

Legal notice

All effort has been made to ensure the accuracy of this translation, which is based on the original Slovenian text. All translations of this kind may, nevertheless, be subject to a certain degree of linguistic discord. In case of any uncertainties regarding the English translation the questions may be addressed to:

Ministry of Finance – Office for Money Laundering Prevention
Cankarjeva 5
1001 Ljubljana
Slovenia
Phone: +386 1 200 1800
Fax: +386 1 425 2087
E-mail: mf.uppd@mf-rs.si

The original text of this act is written in the Slovenian language; in case of any doubt or misunderstanding, the Slovenian text shall therefore prevail. Original text can be found in Official Gazette of Republic of Slovenia, nos: 60/2007 and 19/2010, or on web pages <http://www.uradni-list.si/1/objava.jsp?urlid=200760&stevilka=3206> (ZPPDFT) and <http://www.uradni-list.si/1/objava.jsp?urlid=201019&stevilka=808> (ZPPDFT-A).

PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING ACT

UNOFFICIAL CONSOLIDATED TEXT

of ZPPDFT, published in the Official Gazette of the Republic of Slovenia, No. 60 of 6 July 2007, page 8332, and ZPPDFT-A, published in the Official Gazette of the Republic of Slovenia, No. 19 of 12 March 2010, page 2278

CHAPTER I GENERAL PROVISIONS

1.1 Contents of the Act

Article 1

(Contents of the Act and transposed EU directives)

(1) This Act shall lay down the measures, competent authorities and procedures for identifying and preventing money laundering and terrorist financing pursuant to Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ No L 309, 25.11.2005, p. 15; hereinafter: Directive 2005/70/ES), Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of “politically exposed person” and the technical criteria for simplified customer due diligence procedure and for exemption on grounds of financial activity conducted on an occasional or very limited basis (OJ L No. 214 of 04.08.06, p. 29), and Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, and amended Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ No. L 319 of 5.12.07, p. 1; (hereinafter: Directive 2007/64/EC).

1.2 Definitions and scope

Article 2 (Money laundering and terrorist financing)

(1) For the purposes of this Act, **money laundering** shall mean any conduct for the purpose of disguising the origin of money or other property obtained by an offence and shall include:

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

(2) For the purposes of this Act, **terrorist financing** shall mean 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 by a terrorist (hereinafter: terrorist) or terrorist organisation.

(3) For the purposes of this Act, offence shall mean any offence defined in Article 2 of the Act Ratifying the International Convention for the Suppression of the Financing of Terrorism (Official Gazette – MP, No. 21/04).

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

- commits or intends to commit a terrorist act by any means;
- is involved in the commission of a terrorist act as an accessory, instigator or aide;
- organises a terrorist act to be committed; or
- contributes to a terrorist act of a group of people operating to achieve a common goal, provided such contribution is intentional and with the purpose to perpetuate the terrorist activity, or provided that he/she understands the group's intent to commit a terrorist act.

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

- commit or intend to commit a terrorist act by any means;
- participate in committing a terrorist act;
- organise a terrorist act to be committed; or
- contribute to a terrorist act of a group of people operating to achieve a common goal, provided such contribution is intentional and with the purpose to perpetuate the terrorist activity, or provided that they understand the group's intent to commit a terrorist act.

Article 3 (Definition of other terms)

For the purposes of this Act:

1. *Property shall mean 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.*
2. Assets shall 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 organisations;
 - c) financial instruments stipulated by the law governing financial instruments, namely publicly- and privately-traded securities, including shares and stocks, certificates, debt instruments, bonds, debentures, warrants and derivative financial instruments;

- d) interest, dividends or other income from assets;
 - e) claims, loans and letters of credit;
 - f) other documents proving entitlement to assets or other financial sources.
3. Office shall mean the Office for Money Laundering Prevention of the Republic of Slovenia.
4. Member State shall mean a Member State of the European Union or a signatory state to the European Economic Area Agreement (Official Gazette, No. 59/05).
5. *Third country shall mean a European Union non-Member State or a non-signatory to the European Economic Area Agreement or an equivalent third country referred to in paragraph (5) of Article 25 of this Act.*
6. Trust and company service provider shall mean any natural person or legal entity which by way of business provides any of the following services to third parties:
 - a) forming legal entities;
 - b) acting as or arranging for another person to act as director or secretary of a company or partner (hereinafter: 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;
 - d) 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;
 - e) 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.
7. *The term "payment institution" shall have the same meaning as in the act governing payment services and systems.*
8. For the purposes of this Act, non-profit organisations shall mean societies, establishments, institutions and religious communities predominantly engaged in non-profit activities and established in accordance with the applicable legislation.
9. For the purposes of this Act, other civil law entity shall mean an organised ring of individuals who pool or will pool assets or other property for a particular purpose.
10. *The term "electronic money" shall have the same meaning as in the act governing payment services and systems.*
11. The term credit institution shall have the same meaning as in the Act governing banking.
12. For the purposes of this Act, the term beneficial owner shall include the following:
 - a natural person who ultimately owns or supervises or otherwise exercises control over a customer (provided the party is a legal entity or other similar legal subject), or
 - a natural person on whose behalf a transaction is carried out or services performed (provided the customer is a natural person).
13. Business relationship shall mean a business or other contractual relationship linked with the organisation's operations, concluded or entered into by a party within the organisation.
14. For the purposes of this Act, a correspondent relationship shall mean 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). A correspondent relationship shall also mean an agreement concluded by a domestic credit institution with a respondent foreign credit or similar institution for the purpose of conducting business abroad through the respondent.

15. A shell bank shall mean 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 group.
16. Cash referred to in Article 38 hereof shall mean notes or coins in circulation as a means of payment.
17. Cash referred to in Article 73 hereof shall have the same meaning as in Regulation No. 1899/2005 of the European Parliament and the Council of 26 October 2005 on control of cash entering or leaving the Community (OJ L 309 of 25 November 2005, p. 9).
18. *The term "payment account" shall have the same meaning as in the act governing payment services and systems.*
19. A transaction shall mean any receipt, handover, exchange, safekeeping, disposal or other handling of monies or other property by a person liable.
20. *Cash transaction shall mean any receipt, handover or exchange of cash referred to in point 16 of this Article, in which the person liable receives physical cash from the customer or hands over physical cash to the customer in possession and disposition.*
21. Factoring shall mean factoring with or without recourse.
22. Forfeiting shall mean financing exports based on purchase with discount and without recourse of long-term outstanding receivables secured by financial instrument.
23. *Official personal identification document shall mean 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.*
24. The terms regulated market and stock exchange shall have the same meaning as in the Act governing the financial instruments market.
25. For the purposes of this Act, the term financial institution shall mean organisations referred to in points 3, 5, 6, 7, 8, 10, 16(a) to (i) of paragraph 1 of Article 4 hereof and for institutions of Member States providing equivalent services.
26. For the purposes of this Act, life insurance shall mean insurance defined as life insurance by the Act governing insurance business.
27. Personal name shall consist of a first name and family name, of which each may be composed of several words that form a whole.
28. Information about the activity of a customer (natural person) shall mean data on a customer's private, professional or other similar engagement (employed, retired, student, unemployed, etc.) or data on 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.
29. *"Long-term" shall refer to a period longer than three years.*
30. *According to this Act, a foreign legal entity shall mean an entity with a legal form not existing under the Slovenian legal order; however, this entity may receive, manage or allocate assets for a specific purpose pursuant to its national legislation (e.g. Stiftung or Trust).*

Article 4 **(Persons under obligation)**

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

1. banks, branches of banks from third countries and Member State banks which establish branches in the Republic of Slovenia or which are authorised to directly perform banking services in the Republic of Slovenia;
2. savings banks;
3. *Payment institutions 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 or directly;*
4. *post office if it provides money transmission services (deposits and withdrawals) through postal money orders;*
 5. management companies of investment funds, branches of management companies of investment funds from third countries, management companies of investment funds from Member States which establish branches in the Republic of Slovenia or are authorised to provide services of investment fund management in the Republic of Slovenia, and other persons who may provide particular services or activities of managing investment funds pursuant to the Act governing investment fund management;
 6. founders and managers of mutual pension funds and pension companies;
 7. brokerage companies, branches of brokerage companies from third countries, brokerage companies from Member States which establish branches in the Republic of Slovenia or are authorised to provide services relating to securities directly in the Republic of Slovenia, and other persons who may provide particular services relating to securities pursuant to the Act governing the securities market or the Act governing the financial instruments market;
 8. 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 directly in the Republic of Slovenia;
 9. electronic money undertakings, branches of electronic money undertakings from third countries, and electronic money undertakings from Member States which establish branches in the Republic of Slovenia or which are authorised to provide electronic money services directly in the Republic of Slovenia;
 10. currency exchange offices;
 11. auditing firms and independent auditors;
 12. concessionaires organising special gaming in casinos or gaming halls;
 13. organisers regularly offering sport wagers;
 14. organisers and concessionaires offering games of chance via the Internet or other telecommunications means;
 15. pawnbroker shops;
 16. legal entities and natural persons conducting business relating to:
 - a) granting credits or loans, also including consumer credits, mortgage credits, factoring and financing of commercial transactions, including forfeiting;
 - b) financial leasing;
 - c) *issuing and management of other payment instruments (for instance, bills and traveller's cheques), which are instruments of payment according to the act governing payment services and systems;*
 - d) issuing of guarantees and other commitments;
 - e) portfolio management services to third parties and related advice;
 - f) safe custody services;
 - g) mediation in the conclusion of loan and credit transactions;
 - 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;
 - l) trust and company services;
 - m) trade in precious metals and precious stones and products made from these materials;
 - n) trade in works of art;
 - o) *organisation or execution of auctions or*
 - p) real property transactions
- (hereinafter: organisations).

Pursuant to the provisions of Chapter III herein, the measures for detecting and preventing money laundering and terrorist financing stipulated by the present Act shall be applied by lawyers, law firms and notaries as well.

(3) For the purposes of this Act, the term **obliged person** shall refer collectively to organisations, lawyers, law firms and notaries.

(4) The Government of the Republic of Slovenia may determine the conditions under which the obligation to apply the measures under the present Act shall not apply to legal entities or natural persons referred to in paragraph 1 of this Article who only pursue activity occasionally or in limited scope and who are exposed to a low risk of money laundering or terrorist financing. When determining terms and conditions, the Government of the Republic of Slovenia shall take account of the technical criteria adopted by the European Commission pursuant to Article 40 of Directive 2005/60/EC and the related findings of the office and supervisory bodies referred to in Article 85 hereof.

CHAPTER II DUTIES AND OBLIGATIONS OF ORGANISATIONS

2.1 General provisions

Article 5 (Duties and obligations of organisations)

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

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

1. applying measures to acquire knowledge about the customer (hereinafter: customer due diligence) under the terms and conditions and in the manner provided by the present Act;
2. reporting prescribed and requisite data and submitting evidence to the office in accordance with the provisions of the present Act;
3. appointing an authorised person and assistant authorised person and ensuring conditions for their work;
4. providing regular professional training and education for workers and ensuring regular internal control over the performance of duties under this Act;
5. preparing a list of indicators for identification of customers and transactions in respect of which reasonable grounds to suspect money laundering or terrorist financing exist;
6. ensuring protection and retention of data and management of records required by this Act;
7. applying measures for detecting and preventing money laundering and terrorist financing in branches and majority-owned subsidiaries located in third countries;
8. performing other tasks and duties under this Act and the ensuing regulations.

Article 6 (Risk of money laundering and terrorist financing)

(1) Risk of money laundering or terrorist financing shall mean the risk that the customer would misuse the financial system for money laundering and terrorist financing or that a business relationship, transaction or product would be used, directly or indirectly, for money laundering or terrorist financing.

(2) An organisation shall prepare a risk analysis and establish a risk assessment for individual groups or customers, business relationships, products or transactions with respect to their potential misuse for money laundering or terrorist financing.

(3) An organisation shall draw up the risk analysis referred to in the preceding paragraph in accordance with guidelines issued by and within the powers of the competent supervisory body referred to in Article 85 of this Act.

(4) In respect of point 4 of paragraph 1 of Article 33 of this Act, only persons meeting the criteria set in the rules issued by the minister responsible for finance may be treated by an organisation as customers assessed as representing a low risk of money laundering or terrorist financing. The minister shall take account of the technical criteria adopted by the European Commission pursuant to Article 40 of Directive 2005/60/EC and related data from the office and supervisory bodies.

(5) The risk analysis or the procedure to establish risk assessment referred to in paragraph 2 of this Article shall reflect the specific features of the organisation and its operations (e.g. its size and composition, scope and structure of business, types of customers doing business with the organisation, and types of products offered by the organisation).

2.2 Customer due diligence

2.2.1 General provisions

Article 7 (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. determining the beneficial owner of the customer;
3. obtaining data on the purpose and intended nature of the business relationship or transaction, as well as other data pursuant to this Act;
4. regularly monitoring business activities undertaken by the customer through the organisation.

(2) The organisation shall define procedures for the implementation of the measures referred to in paragraph 1 of this Article in its internal regulations.

Article 8 (Obligation to carry out customer due diligence)

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

1. when establishing a business relationship with a customer;
2. when carrying out a transaction amounting to EUR 15,000 or more, whether the transaction is carried out in a single operation or in several operations which are evidently linked;
3. when there are doubts about the veracity and adequacy of previously obtained customer or beneficial owner information;
4. whenever there is a suspicion of money laundering or terrorist financing in respect of a transaction or customer, regardless of the transaction amount.

(2) When an organisation enters into an additional business relationship with the customer or carries out the transactions referred to in point 2 of the preceding paragraph on the basis of the existing business relationship, the organisation shall obtain the missing information referred to in paragraphs (1) and (2) of Article 21 of this Act provided that the organisation has made a prior customer identification as determined by Article 7 of this Act and that it has provided for appropriate verification and updating of the previously received documents and customer information.

(3) In transactions referred to in point 2 of paragraph 1 of this Article, a concessionaire offering games of chance in a casino or gaming hall shall verify the identity of the customer carrying out the transaction and obtain the required information when the transaction is effected at the cashier's desk.

(4) For the purposes of this Act, the customer's registration for participation in a system of organising games of chance with organisers and concessionaires who offer games of chance via the Internet or other telecommunications means shall be deemed an established business relationship. Pursuant to this Act, the customer's accession to the fund rules of a mutual fund managed by a management company shall be deemed as an established business relationship between the customer and the management company. Accession to the fund rules of another mutual fund managed by same management company shall not be deemed as an established new business relationship between the customer and the management company.

Article 9

(Customer due diligence in the establishment of a business relationship)

(1) When establishing a business relationship referred to in point 1 of paragraph 1 of Article 8 of this Act, an organisation shall apply the measures provided for in points 1, 2 and 3 of paragraph 7 of this Article before the business relationship is established.

(2) Notwithstanding the provisions of the preceding paragraph, an organisation may exceptionally apply measures from points 1 and 2 of paragraph 1 of Article 7 during the establishment of a business relationship with the customer if this is necessary not to interrupt the normal conduct of the organisation's business and where in accordance with Article 6 of this Act there is little risk of money laundering or terrorist financing.

