COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM (MONEYVAL)

MONEYVAL(2015)12ANN

Report on Fourth Assessment Visit - Annexes

Anti-Money Laundering and Combating the Financing of Terrorism

MONTENEGRO

16 April 2015

Montenegro is a member of MONEYVAL. This evaluation was conducted by MONEYVAL and the mutual evaluation report on the 4th assessment visit of Montenegro was adopted at its 47th Plenary (Strasbourg, 14-17 April 2015)

© [2015] Committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL).

All rights reserved. Reproduction is authorised, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-Rom, Internet, etc) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law (DG I), Council of Europe (F-67075 Strasbourg or moneyval@coe.int)

LIST OF ANNEXES

Contents

ANNEX 1. DETAILS OF ALL BODIES MET ON THE ON-SITE VISIT 4

ANNEX 2. LIST OF ALL THE DOCUMENTS AND OTHER MATERIALS PROVIDED TO THE EVALUATION TEAM..5

ANNEX 3. TRAINING ATTENDED BY THE STAFF OF THE FIU..599

ANNEX 4. STATUS OF IMPLEMENTATION OF THE VIENNA CONVENTION, THE PALERMO CONVENTION AND THE UN INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM..607

ANNEX 5. INTERNATIONAL AGREEMENTS SIGNED BY MONTENEGRO 612

ANNEX 6. MEMORANDUMS OF UNDERSTANDING SIGNED BY THE MONTENEGRIN FIU 615

ANNEX 1. DETAILS OF ALL BODIES MET ON THE ON-SITE VISIT

Ministries, other Government Authorities and Bodies

Administration for the Prevention of Money Laundering and Financing of Terrorism (FIU)
Central Business Register
Ministry of Finance
Ministry of Interior
Ministry of Foreign Affairs
Ministry of Justice
National Commission for the Prevention of Money Laundering and Financing of Terrorism
Office for Cooperation with NGOs
Tax Administration

Law Enforcement Bodies, Public Prosecutor' Office, Judiciary

Customs Directorate
High Court of Podgorica and Bijelo Polje
National Security Agency
Police Directorate
Supreme Prosecutor's Office

Financial and non-Financial Sector Bodies

Administration for Inspection Affairs
Agency for Telecommunication and Postal Services
Central Bank of Montenegro
Financial Supervision Authority
Games of Chance Administration
Insurance Supervisory Agency
Securities and Exchange Commission

Private Sector Representatives and Associations

Accountants
Auditors
Banking Association
Bar Association
Casinos (including on-line casinos)

Chamber of Notaries

Dealers in Precious Metals and Stones

Institute of Auditors and Accountants

Lawyers

Notaries Public

Representatives of credit institutions

Representatives of insurance companies

Representatives of investment firms

Representatives of Post

ANNEX 2. LIST OF ALL THE DOCUMENTS AND OTHER MATERIALS PROVIDED TO THE EVALUATION TEAM

Decree on announcement of the Law on prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro , No. 14/07 from 21st Dec 2007, 04/08 from 17th Jan 2008, 14/12 from 7th March 2012)

I announce the Law on Prevention of Money Laundering and Terrorist Financing, adopted by the parliament of Montenegro at the second sitting of the second regular session in 2007 , on 29th November 2007.

No. 01-1425/2

Podgorica, 14th December 2007

President of Montenegro,

Mr. Filip Vujanovic m.p.

Law on Prevention of Money Laundering and Terrorist Financing

I GENERAL PROVISIONS

Subject Matter of the Law

Article 1

This Law shall regulate measures and actions undertaken for the purpose of detecting and preventing money laundering and terrorist financing.

Money Laundering

Article 2

For the purposes of this Law, the following conduct shall be regarded as money laundering:

(a) the conversion or transfer of money or other property, knowing that they are derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or assisting any person involved in the commission of such activity to evade the legal consequences of his action;

(b) the concealment or disguise of the true nature, source, location, movement, disposition or ownership of money or other property, knowing that they are derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the actions mentioned in the points 1, 2 and 3.

Money laundering shall be regarded as such even in cases when the activities from paragraph 1 of this Article were carried out in the territory of another country

Terrorist Financing

Article 3

In the context of this Law, the following shall, in particular, be considered as terrorist financing:

1. providing or collecting or an attempt of providing or collecting money, securities, other assets or property, in any way, directly or indirectly, with the intention or in the knowledge that they will be used, in full or in part, in order to carry out a terrorist activity, and

2. encouraging or assisting in providing or collecting the funds or property from the item 1 of this Article.

