragraphs one and two of this Article, the obliged entity shall ensure that branches and majority-owned subsidiaries in the third country adopt and implement suitable additional measures to effectively manage risks of money laundering and terrorist financing and notify the competent supervisory authorities referred to in Article 152 of this Act thereof. When determining which countries do not allow the implementation of the policies and procedures referred to in Article 78 hereof, possible legal restrictions that might impede the proper implementation of these policies and procedures, including data secrecy and protection, and other barriers limiting the exchange of information that could be relevant for this purpose shall be considered.

(5) If the additional measures referred to in the preceding paragraph prove to be insufficient, the supervisory authorities set out in Article 152 of this Act may request obliged entity to apply further additional supervisory measures, such as

1. the prohibition to enter into business relationships;
2. the termination of business relationships;
3. the prohibition to carry out transactions; or
4. the closure of operations in a third country.

3.6 Authorised person, training and internal control

3.6.1 Authorised person

Article 83

(Appointment of authorised person and his or her deputy)

(1) Obliged entities 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 preceding paragraph, obliged entities who have less than four employees shall not appoint an authorised person and shall not perform internal control under this Act.

(3) If an obliged entity with less than four employees appoints an authorised person and one or more deputies contrary to the provision of the preceding paragraph, these persons shall meet the conditions referred to in Article 84 of this Act and perform the tasks referred to in Article 85 of this Act.

(4) If an obliged entity who has less than four employees performs internal control contrary to the provision of paragraph two of this Article, they shall perform internal control in accordance with Article 88 of this Act.

(5) The obliged entities referred to in Article 4 of this Act who have branches and majority-owned subsidiaries established in third countries shall appoint an authorised person of the group and one or more deputies to carry out the tasks of detecting and preventing money laundering and terrorist financing provided by this Act and the ensuing regulations.

Article 84
(Conditions for the authorised person)

(1) An obliged entity shall ensure that the tasks of an authorised person may only be performed by a person who meets the following requirements:

1. has a highly classified job with the obliged entity which enables them to carry out the tasks referred to in this Act and the ensuing regulations in a rapid, quality and timely, quality and timely manner;

2. has not been convicted by a final judgment, nor is 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 manslaughter, serious bodily injury, grievous bodily injury, threatening work safety, the concealment, disclosure and undue obtaining of trade secrets, money laundering, disclosure of classified information or causing general danger, and the punishment for such has not yet been expunged from the criminal record;

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

4. is well acquainted with the nature of the obliged entity's operations in the fields vulnerable to money laundering and terrorist financing risks.

(2) The deputy authorised person shall be any person who meets the requirements referred to in points 2, 3 and 4 of the preceding paragraph.

Article 85
(Duties of authorised person and deputy authorised person)

(1) The authorised person referred to in Article 83 of this Act shall perform the following tasks:

1. ensures the setting up, functioning and development of the system for detecting and preventing money laundering and terrorist financing within the obliged entity;

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

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

4. participates in the elaboration of guidelines for the control of activities aimed at detecting and preventing money laundering and terrorist financing;

5. monitors and coordinates the obliged entity's activities in detecting and preventing money laundering and terrorist financing;

6. participates in the setting up and development of information support for the activities related to the detection and prevention of money laundering and terrorist financing with the obliged entity;

7. takes initiatives and makes proposals to the obliged entity's management or other administrative bodies for improving the system for detecting and preventing money laundering and terrorist financing;

8. participates in the preparation of the professional education and training programmes for the obliged entity's employees in the field of detecting and preventing money laundering and terrorist financing.

(2) The authorised person referred to in paragraph five of Article 83 of this Act shall perform particularly the following tasks: 1. ensures the establishment of efficient group policies and procedures concerning measures for detecting and preventing money laundering and terrorist financing, including data protection and information exchange policies and procedures aimed at preventing money laundering and terrorist financing;

2. ensures and coordinates compliance of its branches and agents operating in other Member States with the laws of the Member States governing the detection and prevention of money laundering and terrorist financing;

3. ensures the application of appropriate and, when necessary additional measures for detecting and preventing money laundering and terrorist financing in branches and majority-owned subsidiaries established in third countries;

4. ensures the correct and timely implementation of additional control measures in a third country, imposed on the obliged entity by the supervisory authorities referred to in paragraph one of Article 152 of this Act.

(3) The deputy shall act in place of the authorised person in his or her absence with regard to the full scope of the tasks set out in this Article and shall perform other tasks under this Act if so stipulated by the obliged entity's internal regulations.

Article 86
(Duties of the obliged entity)

(1) To enable the authorised person to carry out the tasks of detecting and preventing money laundering and terrorist financing under this Act, their duties in relation to the authorised person shall include the following:

1. ensuring unrestricted access to all data, information and documents required to carry out those tasks;

2. giving appropriate authorisations for the efficient performance of the tasks referred to in paragraph one of Article 42 of this Act;

3. providing appropriate staff, material and other working conditions;

4. ensuring appropriate premises and technical capacities guaranteeing an adequate level of protection of classified information available to the authorised person pursuant to this Act;

5. providing appropriate information and technical support enabling permanent and safe monitoring of activities in this field;

6. ensure regular professional training for detecting and preventing money laundering and terrorist financing;

7. ensuring a replacement for the authorised person during his or her absence.

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

(3) The obliged entity shall ensure that the person acting as the authorised person pursuant to this Act carries out his/her functions and duties as a sole full-time job, provided that due to the large number of employees, the 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 or her duties as an independent organisational unit directly responsible to the management or other administrative body and shall be functionally and organisationally separated from the obliged entity's other organisational units.

(5) The obliged entity shall forward to the Office the full name and title of the position held by the authorised person and his or her deputy and any changes thereof without delay, but no later than within fifteen days following the appointment or change of data. The obliged entity shall also indicate the date of appointment, the date of termination of office, the address where the authorised person and his or her deputy perform their work, if different from the obliged entity's registered office, and the contact details of the authorised person and his or her deputy such as the telephone number or email address and any other contact information.

(6) The obliged entities referred to in items 1 and 2 of paragraph one of Article 4 of this Act shall define the function of the authorised person as a key function in accordance with the Bank of Slovenia's legal act regulating internal management, corporate governance body and the capital adequacy assessment process for banks and savings banks.

3.6.2 Professional training

Article 87

(Duty to participate in regular education and training)

(1) Obliged entities shall take measures to ensure that employees whose duties include the prevention and detection of money laundering and terrorist financing under this Act are familiarised with the provisions of this Act, including with relevant data protection requirements. The measures adopted shall be proportionate to the type and size of the obliged entity and the risk of money laundering and terrorist financing.

(2) Obliged entities shall provide regular professional training for all employees whose duties include the prevention and detection of money laundering and terrorist financing under this Act.

(3) (2) 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 for suspicion of money laundering or terrorist financing exist.

(4) Obliged entities shall draw up annual professional training and education programmes for the prevention and detection of money laundering and terrorist financing activity by the end of March for the current year.

3.6.3 Internal control and implementing regulations for the purpose of carrying out certain tasks

Article 88
(Regular internal control obligation)

Obliged entities shall ensure regular internal control over the performance of tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act.

Article 89
(Detailed regulations concerning the authorised person, method for executing internal control, retention and protect

tion of data, keeping of records and professional training of employees)

The Minister shall prescribe detailed regulations concerning the authorised person, method for executing internal control, retention and protection of data, keeping of records and professional training of obliged entities' employees.

CHAPTER IV

THE TASKS AND DUTIES OF LAWYERS, LAW FIRMS AND NOTARIES

Article 90
(Specific Provisions relating to lawyers, law firms and notaries)

(1) A lawyer, law firm or notary shall act in accordance with the provisions of this Act governing tasks and obligations of obliged entities in applying the measures for detecting and preventing money laundering and terrorist financing when

1. assisting in planning or executing transactions for a client concerning:

a) buying or selling real property or a company;

b) managing customer's money, securities or other property;

c) opening or managing bank, savings or securities accounts;, č) raising funds necessary for the establishment, operation or management of a company;

d) establishing, operating or managing foundations, trusts, companies or similar legal organisational forms; or

2. carrying out a financial or real estate transaction on behalf of and for a customer.

(2) The lawyer, law firm or notary shall report all cases where the client seeks advice for money laundering or terrorist financing purposes to the Office immediately or not later than within three business days of seeking such advice.

Article 91 (Exemptions)

(1) The provisions of this Act shall not apply to lawyers, law firms or notaries while establishing a customer's legal position or when representing a customer in judicial proceedings, including advice concerning the institution or avoidance of such proceedings.

(2) The reporting obligation referred to in Article 76 of this Act shall not apply to lawyers, law firms or notaries with regard to data obtained from or concerning the customer while establishing the customer's legal position or when representing the customer in judicial proceedings, including advice concerning the institution or avoidance of such proceedings, notwithstanding whether such data is obtained before, during or after such proceedings.

(3) Subject to the conditions referred to in the preceding paragraph of this Article, a lawyer, law firm or notary shall not be required to forward the data, information and documents at the request of the Office referred to in paragraphs one and two of Article 100 of this Act. In such cases, notaries shall immediately, but not later than within 15 days of receipt of the request, inform the Office in writing of the reasons for non-compliance with the Office's request.

CHAPTER V

LIST OF INDICATORS FOR IDENTIFYING CUSTOMERS AND TRANSACTIONS IN RESPECT OF WHICH THERE ARE REASONABLE GROUNDS TO SUSPECT MONEY LAUNDERING OR TERRORIST FINANCING

Article 92
(Obligation to compile and use the list of indicators)

(1) Obliged entities shall compile 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 such red flag indicators, obliged entities shall take into account in particular the complexity and scope of implementing transactions, unusual patterns, values or relations between transactions that have no apparent economic or visible lawful purpose and/or are not in compliance with or disproportionate to the usual or expected business of the customer, as well as other circumstances related to the status and other characteristics of the customer.

(3) Obliged entities shall use the list of indicators referred to in paragraph one of this Act when identifying the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto.

(4) (4) The minister may prescribe obligatory inclusion of individual indicators on the 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 93
(Participation in preparing the list of indicators)

The Office, the Bank of Slovenia, the Securities Market Agency of the Republic of Slovenia, the Insurance Supervision Agency, the Financial Administration of the Republic of Slovenia, the Agency for Public Oversight of Auditing, the Chamber of Notaries of Slovenia, the Bar Association of Slovenia, and associations and societies whose members are bound under this Act shall participate in drawing up the list of indicators referred to in paragraph one of the preceding Article hereof.

CHAPTER VI

THE TASKS AND RESPONSIBILITIES OF THE OFFICE

6.1 General provisions

Article 94 (General)

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

(2) The Office shall be the central government body responsible for receiving and analysing reports on suspicious transactions and other data, information and documents concerning potential money laundering, related previous criminal offences, or terrorist financing obtained under this Act and other acts or directly applicable EU legal acts, including rules on non-proliferation of weapons of mass destruction, and for the transmission of the results of its analyses to the competent authorities.

(3) The Office shall performs its tasks referred to in the preceding paragraph in complete autonomy, sovereignly and operationally independently, which shall also involve decisions about accepting and analysing data, information

and documents and reporting the results of analyses to competent authorities.

(4) For the purpose of carrying out its tasks, the Office shall have timely, direct or indirect access to data, information and documents held by obliged entities, state bodies and bearers of public authority, including information regarding the detection and prosecution of criminal offences.

(5) All data, information and documents from personal data records shall be forwarded to the Office under this Act free of charge.

Article 95
(Training)

(1) The Office's activity is the provision of training to obliged entities under the provisions of this Act relating to the prevention and detection of money laundering, previous criminal offences and terrorist financing.

(2) The Office issues detailed internal rules on the method of performing its own activity, the pricing method, the method of disclosing revenues and expenses and other elements of its own activity.

Article 96
(Responding to requests for financial information or financial analysis)

(1) The Minister, in agreement with the Minister of the Interior and the Minister of Justice, shall designate from among the bodies responsible for the prevention, detection, investigation or prosecution of criminal offences the bodies that may request and receive financial information or financial analysis from the Office.

(2) The Office shall cooperate with the bodies designated in accordance with the preceding paragraph and respond in a timely manner to reasoned requests for financial information or financial analysis submitted by those bodies where such financial information or financial analysis is required, on a case-by-case basis and when the reason for such requests is related to the prevention, detection, investigation or prosecution of serious crime.

(3) The use of financial information or financial analyses for purposes beyond those for which the use was originally authorised shall be permitted only with the prior consent of the Office.

(4) The Office may reject the request referred to in paragraph two of this Article when

1. there are objective reasons to believe that the provision of such information would adversely affect ongoing investigations or analyses,; or

2. in exceptional circumstances, the disclosure of information would be manifestly disproportionate to the legitimate interests of a natural person or legal entity or irrelevant to the purposes for which the information was requested.

(5) Any rejection referred to in the preceding paragraph shall be duly substantiated.

(6) The decision on whether to pass on the information shall be taken by the Office.

(7) The bodies designated in accordance with paragraph one of this Article may process financial information and financial analysis received from the Office in accordance with this Article for the specific purpose of preventing, detecting, investigating or prosecuting serious criminal offences that are not intentional and for which personal data are collected pursuant to Article 8 of the Personal Data Protection Act in Dealing with Criminal Offences (Official Gazette of the Republic of Slovenia *[Uradni list RS]*, No. 177/20).

6.2 Detection of money laundering and terrorist financing

Article 97
(Receiving and analysing data and information)

The Office shall be responsible for receiving and analysing the following type of data and information:

1. reports on suspicious transactions received from obliged entities pursuant to paragraphs one, two and four of Article 76 of this Act;

2. reports on cash transactions and remittances received from obliged entities pursuant to paragraphs one and two of Article 75 of this Act;

3. motions received pursuant to paragraphs one and two of Article 108 of this Act;

4. motions received pursuant to Article 109 of this Act;

5. data received from the Financial Administration of the Republic of Slovenia pursuant to Article 131 of this Act;

6. facts received pursuant to Article 168 of this Act;

7. requests, notifications, data, information and documents received pursuant to the provisions of this Act concerning international cooperation;

8. data, information and documents collected pursuant to Articles 99, 100, 101 and 102 of this Act;

9. otherwise obtained data and information for which the Office deems to contain grounds for suspecting money laundering or terrorist financing.

Article 98
(Analytical function of the Office)

Within the scope of its analytical function, the Office shall use data, information and documents received and collected pursuant to the preceding Article and Article 126 of this Act to carry out the following:

1. operational analyses focused on the following:

- individual or selected messages on suspicious transactions, persons, property or assets referred to in point 1 of paragraph one of the preceding Article, and

- other reports, notices, data and information referred to in the preceding Article in order to determine whether there are grounds to suspect money laundering associated with previous criminal offences related to money laundering, or terrorist financing in respect of a transaction, a person, property or assets; and

2. strategic analyses focused on identifying typologies and trends in money laundering and terrorist financing.

Article 99
(Request to an obliged entity for the submission of data on suspicious transactions or persons)

(1) If the Office considers that in respect of a transaction, a person, property or assets there are grounds to suspect money laundering associated with previous criminal offences related to money laundering, or terrorist financing, or in cases set out in Article 108 of this Act, it may require the obliged entity to submit the following:

1. data from records of customers and transactions which is kept by the obliged entity pursuant to paragraph one of Article 150 of this Act;

2. data on assets and other property of said person held with the obliged entity;

3. 3. data on transactions with assets and property of said person held with the obliged entity;

4. data on other business relationships with the obliged entity;

5. any other data and information obtained or retained by the obliged entity in accordance with the relevant Act, which are required to detect and prove money laundering, and terrorist financing.

(2) In its 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 Office may also require data referred to in paragraph one of this Article for the person in respect of whom there are grounds to believe that they have participated or have been engaged in the transactions or business of the 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 two of this Article, the obliged entity shall forward to the Office upon its request all other necessary documents.

(5) The obliged entity shall forward the data, information and documents referred to in the preceding paragraphs to the Office without delay and no later than within five business 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 for 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 documents or due to other justified reasons, the Office may, by written notification, extend the time limit for the obliged entity, upon its written and reasoned request; in such cases, it may inspect the documents at the obliged entity's premises.

Article 100
(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, a person, property or assets, previous criminal offences related to money laundering or terrorist financing, it may require from the lawyer, law firm or notary the data, information and documents relating to the transactions referred to in Article 90 hereof, which are needed for detecting and proving money laundering, previous criminal offences or terrorist financing. 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, previous criminal offences or terrorist financing.

(3) (Regarding the time limit for forwarding the data, information and documents 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 101
(Request to a state body or bearers of public authority 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, previous criminal offences related to money laundering or terrorist financing in connection with a transaction, a person, property or assets, or in the cases referred to in Article 109 hereof, it may require from the lawyer, law firm or notary the data, information and documents which are necessary for detecting and proving money laundering, previous criminal offences or terrorist financing. The Office's request 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 state bodies and bearers of public authority also for the person in respect of whom there are grounds to believe that he or 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, previous criminal offences related to money laundering or terrorist financing.

(3) State authorities and bearers of public authority shall forward to the Office the data, information and documents referred to in the preceding paragraphs without delay and no later than within 15 days of receipt of the request, or shall allow the Office free of charge direct electronic access to certain data and information.

(4) Notwithstanding the preceding paragraph of this Article, the Office may exceptionally set a shorter deadline for the request if this is necessary to determine circumstances relevant for 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 102

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

(1) If the Office considers that there are grounds to suspect money laundering, previous criminal offences related to money laundering or terrorist financing in connection with a transaction, a person, property or assets, or in the cases referred to in Article 109 hereof, it may also request other public and private law entities the data to submit information and documents which are necessary for detecting and proving money laundering, previous criminal offences or terrorist financing. The Office's request 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 public and private law entities also for the person in respect of whom there are grounds to believe that he or 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, previous criminal offences related to money laundering or terrorist financing.