(3) Notwithstanding the provisions of paragraph 1 of this Article, an organisation referred to in point 8 of paragraph 1 of Article 4 hereof may, in relation to life insurance business, verify the identity of the beneficiary under the policy after the business relationship has been established but not later than at or before the time of payout or at or before the time the beneficiary intends to exercise his/her rights vested under the policy.

Article 10

(Customer due diligence in carrying out transactions)

When effecting transactions referred to in point 2 of paragraph 1 of Article 8 hereof, an organisation shall apply the measures provided for in points 1, 2 and 3 of paragraph 1 of Article 7 hereof before the transaction is carried out.

Article 11

(Non-performance of customer due diligence obligation)

An organisation that cannot apply the measures referred to in points 1, 2 and 3 of paragraph 1 of Article 7 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 paragraph 3 of Article 38 hereof.

Article 12
(Exemption from the obligation to carry out customer due diligence for certain products)

(1) Insurance companies authorised to pursue life insurance business and insurance companies from third countries authorised to pursue life insurance business, insurance companies of Member States which establish branches in the Republic of Slovenia or are authorised to pursue life insurance business directly in the Republic of Slovenia, founders and managers of mutual pension funds, pension companies, and legal entities and natural persons conducting business relating to life insurance agency or brokerage business in selling life insurance policies need not apply customer due diligence measures in the following cases:

1. when arranging life insurance contracts where the single premium or multiple premiums to be paid in a year do not exceed EUR 1,000 or where the single premium does not exceed EUR 2,500;
2. in arranging pension insurance contracts, provided that:
 - a) such insurance policies contain no surrender clause and cannot be used as security for a loan; or
 - b) the collective insurance contract is entered into within a pension or other similar scheme guaranteeing the right to pension to the employees and provided the premiums are paid through salary deductions and the scheme rules contain no surrender clause.

(2) Electronic money undertakings, electronic money undertakings from Member States and branches of electronic money undertakings from third countries need not apply customer due diligence measures in the following cases:

1. when issuing electronic money, provided the amount of deposit made for the issue of electronic money stored *on a medium* does not exceed EUR 250;
2. when issuing electronic money and in transactions via e-money, provided that the maximum amount for its issue in respect of the transaction stored *on a medium* does not exceed EUR 2,500 in a calendar year, except when an amount of EUR 1,000 or more is redeemed in that same calendar year by the bearer.

(3) *Organisations referred to in paragraph (1) of Article 4 of this Act may not apply customer due diligence measures also in respect of other products or related transactions when such products and related transactions represent a low risk of money laundering or terrorist financing:*

- a) *products which are related to the financing of physical assets and for which the right of ownership and the right to dispose of property are not transferred to the customer before the termination of contractual relationship (e.g. leasing of physical assets, leasing with purchase option, sale with retention of title) if the amount of down payment related to such product or the total of instalments paid within one year do not exceed EUR 15 000;*
- b) *savings products with characteristics similar to those of an insurance policy (e.g. gradual savings), provided that:*
 - *individual down payments or several down payments payable together in one year do not exceed EUR 1000 or*
 - *in case of saving by a single down payment the amount of such down payment does not exceed EUR 2 500;*
- c) *other products (e.g. small-value consumer loans) if the maximum amount of the product and the related transactions does not exceed EUR 15 000.*

(4) A product and the related transactions represent a low risk of money laundering or terrorist financing provided that the following conditions are satisfied:

- a) the product has a written contractual basis;*
- b) the transactions related to the product are carried out through the customer's account opened with a credit institution in the Republic of Slovenia or with a credit institution established in a Member State of an equivalent third country referred to in paragraph (5) of Article 25 of this Act;*
- c) the product or related transactions are not anonymous and their nature is such that it allows for the timely performance of the customer due diligence when in respect of a transaction or a customer there are grounds to suspect money laundering or terrorist financing notwithstanding the value of the transaction;*
- d) a maximum amount is determined for the product in advance;*
- e) no third party should benefit from the product or the related transaction unless in the case of death, disability, maintenance up to a pre-determined age limit and similar events.*

(5) In case of products and related transactions that facilitate investments in financial assets or receivables, including investments in secured claims of other types of contingent claims, the following conditions shall be satisfied in addition to the conditions from the preceding paragraph:

- a) the benefits of the product and related transactions are only realisable in the long term;*
- b) the product or related transactions cannot be used as collateral;*
- c) during the contractual relationship:*
 - no accelerated payments are made,*
 - surrender clauses used*
 - or early termination takes place.*

(6) The organisation shall notify the office of the product for which it intends not to apply customer due diligence before marketing or selling the product without customer due diligence.

(7) Notwithstanding the provisions of paragraphs (1) to (5) of this Article, the omission of customer due diligence shall not be permitted when reasons for suspicion of money laundering or terrorist financing exist in connection with the customer, product or transaction.

2.2.2 Application of customer due diligence measures

2.2.2.1 Determining and verifying customer identity

Article 13

(Determining and verifying the identity of a natural person or his/her statutory representative, sole proprietor, or self-employed person)

(1) In respect of a customer, namely:

- 1. a natural person or his/her statutory representative (hereinafter: representative),*
- 2. a sole proprietor, or*
- 3. a self-employed person,*

an organisation shall determine and verify the customer's identity and obtain the data referred to in point 4 of paragraph 1 of Article 83 of this Act by examining the customer's official personal identification document in the customer's presence. When all the required data cannot be obtained from the mentioned document, the missing data shall be obtained from another authentic document submitted by the customer or directly from the customer.

(2) Notwithstanding the preceding paragraph and subject to the terms and conditions prescribed by the minister responsible for finance in the rules, an organisation may determine and verify the identity of a customer (natural person or his/her representative, sole proprietor, or self-employed person) based on:

1. a qualified digital certificate issued by a certification authority situated in the Republic of Slovenia in accordance with the Act governing electronic commerce and electronic signature;
2. the customer's qualified digital certificate issued by a certification authority situated in a European Union Member State or in a third country subject to conditions stipulated by the Act governing electronic commerce and electronic signature, and provided that technological possibilities for such purpose are available.

(3) When determining and verifying the identity of the customer pursuant to paragraph 2 of this Article, an organisation shall obtain the required data on the customer referred to in point 4 of paragraph 1 of Article 83 hereof from the qualified digital certificate. Data not available on the mentioned certificate shall be obtained from the copy of the official personal document sent by the customer to the organisation in paper or digital form. When all required data cannot be obtained in the manner described above, the missing data shall be obtained directly from the customer.

(4) The certification authority referred to in paragraph 2 of this Article which issued a qualified digital certificate to the customer shall forthwith submit data on the manner of determining and verifying the identity of the customer-bearer to the organisation upon its request. The data obtained shall be kept by the organisation in accordance with the provisions of the present Act and the Act regulating protection and retention of data.

(5) Notwithstanding paragraphs 2 and 3 of this Article, determining and verifying the identity of the customer by using a qualified digital certificate shall be prohibited in the following cases:

1. when opening *payment* an account with the organisations referred to in points 1, 2 and 3 of paragraph 1 of Article 4 hereof, except when opening a provisional deposit account for payments of start-up capital; or
2. when there is a suspicion that a qualified digital certificate may be misused or an organisation establishes that circumstances substantially affecting the validity of a certificate have changed but the issuing certification authority has not yet revoked it.

(6) When the customer is a sole proprietor or self-employed person, an organisation shall obtain the data referred to in point 5 of paragraph 1 of Article 83 hereof by applying Article 14 of this Act *mutatis mutandis*.

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

(8) When an organisation entering a business relationship determines and verifies the identity of the customer on the basis of paragraph 2 of this Article, it shall be obliged to act in accordance with paragraph 3 of Article 32 hereof.

Article 14 **(Determining and verifying the identity of a legal entity)**

(1) An organisation shall determine and verify the identity of the customer (legal entity) and obtain the data referred to in point 1 of paragraph 1 of Article 83 hereof by inspecting the original or certified documentation 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 documentation referred to in the preceding paragraph shall not be older than three months.

(3) An organisation may determine and verify the identity of a legal entity and obtain the data referred to in point 1 of paragraph 1 of Article 83 of this Act by inspecting a court or other public register. The extract from the register used shall bear a remark by the organisation to indicate the date and time of access and the personal name of the person who inspected the register. The extract from the register shall be kept by the organisation in accordance with the provisions of the present Act and the Act regulating protection and retention of data.

(4) An organisation shall obtain other data from paragraph 1 of Article 83 hereof, with the exception of data on a beneficial owner *which are obtained in accordance with Article 20 of this Act*, by inspecting original or certified documents and other business documentation. When all the data referred to in paragraph 1 of Article 83 hereof cannot be obtained from such documents and documentation, 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 organisation 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 1 and 3 of this Article, an organisation 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 organisation shall determine and verify the identity of the foreign legal entity and its branch.

Article 15

(Determining and verifying the identity of a legal entity's statutory representative)

(1) An organisation shall determine and verify the identity of a statutory representative and obtain the data referred to in point 2 of paragraph 1 of Article 83 of this Act by examining the statutory representative's official personal identification document in the representative's presence. When all required data cannot be obtained from the mentioned document, the missing data shall be obtained from another authentic document submitted by the statutory representative.

~~(2) An organisation may determine and verify the identity of the statutory representative of a legal entity in some other manner if so stipulated in the rules issued by the minister responsible for finance.~~

(2) If, in determining and verifying the identity of a statutory representative, an organisation doubts the reliability of submitted data, it shall request a written statement.

Article 16

(Determining and verifying the identity of an authorised person)

(1) An organisation 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 1 of Article 83 of this Act by examining the authorised person's official personal identification document in his/her presence. When all required data cannot be obtained from the mentioned document, the missing data shall be obtained from another authentic document submitted by the authorised person or directly from the authorised person. An organisation shall obtain the data referred to in point 2 of paragraph 1 of Article 83 hereof about a statutory representative on whose behalf an authorised person acts from the certified written authorisation issued by the statutory representative.

(2) If the customer carries out the transaction referred to in point 2 of paragraph (1) of Article 8 of this Act, the organisation shall obtain from the customer a declaration on whether the customer operates on his own behalf or on behalf of a third party. If this transaction is carried out on the basis of a previously established business relationship, the information whether the transaction is carried out by the customer or his agent shall also be regarded as adequate.

(3) If a transaction referred to in point 2 of paragraph 1 of Article 8 hereof is effected on behalf of the customer by his/her authorised person, an organisation shall determine and verify the authorised person's identity and obtain the data required in point 3 of paragraph 1 of Article 83 hereof as set forth in paragraph 1 of this Article. When an authorised person acts on behalf of a customer (natural person), sole proprietor or self-employed person, an organisation shall obtain the data referred to in point 4 of paragraph 1 of Article 83 hereof from the customer's written authorisation.

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

Article 17 **(Determining and verifying the identity of other civil law entities)**

(1) When the customer is a civil law entity referred to in point 9 of Article 3 hereof which is not a natural person or legal entity, the organisation shall:

1. determine and verify the identity of the person with powers of representation (hereinafter: agent);
2. obtain certified written powers of representation;
3. obtain the data referred to in points 2 and 16 of paragraph 1 of Article 83 of this Act.

(2) The organisation shall determine and verify the identity of the agent referred to in paragraph 1 of this Article and obtain the data referred to in point 2 of paragraph 1 of Article 83 of this Act by examining the agent's official personal identification document in the agent's presence. When all required data cannot be obtained from the mentioned document, the missing data shall be obtained from another authentic document submitted by the agent or directly from the agent.

(3) The organisation shall obtain the data referred to in point 16 of paragraph 1 of Article 83 hereof about a person who belongs to a civil law entity referred to in paragraph 1 of this Article from the certified written powers of representation submitted to the organisation by the agent. When all the data referred to in point 16 of paragraph 1 of Article 83 hereof cannot be obtained from such document, the missing data shall be obtained directly from the agent.

(4) Notwithstanding the provision of point 2 of paragraph (1) and paragraph (3) of this Article, when the organisation'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 organisation 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 1 of this Article, the organisation 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 18

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

(1) Subject to the provisions of Article 8 of this Act, the customer's identity shall also be determined and/or verified in the following cases:

1. upon the customer's entry into a casino or gaming hall;
2. each time the customer accesses the safe.

(2) In determining and verifying the identity of the customer pursuant to paragraph 1 of this Article, a concessionaire offering games of chance in a casino or gaming hall or an organisation providing safekeeping services shall obtain the data required under points 6 and 8 of paragraph 1 of Article 83 of this Act.

(3) Provisions of this Act concerning the obligation to verify the identity of the customer when accessing the safe shall apply to each person actually accessing the safe, regardless of whether or not the person concerned is a party to the safekeeping contract or the party's statutory representative or authorised person.

2.2.2.2 Determining the beneficial owner of the customer

Article 19

(Beneficial owner of a customer)

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

1. any natural person who owns through direct or indirect ownership at least 25% of the business share, stocks or voting or other rights, on the basis of which he/she participates in the management or in the capital of the legal entity with at least 25% share or has the controlling position in the management of the legal entity's funds;
2. any natural person who indirectly provides or is providing funds to a legal entity and is on such grounds given the possibility of exercising control, guiding or otherwise substantially influencing the decisions of the management or other administrative body of the legal entity concerning financing and business operations.

(2) For the purposes of this Act, the beneficial owner of other legal entities, such as foundations and similar foreign law entities which accept, administer or distribute funds for particular purposes, shall mean:

1. any natural person who is the beneficiary of more than 25% of the proceeds of property under management, where the future beneficiaries have already been determined or can be determined;
2. a person or a group of persons in whose main interest the legal entity or similar foreign law entity is set up and operates, where the individuals that benefit from the legal entity or similar foreign law entity have yet to be determined;

3. any natural person exercising direct or indirect control over 25% or more of the property of a legal entity or similar foreign law entity.

Article 20

(Determining the beneficial owner of a legal entity or similar foreign law entity)

(1) The organisation shall determine the beneficial owner of a legal entity or similar foreign law entity by obtaining the data referred to in point 15 of paragraph 1 of Article 83 hereof.

(2) The organisation shall obtain the data referred to in paragraph 1 of this Article by inspecting the original or certified documentation from the court register or other public register, which shall not be older than three months. The organisation may obtain such data by direct inspection of the court or other public register. In this regard, the organisation shall follow the provisions of paragraphs 3 and 5 of Article 14 of this Act.

(3) If all the data on the beneficial owner of a customer cannot be obtained from the court or any other public register, the organisation shall obtain the missing data by inspecting the original or certified documents and business records submitted by the statutory representative or his/her authorised person. When the organisation due to objective reasons cannot obtain the missing data in the manner described in this Article, it shall obtain it from the written statement of the statutory representative or his/her authorised person.

(4) The organisation shall obtain data on the ultimate beneficial owner of a legal entity or similar foreign law entity. With regard to the risk of money laundering or terrorist financing to which the organisation is exposed in conducting business with such customer, the organisation shall verify the data to such an extent that it understands the ownership and control structure of its customer and is satisfied that it knows who the beneficial owner is.

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

Article 21

(Set of data)

(1) Within the customer due diligence referred to in point 1 of paragraph 1 of Article 8 of this Act, the organisation shall obtain the data from points 1, 2, 4, 5, 7, 8 and 15 of paragraph 1 of Article 83 of this Act.