Reporting entities

Article 4

Measures for detecting and preventing money laundering and terrorist financing shall be taken before, during and after the conduct of any business of receiving, investing, exchanging, keeping or other form of disposing of money or other property, or carrying out the transactions for which there is suspicion of money laundering or terrorist financing.

Measures from paragraph 1 of this Article shall be undertaken by business organizations, other legal persons, entrepreneurs and natural persons (hereinafter referred to as: reporting entities), as follows:

1) banks and foreign banks' branches and other financial institutions.

2) savings-banks, and savings and loan institutions;
3) organizations performing payment transactions,
4) post offices,
5) companies for managing investment funds and branches of foreign companies for managing investment funds;
6) companies for managing pension funds and branches of foreign companies for managing pension funds;
7) stock brokers and branches of foreign stock brokers;
8) insurance companies and branches of foreign insurance companies dealing with life assurance, insurance intermediaries and companies providing services in respect of the activities of insurance agents when they act in respect of life insurance;
9) organizers of lottery and special games of chance;
10) exchange offices;
11) pawnshops;
12) audit companies, independent auditor and legal or natural persons providing accounting and tax advice services;
13) institutions for issuing electronic money;
14) humanitarian, non-governmental and other non-profit organizations, and
15) other business organizations, legal persons, entrepreneurs and natural persons engaged in an activity or business of:

- sale and purchase of claims;
- factoring;
- third persons' property management;
- issuing and performing operations with payment and credit cards;
- financial leasing;
- travel organizing;
- investment, and agency in real estate trade;
- motor vehicles trade;
- vessels and aircrafts trade;
- sport organizations;
- safekeeping;
- issuing warranties and other guarantees;
- crediting and credit agencies;
- catering;
- granting loans and brokerage in loan negotiation affairs;
- organizing and conducting biddings, trading in works of art, precious metals and precious stones and precious metals and precious stones products, as well as other goods, when the payment is made in cash in the amount of € 15.000 or more, in one or more interconnected transactions.

By way of exception to item 2 of this Article a regulation of the Government of Montenegro (hereinafter: the Government) can define the other reporting entities that shall take the measures from item 1 of this Article if, considering the nature and manner of carrying out activities or business, there is a more significant risk of money laundering or terrorist financing, or define, in accordance with special conditions prescribe by the international standards, the reporting entities that do not need, in certain cases, to undertake the measures and actions prescribed by this Law.

Definition of Terms

Article 5

The terms used in this Law have the following meaning:

1. **''terrorist act''** shall mean an act defined by the United Nations Convention for the Suppression of the Financing of Terrorism;

2. **''terrorist''** shall mean a person who alone or with other persons:
   - intentionally, directly or indirectly, commits or attempts to commit a terrorist act;
   - encourages or assists in the commission of terrorist act;
   - intentionally or in the knowledge of the intention of a group of persons to commit a terrorist act, has contributed, or is contributing to the commission of a terrorist act;

3. **''terrorist organization''** shall mean an organized group of persons that:
   - intentionally, directly or indirectly, commits or attempts to commit a terrorist act;
   - encourages or assists in the commission of terrorist act;
   - intentionally or in the knowledge of the intention of a group of persons to commit a terrorist act, has contributed, or is contributing to the commission of a terrorist act;

   a. **''transaction''** shall mean receiving, investing, exchanging, keeping or other form of disposing of money or other property;
   b. **''risk of money laundering and terrorist financing''** shall mean the risk that a customer will use the financial system for money laundering or terrorist financing, or that a business relationship, a transaction or a product will indirectly or directly be used for money laundering or terrorist financing;

4. **''correspondent relationship''** shall mean a relationship between a domestic and a foreign credit, established by opening an account of a foreign credit or other institution with a domestic credit institution, or a contract that a domestic credit institution enters into with a foreign credit or other institution, with a view to operating business with foreign countries".
5. **''Shell bank''** shall mean a credit institution[1], or other similar institution, registered in a country in which it does not carry out activity, has no physical presence, employees, meaningful mind and management and which is not related to a financial group subject to supervision for the purpose of detecting and preventing money laundering or terrorist financing.
6. ''insurance intermediary'' means any legal or natural person- entrepreneur who, based on the license issued by the regulatory authority, is engaged into mediation affairs related to establishing connection between the insurer, or contractor of the insurance, and insurance company, for the purpose of negotiating on concluding contract on insurance, on the basis of an order of an insurance company or, or an order of an insurer, or contractor of the insurance.