(3) Other public and private law entities shall forward to the Office the data, information and documents referred to in the preceding paragraphs without delay and no later than within 15 days of receipt of the request, or shall allow the Office free of charge direct electronic access to certain data and information.

(4) Notwithstanding the preceding paragraph of this Article, the Office may exceptionally set a shorter deadline for the request if this is necessary to determine circumstances relevant for 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 103
(Service of requests)

The provisions of the Act regulating the general administrative procedure shall apply mutatis mutandis to the service of requests referred to in Articles 99, 100, 101 and 102 of this Act.

Article 104
(Data accuracy verification)

Notwithstanding other provisions of this Act, the Office may, for the purposes of verifying the accuracy of data transmitted to the Office pursuant to Articles 75 and 76 of this Act, obtain from the competent state body a unique identification mark of the data person to whom data relate.

Article 105
(Order temporarily suspending a transaction)

(1) The Office may issue a written order temporarily suspending a transaction for a maximum of 72 three business days if the Office considers that there are reasonable grounds to suspect a criminal offence of money laundering or terrorist financing, and it shall inform the competent authorities thereof.

(2) The purpose of the measure suspending the transaction is to provide the Office with the necessary time to analyse suspicious transactions, other data and information and to submit its findings to the 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 entity as soon as possible and/or on the same day when the order was issued. The responsible person in the obliged entity 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 in case of the need to gather additional information during pre-criminal or criminal proceedings, or due to other justified reasons, the Office may give the obliged entity instructions on the procedure regarding the persons concerned, including information on the suspension of the transaction that may be disclosed to the customer.

(5) The competent authorities referred to in paragraphs one and two of this Article shall act very promptly after receiving notification and shall, within three business days of the temporary suspension of the transaction, take measures in accordance with their competencies.

Article 106
(Termination of temporary suspension of a transaction)

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

(2) If the Office does not act within the time provided in the preceding paragraph of this Article, the obliged entity may proceed with the transaction immediately.

Article 107
(Request for ongoing monitoring of a customer's financial transactions)

(1) The Office may request in writing from the obliged entity the ongoing monitoring of financial transactions of the person in respect of whom there are reasonable grounds to suspect the commission of a criminal offence of money laundering or terrorist financing, or of another person in respect of whom there are reasonable grounds to believe that he or 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 entity. In its request, the Office shall set a time limit within which the obliged entity must submit the data requested.

(2) The obliged entity shall submit 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.

(3) If the obliged entity cannot, due to the nature of the transaction or business, or due to other justified reasons, act as provided for in the preceding paragraph of this Article, it shall submit the data to the Office as soon as possible or the following business day at the latest. In its notice it shall indicate the reason for not acting in accordance with the preceding paragraph.

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

Article 108
(Petitioners)

(1) If for a transaction or a particular person, property or assets there exists suspicion of money laundering, previous criminal offences related to money laundering or terrorist financing, the Office may start collecting and analysing data, information and documents also on a written and reasoned initiative of the court, the Prosecutor's Office, the Police, the Slovenian Intelligence and Security Agency, the Intelligence and Security Service of the ministry responsible for defence, the Court of Auditors of the Republic of Slovenia, the Commission for the Prevention of Corruption of the Republic of Slovenia, the Budget Supervision Office of the Republic of Slovenia, the Financial Administration of the Republic of Slovenia or the Public Payments Administration of the Republic of Slovenia. The initiative shall include data set out in paragraph eight of Article 150 of this Act.

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

(3) The Office shall not consider the initiatives referred to in paragraphs one and two of this Article if they fail to state substantiated grounds for suspicion of money laundering, previous criminal offences related to money laundering or terrorist financing. The Office shall inform the initiator of the refusal in writing, stating the reasons for which the initiative has not been tabled for consideration.

Article 109
(Initiative of the State Prosecutor's Office relating to forfeiture of assets of illicit origin)

(1) When the State Prosecutor's Office conducts a financial investigation procedure in accordance with the Act governing the forfeiture of assets of illicit origin, the Office may also start collecting and analysing data, information and documents at the reasoned written initiative from the State Prosecutor's Office, which shall include data set out in paragraph eight of Article 150 of this Act.

(2) In collecting data, the Office shall exercise mutatis mutandis the powers set out in Articles 99 to 102 of this Act and the chapter on international cooperation of this Act.

Article 110
(Notification of suspicious transactions)

(1) If the Office considers, on the basis of data, information and documents acquired under this Act, that there are grounds to suspect the commission of criminal offence of money laundering, predicate offences or terrorist financing in connection with a transaction, a person, property or assets, or in the cases referred to in Article 109 of this Act, it shall notify the competent authorities in writing and submit the necessary documents.

(2) In the notification referred to in the preceding paragraph, the Office shall not state information about the obliged entity and its employee who submitted the information pursuant to Article 76 of this Act, unless there are reasons to suspect that the obliged entity 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.

Article 111
(Information on other criminal offences)

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

Article 112
(Feedback)

(1) The Office shall notify in writing the obliged entity referred to in Article 76 of this Act, the initiators referred to in Articles 108 and 109 of this Act and the supervisory authority referred to in Article 168 of this Act of the completion of collecting and analysing data, information and documents in connection with a certain transaction, person, property or assets in respect of which there are grounds to suspect the commission of a criminal offence of money laundering or terrorist financing, or established facts that indicate or may indicate money laundering or terrorist financing, unless the Office judges that such action may jeopardise further proceedings.

(2) The Office shall inform obliged entities who report suspicious transactions to the Office pursuant to the provisions of this Act about the usefulness and applicability of reported suspicious transactions.

6.3 International cooperation

Article 113
(General provisions)

(1) The provisions of this Act concerning international cooperation shall apply unless otherwise provided by a treaty or an EU legal act that applies directly.

(2) The provisions of this Act on international cooperation shall regulate the Office's cooperation with foreign financial intelligence units, regardless of their organisational status and cooperation with the European Commission.

(3) The Office's cooperation with foreign intelligence units shall include the exchange of data, information and documents concerning customers, transactions, assets and property regarding which there are reasons to suspect money laundering, predicate criminal offences or terrorist financing. The cooperation shall include the following:

1. the Office's request to foreign financial intelligence units;

2. the request of foreign financial intelligence units to the Office;

3. exchange on the spontaneous initiative of the Office or foreign financial intelligence units.

(4) The Office shall cooperate with the European Commission and other relevant EU bodies where necessary to facilitate coordination and exchange of information between Member States' financial intelligence units, and shall attend meetings of the Member States' Financial Intelligence Forum on important issues in their field of work and cooperation, relating to:

- detection of suspicious cross-border transactions;

- standardisation of the exchange of data and information through a secure, decentralised computer network for the exchange of data and information related to money laundering and terrorist financing between financial intelligence units;

- joint analysis of cross-border issues; and

- identifying trends and factors relevant to assessing the risk of money laundering and terrorist financing at national and EU level.

(5) For the purposes of exchanging data, information and documents referred to in paragraph three of this Article, the Office may conclude a cooperation agreement with foreign financial intelligence units.

(6) Prior to forwarding personal data to a foreign financial intelligence unit, the Office shall obtain assurances that the foreign financial intelligence unit of the country to which data is being sent has a regulated system of personal data protection, and that data will be used solely for the purposes determined by this Act.

(7) Different definitions of tax crime in individual Member States or third countries shall not impede the exchange of data and information between financial intelligence units of Member States or third countries as far as this exchange is possible under national law.

Article 114
(Request to a foreign financial intelligence unit to provide information)

(1) The Office may, within the scope of its tasks for detecting and preventing money laundering, predicate crime and terrorist financing, request from the a foreign financial intelligence unit in writing to submit the data, information and documents needed for processing, analysing, detecting and preventing money laundering, predicate crime or terrorist financing.

(2) If the Office needs data, information and documents from an obliged entity or from another Member State, it shall send a request to the financial intelligence unit of that Member State.

(3) The Office's request referred to in the preceding paragraphs of this Article shall contain the relevant facts and circumstances concerning the grounds to suspect money laundering or terrorist financing and a definition of the purpose for which the requested data will be used. The Office may request data even if a predicate crime regarding money laundering is not known at the time of submission of the request.

(4) The Office may use the data, information and documents acquired pursuant to this Article solely for the purposes set out in this Act. The Office may not, without prior consent of the foreign financial intelligence unit, forward, allow insight into the received data, information and documents to a third person, or use them contrary to the conditions and restrictions determined by the Office.

(5) In exceptional and urgent cases and under the conditions set out in this Article, the Office may request a financial intelligence unit of a Member State for financial information or financial analysis that may be relevant for processing or analysing information related to terrorism or organised crime related to terrorism.

Article 115
(Submission of data and information upon the request of a foreign financial intelligence unit)

(1) The Office shall submit the data, information and documents concerning customers, 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 other 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 documents referring to an obliged entity with its registered office 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 documents. The Office shall respond to the request referred to in this Article in due time.

(3) The Office shall designate a contact point responsible for receiving requests from the foreign financial intelligence unit.

(4) The request of a foreign financial intelligence unit referred to in this Article shall contain the relevant facts and circumstances concerning the reasons to suspect money laundering or terrorist financing, while 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.

(5) 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 113 hereof is received;

2. if the submission of data and information is contrary to the principles of the legal order of the Republic of Slovenia.

(6) The Office shall inform the foreign financial intelligence unit of the rejection of the request in writing and the notice shall state and clarify the grounds for rejection.

(7) Foreign financial intelligence units may use the data, information and documents submitted pursuant to this Article 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 insight into the received data, information and documents to a third person or use them contrary to the conditions and restrictions determined by the Office.

(8) 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 and information is not compliant with the principles of the legal order of the Republic of Slovenia;

4. if no guarantee concerning personal data protection and the purpose of its use referred to in paragraph six of Article 113 hereof is received.

(9) Any rejection referred to in the preceding paragraph shall be duly substantiated.

(10) The Office may set forth additional conditions and restrictions that must be observed by the foreign financial intelligence unit in order to use the data referred to in paragraph one of this Article.

(11) In exceptional and urgent cases and under the conditions set out in this Article, a Member State financial intelligence unit may request the Office for financial information or financial analysis that may be relevant for processing or analysing information related to terrorism or organised crime related to terrorism.

Article 116
(Submission of data and information upon request from Europol)

(1) The Office shall respond in a timely manner to duly substantiated requests for financial information and financial analysis submitted by Europol through the Europol National Unit and submitted on a case-by-case basis within the remit of Europol and for the purposes of performing its tasks.

(2) The request referred to in the preceding paragraph shall be treated as originating from a financial intelligence unit.

(3) The Office may reject the request referred to in paragraph one of this Article when

1. there are objective reasons to believe that the provision of such information would adversely affect ongoing investigations or analyses; or

2. in exceptional circumstances, the disclosure of information would be manifestly disproportionate to the legitimate interests of a natural person or legal entity or irrelevant to the purposes for which the information was requested.

(4) The Office shall duly substantiate any rejection referred to in the preceding paragraph.

(5) When implementing this Article, the Office shall also take into account the provisions of Article 7(6)(7) of Regulation 2016/794/EU.

(6) The Office shall send the reply referred to in paragraph one of this Article electronically via SIENA or its successor in the language applicable to SIENA or, as appropriate,

FIU.Net or its successor.

Article 117
(Spontaneous submission of data to a foreign financial intelligence unit)

(1) The Office shall submit the data, information and documents concerning customers, 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 other Member State or a third state, to a foreign financial intelligence unit of that Member State of a third country at its request, provided that de facto reciprocity applies.

(2) If the notification of suspicious transactions received by the Office pursuant to Article 76 of this Act indicates that persons, transactions, property or assets are related to another Member State, the Office shall send to the financial intelligence unit of that Member State the information referred to in points 1, 2, 8, 11, 12 and 13 of the paragraph one of Article 150 of this Act.

(3) Provisions of the chapter on international cooperation of this Act shall apply mutatis mutandis to the exchange of information pursuant to this Article.

(4) In exceptional and urgent cases and under the conditions set out in this Article, the Office may request a financial intelligence unit of a Member State to provide financial information or a financial analysis that may be relevant for processing or analysing information related to terrorism or organised crime related to terrorism.

Article 118
(Exchange of information on cash entering or leaving the EU)

The Office shall exchange the information referred to in Article 9(1) of Regulation 2018/1672/EU with relevant financial intelligence units from other Member States in accordance with Articles 113, 114, 115, 117, 119 and 122 of this Act.

Article 119
(Feedback)

At the request of a foreign financial intelligence unit, the Office shall send feedback on the usefulness and applicability of the received data referred to in paragraph one of Article 114 of this Act and information on the results of the analysis based on data received from the foreign financial intelligence unit.

The Office may request feedback from a foreign financial intelligence unit on the usefulness and applicability of the submitted data referred to in paragraph one of Article 115 of this Act and information on the results of the analysis based on the submitted data.

Article 120
(Temporary suspension of a transaction upon 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 business days also on the basis of a reasoned and written request by a foreign financial intelligence unit and inform thereof the bodies responsible for the prevention, detection, investigation or prosecution of criminal offences.

(2) The Office may reject the request of a foreign financial intelligence unit If it considers, based on the facts and circumstances stated in the request, that there are no grounds for suspicion of money laundering or terrorist financing. The Office shall inform the initiator of the refusal in writing, stating the reasons for which the initiative has been refused.

(3) (4) Articles 498, 105 and 106 of this Act shall apply, mutatis mutandis, to the order on temporary suspension of the transaction referred to in paragraph one of this Article.

Article 121
(Request to a foreign financial intelligence unit to temporarily suspend a transaction)

The Office may, within the scope of its tasks for detecting and preventing money laundering and terrorist financing, submit to foreign financial intelligence units a written initiative for the temporary suspension of a transaction if it considers that there are reasonable grounds to suspect money laundering or terrorist financing.

Article 122
(Secure communication systems)

The exchange of data, information and documents between the Office and foreign financial intelligence units pursuant to Articles 113 to 121 of this Act shall take place via secure communication systems.

Article 123
(Diagonal data exchange)

(1) The Office may also indirectly request data, information and documents from foreign authorities of a Member State or third country responsible for detecting and preventing money laundering and terrorist financing, but such exchange of data, information and documents shall take place exclusively through that country's financial intelligence unit via secure communication systems.

(2) The Office may also indirectly submit data, information and documents to foreign authorities of a Member State or third country responsible for detecting and preventing money laundering and terrorist financing, but such exchange of data, information and documents shall take place exclusively through that country's financial intelligence unit via secure communication systems.

(3) Provisions of the chapter on international cooperation of this Act shall apply mutatis mutandis to the exchange of information pursuant to this Article.

Article 124
(Exchange of information between competent authorities)
referred to in Article 3(2) of Directive 2019/1153/EU)

(1) The body designated in accordance with paragraph one of Article 96 of this Act may exchange financial information or financial analyses obtained from the Office on request and on a case-by-case basis with the competent authority of another Member State designated in accordance with Article 3(2) of Directive 2019/1153/EU if this financial information or financial analysis is necessary to prevent, detect and combat money laundering, relate predicate criminal offences and terrorist financing.

(2) The body designated in accordance with paragraph one of Article 96 of this Act may request the competent authorities of other Member States designated in accordance with Article 3(2) of Directive 2019/1153/EU on a case-by-case basis for financial information or financial analysis obtained by those authorities from the financial intelligence units of those Member States where this financial information or financial analysis is necessary to prevent, detect and combat money laundering, related predicate criminal offences and terrorist financing.

(3) The body designated in accordance with paragraph one of Article 96 of this Act may use the financial information or financial analyses obtained in accordance with the preceding paragraph only for the purpose for which they were requested.

(4) The bodies designated in accordance with paragraph one of Article 96 of this Act and the competent authorities of other Member States designated pursuant to Article 3(2) of Directive 2019/1153/EU may use the financial information or financial analyses submitted in accordance with the preceding paragraph only for the purpose for which they were provided.

(5) The body designated pursuant to paragraph one of Article 96 of this Act or the competent authority of another Member State designated pursuant to Article 3(2) of Directive 2019/1153/EU may not send financial information or financial analyses to another body, agency or department or use them for purposes beyond those originally approved without the prior consent of the Office or the financial intelligence unit of a Member State.

(6) The Office may refuse to grant the consent referred to in the preceding paragraph if it does not obtain assurance on the protection of personal data and the purpose of their use set out in paragraph six of Article 113 of this Act or if the transmission of financial information or financial analyses

1. exceeds the scope of application of the provisions of this Act;

2. jeopardise the course of criminal proceedings in the Republic of Slovenia or may in any other way prejudice the interests of these proceedings; or

3. is not compliant with the principles of the legal order of the Republic of Slovenia.

(7) The body designated in accordance with paragraph one of Article 96 of this Act shall send the request and response to the request referred to in this Article, including financial information or financial analyses, via secure communication systems.

6.4 Prevention of money laundering and terrorist financing

Article 125
(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 the list of indicators for the identification of 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 uniform implementation of the provisions of this Act and provisions issued on the basis hereof, for the obliged entities referred to in Article 4 of this Act;

4. participate in the professional training of employees of obliged entities, state bodies, and bearers of public authority;

5. collect and publish statistics on money laundering and terrorist financing;

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

Article 126
(Submission of data to the Office)

(1) The Office may request the obliged entities referred to in Article 4 of this Act, supervisory authorities referred to in Article 152 of this Act and other state bodies and organisations vested with public authority to provide the following information:

1. from all records kept pursuant to this Act;

2. on all business relationships they have entered into with their clients, regardless of their type and form;

3. about all transactions between them and their clients;

4. on all transactions performed by their clients in the

Republic of Slovenia;

5. on all transactions performed by their clients in Member States or third countries;

6. on all transactions performed to their clients in the Republic of Slovenia from the Member States or third countries;

7. other available data and documents kept on the basis of other regulations or obtained in another lawful manner and which the Office needs for the purposes referred to in this Article.