(2) Within the customer due diligence referred to in point 2 of paragraph 1 of Article 8 of this Act, the organisation shall obtain the data from points 1, 2, 3, 4, 5, 9, 10, 11, 12 and 15 of paragraph 1 of Article 83 of this Act.

(3) Within the customer due diligence referred to in points 3 and 4 of paragraph 1 of Article 8 of this Act, the organisation shall obtain the data from paragraph 1 of Article 83 of this Act.

2.2.2.4 Monitoring business activities

Article 22

(Due diligence in monitoring business activities)

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

- verification of the customer's business operations compliance with the purpose and intended nature of the business relationship established between the customer and the organisation;
 - monitoring and verification of the customer's business operations compliance with his regular scope of business;
 - verification and updating obtained documents and data on the customer.
- (2) For a customer who is a legal entity, verification and updating of obtained documents and data referred to in the preceding paragraph shall include at least 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 personal 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 validity of the powers of representation referred to in paragraph (3) of Article 16 of this Act;
 5. determining whether the customer has become a foreign politically exposed person during the period of business relationship.
- (3) When the transactions referred to in paragraph (1) of Article 8 of this Act are carried out on behalf and for the account of a foreign legal entity by its branch, the organisation shall obtain, in addition to the data referred to in paragraph 2 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 personal name and permanent residence of the foreign legal entity's statutory representative.
- (4) The organisation shall ensure the scope and frequency of measures referred to in paragraph (1) of this Article appropriate to the risk of money laundering or terrorist financing to which it is exposed in carrying out individual transactions or in business operations with an individual customer. The organisation shall assess such risk pursuant to Article 6 of this Act. Notwithstanding the above, the organisation shall ensure that the obtained documents and customer data are updated at least after the expiry of five years from the date of the last customer due diligence if the customer carries out his transactions through the organisation.

Article 22a

(Treatment of unusual transactions)

- (1) In connection with intricate and unusually high amount transactions or transactions with an unusual structure or transactions with no apparent or visible economic or lawful purpose or transactions that are not in compliance or are in disproportion with the usual or expected business of a customer, the organisation shall:
- examine the background and the purpose of these transactions to the extent permitted by the circumstances and
 - make a note of its conclusions and keep them on record.
- (2) When dealing with unusual transactions the organisation should pay special attention to its customers, business relationships or transactions associated with the countries that have no appropriate measures in place for preventing and detecting money laundering and terrorist financing or in which such measures are not adequately implemented. In such cases the organisation shall act in accordance with the preceding paragraph. The office shall publish the information about the countries referred to above on its web pages

~~Article 23~~

~~(Annual review of a foreign legal entity)~~

- ~~(1) When a foreign legal entity carries out transactions referred to in paragraph 1 of Article 8 of this Act, the organisation shall, in addition to the tasks referred to in Article 22 of this Act, carry out regular repeated review of the foreign legal entity at least once a year and not later than one year after the last review of the foreign legal entity.~~

~~(2) Notwithstanding the preceding paragraph, the organisation shall carry out review when a customer carrying out transactions from paragraph 1 of Article 8 of this Act is a legal entity with its head office in the Republic of Slovenia and in more than 25% ownership of:~~

- ~~1. a foreign legal entity which is not or may not be engaged in trade, manufacturing or other activity in the country of registration;~~
- ~~2. fiduciary or other similar foreign law companies with unknown or hidden owners or managers.~~

~~(3) The annual review of the customer referred to in paragraphs 1 and 2 of this Article shall include:~~

- ~~1. obtaining or verifying data on the firm, address and legal entity's head office referred to in paragraph 1 or 2 of this Article;~~
- ~~2. obtaining data on the personal name and permanent or temporary residence of the legal entity's statutory representative referred to in paragraph 1 or 2 of this Article;~~
- ~~3. obtaining data on the legal entity's beneficial owner referred to in paragraph 1 or 2 of this Article;~~
- ~~4. obtaining the new authorisation referred to in paragraph 2 of Article 16 of this Act.~~

~~(4) When the transactions referred to in paragraph 1 of Article 8 of this Act are carried out on behalf and for the account of a foreign legal entity by its branch, the organisation shall obtain, in addition to the data referred to in paragraph 2 of this Article, the following data within the annual review of a foreign legal entity:~~

- ~~3. data on the address and head office of the foreign legal entity's branch;~~
- ~~4. data on personal name and permanent residence of the foreign legal entity's statutory representative.~~

~~(5) The organisation shall obtain the data referred to in points 1, 2 and 3 of paragraph 3 of this Article by inspecting the original or certified documentation from the court or other public register, which shall not be older than three months, or by direct inspection of the court or other public register. When the required data cannot be obtained in the described manner, the organisation shall obtain the missing data from the original or certified documents and business records submitted by the legal entity referred to in paragraph 1 or 2 of this Article. When due to objective reasons the organisation cannot obtain the missing data in the prescribed manner, it shall obtain it directly from the written statement of the statutory representative of the legal entity referred to in paragraph 1 or 2 of this Article.~~

~~(6) The organisation shall not effect transactions if it does not or cannot undertake annual review of the customer in accordance with this Article.~~

~~(7) Notwithstanding the provisions of paragraph 1 of this Article, the annual review of a foreign legal entity shall not be required if the foreign legal entity is the organisation referred to in paragraph 1 of Article 33.~~

2.2.3 Customer due diligence via third parties

Article 24 (Due diligence relying on third parties)

(1) Under the conditions stipulated by this Act, the organisation entering into a business relationship may rely on a third party to apply the measures referred to in points 1, 2 and 3 of paragraph 1 of Article 7 of this Act.

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

(3) Customer due diligence performed for the organisation by a third party may not be accepted as appropriate if, within this procedure, the third party determined and verified the identity of a customer in his/her absence.

(4) The organisation 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 25 **(Third parties)**

(1) The third party referred to in paragraph 1 of Article 24 of this Act shall be the following:

1. the organisation referred to in points 1, 2, 4, 5, 6, 7 or 8 of paragraph 1 of Article 4 of this Act;
2. a bank of a Member State or a branch of a Slovenian bank in a Member State;
3. an investment fund management company from a Member State or a branch of a Slovenian investment fund management company in a Member State;
4. founders or managers of mutual pension funds from a Member State or a pension company from a Member State;
5. a brokerage company from a Member State or a branch of a Slovenian brokerage company in a Member State;
6. an *insurance company* or insurance company from a Member State or a branch of a Slovenian insurance company in a Member State;
7. a branch or subsidiary of a bank from a Member State in a third country, a branch or subsidiary of a management company from a Member State in a third country, a branch or subsidiary of a brokerage company from a Member State in a third country, or a branch or subsidiary of an insurance company from a Member State in a third country;
8. other persons meeting the conditions set by the minister responsible for finance in the rules. The minister shall, inter alia, take account of the technical criteria adopted by the European Commission pursuant to Article 40 of Directive 2005/60/EC, data from the competent international organisations and data from the office.

(2) Notwithstanding paragraph 1 of this Article, a notary situated in *Republic of Slovenia* or *other* Member State or in an equivalent third country referred to in paragraph 5 of this Article shall also be considered a third party.

(3) 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.

(4) The third parties referred to in paragraph 1 of Article 24 of this Act shall not include outsourcing service providers and agents.

(5) The minister responsible for finance shall draw up the list of equivalent third countries that impose and comply with money laundering and terrorist financing standards as defined by Directive 2005/60/EC, while taking into account the instrument adopted by the European Commission pursuant to Article 40 of Directive 2005/60/EC, data from the competent international organisations and the office.

Article 26 **(Exceptions relating to customers)**

Notwithstanding paragraph 1 of Article 24 of this Act, the organisation may not rely on a third party to apply customer due diligence procedure when the customer is:

1. a foreign legal entity which is not or may not be engaged in trade, manufacturing or other activity in the country of registration;
2. a fiduciary or other similar foreign law company with unknown or hidden owners or managers.

Article 27

(Obtaining data and documentation from a third party)

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

(2) The third party shall immediately forward to the organisation, 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 organisation in accordance with the provisions of the present Act and the Act regulating protection and retention of data.

(3) When the organisation relies on third parties referred to in points 2 to 8 of paragraph 1 of Article 25 of this Act to apply customer due diligence procedure, the organisation may accept documentation or data used in customer due diligence procedure in the country concerned, even if the documentation and data differ from those required by this Act.

(4) When the organisation assesses that there is good reason to doubt the veracity of applied customer due diligence procedure or the identification documentation or the reliability of obtained data on the customer, it shall immediately demand a written statement from the third party on the veracity of the respective customer due diligence procedure and reliability of obtained customer data.

(5) The organisation 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 25 of this Act;
2. the third party relied on by the organisation to apply customer due diligence procedure determined and verified the identity of a customer in his/her absence;
3. the organisation failed to obtain in advance the data referred to in paragraph 1 of this Article from the third party which applied customer due diligence procedure;
4. the organisation failed to obtain in advance copies of identification documents and other customer documentation from the third party which applied customer due diligence procedure;
5. 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 third party, despite the organisation's request, failed to submit the written statement referred to in paragraph 4 of this Article.

~~(6) When the third party relied upon by the organisation to apply customer due diligence procedure is an organisation referred to in points 1, 2, 4, 5, 6, 7 or 8 of paragraph 1 of Article 4 of this Act, it shall itself be responsible for performing the obligations under this Act, including the obligation to report transactions when reasons for suspicion of money laundering or terrorist financing exist, and to retain data and documentation.~~

2.2.4 Special types of customer due diligence

Article 28

(General)

Customer due diligence procedure shall be applied in accordance with paragraph 1 of Article 7 of this Act; in some cases stipulated by this Act, particularly rigorous measures shall be required or simplified customer due diligence measures allowed. Special types of customer due diligence shall be:

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

2.2.4.1 Enhanced customer due diligence

Article 29 (General)

(1) Enhanced customer due diligence shall, in addition to the measures referred to in paragraph 1 of Article 7 of this Act, include additional measures stipulated by this Act in the following cases:

1. entering into a correspondent banking relationship with a respondent bank or similar credit institution situated in a third country;
2. entering into a business relationship or carrying out a transaction referred to in point 2 of paragraph 1 of Article 8 of this Act with a customer who is a politically exposed person referred to in Article 31 of this Act;
3. when, within customer due diligence, a customer was not physically present for the purpose of determining and verifying his identity.

(2) The organisation shall apply enhanced customer due diligence procedure in all cases referred to in paragraph 1 of this Article. In addition, the organisation shall apply, by analogy, a measure or measures of enhanced customer due diligence from Articles 30, 31 and 32 of this Act in cases where pursuant to Article 6 of this Act it assesses that there is a high risk of money laundering or terrorist financing due to the nature of the business relationship, form or manner of executing the transaction, business profile of the customer, or other circumstances relating to the customer.

Article 30

(Corresponding banking relationships with credit institutions from third countries)

(1) When entering into a corresponding banking relationship with a bank or similar credit institution situated in a third country, the organisation shall apply measures referred to in paragraph 1 of Article 7 of this Act within enhanced customer due diligence procedure and shall in addition obtain the following data, information and documentation:

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

4. a written statement that the bank or other similar credit institution does not operate as a shell bank;
5. a written statement that the bank or other similar credit institution has not established or does not enter into business relationships with shell banks;
6. a written statement that the bank or similar credit institution is subject to administrative supervision in the country of its head office or registration and is, in accordance with the legislation of the country concerned, under the obligation to comply with laws and regulations governing the detection and prevention of money laundering and terrorist financing.

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

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

(4) The organisation shall not enter into or continue a correspondent banking relationship with a respondent bank or other similar credit institution situated in a third country if:

1. no data referred to in points 1, 2, 4, 5 and 6 of paragraph 1 of this Article have been obtained in advance;
2. the employee of the organisation failed to obtain prior written approval of his/her superior and the responsible person in the organisation for entering into the correspondent relationship;
3. the bank or other similar credit institution situated in the third country does not have in place a system for detecting and preventing money laundering and terrorist financing or is, in accordance with the legislation of the third country where it is established or registered, not under the obligation to comply with laws and other relevant regulations concerning the detection and prevention of money laundering and terrorist financing;
4. the bank or other similar credit institution situated in the third country operates as a shell bank or enters into correspondent or other business relationships and effects transactions with shell banks.

Article 31 **(Foreign politically exposed persons)**

(1) The organisation shall establish an appropriate procedure to determine whether a customer or his statutory representative or authorised person is a foreign politically exposed person. It shall define such procedure, which is based on a risk analysis, in its internal act while taking account of the guidelines of the competent supervisory body referred to in Article 85 of this Act. Political exposure shall also be determined for a customer's actual owners.

(2) The foreign 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 shall be the following:

1. heads of state, prime ministers, ministers and their deputies or assistants;
2. elected representatives in legislative bodies;

3. 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;
4. members of courts of audit and boards of governors of central banks;
5. ambassadors, chargés d'affaire and high-ranking officers of armed forces;
6. members of the management or supervisory bodies of undertakings in majority state ownership.

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

(5) The close associate referred to in paragraph 2 of this Article shall mean any natural person who has a joint profit from property or business relationship or has any other close business links.

(6) When the customer entering into a business relationship with or effecting a transaction, or when the customer on whose behalf a business relationship is entered into or a transaction effected, is a foreign politically exposed person, the organisation shall in addition to the measures referred to in paragraph 1 of Article 7 of this Act within the enhanced customer due diligence procedure take the following measures:

1. The organisation shall obtain data on the source of funds and property that are or will be the subject of business relationship or transaction from documents and other documentation submitted by the customer. When such data cannot be obtained in the described manner, the organisation shall obtain it directly from the customer's written statement.
2. An employee of the organisation who conducts the procedure for entering into a business relationship with a customer who is a foreign politically exposed person shall obtain the written approval of his/her superior and the responsible person prior to entering into such relationship.
3. After a business relationship has been entered into, the organisation shall monitor the transactions and other business activities effected through the organisation by a foreign politically exposed person with due diligence.

Article 32

(Physical presence of a customer when determining and verifying identity)

(1) When a customer is not physically present in the organisation *or in the third person referred to in Article 25 of this Act* when determining and verifying identity, the organisation shall, in addition to the measures referred to in paragraph 1 of Article 7 of this Act within enhanced customer due diligence procedure, take one or more additional measures referred to in paragraph 2 of this Article.

(2) The organisation shall compensate for the higher risk of money laundering and terrorist financing occurring where the customer has not been physically present by:

1. obtaining additional documents, data and information on the basis of which it verifies the customer's identity;
2. additional verification of submitted documents or additional confirmation by the financial institution referred to in point 25 of Article 3 of this Act;
3. applying the measure referred to in paragraph 3 of this Article as set by the competent supervisory authority referred to in Article 85 of this Act.

(3) The organisation shall only be allowed to enter into a business relationship without the customer's presence under paragraph 2 of Article 13 of this Act if it takes measures ensuring

that, prior to effecting the customer's subsequent transaction through the organisation, the first payment of the operation is carried out through an account opened in the customer's name with a credit institution.