---

[1] In the Montenegrin version of the existing Law on the Prevention of Money Laundering and Terrorist Financing, the words 'kreditna organizacija' (credit organization) are used. However, the equivalents in the version translated in English are 'credit institution'. Thus, this change of terms applies only to the version of the Law in Montenegrin language.

7. **"property"** means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;
8. **''business relationship''** means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this Law and which is expected, at the time when the contact is established, to have an element of duration;
9. **''Customer identification''** shall be a procedure including:

   - establishment of the identity of a customer, or if the identity has been previously established, verification of the identity on the basis of reliable, independent and objective sources, and

   - gathering data on a customer, or if data have been gathered, verifying the gathered data on the basis of reliable, independent and objective sources.

II DUTIES AND LIABILITIES OF REPORTING ENTITIES

1. Basic Duties

Article 6

This Article is deleted. (Official Gazette of Montenegro , No.14/12)

2. **Customer Identification**

Article 7

This Article is deleted. (Official Gazette of Montenegro , No.14/12)

Risk Analysis

Article 8

A reporting entity shall make risk analysis for determining the risk assessment of an individual client, a group of clients, business relationship, transaction or product related to the possibility of misusage for the purpose of money laundering or terrorist financing.

The analysis from paragraph 1 of this Article shall be prepared pursuant to the guidelines on risk analysis.

The guidelines from the paragraph 2 of this Article shall be determined by the competent supervisory bodies from the Article 86 of this Law, pursuant to the regulation adopted by the ministry that has jurisdiction over financial affairs (hereinafter: the Ministry).

The regulation from paragraph 3 of this Article shall determine more specific criteria for guidelines development (reporting entity's size and composition, scope and type of affairs, customers, or products and the like).

Cases in which CDD measures shall be conducted
Article 9

A reporting entity shall conduct the appropriate measures from Article 10 of this Law and particularly in the following cases:

1. when establishing a business relationship with a client;
2. of one or more linked transactions amounting to €15, 000 or more;
3. when there is a suspicion about the accuracy or veracity of the obtained client identification data, and
4. when there are reasonable grounds for suspicion of money laundering or terrorist financing related to the transaction or client.

If the transactions from paragraph 1 items 2 and 4 of this Article are based on an already established business relationship, a reporting entity shall:

1. verify the identity of the client that carries out the transaction and gather additional data, pursuant to this Law;
2. obtain evidence on the source of funds and check the consistence of the sources of funds with the business activity of the client, if the client is a legal person, or with the profession of the client if the client is a natural person.

An organizer of special games of chances shall in carrying out the transaction in the amount of at least € 2, 000 verify the identity of a client and obtain the data from the Article 71 item 6 of this Law.

In the context of this Law, the following shall also be considered as establishing a business relationship:

1. client registration for participating in the system of organizing games of chances at the organizers that organize games of chances on the Internet or by other telecommunication means, and
2. client's access to the rules of managing a mutual fund at managing companies.

CDD Measures undertaken by a reporting entity

Article 10

A reporting entity shall conduct CDD measures, and particularly the following:

1. to identify and verify a client and beneficial owner, if the client is a legal person;
2. to obtain data on the purpose and nature of a business relationship or transaction and other data pursuant to this Law;
3. to monitor regularly the business activities that a client undertakes with the reporting entity and verify their compliance with the nature of a business relationship and the usual scope and type of client's affairs

Customer control when establishing a business relationship
Article 11

A reporting entity shall apply the measures from Article 10 items 1 and 2 of this Law prior to establishing a business relationship.

By way of exception from paragraph 1 of this Article, a reporting entity can apply the measures from Article 10 items 1 and 2 of this Law during the establishment of a business relationship with a client when a reporting entity estimates it is necessary and when there is insignificant risk of money laundering or terrorist financing.

When concluding a life insurance contract the reporting entity from Article 4 paragraph 2 item 8 of this Law can exert control over the insurance policy beneficiary even after concluding the insurance contract, but not later than the time when the beneficiary according to the policy can exercise his/her rights.