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

(3) Data, information, documents and other available data referred to in paragraph one of this Article shall be used by the Office for the purposes of operational and strategic analysis, assessment of the exposure of the financial and non-financial system of the Republic of Slovenia to money laundering and terrorist financing, and identifying the forms of and trends in money laundering and terrorist financing.

(4) The obliged entities referred to in article 4 of this Act shall communicate to the Office the data, information, documents and other available data referred to in paragraph one of this Article free of charge within fifteen days of receipt of its request.

(5) The supervisory authorities referred to in Article 152 of this Act and other state bodies and organisations vested with public authority shall also submit the required information to the Office free of charge and within the time limit referred to 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 volume of documents or other justified reasons, extend the time limit to the entities referred to in paragraphs four and five of this Article upon their reasoned request in writing.

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

6.5 Other tasks

Article 127

(Submission of data to the court, the State Prosecutor's Office or the Police)

(1) At their reasoned written request, the Office shall submit to the court, the State Prosecutor's Office or the Police data from its records referred to in points 1 to 5 and 9 to 11 of paragraph four of Article 149 of this Act, which they need in order to

1. investigate the circumstances relevant to the detection, prosecution or trial in the case of money laundering, predicate criminal offences or criminal offences of terrorist financing, in accordance with the provisions of the Act governing criminal procedure;

2. investigate circumstances vital for the protection or forfeiture of proceeds, in accordance with the provisions of the Act regulating criminal proceedings or the Act governing the forfeiture of assets of illicit 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 149 of this Act to the court, the State Prosecutor's Office or the Police if the foreign financial intelligence unit has not given its consent.

(3) The reasoned written request referred to in paragraph one of this Article shall clearly indicate if persons, transactions, assets or property of illicit origin are subject to detection, prosecution or investigation of money laundering, predicate crime or terrorist financing procedures or proceedings for forfeiting property of illicit origin.

(4) The Office may reject the request referred to paragraphs one and two of this Article if it deems that

1. there are serious grounds for presuming that the provision of such information would make it difficult or impossible to run the Office's and carry out its tasks, or

2. in exceptional circumstances, the disclosure of information would be manifestly disproportionate to the legitimate interests of a natural person or a legal entity or irrelevant to the purposes for which the information was requested.

(5) The Court, the Public Prosecutor's Office and the Police shall inform the Office of the measures taken on the basis of the information received under this Article and of the results of investigations data at least once a year, but no later than by the end of January for the previous year.

Article 128

(Submission of data to the Financial Administration of the Republic of Slovenia)

(1) The Office shall submit to the Financial Administration of the Republic of Slovenia data from the records referred to in point 1 of paragraph four of Article 149 of this Act, relating to persons and transactions referred to in Article 75 of this Act. The Financial Administration of the Republic of Slovenia

needs this data in order to carry out the tasks within its competence:

1. financial control;

2. financial investigation;

3. gaming inspection;

4. control of declarations of cash entering or leaving the EU;

5. carrying out customs clearance tasks in compliance with EU rules governing mutual legal assistance between Member States' administrative bodies.

(2) The Financial Administration of the Republic of Slovenia may request the data referred to in the preceding paragraph only on the basis of a reasoned written request which must clearly indicate that it performs the tasks referred to in the preceding paragraph in line with its competences.

(3) The Office may reject the request referred to paragraphs one and two of this Article if it deems that

1. there are serious grounds for presuming that the provision of such information would make it difficult or impossible to run the Office's and carry out its tasks; or

2. in exceptional circumstances, the disclosure of information would be manifestly disproportionate to the legitimate interests of a natural person or a legal entity or irrelevant to the purposes for which the information was requested.

(4) The Financial Administration of the Republic of Slovenia shall inform the Office of its findings based on the information received under this Article and of other measures taken on the basis thereof once a year, but no later than by the end of January for the previous year.

Article 129
(Submission of data to the Permanent Coordination Group established under the Act governing restrictive measures)

(1) The Office shall submit to the Permanent Coordination Group established in accordance with the Act governing restrictive measures the data from its records referred to in points 1 to 5 and 9 to 11 of paragraph four of Article 149 of this Act, which this group needs in order to exercise its powers pursuant to the regulations on restrictive measures.

(2) Notwithstanding the provision of the preceding paragraph, the Office shall not submit to the Permanent Coordination Group established in accordance with the Act governing restrictive measures data from its records referred to in points 4 and 5 of paragraph four of Article 149 of this Act without prior consent of the competent foreign authority.

(3) The Permanent Coordination Group may request the data referred to in paragraph one hereof only on the basis of a reasoned written request which must clearly indicate that it performs the tasks referred to in the preceding paragraph in line with its competences.

(4) The Office may reject the request referred to in the preceding paragraph in the following cases:

1. if it considers that there are serious grounds for presuming that the provision of such information would make it difficult or impossible to run the Office's and carry out its tasks; or

2. in exceptional circumstances, the disclosure of information would be manifestly disproportionate to the legitimate interests of a natural person or a legal entity or irrelevant to the purposes for which the information was requested.

(5) The Permanent Coordination Group referred to in paragraph one of this Article shall inform the Office of its findings based on the information received under this Article and of other measures taken on the basis thereof once a year, but no later than by the end of January for the previous year.

Article 130
(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 BODIES AND BEARERS OF PUBLIC AUTHORITY

Article 131
(Financial Administration of The Republic Of Slovenia)

(1) The Financial Administration of the Republic of Slovenia shall communicate to the Office within no later than three days the information obtained pursuant to Article 3(4) of Regulation 2018/1672/EU on any declaration of accompanied cash totalling EUR 10,000 or more when entering or leaving the Republic of Slovenia from or to a third country and on any application for the disclosure of unaccompanied cash totalling EUR 10,000 or more upon entering or leaving the Republic of Slovenia from or to a third country.

(2) The Financial Administration of the Republic of Slovenia shall communicate to the Office data obtained pursuant to Article 5(3) of Regulation 2018/1672/EU if accompanied cash entering or leaving the Republic of Slovenia from or to a third country referred to in the preceding paragraph was not reported to the Financial Administration of the Republic of Slovenia, as well as if unaccompanied cash entering or

leaving the Republic of Slovenia from or to a third country referred to in the preceding paragraph was not reported to the Financial Administration of the Republic of Slovenia when this had been required by the customs authority.

(3) The Financial Administration of the Republic of Slovenia shall communicate to the Office the information about cash entering or attempting entering or leaving or attempting leaving the Republic of Slovenia from and to a third country and on any unaccompanied cash entering or attempting entering or leaving or attempting leaving the Republic of Slovenia from or to a third country totalling less than EUR 10,000 if there are indications of cash being linked to criminal activity.

(4) Upon request, the Bank of Slovenia and the Financial Administration of the Republic of Slovenia shall exchange all information on the control of cash entering or leaving the Republic of Slovenia from or to a third country, which is necessary to perform the tasks within their competence.

(5) Upon request, the Bank of Slovenia and the Financial Administration of the Republic of Slovenia shall exchange all information on the control of cash entering or leaving the Republic of Slovenia from or to a third country, which is necessary to perform their activities.

(6) Notwithstanding point 19 of Article 3 of this Act, the cash referred to in the preceding paragraphs shall have the same meaning as in Article 2 of Regulation 2018/1672/EU.

Article 132
(Courts, public prosecutors' offices and other state bodies)

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

(2) The following information shall be regularly communicated to the Office by the competent state bodies, subject to availability:

1. date of filing the criminal charge;

2. 1. full name, address of permanent and temporary residence, date and place of birth, tax identification number or unique personal identification number or company name, address, registration number and tax identification number of the accused person or defendant who submitted a request for judicial protection in minor offence proceedings;

3. statutory definition of the criminal offence and the place, time and manner of committing the 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 that has signs of a predicate offence.

(3) The following information shall be communicated to the Office by the public prosecutors' offices and court once per year and at the latest by the end of March of the current year for the previous year, subject to availability:

1. full name, address of permanent and temporary residence, date and place of birth, tax identification number or unique personal identification number or company name, address, registration number and tax identification number of the accused person or defendant who submitted a request for judicial protection in minor offence proceedings;

2. the reference number of the case, the stage of the proceedings and the final verdict in each individual stage;

3. statutory designation of the criminal offence or other offence;

4. full name, address of permanent and temporary residence, date and place of birth, tax identification number or unique personal identification number or company name, address, registration number and tax identification number of the person in respect of whom the temporary protection of the request for forfeiting or temporarily forfeiting the proceeds;

5. the date of issue and validity of the order on temporary protection of the request for forfeiture of the proceeds or temporary seizure;

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

7. the date of issuing the order on forfeiture of assets or proceeds;

8. the amount of assets or value of the proceeds forfeited.

(4) The competent state bodies shall 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 their findings made on the basis of the received notifications of suspicious transactions referred to in Article 110 of this Act, or information on other criminal offences referred to in Article 111 of this Act, and other measures taken on the basis hereof.

Article 133
(Additional measures concerning high-risk countries)

In consideration of proper evaluations, assessments or reports drawn up by international organisations and standards bodies with competence in the field of preventing money laundering and combating terrorist financing and, where appropriate, competent state bodies and bearers of public

authority concerning the high-risk country referred to in paragraph six of Article 55 hereof, one or several measures shall be taken:

1. refuse the establishment of subsidiaries, branches or representative offices of the entity conducting any activity of the entities referred to in paragraph one of Article 4 hereof from a high-risk country or otherwise considering the fact that the aforementioned entity is from a country that lacks adequate regimes for the prevention of money laundering and terrorist financing;

2. prohibit the obliged entity from establishing branches or representative offices in the high-risk country or otherwise consider the fact that the relevant branch or representative office would be in a country that lacks adequate regimes for the prevention of money laundering and terrorist financing;

3. require an increased supervisory examination or increased external audit requirements for branches and subsidiaries of the obliged entity located in the high-risk country;

4. set increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the high-risk country;

5. require credit and financial institutions to review and amend or, if necessary, terminate correspondent relationships with respondent institutions in the high-risk country.

CHAPTR VIII

PROTECTION AND STORAGE OF INFORMATION AND MANAGEMENT OF RECORDS

8.1 Data protection

Article 134

(Prohibition on disclosure)

(1) Unless otherwise provided by this Act, obliged entities and their staff, including members of the management, supervisory or other executive bodies, and/or other persons having any access to data on the below facts, shall not disclose to a customer, a third person or other supervisory authority referred to in points b) to h) of paragraph one of Article 152 of this Act that

1. the data, information or documents on the customer or the transaction referred to in Article 76 of this Act have been or will be forwarded to the Office;

2. the Office requested the submission of data referred to in Articles 99, 100, 101 and 102 of this Act;

3. the Office, pursuant to Article 105 of this Act, has temporarily suspended the transaction and/or given instructions to the obliged entity in this regard, except when the disclosure was in compliance with paragraph four of Article 105 of this Act;

4. the Office, pursuant to Article 107 of this Act, required the ongoing monitoring of the customer's business activities;

5. the Office performs or will perform the operational analysis of the customer or a third party referred to in point 1 of Article 98 of this Act;

6. an investigation has been or is likely to be launched against the customer or a third party on the grounds of money laundering or terrorist financing.

(2) The prohibition on disclosure referred to in the preceding paragraph shall cease to apply eight years after the date on which the obliged entity was informed of the fact referred to in the preceding paragraph.

(3) Obliged entities shall protect the facts referred to in paragraph one of this Article and the documents related to these facts and shall take appropriate measures regarding their labelling, access and use, transfer in case of termination, storage and destruction after the expiry of the time limit referred to in Article 142 of this Act in order to ensure their safe treatment.

(4) (2) The facts referred to in the preceding paragraph and the notification of suspicious transactions, and/or information on other criminal offences referred to in Articles 110 and 111 of this Act and data referred to in Articles 127, 128 and 129 of this Act, shall be classified and discussed according to their level of classification, in accordance with the law regulating classified information.

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

(6) The prohibition on disclosure of the facts referred to in paragraph one of this Article shall not apply if the data, information and documents obtained and retained in accordance with this Act by an obliged entity 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.

(7) The disclosure of the facts referred to in paragraph one of this Article may be allowed if the data, information and documents obtained and retained in accordance with this Act by an obliged entity are necessary to protect the interests of the obliged entity in proceedings for the purpose of proving his or her actions, and the disclosure of facts would not would not prejudice the implementation of the measures taken by the competent authorities and their procedures for detecting and preventing money laundering and terrorist financing. The director of the Office shall decide on the permission to disclose the facts under this paragraph on the reasoned initiative of the obliged entity.

(8) The prohibition on disclosure of the facts referred to in

point 1 of paragraph one of this Article shall not apply if the data referred to in point 1 of the preceding paragraph are required by the supervisory authority referred to in paragraph one of Article 152 of this Act for the purpose of supervision of 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 the paragraph one of this Article shall be verified by supervisory authorities directly at the Office.

(9) (5) 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 the client from engaging in illegal activity, this does not constitute disclosure within the meaning of paragraph one of this Article.

Article 135
(Disclosure of information within the group)

(1) The prohibition on disclosure of information referred to in paragraph one of this Article shall not apply in the case of disclosures between credit institutions and between financial institutions from Member States that are part of the same group, and if the group's policies and procedures meet the requirements of this Act.

(2) The prohibition on disclosure of information referred to in point 1 of paragraph one of this Article shall not apply in the case of disclosures between credit institutions and between financial institutions from Member States and their branches and majority-owned subsidiaries established in third countries, provided that the following two conditions are met:

1. branches or majority-owned subsidiaries fully implement group policies and procedures in third countries that are equal to or equivalent to the provisions of Articles 78, 79 and 82 of this Act, and

2. the group's policies and procedures meet the requirements of this Act.

(3) In such an event, obliged entities shall manage a data record which is not subject to the disclosure ban and which was disclosed within the group in which the following data is processed:

– company name, address and registered office of the legal entity, sole trader or self-employed person on whose behalf the transaction is carried out;

– full name and date of birth of a statutory representative or authorised person carrying out a transaction on behalf of a legal entity, sole trader or self-employed person;

- full name and the date of birth of the natural person who carries out the transaction;

– full name and date of birth of a statutory representative or authorised person carrying out a transaction on behalf of a natural person;

- the date and time of the transaction; and

- the amount of the transaction and the currency in which the transaction is carried out.

(4) The obliged entity shall submit the records referred to in the preceding paragraph on request to the Office without delay.

(5) The transmission of data to third countries shall permitted if the conditions set out in Chapter V of the General Personal Data Protection Regulation are met.

Article 136
(Disclosure of information within the network)

(1) The prohibition of disclosure of data referred to in point 1 of paragraph one of Article 134 of this Act shall not apply if it concerns the disclosure of data between lawyers, law firms, notaries, auditing firms and independent auditors, legal entities and natural persons performing transactions related to accounting services and tax advisory services, provided that they pursue their professional activity at the same legal entity or network and are established in the Member States.

(2) The provision of the preceding paragraph shall apply mutatis mutandis in the event that the persons referred to in the preceding paragraph are established in third countries, if measures to detect and prevent money laundering and terrorist financing equivalent to the provisions of this Act are implemented in third countries.

(3) In such an event, obliged entities shall manage a data record which is not subject to the disclosure ban and which was disclosed within the network in which the following data is processed:

– company name of the legal entity, sole trader or self-employed person on whose behalf the transaction is carried out;

– full name and date of birth of a statutory representative or authorised person carrying out a transaction on behalf of a legal entity, sole trader or self-employed person;

- full name and the date of birth of the natural person who carries out the transaction;

– full name and date of birth of a statutory representative or authorised person carrying out a transaction on behalf of a natural person;

- the date and time of the transaction; and

- the amount of the transaction and the currency in which the transaction is carried out.

(4) The obliged entity shall submit the records referred to in the preceding paragraph on request to the Office without

delay.

(5) The transmission of data to third countries shall permitted if the conditions set out in Chapter V of the General Data Protection Regulation are met.

(6) The network referred to in the preceding paragraphs is a large-scale structure to which a person belongs and has a joint owner or joint administration or joint control over compliance with regulations.

Article 137
(Disclosure of information within the same categories)

(1) The prohibition of disclosure of data referred to in point 1 of paragraph one of Article 134 of this Act shall not apply if the disclosure involves persons who are credit and financial institutions, lawyers, law firms, notaries, audit firms and independent auditors and legal entities and natural persons performing activities related to the activity of accounting or tax consulting services, provided that the following conditions are met:

1. the transaction relates to two or more of those persons;

2. the transaction relates to the same customer;

3. the above-mentioned persons are established in a Member State or in a third country which implements measures to detect and prevent money laundering and terrorist financing equivalent to those laid down in this Act;

4. the above-mentioned persons pursue the same activity or belong to the same category of occupation; and

5. they are subject to obligations regarding the protection of professional and business secrecy and personal data (i.e. disclosure of information.