2.2.4.2 Simplified customer due diligence

Article 33 (General)

(1) Notwithstanding the provision of Article 7 of this Act, the organisation may, except when reasons for suspicion of money laundering or terrorist financing exist in connection with the customer, in cases under points 1 and 2 of paragraph 1 of Article 8 of this Act apply simplified customer due diligence if the customer is:

1. the organisation referred to in points 1, 2, 4, 5, 6, 7 and 8 of paragraph 1 of Article 4 of this Act *or the insurance company*, provided the organisation has its head office in a Member State or equivalent third country referred to in paragraph 5 of Article 25 of this Act;
2. a state body, self-governing local community body, public agency, public fund, public institution or chamber, *established in the Republic of Slovenia*;
3. a company whose securities are admitted to trading on a regulated market in one or more Member States in accordance with European Community legislation, or a company situated in a third country whose securities are admitted to trading on a regulated market in a Member State or in that country, provided that its disclosure requirements are consistent with European Community legislation;
4. the *other* person referred to in paragraph 4 of Article 6 of this Act in connection with whom there is little risk of money laundering or terrorist financing.

(2) Notwithstanding paragraph 1 of this Article, the organisation entering into a correspondent banking relationship with a respondent bank or other similar credit institution situated in a third country shall act in accordance with paragraph 1 of Article 30 of this Act.

(3) Notwithstanding the provision of Article 7 of this Act, an auditing firm or independent auditor that establishes a business relationship of mandatory auditing of annual accounts of a legal entity pursuant to the Act governing its operations, may apply simplified due diligence procedure, except when reasons for suspicion of money laundering or terrorist financing exist in connection with the customer or auditing circumstances.

Article 34 (Performance of simplified customer due diligence)

(1) Notwithstanding paragraph (1) of Article 7 of this Act, the simplified customer due diligence procedure referred to in paragraph (1) of the preceding Article shall only include obtaining certain customer, business relationship or transaction data and regular due diligence in monitoring business activities performed by the customer in the organisation, pursuant to Article 22 of this Act. Notwithstanding paragraph (2) of Article 22 of this Act, the customer for which due diligence is permitted shall be subject to verification and updating verified documents and data on the customer only to the extent and in the manner laid down by this Article.

(2) Within the simplified customer due diligence procedure, the organisation shall obtain the following data:

1. when establishing a business relationship:
 - the name, address and registered office of the legal entity establishing the business relationship or legal entity on whose behalf the business relationship is established;

- the personal name of the statutory representative or authorised person establishing the business relationship for a legal entity;
 - the purpose and intended nature of the business relationship and the date of establishment of the business relationship;
2. when conducting transactions under point 2 of paragraph 1 of Article 8 of this Act:
- the name, address and registered office of the legal entity for whom the transaction is conducted;
 - the personal name of the statutory representative or authorised person conducting the transaction for the legal entity;
 - the date and time of the transaction;
 - the amount of transaction, currency of transaction and manner of effecting the transaction;
 - the purpose of transaction and the personal name and permanent address or name and registered office of the person to whom the transaction is directed.

(3) The organisation shall obtain the data referred to in paragraph 2 of this Article by inspecting the original or certified documentation from the court or other public register submitted by the customer or by direct inspection of the court or other public register.

(4) When all required data cannot be obtained in the manner stipulated in paragraph 3 of this Article, the organisation shall obtain the missing data from the original or certified documents and business records submitted by the customer. When due to objective reasons the organisation cannot obtain the missing data even in the manner described, it shall obtain it directly from the written statement of the statutory representative or authorised person.

(5) The submitted documentation referred to in paragraphs 3 and 4 of this Article shall not be older than three months.

2.2.5 Limitations on transactions with customers

Article 35 (Prohibition on using anonymous products)

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

Article 36 (Prohibition on conducting business with shell banks)

The organisation 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 institution known to allow shell banks to use its accounts.

Article 37 (Limitations on cash operations)

(1) Persons pursuing the activity of selling goods in the Republic of Slovenia shall not accept cash payments exceeding EUR 15,000 from their customers or third persons when selling individual goods. Persons pursuing the activity of selling goods shall also include legal entities and natural persons who organise or conduct auctions, deal in works of art, precious metals or stones or products thereof, and other legal entities and natural persons who accept cash payments for goods.

(2) The limitation for accepting cash payments referred to in the preceding paragraph shall also apply where the payment is effected by several linked cash transactions exceeding in total the amount of EUR 15,000.

(3) Persons pursuing the activity of selling goods shall receive payments referred to in paragraphs 1 and 2 of this Article from the customer or *some other person* on their *payment* accounts, unless otherwise provided by other Acts.

2.3 Reporting

Article 38 (Reporting obligation and deadlines)

(1) The organisation shall furnish the office with the data referred to in points 1, 2, 3, 4, 5, 9, 10, 11 and 12 of paragraph 1 of Article 83 of this Act on any cash transaction exceeding EUR 30,000 immediately after the transaction is completed and not later than within three working days following its completion.

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

(3) Notwithstanding the provisions of the preceding paragraphs of this Article, the organisation shall furnish the office with the data referred to in paragraph 1 of Article 83 of this Act where reasons for suspicion of money laundering or terrorist financing exist in connection with the customer or transaction, prior to effecting the transaction, and shall state the time limit in which the transaction is to be carried out. Such report may also be submitted by telephone; however, the written report shall be sent to the office the next working day at the latest.

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

(5) Notwithstanding paragraphs 3 and 4 of this Article, the auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services shall report all cases where the customer 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.

(6) If in cases referred to in paragraphs 3 and 4 of this Article and due to the nature of the transaction or because the transaction was not completed, or due to other justified reasons, the organisation cannot follow the described procedure, it shall furnish the data to the office as soon as is practicable or immediately after the suspicion of money laundering or terrorist financing is raised. The organisation shall explain in the report the reasons for not acting in accordance with the described procedure.

(7) The organisation shall forward to the office the data referred to in paragraphs 1, 3, 4 and 5 of this Article in the manner prescribed in the rules issued by the minister responsible for finance.

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

2.4 Application of measures for detecting and preventing money laundering and terrorist financing in branches and majority-owned subsidiaries located in third countries

Article 39 (Obligation to apply measures in third countries)

(1) The organisation shall 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 the present Act to the same extent, unless explicitly contrary to the legislation of the third country.

(2) If the legislation of a third country does not allow for the application of measures for detecting and preventing money laundering or terrorist financing to the same extent as stipulated by this Act, the organisation shall forthwith inform the office thereof and take appropriate measures to eliminate the risk of money laundering or terrorist financing.

(3) Organisations shall inform their branches and majority-owned subsidiaries with head offices in third countries of internal procedures relating to the detection and prevention of money laundering and terrorist financing, in particular with respect to customer due diligence, reporting obligations, keeping records, internal control and other relevant circumstances relating to the detection and prevention of money laundering and terrorist financing.

2.5 Authorised person, education and internal control

2.5.1 Authorised person

Article 40 (Appointment of authorised person and his/her deputy)

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

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

Article 41 (Conditions for the authorised person)

(1) The organisation shall ensure that the work of the authorised person referred to in Article 40 of this Act is entrusted solely to a person meeting the following requirements:

1. holds a position within the classification of posts ranking high enough to enable rapid, quality and timely execution of tasks stipulated by this Act and ensuing regulations;
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 homicide, serious bodily injury, aggravated bodily injury, threatening work safety, concealment, disclosure and undue obtaining of professional secrecy, money laundering, disclosure of an official secret, causing general danger or disclosure of a state secret, and the penalty has not yet been expunged from the criminal record;

3. holds appropriate professional qualifications for the tasks of preventing and detecting money laundering and terrorist financing and possesses the characteristics and experience necessary to discharge the function of the authorised person;
4. is well acquainted with the nature of the organisation's operations in the fields exposed to risk of money laundering or terrorist financing.

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

Article 42 **(Duties of authorised person and deputy)**

(1) The authorised person referred to in Article 40 of this Act shall perform the following tasks:

1. provide for the setting up, functioning and development of the system for detecting and preventing money laundering and terrorist financing within the organisation;
2. provide for correct and timely reporting to the office in accordance with this Act and ensuing regulations;
3. participate in the drawing up and modification of the operative procedures and in the preparation of internal regulations concerning the prevention and detection of money laundering and terrorist financing;
4. participate in the elaboration of guidelines for the conduct of control related to the prevention and detection of money laundering and terrorist financing;
5. monitor and coordinate the activities of the organisation in the field of detecting and preventing money laundering and terrorist financing;
6. participate in the setting up and development of information support for the activities related to the detection and prevention of money laundering and terrorist financing within the organisation;
7. suggest initiatives and make proposals to the management or other administrative body of the organisation for improvement of the system for detecting and preventing money laundering and terrorist financing within the organisation;
8. participate in preparation of the professional education and training programme for employees in the field of prevention and detection of money laundering and terrorist financing.

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

Article 43 **(Obligations of the organisation)**

(1) To enable the authorised person to carry out tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act, the organisation shall:

1. provide unlimited access to all data, information and documentation required to carry out those tasks;
2. give appropriate authorisations for the efficient performance of tasks referred to in paragraph 1 of Article 42 of this Act;
3. provide appropriate staff, material and other working conditions;
4. ensure appropriate premises and technical capacities guaranteeing an adequate level of protection of classified information available to the authorised person pursuant to this Act;
5. provide appropriate information and technical support enabling permanent and safe monitoring of activities in this field;
6. provide for regular professional training related to the detection and prevention of money laundering and terrorist financing;

7. provide a replacement during the authorised person's absence.

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

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

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

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

2.5.2 Education and professional training

Article 44

(Obligation to undertake regular education)

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

(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.

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

2.5.3 Internal control and risk management

Article 45

(Regular internal control obligation)

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

Article 45a

(Risk management)

The organisation shall carry out an analysis of the impact of all major changes in its business processes, such as the introduction of a new product, introduction of a new technology or a change in organisation, on the organisation's exposure to the risk of money laundering or terrorist financing. The organisation shall adopt appropriate measures in order to reduce the risk of money laundering or terrorist financing in accordance with the findings of the analysis.

2.5.4 Implementing regulation for the purpose of carrying out certain tasks

Article 46

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

The minister responsible for finance shall issue rules laying down detailed rules about the authorised person, the method for executing internal control, retention and protection of data, the administration of records and professional training of employees within the organisations, lawyers, law firms and notaries pursuant to this Act.

CHAPTER III

TASKS AND OBLIGATIONS OF LAWYERS, LAW FIRMS AND NOTARIES

Article 47

(Tasks and obligations of lawyers, law firms and notaries)

Unless otherwise provided in this Chapter, a lawyer, law firm or notary shall act in accordance with the provisions of this Act governing tasks and obligations of organisations 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 client money, securities or other assets;
 - c) opening or managing bank, savings or securities accounts;
 - d) raising funds required to establish, operate or manage a company;
 - e) establishing, operating or managing foundations, trusts, companies or similar legal organisational forms;
2. or conducting a financial or real estate transaction on behalf and for the account of the client.

Article 48

(Client due diligence)

(1) Within the client due diligence referred to in point 1 of paragraph 1 of Article 8 of this Act, the lawyer, law firm or notary shall obtain the data from points 1, 2, 3, 4, 5, 6 and 11 of paragraph 3 of Article 83 of this Act.

(2) Within the client due diligence referred to in point 2 of paragraph 1 of Article 8 of this Act, the lawyer, law firm or notary shall obtain the data from points 1, 2, 3, 4, 7, 8, 9, 10 and 11 of paragraph 3 of Article 83 of this Act.

(3) Within the client due diligence referred to in points 3 and 4 of paragraph 1 of Article 8 of this Act, the lawyer, law firm or notary shall obtain the data from paragraph 3 of Article 83 of this Act.

(4) A lawyer, law firm or notary shall determine and verify the identity of the client or his/her statutory representative or authorised person and shall obtain the data referred to in points 1, 2 and 3 of paragraph 3 of Article 83 of this Act by examining the client's official personal identification document in his/her presence or by inspecting the original or certified documentation from the court or other public register, which shall not be older than three months.

(5) A lawyer, law firm or notary shall determine the beneficial owner of a client who is a legal entity or similar foreign legal entity by obtaining the data referred to in point 4 of paragraph 3 of Article 83 of this Act by inspecting the original or certified documentation from the court or other public register, which shall not be older than three months. When all the data cannot be obtained from such register, the missing data shall be obtained by inspecting the original and certified documents and other business records submitted by the legal entity's statutory representative or agent.

(6) The lawyer, law firm or notary shall obtain the other data referred to in paragraph 3 of Article 83 of this Act by inspecting the original or certified documents and other business records.

(7) When all the data cannot be obtained in the manner prescribed in this Article, the missing data, other than those referred to in points 12, 13 and 14 of paragraph 3 of Article 83 of this Act, shall be obtained directly from the client's written statement.

Article 49

(Reporting data on clients and transactions in respect of which reasonable grounds to suspect money laundering or terrorist financing exist)

(1) When, in carrying out business referred to in Article 47 of this Act, reasons for suspicion of money laundering or terrorist financing exist in connection with the client or transaction, the lawyer, law firm or notary shall report such suspicion prior to effecting the transaction and shall state the time limit in which the transaction is to be carried out. Such report may also be submitted by telephone; however, the written report shall be sent to the office the next working day at the latest.

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

(3) If, in cases referred to in paragraphs 1 and 2 of this Article and due to the nature of the transaction, or because the transaction was not completed or due to other justified reasons, the lawyer, law firm or notary cannot follow the described procedure, they shall furnish the data to the office as soon as is practicable or immediately after the suspicion of money laundering or terrorist financing is raised. The lawyer, law firm or notary shall explain in the report the reasons for not acting in accordance with the described procedure.

(4) 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.

(5) The lawyer, law firm or notary shall forward to the office the data referred to in paragraph 3 of Article 83 in the manner prescribed in the rules issued by the minister competent for finance.

Article 50 (Exceptions)

(1) The provisions of paragraphs 1 and 2 of Article 49 of this Act shall not apply to the lawyer, law firm or notary with regard to the data obtained from or about the client in the course of establishing the client's legal position or when acting as the client's legal representative in a judicial proceeding, including advice on instituting or avoiding such proceeding, irrespective of whether such data is obtained before, during or after such proceedings.

(2) Subject to the conditions referred to in paragraph 1 of this Article, the lawyer, law firm or notary shall not be obliged to forward the data, information and documentation on the basis of a request from the office referred to in paragraphs 1 and 2 of Article 55 of this Act. In such case, they shall immediately and not later than within 15 days of receipt of the request inform the office in writing about the reasons for non-compliance with the office's request.

(3) Notwithstanding the other provisions of this Act, the lawyers, law firms or notaries shall not be obliged to report to the office the cash transactions referred to in paragraph 1 of Article 38 of this Act, unless reasons for suspicion of money laundering or terrorist financing exist in connection with the transaction or client.

CHAPTER IV

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 51 (Obligation to compile and use the list of indicators)

(1) Organisations, lawyers, law firms and notaries shall be obliged to compile a list of indicators for the identification of customers and transactions in respect of which reasonable grounds to suspect money laundering or terrorist financing exist.