If the evidence on the client's identity, from paragraph 3 of this Article, cannot be obtained the business relationship shall not be established, and if the business relationship has already been established it can be terminated

Control of the customer before carrying out a transaction

Article 12

When carrying out transactions from Article 9 paragraph 1 item 2 of this Law a reporting entity shall apply the measures from Article10 items 1 and 2 of this Law before executing the transaction.

If the evidence on the client's identity cannot be obtained the business relationship shall not be established and transactions shall not be executed.

Wire transfers

Article 12a

A reporting entity engaged in payment operations services or money transfer services shall obtain accurate and complete information on the originator and enter them into the form or message related to wire transfers of funds sent or received in any currency that is the subject of the wire transfer.

The data from paragraph 1 of this Article shall accompany the funds transfer through the payment chain.

A provider of payment operations or money transfer services, that is an intermediary or beneficiary person of the funds, shall refuse to transfer the funds unless the originator’s data are complete or shall require the originator’s data to be completed within the shortest time possible.

In the process of gathering the data from paragraph 1 of this Article, providers of payment operations or money transfer services shall identify the originator by checking a personal identification document issued by a competent authority.

The content and type of the data from paragraph 1 of this Article, and other obligations of the providers of payment operations or money transfer services, as well as the exceptions from data gathering requirement when transferring funds that present insignificant risk of money laundering and terrorist financing, shall be more specifically regulated by a regulation of the Ministry.

Exemption from customer due diligence in relation to certain services

Article 13

Insurance companies conducting life insurance business and business units of foreign insurance companies licensed to conduct life insurance business in Montenegro, founders, managers of pension funds, and legal and natural persons performing representation and brokerage activities in insurance, in cases of concluding life insurance contracts, are not obliged to conduct customer due diligence measures when:

1) entering into life insurance contracts where an individual installment of premium or multiple installments of premium, payable in one calendar year, do not exceed the amount of €1, 000, or where the payment of a single premium does not exceed the amount of €2, 500;

2) concluding pension insurance business providing that it is:

- insurance within which it is not possible to assign the insurance policy to a third person or to use it as security for a credit or borrowing;

- a conclusion of a collective insurance contract ensuring the right to a pension.

Domestic and foreign companies and business units of foreign companies that issue electronic money do not need to conduct customer due diligence measures when:

1. issuing electronic money, if the single maximum value issued on the electronic data carrier, upon which it is not possible to re-deposit value, does not exceed the amount of €150;
2. issuing and dealing with electronic money, if the total amount of value kept on the electronic data carrier, upon which it is possible to re-deposit value, and which in the current calendar year does not exceed the amount of €2,500, unless the holder of electronic money in the same calendar year cashes the amount of at least €1,000.

The provisions of paragraphs 1 and 2 of this Article do not apply to cases when in relation to a transaction or client there is suspicion in money laundering or terrorist financing.

2. Applying customer control measures

Establishing and verifying a natural person identity

Article 14

A reporting entity shall establish and verify the identity of a customer that is a natural person or of his/her legal representative, entrepreneurship, or a natural person performing activities, by checking the personal identification document of a customer in his/her presence and obtain data from Article 71 item 4 of this Law. In case the required data cannot be established on the basis of the submitted identification document, the missing data shall be obtained from other valid official document submitted by a customer.

Identity of a customer from paragraph 1 of this Article can be established on the basis of a qualified electronic certificate of a customer, issued by a certification service provider in accordance with the regulations on electronic signature and electronic business.

Within establishing and verifying the identity of a customer in the manner determined in paragraph 2 of this Article a reporting entity shall enter the data on a customer from the qualified electronic certificate into data records from Article 70 of this Law. The data that cannot be obtained from a qualified electronic certificate shall be obtained from the copy of the personal identification document submitted to a reporting entity by a customer in written or electronic form, and if it is not possible to obtain all required data in that manner, the missing data shall be obtained directly from the customer.

Certification service provider from paragraph 2 of this Article that has issued a qualified electronic certificate to a customer shall, upon a reporting entity's request, without delay submit the data on the manner of establishing and verifying the identity of a customer who is a holder of the qualified electronic certificate.