(2) For the purposes of this Article, obliged entities shall manage a data record which is not subject to the disclosure ban and which was disclosed within the same categories in which the following data is processed:

– company name of the legal entity, sole trader or self-employed person on whose behalf the transaction is carried out;

– full name and date of birth of a statutory representative or authorised person carrying out a transaction on behalf of a legal entity, sole trader or self-employed person;

- full name and the date of birth of the natural person who carries out the transaction;

– full name and date of birth of a statutory representative or authorised person carrying out a transaction on behalf of a natural person;

- the date and time of the transaction; and

- the amount of the transaction and the currency in which the transaction is carried out.

(3) The obliged entity referred to in the preceding paragraph shall submit the records referred to in the preceding paragraph on request to the Office without delay.

(4) The transmission of data to third countries shall permitted if the conditions set out in Chapter V of the General Data Protection Regulation are met.

Article 138
(Exemptions from the principle of classification)

(1) When forwarding data, information and documentation to the Office under this Act, the obligation to protect classified data, business and bank secrecy and professional secrecy shall not apply to an obliged entity, state authority or any other bearer of public authority, court, prosecutor's office, lawyer, law firm, notary or their staff.

(2) The organisation, lawyer, law firm, notary and staff shall not be held liable for the damage caused to customers or to third persons if, in compliance with the provisions of this Act or the ensuing regulations, they

1. submit to the Office data, information and documents on their customers;

2. obtain and process data, information and documents on their customers;

3. implement an order on temporary suspension of the transaction or the instruction issued in connection with the said order;

4. implement a request by the Office for the ongoing monitoring of the customer’s financial transactions.

(3) Individuals, including the employees of an obliged entity and their representatives, shall not be subject to the obligation to protect classified information, business and professional secrets as well as confidential bank data if:

1. they submit data, information and documents to the Office in accordance with the provisions of this Act;

2. they process data, information and documents 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 139
(Use of acquired data)

(1) The Office, state authorities and other bearers of public authority, obliged entities, lawyers, law firms, notaries, and their staff, may use the data, information and documents obtained under this Act solely for the purposes stipulated hereof.

(2) The bodies referred to in Articles 127, 128 and 129 of this Act may use the data acquired pursuant to Article 71 of this Act solely for the purpose for which they were acquired.

(3) The processing of data, information and documents obtained under this Act for any other purpose, such as commercial purposes, shall be prohibited.

Article 140
(Informing the individual about the processing of personal data)

Obliged entities who collect personal data directly from an individual pursuant to the provisions of this Act shall inform him or her of the processing of personal data before entering a business relationship or before performing a transaction referred to in paragraph one of Articles 22 and 23 of this Act.

8.2 Data retention

Article 141
(Keeping copies of official identity documents)

(1) When the obliged entity obtains a copy of an identity document in paper or digital form pursuant to paragraph two of Article 32, paragraph three of Article 33, paragraph four of Article 34 or paragraph four of Article 35 of this Act, it shall destroy the copy after obtaining the required data from the identity document.

(2) Notwithstanding the preceding paragraph and the provisions of other Acts, obliged entities who are credit and financial institutions may keep in digital form the copies of identity documents obtained in the framework of implementing measures to establish and verify the identity of a customer under the provisions of this Act for the purpose of evidence, subsequent verification of the veracity of data, implementation of internal controls, more effective provision of organisational and technical conditions for the protection of confidentiality and the prevention of illegal further copying and distribution of such copies.

(3) Obliged entities shall keep the copies referred to in the preceding paragraph for a maximum of five years from their acquisition and shall ensure their protection by storing such copies using organisational, technical and logical-technical procedures and measures in accordance with the Act governing personal data protection.

(4) The retention referred to in paragraph two of this Article shall be permitted for all forms of implementing measures to establish and verify customer identity set out in section 3.3.2.1 of this Act, and for implementing measures to verify and update the acquired documents and customer data referred to in Article 54 of this Act.

Article 142
(Retention period for data held by obliged entities)

(1) Obliged entities shall keep data obtained pursuant to
21., Article 22, Article 23, Article 27, Article 29, Article 30, Article 31, Article 32, Article 33, Article, Article 34, Article 35, Article 36, Article 37,
38., Article 39, Article 47, Article 53, Article 54, Article 55, Article 59, Article 63, Article 64, Article, Article 65, Article 66, Article 68, Article 69,
70., Article 75, Article 76, Article 106 and Article 107 of this Act, including the accompanying documents relating to the customer due diligence and individual transactions, for ten 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 deposit box unless another Act provides for a longer retention period. In the case of retention of data obtained in a business relationship and the accompanying documents, the retention period of all acquired data, including data on individual transactions, shall begin on the first day after the termination of the business relationship.

(2) The accompanying documents referred to in the preceding paragraph shall comprise copies, notes or the following original documents:

- official documents for determining and verifying customer identity;

- documents concerning business relationships and invoices;

- documents concerning business correspondence;

- notes and records that are necessary for identifying and tracing domestic or cross-border transactions;

- documents concerning the determination of the background and purpose of unusual transactions; and

- other accompanying documents obtained or created in the course of customer due diligence or the performance of individual transactions.

(3) Obliged entities shall keep the information and accompanying documents on the authorised person and deputy authorised person, on the professional training of staff, on the performance of internal control and risk management referred to in Articles 18, 83, 84 and 87 of this Act for four years after the appointment of the authorised person or deputy authorised person and after the completion of professional training and the performance of internal control and analysis of the impact of changes in the obliged entity's business processes associated with money laundering or terrorist financing.

(4) After the expiry of the time limits referred to in the preceding paragraphs of this Article, personal data shall be deleted, unless otherwise provided by another Act.

(5) In the event of liquidation of the obliged entity, the body carrying out the liquidation procedure or the change of legal status of the obliged entity without a known successor shall inform thereof the Office before the liquidation of the obliged entity and ensure the storage of data and of the accompanying documents within the time limits set by this Act.

Article 143
(Retention period for data held by the Financial Administration of the Republic of Slovenia)

From the date of submission of the reports referred to in paragraph (4) of Article 150 of this Act. After the expiry of this time limit, the Financial Administration of the Republic of Slovenia shall destroy the data. The retention period may be extended once for a period not exceeding three years, provided that the conditions set out in Article 13(5) of Regulation 2018/1672/EU are met.

Article 144
(Retention period for data held by the Bank of Slovenia)

The Bank of Slovenia shall keep the data from the records referred to in paragraph two of Article 149 of this Act for ten years from the day when a natural or legal entity ceases to be the central contact point. After the expiry of this time limit, the Bank of Slovenia shall destroy the data.

Article 145
(Retention period of data within the Office)

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

(2) Notwithstanding the preceding paragraph, the Office shall keep the data and information from the records referred to in points 16 and 17 of paragraph four of Article 149 of this Act for five years from the day when it was obtained. This data and information shall be destroyed after the expiry of this period.

(3) Notwithstanding paragraph one of this Article, the Office shall keep the data and information from the records referred to in point 20 of paragraph four of Article 149 of this Act for five years after deleting the virtual currency service provider from the registry.

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

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

- points 1, 2, 3, 4, 5, 11, 12, 13, 16 and 17 of paragraph four of Article 149 of this Act, eight years after the data has been obtained;

- points 6, 7, 8, 9 and 10 of paragraph four of Article 149 of this Act, after the judgement or any other decision for a criminal offence or other offence becomes final, 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 146
Collection of statistical data by the Office)

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 entities;

– the number of reported suspicious transactions submitted to the Office pursuant to this Act;

– the number of notifications concerning suspicious transactions that the Office forwarded to competent authorities;

– the number and share of suspicious transactions on the basis of which measures were introduced under the authority of the police, a state prosecutor's office or court;

– the number of received, rejected and answered requests from foreign financial intelligence units, broken down by country;

– the number of requests submitted to foreign financial intelligence units, broken down by country;

– the number of employees at the Office and at law enforcement authorities, courts and supervisory authorities referred to in Article 152 hereof that perform duties concerning the prevention and detection of money laundering and terrorist financing;

– the number of on-site and off-site supervisions performed at obliged entities, the number of violations identified and the number and the nature of measures imposed by supervisory authorities.

Article 147
(Collection of statistical data by other state bodies)

(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 the courts, state prosecutor's offices and other state bodies shall collect, on an annual basis, statistical data concerning:

1. the number of persons under criminal investigation for money laundering or terrorist financing;

2. the number of persons against which a criminal complaint has been lodged for money laundering or terrorist financing;

3. the number of persons under investigation;

4. the number of persons accused of money laundering or terrorist financing;

5. the number of persons convicted for money laundering or terrorist financing;

6. the type of predicate criminal offence of money laundering or terrorist financing, if available;

7. the value of the secured, seized or forfeited illicit proceeds in euros.

(2) The courts, state prosecutor's offices and other state bodies shall communicate to the Office the data referred to in the preceding paragraph once per year, no later than by the end of March of the current year for the previous year.

Article 148
(Publication of statistical data)

The Office shall publish and send to the European Commission statistical data on money laundering and terrorist financing referred to in Articles 146 and 147 of this Act at least once a year.

8.4 Management of records

Article 149
(Management of records)

(1) Obliged entities shall manage the following data records:

1. records of data on all customers, business relationships and transactions referred to in Articles 22 and 23 of this Act;

2. records of data reported to the Office referred to in Articles 75 and 76 of this Act.

(2) The Bank of Slovenia shall manage records on the contact points referred to in Article 80 of this Act.

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

1. any declared or undeclared cash totalling EUR 10,000 or more entering or leaving the Republic of Slovenia from or to a third country and on any declared or undeclared unaccompanied cash totalling EUR 10,000 or more entering or leaving the Republic of Slovenia from or to a third country (paragraphs one and two of Article 131);

2. cash entering or attempting entering or leaving or attempting leaving the Republic of Slovenia from and to a third country and on any unaccompanied cash entering or attempting entering or leaving or attempting leaving the Republic of Slovenia from or to a third country totalling less than EUR 10,000 if there are indications of cash being linked to criminal activity (paragraph three of Article 131).

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

1. records of data on persons and transactions referred to in Articles 75 and 76 of this Act;

2. records of the initiatives received referred to in Articles 108 and 109 of this Act;

3. records of notifications and the information referred to in Articles 110 and 111 of this Act;

4. records of international requests referred to in Articles 114 and 115 of this Act;

5. records of personal data sent abroad under Articles 52, 115 and 117 of this Act;
114.,

records of access to data referred to in	Article 127	;
7. records of access to data referred to in	Article	of this Act;
8. records of access to data referred to in	Article	of this Act;

9. records of criminal offences referred to in Article 132 of this Act;

10. records of the supervisory measures carried out, identified violations and issued decisions and other supervisory measures referred to in Article 167 of this Act;

11. records on the reported facts referred to in Article 168 of this Act;

12. records on the performed operational analyses referred to in point 1 of Article 98 of this Act;

13. records on the performed strategic analyses referred to in point 2 of Article 98 of this Act;

14. records of data on obliged entities for the purpose of reporting to the Office, referred to in Article 77 of this Act.

15. records on authorised persons and their deputies referred to in paragraph 5 of Article 86 of this Act;

16. records of requests referred to in paragraph eleven of Article 115, Article 116 and Article 124 of this Act;

17. records of personal data sent abroad referred to in Article 96, paragraph eleven of Article 115, Article 116 and Article 124 of this Act;

18. records of service ID cards of inspectors referred to in Article 158 of this Act;

19. records of data on supervisory authorities for the purpose of reporting to the Office, referred to in Article 167 of this Act;

20. register of virtual currency service providers referred to in Article 5 of this Act.

(5) Business entities shall manage data records on their beneficial owners referred to in Articles 42, 43 and 44 of this Act.

(6) For the purposes of Article 94 of this Act, the Office may obtain, use and process free charge data, including personal data contained in the databases managed by authorised authorities and organisations in the Republic of Slovenia and obtained from the databases of the following management authorities:

1. The ministry responsible for internal affairs:

- data from the Central Population Register (full name, the personal identification number, citizenship, tax identification number, permanent or temporary residence, country of residence, address for service, marital status, father, mother, spouse, child, change of personal name, withdrawal and return of capacity to contract, date of death, information about the issued residence permit of a foreigner, gender, place of birth, country of birth, permanent or temporary residence abroad, partner to a civil union, number of individuals who have registered permanent or temporary residence at the same address, apartment number);

- data from the record of issued identity cards (full name, personal identification number, identity card number, identity card issue date, identity card issuer);

- data from the record of issued travel documents (full name, personal identification number, travel document number, travel document issue date, travel document issuer);

- data from the record of issued firearm certificates (full name, personal registration number, certificate code, certificate issuance date, certificate issuing authority, certificate status, licence type, weapon category and quantity);

2. The ministry responsible for infrastructure:

- data on the ownership of the vehicle and on the vehicle from the register listing registered motor vehicles and trailer vehicles (date of the vehicle's first registration, ownership data, data on the person to whom the vehicle is registered but is not the owner of the vehicle, data on the vehicle);

- data from the driver's licence records (full name, personal registration date, driver's license number, date of issuance of the driver's license, the competent authority by which the driver's license was issued, the status and category of vehicles that the holder of a driver's license may drive);

3. The Pension and Disability Insurance Institute of Slovenia:

– data on insured persons covered by pension and disability insurance (the basis for insurance, date of registration in and deregistration from the pension and disability insurance scheme, and data on insurance period), beneficiaries of rights under the pension and disability insurance scheme paid by the Pension and Disability Insurance Institute of Slovenia (type, amount, date of payment and date of entitlement to an individual right);

4. The Health Insurance Institute of Slovenia:

– data on insured persons covered by compulsory health insurance (basis for insurance, date of registration in and deregistration from the compulsory health insurance scheme) and data on insured persons covered by pension and disability insurance;

5. The Financial Administration of the Republic of Slovenia:

- data on income indicated in the annual income tax assessment;

- VAT assessment data taken from monthly VAT returns;

- data on corporate income tax assessment taken from the corporate income tax return;

Income tax prepayment calculation and the calculation of personal income tax prepayment on income from self-employment

- data on the assessment of property transaction tax;

- data on tax control procedures;

- data on tax investigation procedures;

- data on bank account number of persons abroad;

- data from the tax register (subject of entry in the court register, natural persons with permanent or temporary residence in the Republic of Slovenia, sole trader, other legal or natural entity that performs an activity and is recorded in another register or other prescribed record in the territory of the Republic of Slovenia, a legal or natural entity not having its registered office or other registered form in the Republic of Slovenia and operating in the territory of the Republic of Slovenia, an association of persons under foreign law having no legal personality, a direct state or municipal budget user, other persons recorded in the tax register);

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

- property ownership data;

- property value data (general market value according to the rules governing mass property valuation);

- data on the type of property (actual parcel use recorded in the land cadastre, actual use of buildings and parts of buildings recorded in the cadastre of buildings)

- residential floor area data;

7. The Slovenian Maritime Administration:

- data on the ownership of seagoing watercraft by an individual and on the seagoing watercraft;

8. Local courts:

- data on property ownership and other real movable and immovable property rights of an individual;

9. The Central Securities Depository:

- computer printout of data entered in the central register of book-entry securities relating to individual holders of such securities;

10. The Bank of Slovenia as regards data from the Central Credit Register:

- data on the indebtedness of natural persons and business entities, which are kept in the information exchange system in accordance with the Act governing the Central Credit Register;

11. The Agency of the Republic of Slovenia for Public Legal Records and Related Services (AJPES):

- data on business entities, their founders and representatives, including all changes (date of registration and deletion, registration number, tax identification number, company name or name, registered office, personal name or company, registered office and address or address of permanent or temporary residence, personal identification number or registration number, tax identification number);

- data on the value of ownership interests (registration number of a private undertaking or legal entity, date of registration and deletion in/from the Business Register of Slovenia, legal form, tax identification number of a private undertaking or legal entity, amount of share capital, ownership interest of a person in a company or cooperative);

- beneficial ownership data;

- data on the profit of private undertakings and legal entities;

– bank account number;

- status of the account (active, closed);

- closing date of the account;

- data on the authorised person of the bank account holder (full name or company name, tax identification number or unique identification and the country of its registered office or residence, registration number);

- data on the beneficial owner of the bank account (full name, tax identification number or unique identification and the country of residence);

- information about the safe deposit box (number or other identification label of the safe and the length of lease);

- data on the lessee of the safe deposit box (full name or company name, tax identification number and the country of its registered office or residence, registration number);

12. The ministry responsible for justice:

- Information from criminal records (full name, personal identification number, registration number, date of entry of the judgment, type criminal offence, sanction);

13. The ministry responsible for labour, family, social affairs and equal opportunities:

- data from the central database, which includes entitlements to public funds (full name, personal identification number, type of entitlement to public funds, amount of entitlement to public funds, information on whether it is a recipient or a beneficiary);

14. Administrative units:

- data on the ownership of inland watercraft by an individual and on the inland watercraft;

15. The Civil Aviation Agency:

- data on ownership, lease and encumbrance over the aircraft.

(7) The Office accesses the written and graphic data from the databases referred to in the preceding paragraph via direct computer link if the technical possibilities allow it.

(8) Notwithstanding the preceding paragraph, the records referred to in points 17 and 18 of paragraph four of this Article shall be used exclusively for checking the legality of processing personal data.

(9) For the purpose of paragraph two of Article 94 of this Act, the records referred to in paragraphs three and four of this Article may be linked to each other and to the records set out paragraph six of this Article.

(10) The link between the records referred to in paragraphs three and four of this Article may be established by using the tax identification number or the personal identification number, the registration number and the registration code determined by the Office.

(11) The link between the personal data records referred to in paragraphs three and four of this Article and the records set out in paragraph six of this Article shall be established by using the tax identification number or the personal identification number, or a business entity's registration

number.