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

(3) Organisations, lawyers, law firms and notaries shall be obliged to use the list of indicators referred to in paragraph 1 hereof when determining the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto.

(4) The minister responsible for finance 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 52

(Participation in preparing the list of indicators)

The Bank of Slovenia, Securities Market Agency of the Republic of Slovenia, Insurance Supervision Agency, Office of the Republic of Slovenia for Gaming Supervision, Agency for Public Oversight of Auditing, Slovenian Audit Institute, Chamber of Notaries of Slovenia, Bar Association of Slovenia, and associations and societies whose members are bound under this Act shall participate in drawing up the list of indicators referred to in paragraph 1 of Article 51 hereof.

CHAPTER V DUTIES AND COMPETENCIES OF THE OFFICE FOR MONEY LAUNDERING PREVENTION OF THE REPUBLIC OF SLOVENIA

5.1 General provisions

Article 53 (General)

- (1) The Office shall perform duties relating to the prevention and detection of money laundering and terrorist financing, and other duties as stipulated by this Act.
- (2) The Office shall receive, collect, analyse and forward data, information and documentation obtained in accordance with the provisions of this Act.
- (3) All data, information and documentation from personal data records shall be forwarded to the Office under this Act free of charge.

5.2 Detection of money laundering and terrorist financing

Article 54 (Request to an organisation for the submission of data on suspicious transactions or persons)

- (1) If the Office considers that in respect of a transaction or a certain person there are grounds to suspect money laundering or terrorist financing, it may demand that the organisation submit to it the following:
 1. data from records of customers and transactions, which shall be kept by organisations pursuant to paragraph 1 of Article 83 hereof;
 2. data on the assets and other property of said person with the organisation;
 3. data on transactions with assets and property of said person with the organisation;
 4. data on other business relationships of the organisation;
 5. all other data and information obtained or retained by the organisation under this Act which are required for detecting and proving money laundering and terrorist financing.In the request the Office shall specify the data required, as well as the legal basis for submission, purpose of processing, and the time limit within which the required data should be submitted to the Office.
- (2) The data referred to in the preceding paragraph may be required by the Office from the organisation 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 or terrorist financing.

(3) In the cases referred to in paragraphs 1 and 2 of this Article, the organisation shall additionally be obliged to forward to the Office upon its request all other necessary documentation.

(4) The organisation shall forward the data, information and documentation referred to in the preceding paragraphs to the Office without delay and at the latest within 15 days of receiving the request. Exceptionally, the Office may set a shorter time limit for the request if this is necessary to determine circumstances relevant 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.

(5) In cases of extensive documentation or due to other justified reasons, the Office may, by written notification, extend to the organisation, upon its written and reasoned initiative, the time limit determined in paragraph 4 of this Article and it may, in such cases, inspect the documentation in the organisation.

Article 55

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

(1) If the Office considers that there are grounds to suspect money laundering or terrorist financing in connection with a transaction or a certain person, it may require from the lawyer, law firm or notary the data, information and documentation relating to the transactions referred to in Article 47 hereof, which are needed for detecting and proving money laundering and terrorist financing. In the request the Office shall specify the data required, as well as the legal basis for submission, purpose of processing, and the time limit within which the required data should be submitted to the Office.

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

(3) Regarding the time limit for forwarding the data, information and documentation referred to in paragraphs 1 and 2 of this Article, the provisions of paragraphs 4 and 5 of Article 54 of this Act shall apply mutatis mutandis.

Article 56

(Request to a state authority or holders of public authority for the submission of data on suspicious transactions or persons)

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

(2) The data referred to in the preceding paragraph may be requested by the Office from the state authorities and holders of public authority 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 or terrorist financing.

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

(4) Notwithstanding paragraph 3 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 57 **(Order temporarily suspending a transaction)**

(1) The Office may issue a written order temporarily suspending a transaction for a maximum of 72 hours if the Office considers that there are reasonable grounds to suspect money laundering or terrorist financing, and it shall inform the competent authorities thereof.

(2) 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 organisation as soon as possible and/or on the same day when the order was issued. The responsible person in the organisation 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.

(3) 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 organisation instructions on procedure regarding the persons concerned in the transaction.

(4) The competent authorities referred to in paragraphs 1 and 2 of this Article shall be obliged to act very promptly after receiving notification and shall, within 72 hours of the temporary suspension of the transaction, take measures in accordance with their competencies.

Article 58 **(Temporarily suspending a transaction)**

(1) If the Office finds, within 72 hours of the time the order on temporary suspension of a transaction was issued, that there are no longer any reasonable grounds to suspect money laundering or terrorist financing, it shall inform the competent authorities and the organisation thereof, which may then execute the transaction immediately.

(2) If the Office does not act within the time provided in paragraph 1 of this Article, the organisation may proceed with the transaction immediately.

Article 59 **(Request for ongoing monitoring of a customer's financial transactions)**

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

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

(3) If the organisation cannot, due to the nature of the transaction or business, or due to other justified reasons, act as provided for in paragraph 2 of this Article, it shall be obliged to forward the data to the Office as soon as possible or the following working day at the latest. The organisation shall be obliged to explain in the report the reasons for not acting in accordance with the provisions of paragraph 2 of this Article.

(4) The application of the measure referred to in paragraph 1 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 of no more than six months.

Article 60 (Initiators)

(1) Notwithstanding the provisions of paragraphs 3, 4 and 6 of Article 38 and paragraph 1 of Article 49 hereof, if a transaction or a particular person raises suspicion of money laundering or terrorist financing, the Office may start collecting and analysing data, information and documentation also on the basis of a written and reasoned initiative from the court, prosecutor's office, police, Slovenian Intelligence and Security Agency, Intelligence and Security Service of the Ministry of Defence, Court of Auditors, the authority responsible for the prevention of corruption, Office of the Republic of Slovenia for Budgetary Supervision, or Customs Administration of the Republic of Slovenia. The initiative must contain at least the information referred to in paragraph 1 of Article 83 hereof.

(2) When there are grounds to suspect 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 documentation on the basis of a reasoned written initiative by 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 refuse the initiative referred to in paragraphs 1 and 2 of this Article if the initiative fails to state substantiated 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 not been tabled for discussion.

Article 61 (Notification of suspicious transactions)

(1) If the Office considers, on the basis of data, information and documentation acquired under this Act, that there are grounds to suspect money laundering or terrorist financing in

connection with a transaction or a certain person, it shall notify the competent authorities in writing and submit the necessary documentation.

(2) In the notification referred to in the preceding paragraph, the Office shall not state information about the employee and his/her respective organisation which first forwarded the information on the basis of paragraphs 3, 4 and 6 of Article 38 hereof, unless there are reasons to suspect that the organisation or its employee committed the criminal offence of money laundering or terrorist financing, or if such data are necessary in order to establish facts during criminal proceedings and if the submission of said data is requested in writing by the competent court.

Article 62 **(Information on other criminal offences)**

Notwithstanding the provision of paragraph 1 of Article 61 hereof, the Office shall forward written notification to competent authorities also in cases whereby the Office considers, on the basis of data, information and documentation obtained under this Act, that in connection with a transaction or a certain person there are grounds to suspect that the following criminal offences have been committed:

1. *Violation of the independent decisions of voters as stipulated in Article 151 of the Penal Code (Official Gazette Official Gazette of the RS, Nos. 55/08, 66/08 – amdt. and 39/09; hereinafter: KZ-1), acceptance of a bribe during elections as stipulated in Article 157 of KZ-1; fraud in Article 211 of KZ-1; organising “money chains” and illegal gambling in Article 212 of KZ-1; fraud in obtaining loans or related benefits in Article 230 of KZ-1; fraud in trading securities in Article 231 of KZ-1, forgery or destruction of business documents in Article 235 of KZ-1; abuse of power or trust in the performance of an economic activity in Article 240 of KZ-1, prohibited acceptance of gifts in Article 241 of KZ-1; prohibited giving of gifts in Article 242.a of KZ-1, tax evasion in Article 249 of KZ-1 and participation in a criminal organisation in Article 294 of KZ-1;*
2. other criminal offences for which the law prescribes a prison sentence of five or more years.

Article 63 **(Feedback)**

The Office shall notify in writing the person under obligation referred to in paragraphs 3, 4 and 6 of Article 38 and paragraph 1 of Article 49 of this Act, the initiator referred to in Article 60 of this Act, stock exchanges and the central securities clearing corporation referred to in Article 74 of this Act, and the supervisory body referred to in Article 89 of this Act, of the completion of collecting and analysing data, information and documentation in connection with a certain person or transactions in respect of which there are grounds to suspect 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.

5.3 International cooperation

Article 64 **(General rule)**

(1) The provisions of this Act concerning international cooperation shall apply unless otherwise stipulated by international agreement.

(2) Prior to forwarding personal data to the authority of the Member State or third country responsible for the prevention of money laundering and terrorist financing, the Office shall obtain assurances that the authority of the country to which the data is being forwarded has a regulated system of personal data protection, and that the authority of the Member State or third country shall use the data solely for the purposes stipulated by this Act.

Article 65
(Request to a foreign authority for the submission of data)

The Office may, within the scope of its tasks for detecting and preventing money laundering and terrorist financing, request from the authorities of Member States or third countries responsible for the prevention of money laundering and terrorist financing, to submit the data, information and documentation needed for detecting and preventing money laundering and terrorist financing.

(2) The Office may use the data, information and documentation acquired pursuant to the preceding paragraph solely for the purposes stipulated by this Act. The Office may not, without prior consent of the authority of the Member State or third country responsible for the prevention of money laundering and terrorist financing, forward or allow insight into the acquired data, information and documentation to a third person or use them in contravention of conditions and restrictions stipulated by the authority of whom the request was made.

Article 66
(Submission of data and information upon the request of a foreign authority)

(1) The Office shall submit the data, information and documentation on customers or transactions in respect of which there are grounds for suspicion of money laundering or terrorist financing, which were acquired or retained in accordance with the provisions of this Act, to the authority of the Member State or third country responsible for the prevention of money laundering and terrorist financing, upon its request and under the condition of effective reciprocity.

(2) The Office may refuse to satisfy the request of the authority of the Member State or third country responsible for money laundering and terrorist financing in the following cases:
if it considers, on the basis of the facts and circumstances stated in the request, that there are no grounds for suspicion of money laundering or terrorist financing;
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) The Office shall notify the authority of the Member State or third country responsible for money laundering and terrorist financing which submitted the request of its refusal, stating the reasons.

(4) The Office may prescribe additional conditions and restrictions that, if taken into account, would allow the authority of the Member State or third country responsible for money laundering and terrorist financing to use the data referred to in paragraph 1 of this Article.

Article 67
(Submission of data to a foreign authority upon its own initiative)

(1) The Office may submit the data and information on customers or transactions in respect of which there are grounds to suspect money laundering or terrorist financing, which were acquired or kept in accordance with the provisions of this Act, to the authority of the Member

State or third country responsible for the prevention of money laundering and terrorist financing, also upon its own initiative under the condition of effective reciprocity.

(2) The Office may, when submitting the data on its own initiative, prescribe additional conditions and restrictions under which the authority of the Member State or third country responsible for money laundering and terrorist financing may use the data referred to in paragraph 1 of this Article.

Article 68

(Temporary suspension of a transaction upon the initiative of a foreign authority)

(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 72 hours also on the basis of a reasoned and written request by the authority of a Member State or third country responsible for the prevention of money laundering and terrorist financing, and inform the competent authorities thereof.

(2) The Office may refuse the initiative taken by the authority of the Member State or third country responsible for money laundering and terrorist financing if it assesses, on the basis of the facts and circumstances referred to in the initiative of paragraph 1 of this Article, there are no reasonable grounds to suspect 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) With respect to the order on temporary suspension of a transaction under this Article, the provisions of Articles 57 and 58 herein shall apply mutatis mutandi.

Article 69

(Initiative to a foreign authority for the temporary suspension of a transaction)

The Office may, within the scope of its tasks for detecting and preventing money laundering and terrorist financing, submit to the authorities of Member States or third countries responsible for the prevention of money laundering and terrorist financing, 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.

5.4 Prevention of money laundering and terrorist financing

Article 70

(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 persons under obligation referred to in paragraphs 1 and 2 of Article 4 of this Act;
4. participate in professional training of the staff of organisations, state authorities, holders of public authority, lawyers, law firms and notaries;

5. publish, at least once per year, statistical data on money laundering and terrorist financing, in particular the number of suspicious transactions submitted to the Office in accordance with this Act, the number of cases handled annually, the number of persons subject to criminal prosecution, the number of persons convicted of criminal offence concerning money laundering or terrorist financing, and the scope of frozen, forfeited or seized assets;
6. inform the public, in an appropriate manner, of the various forms of money laundering and terrorist financing.

5.5 Other duties

Article 71

(Submission of data to the court, prosecutor's office or customs authorities)

(1) The Office shall submit to the court or prosecutor's office, upon its written and reasoned request, the data from the records of persons and transactions referred to in paragraph 1 of Article 38 and in Article 73 of this Act, which the court or prosecutor's office need for the purposes of investigating circumstances vital for the protection or forfeiture of proceeds, in accordance with the provisions of the law regulating criminal proceedings.

(2) The Office shall submit to the customs authorities, upon their written and reasoned request, the data from the records of persons and transactions referred to in paragraph 1 of Article 38 of this Act, which the customs authorities need for the purposes of implementing tasks under Community regulations governing mutual assistance between administrative authorities of the Member States.

Article 72

(Reporting to the Government)

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

CHAPTER VI

DUTIES OF STATE AUTHORITIES AND HOLDERS OF PUBLIC AUTHORITY

Article 73

(Customs authorities)

(1) Customs authorities shall be obliged to forward to the Office, at the latest within three days, the data referred to in paragraph 5 of Article 83 of this Act on any declared import or export of cash amounting to or exceeding EUR 10,000 when entering or leaving the Community.

(2) Customs authorities shall be obliged to forward to the Office the data referred to in paragraph 5 of Article 83 of this Act, even if the import or export of cash when entering or leaving the Community referred to in paragraph 1 of this Article was not declared to the customs authorities.

(3) Customs authorities shall forward to the Office the data referred to in paragraph 6 of Article 83 of this Act also in the event of import and/or export of cash, or attempted import and/or export of cash, in the amount of less than EUR 10,000 when entering or leaving the Community if, in connection with the person who carries the cash, the manner of carrying or

other circumstances thereof, there are grounds to suspect money laundering or terrorist financing.

Article 74
(Stock exchanges and the Central Securities Clearing Corporation)

(1) Stock exchanges and the Central Securities Clearing Corporation shall immediately notify the Office in writing if, during the performance of their activities and/or business operations, they discover facts that indicate or may indicate money laundering or terrorist financing.

(2) On the basis of the reported facts referred to in paragraph 1 of this Article, the Office, if it deems appropriate, may start collecting and analysing data, information and documentation in compliance with its authorisations stipulated by this Act.

Article 75
(Courts, prosecutors' offices and other national authorities)

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

(2) State authorities shall be obliged to forward regularly to the Office the following data:

1. date of filing the criminal charge;
2. personal name, date of birth and address, or the name of the company and registered office of the denounced person;
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 which has signs of a predicate offence.