Establishing and verifying the identity of a customer using a qualified electronic certificate is not permitted when:

1. opening accounts at reporting entities from Article 4 paragraph 2 items 1 and 2 of this Law, except in the case of opening a temporary deposit account for paying in founding capital, and
2. there is suspicion of qualified electronic certificate misuse or when a reporting entity determines that the circumstances that have significant effect on the certification validity have changed.

If a reporting entity, when establishing and verifying the identity of a customer, doubts the accuracy of obtained data or veracity of documents and other business files from which the data have been obtained, he/she/it shall request a written statement from a customer.

Establishing and verifying the identity of a legal person

Article 15

A reporting entity shall establish and verify the identity of a customer that is a legal person and obtain the data from Article 71 item 1 of this Law by checking the original or certified copy of the document from the Central Business Register (hereinafter: CBR) or other appropriate public register, submitted by an agent on behalf of a legal person.

The document from paragraph 1 of this Article may not be older than three months of its issue date.

A reporting entity can establish and verify the identity of a legal person and obtain data from Article 71 item 1 of this Law by checking the CBR or other appropriate public register. On the register extract that has been checked a reporting entity shall state date and time and the name of the person that has made the check. An organization shall keep the excerpt from the register in accordance with law.

A reporting entity shall obtain data from Article 71 items 2, 7, 9, 10, 11, 12, 13 and 14 of this Law by checking the originals or certified copies of documents and other business files. If data cannot be determined by checking identifications and documentation, the missing data shall be obtained directly from an agent or authorized person.

A reporting entity shall keep, in its documentation, the original or verified copy of

the costumer's documents.

If , during establishing and verifying the identity of a legal person, a reporting entity doubts the accuracy of the obtained data or veracity of identification and other business files from which the data have been obtained, he/she/it shall obtain a written statement from an agent or authorized person before establishing a business relationship or executing a transaction.

If a customer is a foreign legal person performing activities in Montenegro through its business unit, a reporting entity shall establish and verify the identity of a foreign legal person and its business unit.

Establishing and verifying the identity of the agent of a legal person

Article 16

A reporting entity shall establish and verify the identity of an agent and obtain data from Article 71 item 2 of this Law by checking the personal identification document of the agent in his/her presence.

If the required data cannot be determined from the personal identification document, the missing data shall be obtained from other official document submitted by the agent or authorized person.

If a reporting entity doubts the accuracy of the obtained data when establishing and verifying the identity of an agent, he/she/it shall require agent's written statement.

Establishing and verifying the identity of an authorized person

Article 17

If an authorized person establishes a business relationship on behalf of a customer that is a legal person, a reporting entity shall establish and verify the identity of an authorized person and obtain data from Article 71 item 2 of this Law by checking the personal identification document of an authorized person and in his presence. If the required data cannot be determined from the personal identification document, the missing data shall be obtained from other official document submitted by the authorized person.

A reporting entity shall obtain data from paragraph 1 of this Article on the legal representative on whose behalf the authorized person acts, from a certified written power of authorization, issued by a legal representative.

If the transaction from Article 9 paragraph 1 item 2 of this Law is executed by an authorized person on customer's behalf, a reporting entity shall verify the identity of the authorized person and obtain data from Article 71 item 3 of this Law on a customer that is a natural person, an entrepreneur or a natural person performing a business activity.

If a reporting entity doubts the accuracy of the obtained data when establishing and verifying the identity of a legal representative that acts on behalf of a legal person, it shall obtain a legal representative's written statement thereon.

Special cases of establishing and verifying customer identity

Article 18

The customer's identity, pursuant to Article 7 of this Law, shall be established, or verified particularly in the following cases:

1. when a customer enters the premises where special games of chance are organized;
2. on any approach of a lessee or his/her agent, or a person he/she has authorized, to the safe deposit box.

When establishing and verifying the customer's identity pursuant to paragraph 1 of this Article an organizer of games of chance or a reporting entity performing the activity of safekeeping shall obtain the data from Article 71 items 6 and 8 of this Law.

3. Establishing the beneficial owner

Beneficial Owner

Article 19

Beneficial owner is the natural person who ultimately owns or controls the client and/or the natural person on whose behalf a transaction is being conducted, and as well as the person that ultimately exercises control over a legal entity or legal arrangement.