Article 150
(The content of records)

(1) In the records on customers, business relationships and transactions which are managed by obliged entities the following data shall be processed:

1. company name, address, registered office, registration number and tax identification number of a legal entity, sole trader or self-employed person entering into a business relationship or carrying out a transaction or on whose behalf a business relationship is established or a transaction carried out;

2. full name, permanent residence, temporary residence in the Republic of Slovenia; if permanent residence is not in the Republic of Slovenia, permanent residence abroad; date and place of birth, tax identification number or personal identification number, nationality, and the number, type of and date of issue, validity date and the name of the authority that issued the official identity document of

- the natural person or his or her statutory representative, sole proprietor or self-employed person who establishes a business relationship or carries out a transaction, or of the natural person on whose behalf a business relationship is established or a transaction carried out;

- the legal representative of the legal entity establishing a business relationship or carrying out a transaction;

- the authorised representative of a natural person, sole trader or self-employed person establishing a business relationship or carrying out a transaction;

- the statutory representative carrying establishing a business relationship or carrying out a transaction for the legal entity or any other civil law entity referred to in point 5 of Article 3 of this Act;

3. full name, address of permanent and temporary residence, and date and place of birth of the natural person entering a casino or gaming hall and receiving payment of a winning or placing a bet referred to in point 3 of paragraph one of Article 22 of this Act, or a natural person accessing a safe deposit box;

4. the number or other unique identification mark of a business relationship, the purpose and the intended nature of the business relationship including information about the activity of the customer;

5. date of establishing a business relationship or the date and time of entering the casino or gaming hall or approaching the safe;

6. date and time of transaction;

7. the amount of a transaction and currency in which the transaction is carried out;

8. the purpose of the transaction and the full name, address of permanent and temporary residence or the company name and registered office of the person for whom the transaction is intended, and the country in which the transaction is carried out, or the data that the obliged entity is obliged to obtain when carrying out transactions in accordance with Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006 (OJ L No. 141, 5.6.2015, p. 1), last amended by Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No. 1093/2010 on the establishment of the European Supervisory Authority (European Banking Authority), Regulation (EU) No. 1094/2010 on the establishment of the European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No. 1095/2010 on the establishment of the European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No. 600/2014 on markets in financial instruments, Regulation (EU) No. 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) No. 2015/847 on information accompanying transfers of funds (OJ L No. 334, 27.12. 2019, p. 1);

9. transaction execution method;

10. the data on the origin of property and assets of the customer, its statutory representative, authorised person and beneficial owner and the data on the origin of property and assets that is, or will be, the subject of the business relationship or transaction;

11. full name, permanent and temporary residences, date and place of birth, tax identification number or personal identification number, citizenship and the number, type and title of the issuer of the official identity document or company name, address, registered office and personal identification number of the person for whom there are grounds for suspecting money laundering or terrorist financing;

12. transaction, asset and property data for which there are grounds for suspecting money laundering or terrorist financing (amount, currency, type of assets and property, value of assets and property, date or period of execution of the transactions);

13. grounds for suspecting money laundering or terrorist financing;

14. for beneficial owners referred to in Articles 42, 43 and 44 hereof:

a) full name, permanent and temporary residence, date of birth, nationality, ownership interest or other method of supervision;

b) in the case referred to in item b) of paragraph one of Article 44 hereof: the data on the category of persons with an interest in establishing a foreign trust, foreign institution or similar foreign law entity;

15. the name of the other civil law entity referred to in point five of Article 3 of this Act and full name, permanent or temporary residence, date and place of birth and tax identification number or personal identification number of the member;

16. information on whether the customer or its beneficial owner is a politically exposed person.

(2) In the records managed by obliged entities of the data reported to the Office, the data referred to in the preceding paragraph of this Article shall be processed for the purpose of implementing the provisions of Articles 75 and 76 of this Act.

(3) For the purposes of Article 80 of this Act, the following data from the records on contact points managed by the Bank of Slovenia shall be processed:

1. full name, permanent and temporary residence, date and place of birth, tax identification number and personal identification number, nationality, and number and type of and name of the authority that issued the official personal document to a natural person designated as the central contact point;

2. company name, registered office, registration number and tax identification number of a legal entity designated as the central contact point.

(4) Cash data records referred to in paragraph three of Article 149 of this Act shall contain data obtained pursuant to Article 5(3,4)(3) or Article 6 of Regulation 2018/1672/EU.

(5) In the records managed by the Office of the data on persons and transactions acquired pursuant to Articles 75 and 76 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 94 hereof.

(6) For the purpose of implementing Articles 94, 113 and 125 of this Act, the following data shall be processed in the records of the carried out operational analyses referred to in point 1 of Article 98 of this Act: full name, permanent and temporary residence, date and place of birth, tax identification number or personal identification number, number, type and title of the issuer of the official personal identification document as well as company name, address, registered office, registration number and the tax identification number of the person for which the Office performed an operational analysis.

(7) For the purpose of Articles 94, 113 and 125 of this Act, the following data shall be processed in the records of the carried out strategic analyses referred to in point 2 of Article 98 of this Act: full name, permanent and temporary residence, date and place of birth, tax identification number or personal identification number, the number, type and title of the issuer of the official personal identification document as well as the company name, address, registered office, registration number and the tax identification number of the person for which the Office performed a strategic analysis.

(8) For the purposes of Articles 94 and 125 of this Act, the following data of the records managed by the Office relating to the initiatives received referred to in Articles 108 and 109 of this Act shall be processed:

1. full name, permanent and temporary residences, date and place of birth, tax identification number or personal identification number, nationality and the number, type and title of the issuer of the official identity document or company name, address, registered office and personal identification number of the person for whom there are grounds for suspecting 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. grounds for suspecting money laundering or terrorist financing or grounds for launching the procedure of forfeiting illicit proceeds;

(9) For the purposes of Articles 94 and 125 of this Act, the following data of the records of notifications and information referred to in Articles 110 and 111 of this Act, the following data shall be processed:

1. full name, permanent and temporary residences, date and place of birth, tax identification number or personal identification number, nationality and the number, type and title of the issuer of the official identity document or company name, address, registered office and personal identification number of the person to whom the Office sent a notification or information;

2. data on the transaction in respect of which there are grounds to suspect money laundering (amount, currency, date or period of execution of transaction);

3. data on previous criminal offence;

4. data on the authority to which the notification or information was sent.

(10) For the purposes of Articles 94 and 125 of this Act, the following data of the records managed by the Office relating to international requests referred to in Articles 114 and 115 of this Act shall be processed:

1. full name, permanent and temporary residence, date and place of birth, tax identification number or personal identification number, and the number, type and title of the issuer of the official personal identification document as well as company name, address, registered office, registration number and the tax identification number of the person to whom the request relates;

2. name of the country, title of the authority to whom the request was sent or of the authority issuing the request.

(11) For the purposes of Articles 94 and 125 of this Act, the following data from the records of personal data managed by the Office and sent abroad, referred to in Articles 114, 115 and 117 of this Act
52., , shall be processed:

1. full name, permanent and temporary residence, date and place of birth, tax identification number or personal identification number, the number, type and title of the issuer of the official personal identification document as well as company name, address, registered office, registration number and the tax identification number of the person whose data is being exported from the country;

2. name of the country and title of the authority to whom the data is being sent.

(12) For the purposes of Article 94 of this Act, the following data from the records managed by the Office relating to the requests, referred to in Articles 115, 116 and 124 of this Act, shall be processed:

1. the name and contact details of the organisation and staff member requesting the information and, if possible, the recipient of the query or search results;

2. reference to the case for which information is requested;

3. the subject of the requests;

4. all measures necessary for the Implementation of the requests.

(13) For the purposes of Article 95 of this Act, records managed by the Office of the following personal data sent abroad referred to in paragraph eleven of Article 115, Article 116 and Article 124 of this Act;
96., , shall be processed:

1. full name, permanent and temporary residence, date and place of birth, tax identification number or personal identification number, the number, type and name of the issuer of the official identification document as well as company name, address, registered office, registration number and the tax identification number of the person whose data is being exported from the country;

2. name of the country and name of the authority to whom the data is being sent.

(14) In the records managed by the Office of criminal offences and other offences under Article 132 of this Act, the following data on money laundering and terrorist financing shall be processed for the purpose of centralisation and analysis:

1. full name, permanent and temporary residence, date and place of birth, tax identification number or personal identification number, the number, type and name of the issuer of the official identification document as well as company name, address, registered office, registration number and the tax identification number of the person in respect of whom the temporary protection of the request for forfeiting or temporarily forfeiting the proceeds;

2. place, time and manner of committing the act which has signs of a criminal offence or other offence;

3. stage of proceedings of the case, statutory definition of the criminal offence of money laundering and the predicate offence, or the statutory definition of the other terrorist financing offence;

4. amount of money seized or the value of illicit proceeds and the date of forfeiture thereof.

(15) In the records managed by the Office relating to the supervisory measures carried out, identified violations and issued decisions and other supervisory measures taken with respect to identified offences by the supervisory authorities referred to in Article 152 of this Act, the following data shall be processed for the purpose of implementing the provisions of Article 167 of this Act:

1. full name and personal identification number for an obliged entity - natural person or, if a foreigner, date and place of birth and permanent and temporary for a foreign natural person;

name, registered office and registration number for an obliged legal entity;

3. place and date of supervision;

4. the subject of supervision;

5. findings;

6. data on the supervisory measures imposed;

7. data on the offender – natural person: full name, personal identification number 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 or her);

8. data on the offender – legal entity (name, registered office and registration number);

9. the number and the date of issue of the minor offence decision;

10. date of finality of minor offence decision;

11. the legal definition of the offence,

12. description of the offence.

(16) For the purposes of Articles 94 and 125 of this Act, the following data of the records managed by the Office relating to reported facts referred to in Articles 108 and 168 of this Act shall be processed:

1. full name, permanent and temporary residences, date and place of birth, tax identification number or personal identification number, nationality and the number, type and name of the issuer of the official identification document or company name, address, registered office and registration number and tax identification number of the person for whom there are grounds for suspecting 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 indicate or may indicate money laundering or terrorist financing.

(17) For the purposes of Articles 94 and 125 of this Act, the following data from the records of the submission of data managed by the Office and referred to in Articles 127, 128 and 129 of this Act shall be processed:

1. full name, permanent and temporary residences, date and place of birth, tax identification number or personal identification number, nationality and the number, type and name of the issuer of the official identification document or company name, address, registered office and registration number and tax identification number of the person in respect of whom the State Prosecutor's Office, the Police, the Financial Administration of the Republic of Slovenia or the body responsible for imposing and implementing restrictive measures accessed the Office's data;

2. data on the transaction in respect of which the State Prosecutor's Office, the Police, the Financial Administration of the Republic of Slovenia or the body responsible for imposing and implementing restrictive measures accessed the Office's data (amount, currency, date or period of executing the transaction);

3. a description of circumstances and grounds for submitting the Office's data and the purpose of the use of the requested data.

(18) For the purposes of Articles 42, 43 and 44 of this Act, the following data from the records on beneficial owners managed by business entities shall be processed:

1. full name, permanent and temporary residence, date of birth, nationality, tax identification number and ownership interest or other method of supervision;

2. in the case referred to in item b) of paragraph one of Article 44 hereof: the data on the category of persons with an interest in establishing a foreign trust, foreign institution or a similar foreign law entity.

(19) Notwithstanding the provisions of the preceding paragraphs, the records referred to in Article 148 of this Act shall not include the registration number or tax number in the case of non-residents and in the case that no personal identification number, registration number or tax identification number has been assigned to non-resident.

(20) For the purposes of Article 76 of this Act, the following data from the records of data on obliged entities for the purpose of reporting to the Office shall be reported:

1. for a legal person, a sole trader or a self-employed person: company name, registration number and activity;

2. for a natural person: full name, job title, hexadecimal number of an electronic identification means, e-mail address and telephone number.

(21) For the purposes of Article 85 of this Act, the following data from the records on authorised persons and their deputies shall be processed:

1. data on the obliged entity: company name and registration number;

2. data on authorised persons and their deputies: full name, job title, date of appointment, date of termination of office, address if different from the address of the registered office, telephone number and e-mail address.

(22) For the purpose of monitoring the issuance of service ID cards to inspectors referred to in Article 158 of this Act, the following data shall be processed: the full name of the inspector, the date of issue, the date of expiry, the date of

withdrawal, destruction or replacement, serial number of the card and the grounds for its expiry, withdrawal, destruction or replacement.

(23) For the purposes of Article 167 of this Act, the following data from the records on the registration of supervisory authorities for electronic data reporting shall be processed:

1. for legal entities: company name (name of the supervisory authority), registration number, activity;

2. for natural persons: full name, duties of the office, hexadecimal number of an electronic identification means, e-mail address and telephone number.

(24) For the purposes of Article 5 of this Act, the following data from the register of virtual currency service providers shall be processed:

1. for legal entities, sole traders or self-employed persons: company name, address, registered office, registration number, tax identification number, standard industrial classification of all economic activities, description of the provision of virtual currency services;

2. for their statutory representatives or sole trader activity holders or self-employed persons: full name, permanent and temporary residence, personal identification number or date and place of birth, tax identification number, nationality, extract from criminal records;

3. for beneficial owners: full name, permanent and temporary residence, date of birth, nationality, ownership interest or other method of supervision, extract from criminal records.

Article 151
(Records of access to data, information and documents by supervisory authorities)

(1) Obliged entities shall keep separate records of access by supervisory authorities referred to in paragraph one of Article 152 of this Act to data, information and documents referred to in paragraph one of Article 134 of this Act.

(2) The records referred to in the preceding paragraph shall comprise the following data:

1. the name of the supervisory authority;

2. the full name of personal name of the authorised official who inspected the data;

3. the date and time of inspection of the data;

4. data, information and documents accessed by a supervisory authority.

(3) Obliged entities shall notify the Office of any access to the data referred to in paragraph one of this Article by the supervisory authorities referred to in paragraph one of Article 152 of this Ac in writing and at the latest within three business days following the inspection of said data.

CHAPTER IX

SUPERVISION

9.1 Supervisory authorities

Article 152

(Supervisory authorities and their activity)

(1) Supervision of implementing the provisions of this Act and the ensuing regulations shall be exercised within their competencies by

(a) the Office,

(b) the Bank of Slovenia;

c) (c) the Securities Market Agency;

(č) the insurance Supervision Agency;

d) (d) the Financial Administration of the Republic of Slovenia;

e) (e) the Market Inspectorate of the Republic of Slovenia;

f) (f) the Agency for Public Oversight of Auditing;

g) (g) the Bar Association of Slovenia; and

h) (h) the Chamber of Notaries of Slovenia.

(2) (2) If the supervisory authority referred to in the preceding of this Article establishes violations during the performance of its supervisory duties, it shall have the right and duty to

1. order measures for eliminating of irregularities and deficiencies within a specified period of time;

carry out the procedures to remedy the violations referred to in Articles 178, 179, 180, 183, 184 and 185 of this Act in accordance with the Act governing offences;

3. propose the adoption of appropriate measures to the competent authority;

4. impose other measures and perform acts for which it is authorised by law or any other regulation.

(3) The implementation of the procedures pursuant to the Act governing offences referred to in Articles 181 and 182 of this Act shall be the responsibility of the Office and of the Financial Administration of the Republic of Slovenia.

(4) Offence proceedings shall be conducted and decided on by an official person authorised by the supervisory authority referred to in paragraph one of this Article who meets the conditions stipulated by the Act governing offences and the

regulations adopted on the basis thereof.

(5) The Office shall communicate to the European Commission the list of competent supervisory authorities referred to in this Article, including their contact information.

(6) The Office as the competent supervisory authority may order a prohibition on conducting activities referred to in Article 4 hereof for up to three years applicable to an obliged entity referred to in points 16, sub-points (j). (k) and (p) of point 19 of paragraph one of Article 4 hereof, and applicable to an obliged entity referred to in paragraph two of Article 4 hereof, if an obliged entity or a member of the management of an obliged entity or the beneficial owner of an obliged entity has been convicted in a final judgement of the following offences: terrorism, travel abroad for terrorist purposes, terrorist financing, incitement and public glorification of terrorist acts, recruitment and training for terrorism and money laundering, if the Office has reasonable grounds to believe that regarding an obliged entity there is an increased risk of money laundering or terrorist financing. The prohibition ordered against the obliged entity on conducting activities referred to in paragraph two of Article 4 in this Act shall be ordered by the Office, subject to the specifics and exceptions provided for in Articles 90 and 91 of this Act. Information on final judgements shall be submitted to the Office by the courts pursuant to Article 132 of this Act. In determining the duration of the prohibition on the activity, the Office shall take into account the obliged entity's attitude towards the commission of the criminal offence and the attitude towards the consequences of the criminal offence, including the benefit gained.

(7) Time served in prison or spent in an institution for treatment and detention by a person who is a sole trader or a self-employed person shall not be counted as part of the duration of such a measure.

(8) In the case of an obliged entity referred to in point 16 of paragraph one of Article 4 of this Act, the Office, as the competent supervisory authority, shall inform the Agency for Public Oversight of Auditing; in the case of an obliged entity referred to in item (p) of point 19 of paragraph one of Article 4 of this Act, the Market Inspectorate of the Republic of Slovenia; in the case of an obliged entity that is a lawyer or law firm, the Bar Association of Slovenia, and, in the case of an obliged entity who is a notary, the Chamber of Notaries of Slovenia.

Article 153
(Supervision and risk assessment)

(1) An approach based on the risks of money laundering and terrorist financing shall be used in the supervision of the obliged entities referred to in Article 4 of this Act.