(3) Prosecutors' offices and courts shall be obliged to forward twice annually to the Office the following information:

personal name, date of birth and address, or the company, address and registered office of the denounced person or the person who lodged a request for judicial protection within the offence proceedings;

stage of proceedings and the final verdict in each individual stage;

statutory designation of the criminal offence or other offence;

personal name, date of birth and address, or the company and registered office of the person in respect of whom an order for temporary protection of a request for forfeiture of proceeds or temporary seizure has been issued;

date of issue and duration of the order on temporary protection of the request for forfeiture of proceeds or temporary seizure;

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

date of issuing the order on forfeiture of assets or proceeds;

amount of assets or value of the proceeds forfeited.

(4) The competent state authorities shall be obliged to report to the Office, once per year and at the latest by the end of January of the current year for the previous year, on its findings made on the basis of the received notifications of suspicious transactions referred to in Article 61 of this Act, or information on other criminal offences referred to in Article 62 of this Act, and other measures taken on the basis hereof.

CHAPTER VII
PROTECTION AND RETENTION OF DATA AND MANAGEMENT OF RECORDS

7.1 Data protection

Article 76
(Prohibition on disclosure)

(1) Persons under obligation 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 or third person that:

1. the data, information or documentation about the customer or the transaction referred to in paragraphs 3, 4 and 6 of Article 38, paragraph 1 of Article 49, paragraphs 1, 2 and 3 of Article 54 and paragraphs 1 and 2 of Article 55 of this Act have been or will be forwarded to the Office;
2. the Office, pursuant to Article 57 of this Act, temporarily suspended the transaction and/or in this regard gave instructions to the person under obligation;
3. the Office, pursuant to Article 59 of this Act, required the ongoing monitoring of the customer's business operations;
4. an investigation has been or is likely to be launched against him/her or a third person on grounds of money laundering or terrorist financing.

(2) The facts referred to in the preceding paragraph and notification of suspicious transactions, and/or information on other criminal offences referred to in Articles 61 and 62 of this Act, shall be classified and discussed according to their level of classification, in accordance with the law regulating classified information.

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

(4) The prohibition on disclosure of facts referred to in paragraph 1 of this Article shall not apply:

1. if the data, information and documentation obtained and retained in accordance with this Act by a person under obligation 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;
2. if the data referred to in the preceding point are required by the supervisory body referred to in Article 85 of this Act for the supervision of implementation of the provisions of this Act and the ensuing regulations, conducted within its competencies.

(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 1 of this Article.

Article 77
(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 organisation, state authority or any other holder 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 documentation on their customers;
2. obtain and process data, information and documentation 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) The staff of organisations, law firms and notaries shall not be held criminally or disciplinarily liable for the breach of obligation to protect classified data, business and bank secrecy and professional secrecy due to:

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

Article 78 (Use of acquired data)

(1) The Office, state authorities and other holders of public authority, organisations, lawyers, law firms, notaries, and their staff, may use the data, information and documentation obtained under this Act solely for the purposes stipulated hereof.

(2) Courts, prosecutors' offices and customs authorities may use the data acquired pursuant to Article 71 of the present Act exclusively for the purpose for which they were acquired.

7.2 Retention of Data

Article 79 (Retention period of data with an organisation, lawyer, law firm or notary)

(1) An organisation shall keep the data obtained on the basis of Articles 8, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 22.a, 27, 29, 30, 31, 32 and 34 of this Act and the corresponding documentation for 10 years after the termination of a business relationship, the completion of a transaction, a customer's entry into the casino or gaming hall, or a customer's access to the safe.

(2) The organisation shall keep the information and corresponding documentation on the authorised person and deputy authorised person, on the professional training of staff, on the execution of internal control and risk management referred to in Article s 40, 44, 45 and 45.a of this Article for four years after the appointment of the authorised person or deputy authorised person and after the completion of professional training and the execution of internal control and analysis of the impact of changes in the organisation's business processes associated with money laundering or terrorist financing.

(3) A lawyer, law firm or notary shall keep the data obtained on the basis of paragraph 1 of Article 48 and the corresponding documentation for 10 years after the identification of the customer.

(4) A lawyer, law firm or notary shall keep the data and corresponding documentation on the professional training of staff for four years after the completion of professional training.

Article 80
(Retention period of data by customs authorities)

Customs authorities shall keep data from the records referred to in paragraphs 5 and 6 of Article 83 of this Act for a period of 12 years from the date they acquired them. These data and information shall be destroyed after the expiry of this period.

Article 81
(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 the period of 12 years from the date the Office acquired them. These data and information shall be destroyed after the expiry of this period.

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

(3) The person to whom the data and information refer shall have the right to inspect his/her personal data and/or to obtain their original, print-out or copy:
for the records referred to in points 1, 2, 3, 4, 5, 6 and 9 of paragraph 4 of Article 82 of this Act, eight years after the data have been collected;
for the records referred to in points 7 and 8 of paragraph 4 of Article 82 of this Act, after the final verdict or any other decision on criminal offence or other offence, and/or after the limitation of criminal prosecution, and/or immediately after the final decision of the competent authority that no measures shall be taken against the person to whom the data and information refer.

7.3. Management of records

Article 82
(Management of records)

(1) Organisations shall manage the following data records:

1. records of data on all customers, business relationships and transactions referred to in Article 8 of this Act;
2. records of data reported to the Office referred to in Article 38 of this Act.

(2) Lawyers, law firms and notaries shall manage the following data records:

1. records of clients, business relationships and transactions referred to in Article 8 of this Act;
3. records of reported data referred to in paragraph 1 of Article 49 of this Act.

(3) Customs authorities shall manage the following data records:

1. records on declared and undeclared import or export of cash in the amount of EUR 10,000 or more when entering or leaving the Community referred to in paragraphs 1 and 2 of Article 73 of this Act;

2. records on import or export of cash, or attempted import or export of cash, in the amount of less than EUR 10,000 when entering or leaving the Community, if there exist grounds to suspect money laundering or terrorist financing, referred to in paragraph 3 of Article 73 of this Act.

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

1. records of data on persons and transactions referred to in Article 38 of this Act;
2. records of data on persons and transactions referred to in paragraph 1 of Article 49 of this Act;
3. records of initiatives received, referred to in Article 60 of this Act;
4. records of notifications and the information referred to in Articles 61 and 62 of this Act;
5. records of international requests referred to in Articles 65 and 66 of this Act;
6. records of personal data sent abroad under Article 67 of this Act;
7. records of criminal offences and other offences referred to in Article 75 of this Act;
8. records of violations and supervisory measures referred to in Article 88 of this Act;
9. records of reported facts referred to in Articles 74 and 89 of this Act.

Article 83 (Content of records)

(1) In the records managed by organisations of customers, business relationships and transactions, the following data shall be processed for the purpose of implementing the provisions of Article 8 of this Act:

1. company name, address, registered office and registration number of the legal entity establishing a business relationship or carrying out a transaction, and/or of the legal entity on whose behalf a business relationship is established or a transaction is carried out;
2. personal name, permanent or temporary address, date and place of birth, and tax number of the statutory representative or authorised person establishing a business relationship or carrying out a transaction for a legal entity or any other civil law entity referred to in point 9 of Article 3 of this Act, and the number, type and name of the authority that issued the official personal document;
3. personal name, permanent or temporary address, date and place of birth, and tax number of the authorised person who for the customer conducts a transaction or requires a transaction to be effected, and the number, type and name of the authority that issued the official personal document;
4. personal name, permanent or temporary address, date and place of birth, and tax number of the natural person or his/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, and the number, type and name of the authority that issued the official personal document;
5. company name, address and registration number, if applicable, of the sole proprietor or self-employed person;
6. personal name, permanent or temporary address, date and place of birth of the natural person entering the casino or gaming hall or approaching the safe;
7. purpose and intended nature of the business relationship, including information about the activity of the customer;
8. date of entering into the business relationship or the date and time of entering the casino or gaming hall or approaching the safe;
9. date and time of the transaction;
10. amount of the transaction and currency in which the transaction is being carried out;

11. purpose of the transaction and the personal name and permanent address or name and registered office of the person to whom the transaction is directed;
12. manner of executing the transaction;
13. information about the source of assets or property that is or will be the subject of the business relationship or transaction;
14. grounds to suspect money laundering or terrorist financing;
15. personal name *and* permanent or temporary address, ~~date and place of birth~~ of the beneficial owner of the legal entity or, in case of point b of paragraph 2 of Article 19 of this Act, data on the category of persons interested in the establishment and activity of the legal entity or similar foreign law entity;
16. name of the other civil law entity referred to in point 9 of Article 3 of this Act and the personal name, permanent or temporary address, date and place of birth and tax number of the member.

(2) In the records managed by organisations of the data reported to the Office, the data referred to in paragraph 1 of this Article shall be processed for the purpose of implementing the provisions of Article 38 of this Act.

(3) In the records managed by lawyers, law firm and notaries of customers, business relationships and transactions, the following data shall be processed for the purpose of implementing the provisions of Article 8 of this Act:

1. personal name, permanent address, date and place of birth of the natural person, sole proprietor or self-employed person, or the company, address and registered office and registration number of the legal entity, sole proprietor or self-employed person for whom the lawyer, law company or notary performs services;
2. personal name, permanent address, date and place of birth of the statutory representative who establishes the permanent business relationship or carries out the transaction for the person referred to in point 1 of this paragraph;
3. personal name, permanent address, date and place of birth of the authorised person who carries out the transaction for the person referred to in point 1 of this paragraph;
4. data from point 15 of paragraph 1 of this Article in connection with the legal entity for which a lawyer, law firm or notary performs services;
5. purpose and intended nature of the business relationship, including information about the activity of the customer;
6. date of establishing the business relationship;
7. date of the transaction;
8. amount of the transaction and currency in which the transaction is being carried out;
9. purpose of the transaction and the personal name and address, or the company and registered office of the person to whom the transaction is directed;
10. manner of executing the transaction;
11. information about the source of assets or property that is or will be the subject of the business relationship or transaction;
12. personal name, date and place of birth, permanent address, or name of the company, address and registered office of the person in respect of whom there are grounds to suspect money laundering or terrorist financing;
13. data about the transaction in respect of which there are grounds for suspicion of money laundering or terrorist financing (amount, currency, date or period of execution of transaction);
14. grounds to suspect money laundering or terrorist financing.

(4) In the records managed by lawyers, law firms and notaries of the data reported to the Office, the data referred to in paragraph 3 of this Article shall be processed for the purpose of implementing paragraph 1 of Article 49 of this Act.

(5) In records managed by customs authorities of declared and undeclared import or export of cash in the amount of EUR 10,000 or more when entering or leaving the Community, the following data shall be processed for the purpose of implementing paragraphs 1 and 2 of Article 73 of this Act:

1. personal name, permanent address, date and place of birth, and citizenship of the natural person importing or exporting cash across the Community border;
2. name of the company, address and registered office of the legal entity, or personal name, permanent address and citizenship of the natural person on whose behalf the import or export of cash across the Community border is being carried out;
3. personal name, permanent address and citizenship of the natural person or the name of the company, address and registered office of the legal entity which is the intended recipient of cash;
4. amount, currency and type of cash being imported or exported across the Community border;
5. source and intended use of cash being imported or exported across the Community border;
6. date, place and time of crossing the Community border;
7. information on whether the import or export of cash was reported to the customs authorities.

(6) In the records managed by customs authorities of import or export of cash, or the attempted import or export of cash, in the amount of less than EUR 10,000 when entering or leaving the Community, if there are grounds to suspect money laundering or terrorist financing, the following data shall be processed for the purpose of implementing paragraph 3 of Article 73 of this Act:

1. personal name, permanent address, date and place of birth, and citizenship of the natural person importing or exporting cash, or attempting to import or export cash across the Community border;
2. name of the company, address and registered office of the legal entity, or personal name, permanent address and citizenship of the natural person on whose behalf the import or export of cash across the Community border is being carried out;
3. personal name, permanent address and citizenship of the natural person, or the name of the company, address and registered office of the legal entity which is the intended recipient of cash;
4. amount, currency and type of cash being imported or exported across the Community border;
5. source and intended use of cash being imported or exported across the Community border;
6. place, date and time of crossing or attempting to cross the Community border;
7. grounds to suspect money laundering or terrorist financing.

(7) In the records managed by the Office of the data on persons and transactions acquired pursuant to Article 38 of this Act, the data referred to in paragraph 1 of this Article shall be processed for the purpose of implementing the provisions of Article 53 hereof.

(8) In the records managed by the Office of the data on persons and transactions acquired pursuant to paragraph 1 of Article 49 of this Act, the data referred to in paragraph 3 of this Article shall be processed for the purpose of implementing the provisions of Article 53 of this Act.

(9) In the records managed by the Office of the initiatives received under Article 60 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 53 and 70 of this Act:

1. personal name, date and place of birth, and permanent address, or name of the company, address and registered office of the person in respect of whom there are grounds to suspect money laundering or terrorist financing;
2. data on the transaction in respect of which there are grounds to suspect money laundering or terrorist financing (amount, currency, date or period of execution of transaction);
3. grounds to suspect money laundering or terrorist financing.

(10) In the records managed by the Office of the notifications and information referred to in Articles 61 and 62 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 53 and 70 of this Act:

1. personal name, date and place of birth, and permanent address, or name of the company and registered office of the person in respect of whom the Office forwarded the 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.

(11) In the records managed by the Office of international requests under Articles 65 and 66 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 53 and 70 of this Act:

1. personal name, date and place of birth, and permanent address, or name of the company, address and registered office of the person to whom the request refers;
2. name of the country, title of the authority to whom the request was sent or of the authority issuing the request.

(12) In the records managed by the Office of personal data sent abroad, referred to in Article 67 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 53 and 70 of this Act:

1. personal name, date and place of birth, and permanent address, or name of the company, address and registered office of the person whose data are being sent abroad;
2. name of the country and title of the authority to whom the data are being sent.

(13) In the records managed by the Office of criminal offences and other offences under Article 75 of this Act, the following data on money laundering and terrorist financing shall be processed for the purpose of centralisation:

1. personal name, date and place of birth, and permanent address, or name of the company and registered office of the denounced person, the person in respect of whom an order for temporary protection of the request for forfeiture of proceeds has been filed, or the person against whom offence proceedings are taken before the court;
2. place, time and manner of committing the action 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 offence;
4. amount of money seized or the value of unlawfully acquired assets and the date of forfeiture.

(14) In the records managed by the Office of initiated offence proceedings, issued decisions and other measures taken with respect to noted offences by the supervisory bodies referred to in Article 85 of this Act, the following data shall be processed for the purpose of implementing the provisions of Article 88 of this Act:

1. data on the offender – natural person (personal name, unique 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/her);
2. data on the offender – legal entity (name, registered office and registration number);
 3. description of the offence;
 4. data on the supervisory measures imposed.

(15) In the records managed by the Office of the reported facts referred to in Articles 74 and 89 of this Act, the following data shall be processed for the purpose of implementing the provisions of Articles 53 and 70 hereof:

1. personal name, date and place of birth, and permanent address, or name of the company, address and registered office of the person in respect of whom there are facts that indicate or may indicate 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.