(2) When planning the frequency, scope and intensity of supervision and conducting supervision the supervisory authorities referred to in the preceding Article shall take into account the following:

- national risk assessment-based information on identified money laundering and terrorist financing;

- information on specific national and international risks related to customers, products and services;

- information on the risk of individual taxpayers and other available data; and - important events or changes relating to the obliged entity's management and governance and change in activity.

(3) At least every two years, the supervisory authorities referred to in the preceding paragraph shall update and properly adjust the planning the frequency, scope, intensity, and implementation of supervision.

(4) The Office shall propose to the other supervisory authorities referred to in the preceding Article to carry out supervision of a certain obliged entity or type of obliged entity based on the information and data available to the Office and based on the strategic and operational analyses.

Article 154
(General powers and responsibilities of the Office)

(1) The Office shall supervise the implementation of the provisions of this Act by the obliged entities referred to in Article 4 of this Act and the implementation of the obligation to determine the beneficial owner and the obligation to enter data on the beneficial owner referred to in Articles 45 and 48 of this Act by business entities referred to in Article 42, paragraph one of Article 43 and Article 44 of this Act.

(2) The Office shall supervise the implementation of the provisions of this Act by gathering and verifying the data, information and documents obtained pursuant to this Act.

(3) (3) Obliged entities shall submit to the Office in writing data, information and documents relating the performance of their duties as provided by this Act, as well as other information that the Office requires for conducting supervision, without delay and no later than within fifteen days of receiving the request.

(4) The obliged entities referred to in Article 42 of this Act, paragraph one of Article 43 and Article 44 of this Act shall send to the Office in writing data, information and documents concerning the implementation of the obligation to determine the beneficial owner and the obligation to enter data on the beneficial owner referred to in Articles 45 and 48 of this Act without delay, but no later than within eight days of receipt of the request.

(5) The Office may also demand from state bodies and from bearers of public authority the data, information and documents required for exercising supervision under this Act and for conducting offence proceedings.

9.2 (Inspection of the Office)

Article 155
(Supervisory powers and responsibilities of the Office)

(1) In addition to supervision performed by supervisory authorities pursuant to Articles 153 and 154 if this Act, the Office shall perform inspection over the implementation of this Act and other regulations on detecting and preventing money laundering and terrorist financing on-site and off-site.

(2) In its report referred to in Article 130 of this Act, the Office shall report to the Government on its inspection activities.

Article 156
(Anti-money laundering prevention inspector)

The duties of the anti-money laundering inspector shall be carried out by officials. Under this Act, officials shall be anti-money laundering inspectors.

Article 157
(Scope of the Act)

Anti-money laundering inspectors shall independently perform their supervisory tasks under this Act, conduct procedures and issue notices and decisions in the administrative and offence procedures.

Article 158
(Service ID cards)

(1) Inspectors shall prove their identity by producing their service ID card issued by the Minister.

(2) The general form of the identity card and the procedure for its issuing shall be prescribed by the Minister, unless otherwise provided by a special Act.

(3) For the purpose of inspecting of the issued service ID cards referred to in this Article, a record of service ID cards issued to anti-money laundering inspectors shall be established.

Article 159
(Powers of inspectors)

(1) In addition to the powers defined by the Act governing inspections, the anti-money laundering inspector shall have the following rights when inspecting a natural person or a legal entity:

- to enter and inspect the premises, land plots and means of transport (hereinafter: premises) at an obliged entity's head office as well as elsewhere;

- to examine internal regulations, books of account, contracts, papers, business correspondence, business records and other information and documents relating to the obliged entity's business and implementation of money laundering and terrorist financing detection and prevention measures, irrespective of the medium on which they are stored (hereinafter: books of account and other documents);

- to seize or obtain copies, forensic copies or extracts from books of account and other documents in any form using the obliged entity's or the Office's photocopiers and computer equipment; if for technical reasons it is not possible to make copies using the obliged entity's or the Office's photocopiers and computer equipment, the inspector may take away books of account and other documents for the time needed to make copies, making an official note thereof;

- to seal any business premises and books of account and other documents for the duration of, and to the extent necessary for, the inspection;

- to seize items and books of account and other documents for a period no longer than twenty business days;

- to ask any representative or member of staff of the undertaking to give an oral or written explanation of facts or documents relating to the subject matter and purpose of the inspection and record it in the minutes. If a written explanation is required, the inspector shall determine the date for its submission;

- to inspect papers disclosing the identity of persons;

- to perform other actions in accordance with the aim of the inspection.

(2) The obliged entity shall provide the inspector with access to the premises and to the books and other documents and shall not obstruct the conduct of the inspection in any way, unless it is a matter of enforcing legal confidentiality. At the request of the inspector, the obliged entity shall ensure the conditions for work on the obliged entity's premises.

(3) In the exercise of their powers referred to in paragraph one of this Article, anti-money laundering inspectors shall pay due regard to the principle of proportionality. In exercising its powers and imposing measures on obliged entities, inspectors shall not exceed what is of vital importance for meeting the objectives under this Act. When choosing between several possible authorisations and measures, inspectors shall choose those that are more favourable for the obliged entity if by doing so the intention of the Act has been reached. When in doubt, inspectors shall decide in favour of obliged entities.

(4) Anti-money laundering inspectors shall give prior notice to the Bar Association of Slovenia of the indicative time frame and the location of the intended inspection with a view to ensuring the presence of their representative in the inspection.

(5) The inspected lawyers and inspected law firms shall have the right to request that the inspection be carried out in the presence of a representative of the Bar Association of Slovenia. Until his or her arrival, all inspection operations shall be suspended, but for not more than two hours from the moment the lawyer or law firm requests his or her presence. After the expiry of this period, inspection shall continue without his or her presence.

(6) In the performance of his or her duties of inspection with a lawyer or a law firm, the anti-money laundering inspector shall be entitled to exercise all the inspection powers under Article 146 of this Act, unless the exercise of his or her powers would interfere with legal confidentiality.

(7) A lawyer, law firm or representative of the Slovenian Bar Association, if present, shall have the right to object to the consultation of data and documents or their seizure in order to safeguard legal confidentiality. In the event of objection, the procedure shall continue with the application, mutatis mutandis, of the provisions of the Act governing criminal proceedings.

(8) The obliged entity may deny an inspector entry into residential premises if the inspector does not have a warrant from the competent court.

Article 160
(Obstruction of inspection)

If the obliged entity refuses to permit, or interferes with, the entry of the inspector into the premises or denies access to books of account or other documents or obstructs or otherwise interferes with an inspection or where this is reasonably expected, the inspector shall have the right to enter the premises or access books of account and other documents against the will of the obliged entity with the assistance of the police, unless the obliged entity is a lawyer or a law firm. The costs of entry or access and any damage suffered shall be borne by the obliged entity.

Article 161
(Records)

The inspector shall draw up a record of the completed inspection, which shall contain, in particular, information on

- the start and the completion or the duration of the inspection;

- the obliged entity;

- the established facts;

- statements of persons present during the inspection;

– seizure of documents;

- authorised official performing the inspection and other persons present during the inspection;

Article 162
(Decision)

(1) Once the inspection has been completed, the inspector shall have the authority to order the obliged entity to ensure the implementation of the laws and other regulations within his or her jurisdiction by means of action, omission of action, or act within the time limit set by the inspector.

(2) Any appeal against the decision referred to in the preceding paragraph shall be lodged within fifteen days of its service. An appeal shall not stay the execution of the decision.

(3) The obliged entity shall report to the inspector on the execution of the decision within eight days after the expiry of the deadline for its execution.

Article 163
(The appellate body)

An appeal lodged against a decision referred to in paragraph one of this Article shall be decided upon by the ministry responsible for finance.

9.3 8.2 Competencies of other supervisory authorities

Article 164
(Other supervisory authorities)

(1) (1) The Bank of Slovenia shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over the implementation of the provisions of this Act with the obliged entities referred to in points 1, 2, 3, 14, 15 and sub-point (č) of point 19 of paragraph one of Article 4 hereof.

(2) The Securities Market Agency shall, in accordance with its competences stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with the obliged entities referred to in points 2, 3, 5, 6, 7, 8, 9, 10, 11 and 12 of paragraph one of Article 4 of this Act.
1., The Securities Market Agency shall supervise the obliged entities referred to in points 1, 2 and 3 of paragraph one of Article 4 of this Act only in the part that relates to the obliged entity's investment banking services and activities and to which the provisions of the Act governing the market in financial instruments are applied. The Agency shall carry out its supervisory activities independently or in cooperation with the Bank of Slovenia.

(3) The Insurance Supervision Agency shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over the implementation of the provisions of this Act with the obliged entities referred to in points 11, 12, sub-points (h) and (i) and point 19 of Article 4 of this Act.
13.,

(4) The Financial Administration of the Republic of Slovenia shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over the implementation of the provisions of this Act with the obliged entities referred to in point 17 of paragraph one of Article 4 of this Act.

(5) The Financial Administration of the Republic of Slovenia shall, in accordance with its competencies, exercise supervision over the implementation of prohibitions against the acceptance of payments for goods in cash in the amount exceeding EUR 5,000 with the legal entities and natural persons referred to in Article 74 of this Act.

(6) The Financial Administration of the Republic of Slovenia shall, in accordance with its competencies, exercise supervision over compliance of the obliged entities referred to in Articles 42, 43 and 44 of this Act with obligations to identify beneficial ownership and register beneficial ownership data referred to in Articles 45 and 48 of this Act.

(7) The Market Inspectorate of the Republic of Slovenia shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over the implementation of the provisions of this Act with the obliged entities referred to in sub-points (a), (b), (g), (m) and (p) of point 19 of paragraph one of Article 4 of this Act.
18.,

(8) The Agency for Public Oversight of Auditing shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with the obliged entities referred to in point 11 of paragraph one of Article 4 of this Act.
16.

(9) The Bar Association of Slovenia shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with lawyers and law firms.

(10) The Chamber of Notaries of Slovenia shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with notaries.

(11) The supervisory authorities referred to in this Article shall submit to any other supervisory authority, upon its request, all necessary information needed by that supervisory authority for exercising its supervisory tasks.

(12) The supervisory authorities referred to in this Article may, for the purposes of performing their supervisory duties under this Act, request from persons under public and private law, which are not the supervisory authorities referred to in the paragraph one of Article 152 of this Act, data, information and documents that such persons have at their disposal and which are necessary to determine compliance with obligations of the obliged entities under this Act and the exercise of other powers of the supervisory authority in connection with detecting and preventing money laundering and terrorist financing without delay, but no later than within eight days of receiving the request.

Article 165
(Access to information contained in the register of transaction accounts)

For the purposes of exercising the powers and duties concerning the prevention and detection of money laundering and terrorist financing, the supervisory authorities referred to in Article 152 hereof shall, free of charge, access, use and process data, including personal data, contained in the register of transaction accounts kept by the Agency of the Republic of Slovenia for Public Legal Records and Related Services pursuant to the Act governing payments, electronic money issuance and payment systems.

Article 166
(Submission of data by the Office to other supervisory authorities)

(1) *Upon a reasoned proposal from the supervisory authorities referred to in Article 164 of this Act , the Office shall provide them with data from the records referred to in point four of Article 149 on the persons and transactions set out in Article 75 of this Act, and on the number of persons and transactions set out in Article 76 of this Act, which are reported by obliged entities within the competence of individual supervisory authorities pursuant to paragraph one of Article 164 of this Act, and which are required by them for carrying out supervision, which also includes analyses for the planning of 0supervisory activities in accordance with Article 153 and issuing recommendations and guidelines in in accordance with Article 169 of this Act.*

(2) The Office shall send the data referred to in the preceding paragraph in anonymised or pseudo-anonymised form, as far as the latter is technically feasible, in which case the Office may not provide the supervisory authorities with information on the basis of which the recipient could independently attribute the data to a specific entity to which they refer.

(3) The supervisory authorities referred to in Article 164 of this Act shall inform the Office of its findings based on the information received under this Article and of other measures

taken on the basis thereof once a year, but no later than by the end of January for the previous year.

(4) The Office may refuse, in part or in full, the request for data referred to in paragraph one of this Article 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.

(5) The Minister shall determine in more detail the method of anonymising or pseudo-anonymising and sending the data referred to in paragraph one of this Article.

(6) The supervisory authorities may associate data referred to in paragraph two of this Article with other data that they acquire and process within the scope of their powers, for the purposes of carrying out supervision in accordance with paragraph one of this Article.

9.4 9.4 Reporting data on supervision

Article 167
(Notification of violations and measures)

(1) The supervisory authorities referred to in paragraph one of Article 152 of this Act shall notify the office via protected electronic means within 15 days of the supervision carried out, violations found, decisions issued, other supervisory measures and other important findings.

(2) The notification referred to in the preceding paragraph shall include data set out in paragraph fifteen of Article 150 of this Act.

(3) The supervisory authority that identifies a violation shall also inform other supervisory authorities of its findings and/or any irregularities if relevant for their work.

(4) To enable centralisation and analysis of all data related to money laundering and terrorist financing, supervisory authorities shall forward to the Office a copy of the decision issued in offence proceedings as well as decisions or orders imposing other measures.

(5) For the purposes of electronic data reporting under this Article, supervisory authorities shall register with the office by reporting data on their institution referred to in paragraph twenty-three of Article 150 of this Act and data on the natural person of a supervisory authority whose responsibility is to report data, and on electronic identification means to be used for electronic data reporting.

Article 168
(Notification of facts)

(1) The supervisory authorities referred to in paragraph one of Article 152 hereof shall notify the Office forthwith in writing if, during carrying out supervision under this Act or during the performance of their activities or business transactions in accordance with their responsibilities defined by other Acts, they have established or discovered facts that are may be associated with money laundering or terrorist financing.

(2) On the basis of the reported facts referred to in paragraph one of this Article, the Office, if it deems appropriate, may start collecting and analysing data, information and documents in compliance with its authorisations determined by this Act.

9.5 (Issuing recommendations and guidelines)

Article 169
(Issuing recommendations and guidelines)

With a view to ensuring a uniform implementation of the provisions of this Act and the ensuing regulations by obliged entities, the supervisory authorities referred to in Article 152 hereof shall independently, or in cooperation with other supervisory authorities, issue recommendations and guidelines relating to implementation of the provisions of this Act for the obliged entities referred to in Article 4 hereof.

Article 170
(National cooperation)

(1) (1) The Office and the supervisory authorities referred to in paragraph one of Article 152 of this Act shall work together to perform their tasks and exercise their powers in the area of supervision and strive together for effective anti-money laundering and terrorist financing measures and supervision.

(2) The cooperation referred to in the preceding paragraph shall also include the possibility that the supervisory authority, within its sphere of competence, performs procedural acts for the requesting supervisory authority and later exchanges information obtained in this context.

(3) The Office and the supervisory authorities referred to in paragraph one of Article 152 of this Act shall strive to the greatest possible extent to achieve uniform supervisory practices and, in this context, also the comparability of the methodological approach used in the implementation of measures and supervision.

(4) For the purpose of effective national cooperation, the supervisory authorities shall appoint a person who is suitably qualified in the field of prevention of money laundering and terrorist financing to take care of the implementation of the tasks within their supervisory authorities under this Act and to cooperate with the Office and other supervisory authorities.

9.6 (Cooperation with the competent supervisory authorities of the Member States, third countries and European Supervisory Authorities)

Article 171
(Consulting the competent supervisory authorities of the Member States)

(1) The Office shall cooperate with the competent authorities of the Member States responsible for anti-money laundering and terrorist financing supervision regarding the supervision of the operations of the obliged entities that operate in particular through their branches and subsidiaries in the Republic of Slovenia and other Member States in which they do not have a registered office.

(2) The Office and other supervisory authorities referred to in paragraph one of Article 152 of this Act shall cooperate with the competent authorities of other Member States, in particular by exchanging all information that could facilitate the supervision of obliged entities.

Article 172
(Consulting the competent third country supervisory authorities)

(1) The Office and other supervisory authorities referred to in paragraph one of Article 152 of this Act shall cooperate with third country supervisory authorities responsible for anti-money laundering and terrorist financing supervision regarding the supervision of the operations of the obliged entities that operate in particular through their branches and subsidiaries in the Republic of Slovenia and other Member States in which they do not have a registered office.

(2) The Office and other supervisory authorities referred to in paragraph one of Article 152 of this Act shall cooperate with the competent authorities of third countries, in particular by exchanging all information that could facilitate the supervision of obliged entities.

(3) Cooperation with the competent supervisory authorities of third countries shall be possible if relevant anti-money laundering and terrorist financing standards, which are equivalent to the provisions of this law, international standards or other regulations, are established in these third countries.

Article 173
(Cooperation with the European Banking Authority)

The Bank of Slovenia, the Securities Market Agency and the Insurance Supervision Agency shall provide the European Banking Authority with all the information necessary to enable the performance of its tasks related to the prevention of money laundering and terrorist financing.

9.7 Breach reporting system

Article 174
(Internal breach notification system)

(1) Obliged entities shall establish a system for notifying internal breaches that allows bank employees and to report breaches of the provisions of this Act via independent and autonomous reporting lines.

(2) The system shall include clearly defined procedures for receiving and examining notifications that are comprehensive and proportionate to the nature and the scale of the activity of the obliged entity.

(3) When, notwithstanding the provision of paragraph one of this Article, an obliged entity that knows the identity of the reporting party, it shall ensure that all information on persons who have filed a report on violations will be treated as confidential pursuant to the act governing personal data protection. The obliged entity may not disclose such data without the consent of those persons except when disclosure of the identity of the reporting party is required in order to carry out pre-trial investigation or subsequent criminal proceedings.

Article 175
(System for notifying breaches to supervisory authorities)

(1) The supervisory authorities referred to in paragraph one of Article 152 of this Act shall establish an effective and reliable notification system enabling employees and persons in comparable positions working for obliged entities to file reports concerning possible or actual violations of the provisions of this Act through one or several secure communication channels. These channels shall ensure that the identity of persons providing information is known only to the supervisory authorities referred to in Article 152 hereof.

(2) The supervisory authorities referred to in paragraph one of Article 152 of this Act shall ensure the following in connection with the notification system referred to in the preceding paragraph:

1. a simple, easily accessible and secure method of reporting violations;

2. internal procedures for receiving and considering reports;

3. appropriate protection of the personal data of persons who have filed a report against an obliged entity and of persons who are allegedly responsible for the breach in accordance with the Act governing personal data protection.

(3) Information referred to in point 3 of the preceding paragraph may not be disclosed without the consent of the person who has filed the report, unless the disclosure of the identity of the reporting person in accordance with the law is

necessary to conduct criminal proceedings or any further judicial proceedings. The supervisory authorities referred to in paragraph one of Article 152 of this Act may not disclose the information about the notifying party or the alleged infringer to the obliged entity that is the subject of notification or to a third party. The supervisory authorities referred to in paragraph one of Article 152 of this Act shall make every effort to prevent the disclosure of the identity of the notifying party or the alleged infringer when identifying and processing the reported violations.

9.8 Disclosures relating to supervision

Article 176

(Disclosure of information on measures imposed)

(1) The supervisory authorities referred to in paragraph one of Article 152 of this Act shall, in order to prevent and deter practices that constitute an infringement of this Act, make public information on supervisory measures and sanctions for infringements imposed due to infringements of this Act.

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

1. information about the infringer and the person liable for the implementation of the measure;

- company name and registered office of the legal entity, or

- full name of the natural person;

2. information about the violation and on the nature of the measure imposed:

- the description of circumstances and practices that constitute violation of this Act and require the implementation of the imposed measure;

- the nature of the identified violations or the type of deficiencies for which the measure has been imposed;

3. - the operative part of the decision legally ending the procedure;

4. - eventual remedy of the violation or implementation of the measure imposed.

(3) When the decision establishing a violation or imposing a measure becomes final, i.e. when the decision identifying a violation becomes final and the infringer or the person liable for the implementation of the measure is aware of it, the information referred to in the preceding paragraph shall be published the websites of the supervisory authorities referred to in Article 152 of this Act and shall be available on the websites for five years after publication. The purpose of the publication of the information referred to in the preceding paragraph is to prevent violations of legal provisions and thus greater legal security when entering into business relationships and the integrity of the business environment, as well as to inform the interested public about the operation of business entities that operate in the business environment and legal transactions in the area of anti-money laundering and terrorist financing regulations.

(4) The Bank of Slovenia, the Securities Market Agency and the Insurance Supervision Agency referred to in paragraph two of this Article shall transmit this information top the European Banking Authority.

Article 177
(Disclosure of identity of infringer)

(1) Notwithstanding paragraphs one and two of the preceding Article, the supervisory authorities referred to in paragraph one of Article 152 of this Ac shall decide not to publish the information on the infringer's identity if:

1. the supervisory measure or sanction was imposed due to minor violations set out in Article 180 of this Act or violations that do not represent an offence under this Act; or

2. the publication of information on the identity of the infringer would jeopardise the interests of successful pre-trial or criminal procedure; or

3. the publication of information on the identity of the infringer would jeopardise the stability of financial markets.

(2) Should the supervisory authority referred to in paragraph one of Article 152 deem that the grounds referred to in the preceding paragraph exist as regards the publication of the identity of the infringer when issuing a decision, they shall decide concurrently with the supervisory measure

- not to publish the identity of the infringer; or

- to temporarily suspend the publication of the infringer's identity and to set the time limit for the suspension if the grounds for suspension of the publication are likely to cease to exist during this period.

(3) If the options referred to in the preceding paragraph are deemed insufficient to ensure the effective protection of relevant personal data or prevent the destabilisation of financial markets, the supervisory authorities referred to in Article 152 hereof shall, in addition to issuing a decision imposing supervisory measures, decide not to publish the information on supervisory measures and sanctions for violations imposed due to the violations of this Act.

CHAPER X

PENALTY PROVISIONS

Article 178

(Most serious offences)

(1) (1) A legal person whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 60,000 for the offences of:

1. failing to make a risk assessment or failing to determine the assessment of the risk individual groups or types of customers, business relationships, transactions, products, services or distribution channels or failing to take into account geographical risk factors or failing to make an adequate assessment of the impact of changes in business processes on risk exposure (paragraphs two, three, four, five and nine of Article 18 hereof);

2. failing to create efficient policies and set up controls and procedures to effectively mitigate and manage the risks of money laundering and terrorist financing (paragraph one of Article 20 hereof);

3. failing to carry out customer due diligence (paragraph one of Article 22, paragraph one of Article 23 and paragraph four of Article 27 hereof);

4. establishing a business relationship with a customer without prior application of the prescribed measures (paragraph one of Article 24 hereof);

5. carrying out a transaction without prior application of the prescribed measures (Article 25 hereof);

6. failing to notify the Office of the intended omission of customer due diligence before starting to market the product (paragraph four of Article 27 hereof) and failing to enclose with the notification documents demonstrating compliance with the conditions and risk assessment referred to in paragraph one of Article 27 hereof;

7. failing to determine and verify the identity of a natural person or his or her statutory representative, sole trader or self-employed person, statutory representative of a legal entity, authorised person of a natural person, sole trader or self-employed person, authorised person of a legal entity, legal entity, representative of another civil law entity and beneficial owner of the legal entity, or failing to obtain the required data, or failing to obtain them in the prescribed manner, or failing to obtain a certified written authorisation or a written power of attorney (Articles 29, 30, 31, 32, 36, 37, 42, 43, 44 in 47 hereof);

8. determining and verifying the identity of a customer by using electronic means of identification in a prohibited manner (paragraph 5 of Article 33);

9. determining and verifying a customer's identity by using video-based electronic identification although the conditions for it have not been met (Article 34);

10. determining and verifying a customer's identity by using remote controlled or electronic procedures and identification methods although the conditions for it have not been met (Article 35);

11. failing to determine or verify the identity of a customer upon the customer's entry into a casino or gaming hall run by a concessionaire offering games of chance, or each time the customer accesses the safe or failing to obtain the required data or failing to obtain it in the required manner (Article 38 hereof);

12. contrary to the provisions of this Act, failing to establish and verify the identity of banks and other similar credit institutions when a bank or other similar credit institution is established in a high-risk third country (paragraph three of Article 55 hereof);

13. failing to retain data and documents obtained in connection with the identification of the beneficial owner in accordance with the provisions of this Act (paragraph three of Article 41 hereof);

14. failing to obtain data on the purpose and the intended nature of the business relationship or transaction, as well as other data pursuant to this Act, or failing to obtain all the required data (Article 53 hereof);

15. entering into a business relationship in contravention of the provisions of this Act (paragraph five of Article 59 hereof);

16. performing simplified customer due diligence even though, pursuant to paragraph one of Article 19 of this Act, failing to determine that a customer, business relationship, transaction, product, service, state or geographical area present a minor risk of money laundering or terrorist financing (paragraph one of Article 62 hereof);

17. failing to obtain, within simplified customer due diligence, the prescribed data on a customer, business relationship or transaction, or failing to obtain data in the prescribed manner (Article 63 hereof);

18. failing to apply the prescribed measures and, in addition, obtain data, information and documents in accordance with paragraph one of Article 65 when entering a correspondent banking relationship with a credit or financial institution established in a third country, or failing to obtain data in the prescribed manner (paragraphs one and three of Article 65 hereof);

19. entering into or continuing, contrary to law, a correspondent banking relationship with a credit or financial institution established in a third country (paragraph five of Article 65 hereof);

20. failing to obtain data on the sources 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 for a customer who is a foreign politically exposed person, or for failing to obtain data in the prescribed manner (point 11 of paragraph six of Article 66 hereof);

21. entering into or continuing a business relationship with a customer who is a politically exposed person that enters into a business relationship for a politically exposed person or whose beneficial owner is a politically exposed person, without the written approval of a superior responsible person occupying a senior management position (point 2 of paragraph seven of Article 66 hereof);

22. failing to establish and implement measures regarding politically exposed persons in life insurance transactions and life insurance linked to investment fund units (Article 68 hereof);

23. failing to take due diligence measures when customers or transactions are associated with a high-risk third country (Article 69 hereof);

24. in the cases referred to in paragraph two of Article 64 of this Act, failing to take one or more additional measures in addition to those referred to in paragraph one of Article 21 of this Act (Article 70 hereof)

25. opening, issuing or keeping for a customer anonymous accounts, passbooks or bearer passbooks, or other products enabling, directly or indirectly, concealment of the customer's identity (Article 71 hereof);

26. entering into a business relationship or carrying out a transaction referred to in Articles 22 and 23 of this Act when 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 Securities Depository or similar register (Article 72 hereof);

27. entering into or continuing a correspondent banking relationship with a respondent 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 73 hereof);

28. accepting cash payment from a customer or third person when selling goods or providing services, which exceeds EUR 5,000, or accepting payment effected by several linked cash transactions exceeding in total the amount of EUR 5,000 (paragraphs one and two of Article 74 hereof);

29. making cash payment to a customer or third person in the framework of its activities, which exceeds EUR 5,000, or making cash payment in several linked cash transactions exceeding in total the amount of EUR 5,000 (paragraphs one and two of Article 74 hereof);

30. failing to provide the Office with the prescribed data where grounds to suspect money laundering or terrorist financing exist in connection with a customer or a transaction or an intended transaction (paragraphs three, four and six of Article 76);

31. failing to communicate to the Office within the prescribed time limit the required data, information and documents when reasons for suspecting money laundering or terrorist financing are given in connection with a transaction, person, property or funds (Articles 99 and

102 hereof);

32. failing to comply with the Office's order temporarily suspending a transaction or the Office's instructions issued in this regard (Article 105 and paragraphs one and three of Article 120 hereof);

33. failing to comply with the Office's written request for ongoing monitoring of a customer's financial transactions (paragraphs one, two and three of Article 107 hereof);

34. disclosing facts referred to in paragraph one of Article 134 of this Act to the customer or to a third party;

35. failing to remedy irregularities and deficiencies within the time limit as specified by an official authorised person (point 1 of paragraph two of Article 152 hereof);

36. failing to comply with a prohibition ordered on conducting activities referred to in paragraph six of Article 152 of this Act;

37. failing to submit to the Office, within the prescribed time limit and in the prescribed manner, data, information and documents on the performance of duties as provided by this Act, as well as other information which the Office requires for conducting supervision, or data, information and documents concerning compliance with the obligation to identify the beneficial owners and to record data on the beneficial owner referred to in Articles 45 and 48 of this Act (paragraphs three and four of Article 154 hereof);

38. failing to allow anti-money laundering inspectors access to premises, books of account and other documents or otherwise inhibiting inspectors in the exercise of their duties and powers (paragraph two of Article 159);

39. failing to submit to the Office, within the prescribed time limit and in the prescribed manner, data, information and documents on the performance of supervisory duties as provided by this Act (paragraph twelve of Article 164 hereof).

(2) A legal person whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 120,000.

(3) A legal person whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last

two consecutive financial years shall be fined between EUR 12,000 and EUR 120,000.

(4) A sole trader or a self-employed person shall be fined between EUR 1,000 and EUR 40,000 for the offence referred to in paragraph one of this Article.

(5) The responsible person of a legal entity or the responsible person of a sole trader or the responsible person of a self-employed person shall be fined between EUR 400 and EUR 4,000 for the offence referred to in paragraph one of this Article.

(6) Where the committed offence referred to in paragraph one of this Article is of a particularly serious nature due to the amount of the damage caused or the amount of the illegal proceeds obtained, or because of the perpetrator's intent or intention of unlawful gain, a legal person shall be fined up to:

1. EUR 1,000,000 or

2. twice the amount of the proceeds gained from the minor offence, where determinable, when this amount exceeds the amount referred to in the preceding point.

(7) Where the committed offence referred to in paragraph one of point 22 of this Article is of a particularly serious nature due to the amount of the damage caused or the amount of the illegal proceeds obtained, or because of the perpetrator's intent or intention of unlawful gain, a sole trader or a self-employed person shall be fined up to:

1. EUR 500,000 or

2. twice the amount of the proceeds gained from the minor offence, where determinable, when this amount exceeds the amount referred to in the preceding point.

(8) A responsible person of the legal person referred to in paragraph six of this Article or a responsible person of the sole trader or a responsible person of the self-employed person referred to in paragraph seven of this Article shall be fined up to EUR 250,000.

(9) A legal person referred to in paragraph six of this Article which is a credit or financial institution shall be fined up to:

1. EUR 5,000,000 or

2. ten percent of its total annual turnover in the preceding financial year when this amount exceeds the amount referred to in the preceding point.

(10) Where the legal person referred to in the preceding paragraph is a credit or financial institution that controls one or more subsidiaries or is itself a subsidiary, the total annual turnover in the preceding financial year shall be the figure from the annual consolidated report under the act governing companies.

(11) A sole trader or a self-employed person referred to in paragraph seven of this Article which is a credit or financial institution shall be fined up to:

EUR 5,000,000 or

1. ten percent of its total annual turnover in the preceding financial year when this amount exceeds the amount referred to in the preceding point.

(12) A responsible person of the legal person referred to in paragraph nine of this Article or a responsible person of the sole trader or a responsible person of the self-employed person referred to in paragraph eleven of this Article shall be fined up to EUR 500,000.

(13) In addition to a fine, a withdrawal of the authorisation for the pursuit of activity may be imposed under the provisions of Articles 258 and 259 of this Act on a legal entity referred to in six and nine of this Article or on a sole trader or a self-employed person referred to in paragraphs seven and eleven of this Article when such an authorisation is required to perform the activity of the legal person, sole trader or self-employed person.

(14) The order for the temporary withdrawal of the authorisation for the pursuit of activity referred to in the preceding paragraph shall be issued by the authority that authorised that issued such an authorisation in a procedure by applying its own procedure, or on the proposal of the Office.

(15) (10) In addition to the imposition of a fine, a responsible person referred to in paragraphs eight and twelve of this Article shall be temporarily disqualified from acting as director.

(16) The order for the temporary disqualification from acting as director referred to in the preceding paragraph shall be issued by the authority that authorised the responsible person's assuming such a position by applying its own procedure, or on the proposal of the Office.

Article 179 (Serious offences)

(1) A legal entity whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 1,500 and EUR 30,000 for the offences of:

1. failing to carry out customer due diligence within the prescribed scope (paragraph one of Article 21 hereof);

failing to define procedures for implementation of the measures referred to in paragraph one of Article 21 of this Act (paragraph six of Article 21 hereof);

2. failing to demand a written statement from the customer, statutory representative, authorised person or the agent of other civil law entities (paragraph three of Article 29, paragraph four of Article 30, paragraph four of Article 31,

paragraph five of Article 36 and paragraph five of Article 37 hereof);

3. failing to monitor business activities undertaken by a customer through the obliged entity with due diligence (paragraph one of Article 54 hereof);

4. failing to obtain the required data when verifying and updating the data (paragraphs three, four and five of Article 54 of this Act);

5. entrusting a third party to carry out customer due diligence without having verified whether that third party meets all the conditions provided by this Act (paragraph two of Article 56 hereof);

6. accepting customer due diligence as appropriate, in which the third party determined and verified the identity of a customer in his or her absence (paragraph three of Article 56 hereof);

7. entrusting 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 five of Article 57 hereof);

8. entrusting customer due diligence to a third party, where 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 58 hereof);

9. failing to define the procedure for determining foreign politically exposed persons in its internal act (paragraph one of Article 66 hereof);

10. not monitoring with due diligence the transactions and other business activities carried out for an organisation by a customer who is a politically exposed person, a customer entering into a business relationship with a politically exposed person, or a customer whose beneficial owner is a politically exposed person after entering into a business relationship with such customer (point 3 of paragraph seven of Article 66 hereof);

11. failing to furnish the Office, within the prescribed time limit, with the prescribed data on any cash transaction exceeding EUR 15,000 (paragraph one of Article 75 hereof);

12. failing to furnish the Office, within the prescribed time limit, with the prescribed data on any transaction exceeding EUR 15,000 crediting the payment accounts referred to in paragraph two of Article 75 of this Act (paragraph one of Article 75 hereof);

13. failing to ensure the implementation of the policies and procedures of the group of which the legal entity is a part concerning measures for detecting and preventing money laundering and terrorist financing (paragraph one of Article 78 hereof);

14. failing 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 82 hereof);

15. failing to appoint an authorised person and one or more deputies for particular tasks of detecting and preventing money laundering and terrorist financing determined by this Act and the ensuing regulations (Article 83 hereof);

16. failing to provide the authorised person with appropriate authorisations, conditions and support for the performance of his or her duties and tasks (Article 86 hereof);

17. failing to ensure regular and effective internal control over the performance of tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act (Article 88 hereof);

18. failing to draw up the list of indicators for the identification of customers and transactions in respect of which there are reasonable grounds to suspect money laundering or terrorist financing, or failure to draw up said list in the prescribed manner and time limit (Article 92 hereof);

19. failing to keep data and documents for 10 years after the termination of a business relationship, completion of a transaction, or the customer's entry into the casino or gaming hall or access to the safe (paragraph one of Article 142 hereof).

(2) A legal entity whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 60,000.

(3) A legal entity whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 60,000.

(4) A sole trader or a self-employed person shall be fined between EUR 500 and EUR 20,000 for the offence referred to in paragraph one of this Article.