(16) Notwithstanding the provisions of the preceding paragraphs, the records referred to in Article 82 of this Act shall not include the birth registration number and/or tax number in the case of non-residents, unless otherwise specified by the present Act.

Article 84

(Records of access to data, information and documentation by supervisory bodies)

(1) The organisation, lawyer, law firm or notary shall keep separate records of access to data, information and documentation referred to in paragraph 1 of Article 76 hereof by the supervisory bodies referred to in Article 85.

(2) The records referred to in paragraph 1 of this Article shall contain the following information:

1. name of the supervisory body;
2. personal name of the official person authorised by the supervisory body, who inspected the data;
3. date and time of inspecting the data.

(3) Any access to the data referred to in paragraph 1 of this Article which was held by the supervisory body referred to in Article 85 hereof, shall be reported to the Office by the organisation, lawyer, law firm or notary, in writing and at the latest within three working days following the inspection of said data.

CHAPTER VIII SUPERVISION

8.1 Supervisory bodies

Article 85

(Supervisory bodies 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) Bank of Slovenia,

- c) Securities Market Agency ~~of the Republic of Slovenia~~,
- d) Insurance Supervision Agency,
- e) Office of the Republic of Slovenia for Gaming Supervision,
- f) Tax Administration of the Republic of Slovenia,
- g) Market Inspectorate of the Republic of Slovenia,
- h) *Agency for Public Oversight of Auditing and* Slovenian Audit Institute,
- i) Bar Association of Slovenia, and
- j) Chamber of Notaries of Slovenia.

(2) If, in exercising supervision, the supervisory body referred to in paragraph 1 of this Article establishes offences referred to in Articles 91, 92, 93, 94, 95, 96, 97, 98 and 99 hereof, it shall have the right and duty to:

1. order measures to remedy the irregularities and deficiencies within the time limit as specified by it;
2. carry out proceedings in accordance with the law regulating offences;
3. propose the adoption of appropriate measures to the competent authority;
4. order other measures and perform acts for which it is authorised by law or any other regulation.

(3) Offence proceedings shall be led and decided on by an official person authorised by the supervisory body referred to in paragraph 1 of this Article who meets the conditions stipulated by the stated Act and the regulations adopted on the basis therein.

(4) A person who has committed the offence laid down by this Act may be imposed a fine in a summary proceeding in an amount which is higher than the statutory minimum level, provided the fine range is determined.

8.2 Competencies of supervisory bodies

Article 86 (The Office)

(1) The Office shall supervise implementation of the provisions of this Act within the organisations referred to in paragraph 1 of Article 4 hereof, and with lawyers, law firms and notaries.

(2) The Office shall supervise implementation of the provisions of this Act by gathering and verifying the data, information and documentation obtained on the basis of the provisions of this Act.

(3) The organisations referred to in paragraph 1 of Article 4 hereof and lawyers, law firms and notaries shall be obliged to submit to the Office in writing the data, information and documentation on the performance of their duties as provided by this Act, as well as other information which the Office requires for conducting supervision, without delay and at the latest within fifteen days of receiving the request.

(4) The Office may also demand from state authorities and from holders of public authority the data, information and documentation required for exercising supervision under this Act and for conducting offence proceedings.

Article 87 (Other supervisory bodies)

(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 persons under obligation referred to in points 1, 2, 3, 9 and 10 of paragraph 1 of Article 4 hereof and with other persons.

(2) The Securities Market Agency of the ~~Republic of Slovenia~~ shall, in accordance with its competences stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with the persons under obligation referred to in points 5, 6, and 7 of paragraph 1 of Article 4 hereof and with other persons.

(3) The Insurance Supervision Agency shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with the persons under obligation referred to in points 6, 8, 16(h) and 16(i) of paragraph 1 of Article 4 hereof and with other persons.

(4) The Office of the Republic of Slovenia for Gaming Supervision shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with the persons under obligation referred to in points 12, 13 and 14 of paragraph 1 of Article 4 hereof and with other persons.

(5) The Tax 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 15,000 with the legal entities and natural persons referred to in Article 37 of this Act.

(6) The Market Inspectorate of the Republic 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 the persons under obligation referred to in points 15, 16(a), 16(b), 16(g) and 16(p) of paragraph 1 of Article 4 hereof and with other persons.

(7) The *Agency for Public Oversight of Auditing* Slovenian Audit Institute shall, in accordance with its competencies stipulated herein and in other laws, exercise supervision over implementation of the provisions of this Act with the persons under obligation referred to in point 11 of paragraph 1 of Article 4 hereof and with other persons.

(8) 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, law firms and with other persons.

(9) 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 and other persons.

(10) Supervisory bodies referred to in this Article shall forward to any other supervisory body, upon its request, all necessary information needed by that supervisory body for exercising its supervisory tasks.

8.3 Reporting data on supervision

Article 88

(Notification of offences and measures)

(1) The supervisory body referred to in Article 85 hereof shall notify the Office in writing and without delay of supervisory measures imposed, offences established and other significant findings.

(2) The notification referred to in the preceding paragraph shall include the following in particular:

- data on the offender (personal name, unique personal identification number or, if the natural person is a foreigner, date and place of birth), citizenship and permanent or temporary address of the natural person, and for the responsible person of a legal entity, also employment and tasks and duties performed by him/her, or name and registered office of the legal entity having committed the offence, and the registration number;
- description of the offence;
- data on supervisory measures imposed and findings.

(3) The supervisory body which detected the offence shall also inform other supervisory bodies of its findings and/or any incompliance, if relevant for their work.

(4) To enable centralisation and analysis of all data related to money laundering and terrorist financing, supervisory bodies shall forward to the Office a copy of the decision issued in offence proceedings.

Article 89 (Notification of facts)

(1) The supervisory bodies referred to in Article 85 hereof shall immediately notify the Office in writing if, during supervision under this Act or during the performance of their activities or business operations in accordance with the competencies stipulated in other laws, they establish or discover facts that indicate or may indicate money laundering or terrorist financing.

(2) On the basis of the notified facts referred to in paragraph 1 of this Article, the Office, if it deems appropriate, may start collecting and analysing data, information and documentation in compliance with its authorisations stipulated by this Act.

8.4 Issuing recommendations and guidelines

Article 90 (Issuing recommendations and guidelines)

With a view to ensuring uniform implementation of the provisions of this Act and the ensuing regulations by organisations, lawyers, law firms and notaries, the supervisory bodies referred to in Article 85 hereof shall independently, or in cooperation with other supervisory bodies, issue recommendations and guidelines relating to implementation of the provisions of this Act for the persons under obligation referred to in paragraphs 1 and 2 of Article 4 hereof.

CHAPTER IX PENALTY PROVISIONS

Article 91
(Most serious offences)

(1) A fine from EUR 12,000 to 120,000 shall be imposed on a legal entity for the following offences:

1. failure to prepare a risk analysis or establish a risk assessment for individual groups or customers, business relationships, products or transactions (paragraph 2 of Article 6 hereof);
2. failure to carry out customer due diligence (paragraph 1 of Article 8 and paragraph 7 of Article 12 hereof);
3. establishing a business relationship with a customer without prior application of the prescribed measures (paragraph 1 of Article 9 hereof);
4. effecting a transaction without prior application of the prescribed measures (Article 10 hereof);
5. failure to determine and verify the identity of a natural person or his/her statutory representative, sole proprietor or self-employed person, legal entity, statutory representative of a legal entity, authorised person, agent of other civil law entities or beneficial owner of the legal entity or similar foreign law entity, or failure to obtain the prescribed data, or failure to obtain them in the prescribed manner, or failure to obtain the certified written authorisation *or written authorisation* for representation (Articles 13, 14, 15, 16, 17 and 20 hereof);
6. determining and verifying the identity of a customer by using a qualified digital certificate in a prohibited manner (paragraph 5 of Article 13);
7. failure to determine or verify the identity of a customer upon the customer's entry into a casino or gaming hall, or each time the customer accesses the safe (Article 18 hereof);
8. failure to obtain data on the purpose and intended nature of the business relationship or transaction, as well as other data pursuant to this Act, or failure to obtain all the prescribed data (Article 21 hereof);
9. entering into a business relationship in contravention of the provisions of this Act (paragraph 5 of Article 27 hereof);
10. failure to apply the prescribed measures and, in addition, obtain data, information and documentation in accordance with paragraph 1 of Article 30 when entering a correspondent banking relationship with a bank or other similar credit institution situated in a third country, or failure to obtain the data in the prescribed manner (paragraphs 1 and 3 of Article 30 hereof);
11. entering into or continuing, contrary to law, a correspondent banking relationship with a respondent bank or other similar credit institution situated in a third country (paragraph 4 of Article 30 hereof);
12. failure to obtain data on the source of funds and property that are or will be the subject of a business relationship or transaction when entering into a business relationship or effecting a transaction for a customer who is a foreign politically exposed person, or for failure to obtain the data in the prescribed manner (point 1, paragraph 6 of Article 31 hereof);
13. failure to apply, within enhanced due diligence towards a customer who is not physically present in the organisation when determining and identifying his/her identity, measures referred to in paragraph 1 of Article 7 and one or two additional measures referred to in paragraph 2 of Article 32 (paragraph 1 of Article 32 hereof);
14. applying simplified customer due diligence despite the fact that in respect of a customer or transaction grounds for money laundering exist, or entering into a correspondent banking relationship with a respondent bank or other similar credit institution situated in a third country when such organisation fails to act in accordance with paragraph 1 of Article 30 of this Act (paragraphs 1 and 2 of Article 33 hereof);
15. failure to obtain, within simplified customer due diligence, the prescribed data on a customer, business relationship or transaction, or for failure to obtain the data in the prescribed manner (Article 34 hereof);

16. 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 35 hereof);
17. 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 36 hereof);
18. accepting cash payment from a customer or third person when selling goods, which exceeds the amount of EUR 15,000, or accepting payment effected by several linked cash transactions exceeding in total the amount of EUR 15,000 (paragraphs 1 and 2 of Article 37 hereof);
19. failure to furnish the Office with the prescribed data where grounds to suspect money laundering or terrorist financing exist in connection with a customer or transaction or an intended transaction (paragraphs 3, 4 and 6 of Article 38);
20. failure to submit to the Office, within the prescribed time limit, the required data, information and documentation where in respect of a customer or transaction grounds to suspect money laundering or terrorist financing exist (paragraphs 1, 2, 3 and 4 of Article 54 hereof);
21. failure to comply with the Office's order temporarily suspending a transaction or the Office's instructions issued in this regard (Article 57 and paragraphs 1 and 3 of Article 68 hereof);
22. failure to comply with the Office's written request for ongoing monitoring of a customer's financial transactions (paragraphs 1, 2 and 3 of Article 59 hereof);
23. failure to submit to the Office, within the prescribed time limit and in the prescribed manner, data, information and documentation on the performance of duties as provided by this Act, as well as other information which the Office requires for conducting supervision (paragraph 3 of Article 86 hereof);
24. failure to remedy irregularities and deficiencies within the time limit as specified by an official authorised person (point 1, paragraph 2 of Article 85 hereof);
25. *disclosure of facts referred to in paragraph (1) of Article 76 of this Act to the customer or to a third party;*
26. *Failure to notify the Office of the product for which it intends to omit customer due diligence even before marketing or selling the product (paragraph (6) of Article 12 of this Act);*
27. *Failure to carry out an analysis of the impact of changes in business processes on its exposure to the risk of money laundering or terrorist financing (Article 45a of this Act).*

(2) *A fine of EUR 800 to 4000 shall be imposed for an offence on the responsible person of a legal entity or the responsible person of a sole trader committing an offence referred to in the preceding paragraph.*

(3) A fine from EUR 4,000 to 40,000 shall be imposed on a sole proprietor or self-employed person for the offence referred to in paragraph 1 of this Article.

Article 92 (Serious offences)

(1) A fine from EUR 6,000 to 60,000 shall be imposed on a legal entity for the following offences:

1. failure to carry out customer due diligence within the prescribed scope (paragraph 1 of Article 7 hereof);
2. failure to define procedures for implementation of the measures referred to in paragraph 1 of Article 7 in its internal regulations (paragraph 2 of Article 7 hereof);
3. *failure to demand a written statement from the customer, statutory representative, authorised person or the agent of other civil law entities (paragraph (7) of Article 13,*

paragraph (5) of Article 14, paragraph (2) of Article 15, paragraph (4) of Article 16 and paragraph (5) of Article 17 hereof);

4. failure to act in accordance with paragraph 3 of Article 32 of this Act (paragraph 8 of Article 13 hereof);
5. failure to monitor business activities undertaken by a customer through the organisation with due diligence (paragraph 1 of Article 22 hereof);
6. *failure to obtain the required data when verifying and updating the data (paragraphs (2) and (3) of Article 22 of this Act);*
7. entrusting a third party to carry out customer due diligence without having verified whether that third party meets all the conditions stipulated by this Act (paragraph 2 of Article 24 hereof);
8. accepting customer due diligence as appropriate, in which the third party determined and verified the identity of a customer in his/her absence (paragraph 3 of Article 24 hereof);
9. 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 3 of Article 25 hereof);
10. 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, or is a fiduciary or other similar foreign law company with unknown or hidden owners or managers (Article 26 hereof);
11. failure to obtain in addition all data, information and documentation in accordance with paragraph 1 of Article 30 when entering into a correspondent banking relationship with a bank or other similar credit institution situated in a third country (Article 30 hereof);
12. failure of an organisation to define the procedure for determining foreign politically exposed persons in its internal act (paragraph 1 of Article 31 hereof);
13. entering into a business relationship with a customer who is a foreign politically exposed person, but not monitoring with due diligence the transactions and other business activities carried out by that person (point 3, paragraph 6 of Article 31 hereof);
14. entering into a business relationship in the absence of the customer under paragraph 2 of Article 13 in contravention of paragraph 3 of Article 32 (paragraph 3 of Article 32 hereof);
15. failure to furnish the Office, within the prescribed time limit, with the prescribed data on any cash transaction exceeding EUR 30,000 (paragraph 1 of Article 38 hereof);
16. failure 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 1 of Article 39 hereof);
17. failure to appoint an authorised person and one or more deputies for particular tasks of detecting and preventing money laundering and terrorist financing stipulated by this Act and the ensuing regulations (Article 40 hereof);
18. failure to provide the authorised person with appropriate authorisations, conditions and support for performance of his/her duties and tasks (paragraphs 1, 2, 3 and 4 of Article 43 hereof);
19. failure 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 51 and paragraph 2 of Article 100 hereof);
20. failure to keep data and documentation 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 1 of Article 79 hereof);
21. failure to carry out due diligence for all existing customers in respect of whom, based on Article 6 of this Act, it establishes that there exist or may exist significant risks of money laundering or terrorist financing (Article 101 hereof);
22. failure to carry out, in respect of anonymous products existing on the day of entry into force of this Act and for which it is impossible to identify the owner, due diligence towards the customer or other user of the product in accordance with Article 5 of this Act upon the

first transaction effected by the customer or other user on the basis of such a product (Article 102 hereof);

23. failure to bring its business operations into compliance or to terminate existing correspondent banking relationships within the prescribed time limit (Article 103 thereof).