(5) The responsible person of a legal entity or the responsible person of a sole trader or the responsible person of a self-employed person shall be fined between EUR 200 and EUR 2,000 for the offence referred to in paragraph one of this Article.

Article 180
(Minor offences)

(1) A legal entity whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 750 and EUR 15,000 for the offences of:

1. failing to examine beforehand, when determining and verifying the identity of a customer, the nature of the register from which data on the customer shall be obtained (paragraph six of Article 36 hereof);

2. failing to ensure that the scope and frequency of measures referred to in paragraph one of Article 54 are appropriate to the risk of money laundering or terrorist financing to which the obliged entity is exposed in carrying out individual transactions or in business operations with individual customers (paragraph four of Article 54 hereof);

3. failing to inform the competent supervisory authorities referred to in Article 152 of this Act and failing to take appropriate measures to eliminate the risk of money laundering or terrorist financing (paragraph four of Article 82 hereof);

4. failing to ensure that the work of an authorised person or his or her deputy is entrusted solely to a person meeting the prescribed requirements (paragraphs one and two of Article 84 hereof);

5. failing to forward to the Office, within the prescribed time limit, the personal data on the authorised person and his or her deputy and any changes thereof (paragraph five of Article 86 hereof);

6. failing to provide regular professional training for all employees whose duties include the prevention and detection of money laundering and terrorist financing under this Act (paragraph two of Article 87);

7. failing 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 87 hereof);

8. failing to use the list of indicators referred to in paragraph one of Article 92 of this Act when determining the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto (paragraph three of Article 92 hereof);

9. failing to keep the information and accompanying documents on the authorised person and deputy authorised person, on the professional training of staff, on the performance of internal control and risk management referred to in Articles 18, 83, 84 and 87 of this Act for four years after the appointment of the authorised person or deputy authorised person and after the completion of professional training and the performance of internal control and analysis of the impact of changes in the obliged entity's business processes associated with money laundering or terrorist financing (paragraph three of Article 142);

10. failing to keep separate records of access to data, information and documents referred to in paragraph one of Article 134 hereof by the supervisory authorities referred to in Article 152, or for keeping incomplete records (paragraphs one and two of Article 151 hereof);

11. failing to inform the Office, within the prescribed time limit and in the prescribed manner, of any access of the supervisory authorities to data, information and documents referred to in paragraph one of Article 134 hereof (paragraph three of Article 151 hereof);

12. failing to report to the inspector within eight days after the expiry of individual deadlines for the implementation of the inspector's decision imposing on the obliged entity the obligation to ensure the implementation of the laws and other regulations (paragraph three of Article 162 hereof).

(2) A legal entity whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 1,500 and EUR 30,000 for committing the offence referred to in the preceding paragraph.

(3) A legal entity whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 30,000 for committing the offence referred to in paragraph one of this Article.

(4) A sole trader or a self-employed person shall be fined from EUR 250 to EUR 10,000 for the offence referred to in paragraph one of this Article.

(5) The responsible person of a legal entity or the responsible person of a sole trader or the responsible person of a self-employed person shall be fined between EUR 100 and EUR 1,000 for the offence referred to in paragraph one of this Article.

Article 181
(Violations by business entities relating to beneficial ownership data)

(1) Legal entities whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 30,000 for the offences of:

1. failing to identify data or finding false data on their beneficial owner or owners; failing to establish and manage accurate records of data concerning their beneficial owners, or if they fail to update such records upon each modification of data, or failing to keep the data on their beneficial owners for five years following the date of the termination of beneficial owner status (paragraphs one, two, four and six of Article 45 hereof);

2. failing to provide without delay data on their beneficial owners or providing false data at the request of obliged entities or law enforcement bodies, courts and supervisory authorities referred to in paragraph one of Article 152 of this

Act (Article 46 hereof);

3. failing to enter in the register the data concerning their beneficial owner and their modifications within the prescribed time or entering false data (paragraph three of Article 48 hereof).

(2) A legal entity whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

(3) A legal entity whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph one of this Article.

(4) A sole trader or a self-employed person shall be fined from EUR 1,500 to EUR 15,000 for the offence referred to in paragraph one of this Article.

(5) The responsible person of a legal entity or the responsible person of a sole trader or the responsible person of a self-employed person shall be fined between EUR 400 and EUR 2,000 for the offence referred to in paragraph one of this Article.

Article 182
(Violations of beneficial owners concerning the provision of information to business entities)

An individual who is a beneficial owner of a business entity shall be fined from EUR 400 to EUR 2,000 for failing to provide the business entity with all data required for the fulfilment of obligations referred to in paragraphs one, two, four and six of Article 45 hereof (paragraph five of Article 45 hereof).

Article 183

(Specific offences by auditing firms, legal entities and natural persons performing accounting or tax advisory services)

(1) An auditing firm or a legal entity performing accounting or tax advisory services whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 60,000 for an offence of failing to inform the Office within the statutory time limit that it was approached by a customer seeking advice on money laundering and terrorist financing (paragraph five of Article 76 hereof).

(2) An auditing firm or a legal entity performing accounting or tax advisory services whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

(3) An auditing firm or a legal entity performing accounting or tax advisory services whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph one of the preceding paragraph.

(4) A sole trader or a self-employed person performing accounting and tax advisory services shall be fined between EUR 2.000 and EUR 40.000 for committing the offence referred to in paragraph one of this Article.

(5) The responsible person of a legal entity or the responsible person of a sole trader or the responsible person of a self-employed person shall be fined between EUR 400 and EUR 2,000 for the offence referred to in paragraph one of this Article.

Article 184
(Offences by lawyers, law firms and notaries)

(1) A law firm whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 60,000 for an offence of failing to inform the Office within the prescribed time limit that it was approached by a customer seeking advice on money laundering and terrorist financing (paragraph five of Article 90 hereof).

(2) A law firm whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

(3) A law firm whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph one of this Article.

(4) A lawyer or a notary shall be fined between EUR 2,000 and EUR 40,000 for failing to notify the Office within the prescribed time limit that it was approached by a customer seeking advice on money laundering or terrorist financing (paragraph two of Article 90).

(5) A law firm whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000

to EUR 60,000 for the offence of failing to communicate to the Office within the prescribed time limit the required data, information and documents when reasons for suspecting money laundering or terrorist financing are given in connection with a transaction, person, property or funds (paragraphs one, two and three of Article 100).

(6) A law firm whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

(7) A law firm whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph five of this Article.

(8) A lawyer or a notary shall be fined between EUR 12,000 and EUR 120,000 of the offence of failing to 0communicate to the Office within the prescribed time limit the required data, information and documents when reasons for suspecting money laundering or terrorist financing are given in connection with a transaction, person, property or funds (paragraphs one, two and three of Article 100).

(9) The responsible person of a law firm, lawyer or notary shall be fined from EUR 800 to EUR 4,000 for the offence referred to in paragraphs one, four, five or eight of this Article.

Article 185
(Offences by virtual currency service providers)

(1) (1) A legal entity whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 3,000 and EUR 60,000 for the offences of:

1. performing an exchange service between virtual and fiat currencies or provides a custodian wallet service prior to being entered in the register of providers engaged in exchange services between virtual and fiat currencies and custodian wallet providers (paragraph two of Article 5 hereof);

2. 2. providing virtual currency services in contravention of paragraph two of Article 6 of this Act;

3. 3. as a provider engaged in exchange services between virtual and fiat currencies failing to notify the Office in writing of the providers involved in their exchange services between virtual and fiat currencies (paragraph ten of Article 5 hereof).

(2) A legal entity whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

(3) A legal entity whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years shall be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph one of this Article.

(4) A sole trader or a self-employed person shall be fined between EUR 2.000 and EUR 40.000 committing the offence referred to in paragraph one of this Article.

(5) The responsible person of a legal entity, the responsible person of a sole trader or the responsible person of a self-employed person shall be fined between EUR 800 and EUR 4,000 for the offence referred to in paragraph one of this Article.

Article 186
(Imposition of a fine in a fast-track procedure)

A fine exceeding the statutory minimum may also be imposed in an amount that is higher than the minimum prescribed fine under this Act.

Article 187
(Application of minor offence provisions)

Until the provisions of the Act governing offences relating to fines and the ranges of fines are amended, the fines and ranges of fines laid down by Article 178 of this Act shall apply, notwithstanding the provisions of the Act governing offences.

CAPTER XI

TRANSITIONAL AND FINAL PROVISIONS

Article 188
(Transition to a new regime)

(1) The provisions of of this Article shall apply until the date of application of the provisions of paragraph two of Article 193 of this Act.

(2) The register of beneficial owners in which accurate and updated data on beneficial owners is kept shall be set up to ensure the transparency of ownership structures of business entities, thereby preventing the abuse of business entities for money laundering and terrorist financing. By setting up the aforementioned register, obliged entities are provided access to the relevant data for the needs of implementing customer due diligence, and the law enforcement, courts and supervisory authorities referred to in paragraph one of Article 152 hereof are provided with respective access for the needs of performing the powers and duties concerning the prevention and detection of money laundering and terrorist financing.

(3) The register shall be maintain and managed by an administrator.

(4) Business entities referred to in Article 42, paragraph one of Article 43 and Article 44 of this Act except

– sole traders;

- self-employed persons and single-member limited liability

companies shall enter data on their beneficial owners in the

register within

eight days of 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 of the change of data.

(5) The trustee of a trust or a person in an equivalent position at the entity referred to in Article 44 hereof with its registered office or permanent residence in the Republic of Slovenia shall enter the data on the beneficial owners of the entity referred to in Article 44 hereof or within eight days from the entry of the business entity who is a trustee of a trust or a person in equivalent position in the Slovenian Business Register or within eight days from the registration of permanent residence in the Republic of Slovenia.

(6) The trustee of a trust or a person in an equivalent position at the entity referred to in Article 44 hereof with its registered office or permanent residence in a third country shall enter the data on the beneficial owners of the entity referred to in Article 44 hereof within eight days from the entry into a business relationship or the entry of the acquisition of the property right to a real estate into the land register.

(7) Where the trustee of a trust or a person in equivalent position at the entity referred to in Article 44 hereof has its registered office or permanent residence in different Member States or enters into several business relationships in different Member States, the obligation of being entered in the register of beneficial owners is deemed fulfilled if the trustee submits a certificate of proof of registration or an extract of the beneficial ownership information held in a register kept by a Member State.

(8) The provisions of this Article shall not apply to business entities that are companies on a regulated market that is subject to disclosure requirements that provide suitable transparency of ownership information in conformity with European Union legislation or subject to the equivalent international standards.

(9) The responsibility for the correctness of the registered data lies with individual business entities.

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

a) data on the business entity:

− company name, address, registered office, registration number and tax identification number, date of entry and deletion of a business entity – for business entities entered in the Slovenian Business Register;

− company name, address, registered office, tax identification number, date of entry and deletion of a business entity from the Tax Register – for business entities not entered in the Slovenian Business Register;

b) data on the beneficial owner: personal name, address of permanent and temporary residence, date of birth, tax identification 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 item (b) of paragraph one of Article 44 hereof: the data on the category of persons with an interest in establishing a foreign trust, foreign institution or similar foreign law entity.

(11) The register administrator shall maintain and control 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 type 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 to the law enforcement authorities, courts and supervisory authorities referred to in Article 152 hereof.

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

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

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

(15) Upon entry, the personal data on the beneficial owner who is a natural person not entered in the Central Population Register shall be automatically obtained from the Tax Register on the basis of the tax identification number. The register 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 identification number.

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

Article 189
(Issuance of implementing regulations)

(1) The Government shall issue the regulations referred to in paragraph one of Article 9 and paragraph one of Article 67 of this Act within one year following the entry into force of this Act.

(2) The Government shall issue the regulation referred to in paragraph four of Article 14 of this Act within six months after having taken note of the report on the findings of the national money laundering and terrorist financing risk assessment referred to in paragraph one
13. of Article [missing!]of this Act.

(3) The Minister shall issue the regulations referred to in paragraph nine of Article 5, paragraph five of Article 34, paragraph five of Article 35, paragraph five of Article 38, paragraph nine of Article 50, paragraph three of Article 62, paragraph three of Article 64, paragraph six of Article 75, Article 77, Article 89, paragraph one of Article 96 and paragraph five of Article 166 of this Act within one year of the entry into force of this Act.

Article 190
(End of validity and application of implementing regulations)

(1) Upon the entry into force of this Act, the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia *[Uradni list RS]*, Nos. 68/16, 81/19, 91/20 and 2/21 - corrigendum; hereinafter: the ZPPDFT-1) shall cease to be in force.

(2) Upon entry into force of this Act, the following regulations shall cease to be in force, but shall, with the exception of the regulation referred to in point 3 of this paragraph, continue to apply until entry into force of the regulations based on this Act:

1. Decree on the exemption of organisers of classic games of chance from the implementation of measures for detecting and preventing money laundering and terrorist financing (Official Gazette of the Republic of Slovenia *[Uradni list RS],* No. 66/18);

2. Decree on the list of functions qualifying as prominent public functions in the Republic of Slovenia (Official Gazette of the Republic of Slovenia *[Uradni list RS],* No. 164/20);

3. Rules on determining the conditions for establishing and verifying customers' identity by means of electronic identification (Official Gazette of the Republic of Slovenia *[Uradni list RS]*, No. 50/17);

4. Rules on technical requirements to be met by means of video-based electronic identification (Official Gazette of the Republic of Slovenia [*Uradni list RS*], No. 32/18);

5. Rules on the establishment, maintenance and keeping of the Register of Beneficial Owners (Official Gazette of the Republic of Slovenia [*Uradni list RS*], No. 66/17);

6. Tariff for accessing data in the register of beneficial owners (Official Gazette of the Republic of Slovenia [*Uradni list RS*], No. 76/17);

7. Rules on factors of low risk and increased risk for money laundering and terrorist financing (Official Gazette of the Republic of Slovenia *[Uradni list RS]*, Nos. 6/18 and 152/20);

8. Rules laying down the conditions under which information on cash transactions executed by certain customers need not be reported (Official Gazette of the Republic of Slovenia *[Uradni list RS],* No. 31/18);

9. Rules on the performance of internal control, authorised persons, the storage and protection of data, professional training and management of the records of liable persons (Official Gazette of the Republic of Slovenia [*Uradni list RS*], No. 54/17);

10. Rules on the method for reporting information to the Office of the Republic of Slovenia for Money Laundering Prevention (Official Gazette of the Republic of Slovenia *[Uradni list RS],* No. 32/17).

Article 191
End of validity of implementing regulations

Rules on service ID cards for inspectors in the field of prevention of money laundering (Official Gazette of the Republic of Slovenia, *[Uradni list RS]*, No. 30/17) shall remain in force as regulation issued pursuant to paragraph two of Article 158 of this Act.

Article 192
(Harmonis ation)

(1) The guidelines issued pursuant to Article 154 of the ZPPDFT-1 shall be brought into line with this Act within six months of the entry into force thereof.

(2) Obliged entities shall carry out a risk assessment referred to in paragraphs two, three and four of Article 18 by no later than 18 months after the entry into force of this Act...

(3) The register administrator shall establish an IT solution for entering, accessing and managing the data entered in the register within 12 months of the entry into force of the rules referred to in paragraph nine of Article 50 hereof.

(4) Within eight days after the IT solution referred to in paragraphs one, two, three, four, five, six, seven and eight of Article 50 of this Act has been established, the register administrator shall automatically transfer to the register the data on the business entities referred to in paragraph seven of the amended Article 48 hereof, except on those business entities that were already registered on the date of establishment of the IT solution referred to in the preceding paragraph hereof.

(5) The business entities entered in the Slovenian Business Register and business entities entered in the Slovenian Tax Register and not entered in the Slovenian Business Register before the start of application of Article 48 and paragraphs one, two, three, four, five, six, seven and eight of Article 50 of this Act pursuant to paragraph two of Article 193 of this Act shall be deemed to have fulfilled the obligation referred to in paragraphs three of Article 48 hereof within the prescribed time limit by entering the data on their beneficial owners in the register of beneficial owners within six months after the beginning of application of Article 48 and paragraphs one, two, three, four, five, six, seven and eight of Article 50 of this Act.

(6) The Office shall establish an IT solution for anonymising and transmitting the data referred to in paragraph one of Article 166 of this Act within 12 months after entry into force of the regulation referred to in paragraph five of Article 166 of this Act.

Article 193
(Date of application of individual provisions of the Act)

(1) Paragraph two of Article 26 of this Act shall start to apply within six months of the entry into force of this Act.

(2) The provisions of Article 48 and paragraphs one, two, three, four, five, six, seven and eight of Article 50 of this Act shall start to apply after the IT solution referred to in paragraph three of Article 192 of this Act has been established.

(3) The Minister shall publish a notice in the Official Gazette of the Republic of Slovenia that the IT solution referred to in paragraph three of Article 192 of this Act has been established and that the provisions of Article 48 and paragraphs one, two, three, four, five, six, seven and eight of Article 50 of this Act shall start to apply.

(4) (2) The provisions of Article paragraphs two, three and four of Article 166 of this Act shall start to apply after the IT solution referred to in paragraph six of Article 192 of this Act has been established.

(5) The Minister shall publish a notice in the Official Gazette of the Republic of Slovenia that the IT solution referred to in paragraph six of Article 192 of this Act has been established and that the provisions of paragraphs two, three and four of Article 166 of this Act shall start to apply.

Article 194
(Entry into force)

This Act shall enter into force on the day following its publication in the Official Gazette of the Republic of Slovenia.

(Published on 4 April 2022)

TABLE OF CONTENTS