(2) A fine of EUR 400 to 2000 shall be imposed for an offence on the responsible person of a legal entity or the responsible person of a sole trader committing an offence referred to in the preceding paragraph.

(3) A fine from EUR 2,000 to 20,000 shall be imposed on a sole proprietor or a self-employed person for the offence referred to in paragraph 1 of this Article.

Article 93 (Minor offences)

(1) A fine from EUR 3,000 to 30,000 shall be imposed on a legal entity for the following offences:

1. failure 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 6 of Article 14 hereof);
2. failure to ensure that the scope and frequency of measures referred to in paragraph 1 of Article 22 are appropriate to the risk of money laundering or terrorist financing to which the organisation is exposed in carrying out individual transactions or in business operations with individual customers (paragraph 4 of Article 22 hereof);
3. failure to inform the Office and take appropriate measures to eliminate the risk of money laundering or terrorist financing (paragraph 2 of Article 39 hereof);
4. failure to inform its branches and majority-owned subsidiaries with head offices in third countries of the internal procedures relating to the detection and prevention of money laundering and terrorist financing (paragraph 3 of Article 39 hereof);
5. failure to ensure that the work of an authorised person or his/her deputy is entrusted solely to a person meeting the prescribed requirements (paragraphs 1 and 2 of Article 41 hereof);
6. failure to forward to the Office, within the prescribed time limit, the personal name and title of the position held by the authorised person and his/her deputy and any changes thereof (paragraph 5 of Article 43 hereof);
7. failure to provide regular professional training and education to all employees carrying out tasks for the prevention and detection of money laundering and terrorist financing pursuant to this Act (paragraph 1 of Article 44 hereof);
8. failure 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 3 of Article 44 hereof);
9. failure to ensure regular internal control over the performance of tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act (Article 45 hereof);
10. failure to use the list of indicators referred to in paragraph 1 of Article 51 when determining the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto (paragraph 3 of Article 51 hereof);
11. *failure to keep the information and corresponding documentation on the authorised person and deputy authorised person, on the professional training of staff, on the execution of internal control referred to in Articles 40, 44, 45 and 45.a 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 execution of internal control and analysis of the impact of changes in the organisation's business processes associated with money laundering or terrorist financing (paragraph (2) of Article 79 of this Act);*

12. failure to keep separate records of access to data, information and documentation referred to in paragraph 1 of Article 76 hereof, which was held by supervisory bodies referred to in Article 85, or keeping incomplete records (paragraphs 1 and 2 of Article 84 hereof);
13. failure to inform the Office, within the prescribed time limit and in the prescribed manner, of any access held by the supervisory bodies referred to in Article 85 hereof (paragraph 3 of Article 84 hereof);

(2) A fine of EUR 200 to 1000 shall be imposed for an offence on the responsible person of a legal entity or the responsible person of a sole trader committing an offence referred to in the preceding paragraph.

(3) A fine from EUR 1,000 to 10,000 shall be imposed on a sole proprietor or self-employed person for the offence referred to in paragraph 1 of this Article.

Article 94

(Offences of certification authorities issuing qualified digital certificates)

(1) A fine from EUR 12,000 to 120,000 shall be imposed for the offence of a certification authority issuing a qualified digital certificate if the latter fails to submit to the organisation, upon its request, data on the manner of determining and verifying the identity of the customer-bearer (paragraph 4 of Article 13 hereof).

(2) A fine from EUR 800 to 4,000 shall be imposed on the responsible person of a certification authority issuing a qualified digital certificate for the offence referred to in paragraph 1 of this Article.

~~Article 95~~

~~(Offences of third persons)~~

~~(1) A fine of EUR 6,000 to 60,000 shall be imposed on a third person who fails to meet the obligations under paragraph 6 of Article 27 of this Act.~~

~~(2) A fine from EUR 400 to 2,000 shall be imposed on the responsible person of a third person for the offence referred to in paragraph 1 of this Article.~~

Article 96

(Offence by employees of an organisation)

(1) A fine from EUR 200 to 1,000 shall be imposed for an offence by the employee of an organisation establishing the correspondent relationship referred to in paragraph 1 of Article 30 and carrying out the enhanced customer due diligence procedure if he/she fails to obtain the written consent of his/her superior and the responsible person in the organisation prior to entering into such a relationship (paragraph 2 of Article 30 hereof).

(2) A fine from EUR 200 to 1,000 shall be imposed for an offence by the employee of an organisation who carries out the procedure for entering into a business relationship with a customer who is a foreign politically exposed person if he/she fails to obtain the written consent of his/her superior and the responsible person prior to entering into such a relationship (point 2 of paragraph 6 of Article 31 hereof).

Article 97

(Specific offences by auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services)

(1) A fine from EUR 12,000 to 120,000 shall be imposed for an offence by an auditing firm or independent auditor for carrying out simplified due diligence procedure despite the fact that in respect of the customer or auditing circumstances, grounds to suspect money laundering or terrorist financing exist (paragraph 3 of Article 33 hereof).

(2) A fine from EUR 12,000 to 120,000 shall be imposed for an offence by auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services if they fail to report to the Office, within the prescribed time limit, all cases in which a customer has sought advice for money laundering or terrorist financing (paragraph 5 of Article 38 hereof).

(3) A fine from EUR 800 to 4,000 shall be imposed on the responsible person of an auditing firm or legal entity performing accounting or tax advisory services, for the offence referred to in paragraph 1 of this Article.

**Article 98
(Offences by lawyers, law firms and notaries)**

(1) A fine from EUR 12,000 to 120,000 shall be imposed on a lawyer, law firm or notary for the following offences:

1. failure to, within customer due diligence, obtain the prescribed data pursuant to this Act (paragraphs 1, 2 and 3 of Article 48 hereof);
2. failure to obtain data on the purpose and intended nature of the business relationship or transaction, as well as other data pursuant to this Act, or failure to obtain all the prescribed data (Article 21 hereof);
3. failure to determine and verify the identity of the client or his/her statutory representative or authorised person, or failure to obtain the prescribed data in the prescribed manner (paragraphs 4 and 7 of Article 48 hereof);
4. failure to inform the Office, within the prescribed time limit and manner, that in respect of a transaction or an intended transaction or a particular person there are grounds to suspect money laundering or terrorist financing (paragraphs 1, 2 and 3 of Article 49);
5. failure to furnish the Office with the prescribed data where grounds to suspect money laundering or terrorist financing exist in respect of a customer or transaction or an intended transaction (paragraphs 3, 4 and 6 of Article 49);
6. failure to report to the Office the cash transactions referred to in paragraph 1 of Article 38 hereof, where in respect of a transaction or customer there are grounds to suspect money laundering or terrorist financing (paragraph 3 of Article 50 hereof);
7. failure to submit to the Office, within the prescribed time limit, the required data, information and documentation, where in respect of a transaction or person grounds to suspect money laundering or terrorist financing exist (paragraphs 1, 2 and 3 of Article 55 hereof);
8. failure to keep data obtained on the basis of paragraph 1 of Article 48 hereof and corresponding documentation for 10 years after identification of the customer (paragraph 3 of Article 79 hereof).

(2) A fine from EUR 6,000 to 60,000 shall be imposed on a lawyer, law firm or notary for the following offences:

1. failure to appoint an authorised person and one or more deputies for particular tasks of detecting and preventing money laundering and terrorist financing stipulated by this Act and the ensuing regulations (Article 40 with regard to Article 47 hereof);
2. failure to provide the authorised person with appropriate authorisations, conditions and support for the performance of his/her duties and tasks (paragraphs 1, 3 and 4 of Article 43 with regard to Article 47 hereof);
3. failure to determine the beneficial owner of a client who is a legal entity or similar foreign legal entity, or for failure to obtain the prescribed data, or for failure to obtain them in the prescribed manner (paragraphs 5 and 7 of Article 48 hereof);
4. failure to draw up a 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 for failure to draw up said list in the prescribed manner and/or time limit (paragraphs 1 and 2 of Article 51 and paragraph 2 of Article 100 hereof);
5. failure to submit to the Office, within the prescribed time limit and in the prescribed manner, data, information and documentation on the performance of duties as provided by this Act, as well as other information which the Office requires for conducting supervision (paragraph 3 of Article 86 hereof).

(3) A fine from EUR 3,000 to 30,000 shall be imposed on a lawyer, law firm or notary for the following offences:

1. failure to ensure that the work of an authorised person or his/her deputy is entrusted solely to a person meeting the prescribed requirements (paragraphs 1 and 2 of Article 41 with regard to Article 47 hereof);
2. failure to forward to the Office, within the prescribed time limit, the personal name and title of the position held by the authorised person and his/her deputy and any changes thereof (paragraph 5 of Article 43 with regard to Article 47 hereof);
3. failure to provide regular professional training and education to employees carrying out tasks for the prevention and detection of money laundering and terrorist financing pursuant to this Act (paragraph 1 of Article 44 with regard to Article 47 hereof);
4. failure 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 3 of Article 44 with regard to Article 47 hereof);
5. failure to ensure regular internal control over the performance of tasks for detecting and preventing money laundering and terrorist financing pursuant to this Act (Article 45 with regard to Article 47 hereof);
6. failure to inform the Office of the reasons for non-compliance with the Office's request, or failure to inform them within the prescribed time limit (paragraph 2 of Article 50 hereof);
7. failure to use the list of indicators referred to in paragraph 1 of Article 51 when determining the grounds to suspect money laundering or terrorist financing or other circumstances relating thereto (paragraph 3 of Article 51 hereof);
8. failure to keep data and corresponding documentation for four years after the completion of professional training (paragraph 4 of Article 79 hereof);
9. failure to keep separate records of access to data, information and documentation referred to in paragraph 1 of Article 76 hereof, which was held by supervisory bodies referred to in Article 85, or for keeping incomplete records (paragraphs 1 and 2 of Article 84 hereof);
10. failure to inform the Office, within the prescribed time limit and in the prescribed manner, of any access held by the supervisory bodies referred to in Article 85 hereof (paragraph 3 of Article 84 hereof).

(4) A fine from EUR 800 to 4000 shall be imposed on the responsible person of a law firm for the offence referred to in paragraph 1 of this Article.

Article 99

(Persons pursuing the activity of selling goods)

(1) A fine from EUR 6,000 to 60,000 shall be imposed on a self-employed legal entity or natural person or a sole trader pursuing the activity of selling goods, for failure to bring its business into compliance with the provision of Article 37 hereof within the prescribed time limit (Article 104 hereof).

(2) A fine of EUR 400 to 2000 shall be imposed for an offence on the responsible person of a legal entity or the responsible person of a sole trader committing an offence referred to in the preceding paragraph.

**CHAPTER X
TRANSITIONAL AND FINAL PROVISIONS**

**Article 100
(Implementing regulations and list of indicators)**

(1) The minister responsible for finance shall adopt the rules referred to in paragraph 4 of Article 6, paragraph 2 of Article 13, point 8 of paragraph 1 and paragraph 5 of Article 25, paragraphs 7 and 8 of Article 38, Article 46, and paragraph 5 of Article 49 of this Act, at the latest within six months following its entry into force.

(2) Organisations, lawyers, law firms and notaries shall draw up 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, at the latest within six months following the entry into force of this Act.

(3) The list of indicators for the identification of customers and transactions in respect of which there are grounds to suspect money laundering or terrorist financing which were adopted by organisations, lawyers, law firms and notaries pursuant to the Prevention of Money Laundering Act (Official Gazette, Nos. 79/01 and 59/02) shall remain in force.

**Article 101
(Due diligence towards existing customers)**

Organisations shall, within one year following the entry into force of this Act, perform due diligence towards all existing customers in respect of whom, based on Article 6 of this Act, they establish that there exist or may exist significant risks of money laundering or terrorist financing.

**Article 102
(Compliance for anonymous products)**

Notwithstanding the provision of Article 35 of this Act, the organisation shall carry out, in respect of anonymous products existing on the day of entry into force of this Act and for which it is impossible to identify the owner, due diligence towards the customer or other user of the product in accordance with Article 7 of this Act, upon the first transaction effected by the customer or other user on the basis of such a product.

**Article 103
(Compliance for organisations)**

Organisations shall bring their business into compliance with the provision of Article 36 of this Act within one year following the entry into force of this Act.

Article 104

(Compliance for legal entities and natural persons pursuing the activity of selling goods)

Legal entities and natural persons pursuing the activity of selling goods shall bring their business into compliance with the provision of Article 37 of this Act at the latest within 90 days following the entry into force of this Act.

Article 105

(Repealed regulations)

(1) Upon the entry into force of this Act, the Prevention of Money Laundering Act (Official Gazette, Nos. 79/01 and 59/02) shall cease to apply, with the exception of Articles 4, 5, 6, 7, 8, 9, 10, 11, 28, 28a and 28b, which shall be used pending the application of Chapters II and III, with the exception of Articles 38, 40, 41, 42, 43, 44 and 49 of this Act.

(2) On the day of entry into force of this Act, the following implementing regulations shall cease to apply:

Rules on organisations that do not need to be identified during the execution of certain transactions (Official Gazette, No. 1/04);

Rules on the method of communicating information to the Office for Money Laundering Prevention of the Republic of Slovenia (including the forms, annex and instructions on the manner of filling out the forms as an integral part of these Rules) (Official Gazette, Nos. 84/01, 83/02 and 1/04);

Rules laying down the terms and conditions under which organisations from Article 2 of the Money Laundering Prevention Act are not under the obligation to report cash transaction data for certain customers (Official Gazette, No. 1/04);

Rules on the method of communicating data to the Office of the Republic of Slovenia for Money Laundering Prevention by lawyers, law firms, notaries, auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services (Official Gazette, No. 83/02);

Rules on the authorised person, method of performing internal control, retention and protection of data, keeping of records and professional training provided for employees of organisations, lawyers, law firms, notaries, auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services (Official Gazette, No. 88/02);

Rules on the credit and financial institutions with the registered office in the European Union or in those countries which, according to the information provided by international organisations and other relevant international operators, observe international standards in the field of preventing and detecting money laundering, and need not be identified in carrying out certain transactions (Official Gazette, Nos. 94/02 and 48/04);

Rules on customer identification when opening an account or entering into a business relationship in the absence of the customer (Official Gazette, Nos. 94/02, 1/04 and 48/04);

Rules determining the list of countries which do not comply with the standards in the field of prevention and detection of money laundering (Official Gazette, No. 72/05).

(3) The implementing regulations referred to in paragraph 2 of this Article shall apply pending the issuing of new regulations, provided they do not contravene this Act.

Article 106

(Entry into force and application)

(1) This Act shall enter into force on the 15th day following that of its publication in the Official Gazette of the Republic of Slovenia (*Uradni list*).

(2) The provisions referred to in Chapter II, with respect to duties and obligations of organisations, and in Chapter III, with respect to duties of lawyers, law firms and notaries, except for Articles 38, 40, 41, 42, 43, 44 and 49, shall start to apply six months following the entry into force of the Act.

No. 480-01/00-1/6
Ljubljana, 22 June 2007
EPA 1407-IV

President
of the National Assembly
of the Republic of Slovenia
France Cukjati, MD, m.p.