A beneficial owner of a business organization, i.e. legal person, in the context of this Law, shall be:

1) a natural person who indirectly or directly owns at least 25% of the shares, voting rights and other rights, on the basis of which he/she participates in the management, or owns at least 25% share of the capital or has a dominating influence in the assets management of the business organization;

2) a natural person that indirectly ensures or is ensuring funds to a business organization or legal entity and on that basis has the right to influence significantly the decision making process of the managing body of the business organization or legal entity when decisions concerning financing and business are made.

As a beneficial owner of a foreign legal entity (trust, fund and the like) that receives, manages or allocates assets for certain purposes, in the context of this Law, shall be considered

1) a natural person, that indirectly or directly controls at least 25% of a legal person's asset or of a similar foreign legal entity;

2) a natural person, determined or determinable as a beneficiary of at least 25% of the income from property that is being managed.

Establishment of a beneficial owner of a legal person or foreign legal entity

Article 20

A reporting entity shall be bound to establish the beneficial owner of a legal person or foreign legal person by obtaining data from Article 71 item 15 of this Law.

A reporting entity shall obtain the data from paragraph 1 of this Article by checking the original or certified copy of the documentation from the CBR or other appropriate public register that may not be older than three months of its issue date or obtain them on the basis of the CBR or other public register in accordance with Article 14 paragraphs 3 and 5 of this Law.

If the required data cannot be obtained in the manner determined in paragraphs 1 and 2 of this Article, a reporting entity shall obtain the missing data from a written statement of an agent or authorized person.

Data on beneficial owners of a legal person or similar foreign legal entity shall be verified to the extent that ensures complete and clear insight into the beneficial ownership and managing authority of a customer respecting risk-degree assessment.

4. Obtaining data on the client, business relationship, product and transaction

Article 21

Within the control of a client from Article 9 paragraph 1 item 1 of this Law, a reporting entity shall obtain data and keep records from Article 71 items 1, 2, 4, 5, 7, 8 and 15 of this Law.

Within the control of a client from Article 9 paragraph 1 item 2 of this Law, a reporting entity shall obtain data and keep records from Article 71 items 1, 2, 3, 4, 5, 9, 10, 11, 12, 13 and 15 of this Law.

Within the control of a client from Article 9 paragraph 1 items 3 and 4 of this Law, a reporting entity shall obtain data and keep records shall obtain data from Article 71 of this Law.

5. Monitoring business activities

Article 22

A reporting entity shall monitor customer's business activities, including the sources of funds the customer uses for business.

Monitoring business activities from paragraph 1 of this Article at a reporting entity shall particularly include the following:

1. verifying the compliance of customer's business with nature and purpose of contractual relationship;
2. monitoring and verifying the compliance of customer's business with usual scope of her/his affairs, and
3. monitoring and regular updating of documents and data on a customer, which includes conducting repeated annual control of a customer in the cases from Article 23 of this Law.

A reporting entity shall ensure and adjust the dynamics of undertaking measures from paragraph 1 of this Article to the risk of money laundering and terrorist financing, to which a reporting entity is exposed when performing certain work or when dealing with a customer.

Repeated annual control of a foreign legal person

Article 23

If a foreign legal person executes transactions from Article 9 paragraph 1 of this Law at a reporting entity, the reporting entity shall, in addition to monitoring business activities from Article 22 of this Law, conduct repeated annual control of a foreign legal person at least once a year, and not later than after the expiry of one year period since the last control of a customer.

By the way of exception to paragraph 1 of this Article a reporting entity shall, at least once a year, and not later than after the expiry of one year period since the last control of a customer, also conduct repeated control when the customer executing transactions from Article 9 paragraph 1 of this Law is a legal person with a

registered office in Montenegro, if the foreign capital share in that legal person is at least 25%.

Repeated annual control of a customer from paragraphs 1 and 2 of this Article shall include:

1. obtaining or verifying data on the company, address and registered office;
2. obtaining data on personal name and permanent and temporary residence of an agent;
3. obtaining data on a beneficial owner, and
4. obtaining a new power of authorization from Article 17 paragraph 2 of this Law.

If the business unit of a foreign legal person executes transactions from Article 9 paragraph 1 of this Law on behalf and for the account of a foreign legal person, a reporting entity, when conducting repeated control of a foreign legal person, in addition to data from paragraph 3 of this Article, shall also obtain:

1. data on the address and registered office of the business unit of a foreign legal person, and
2. data on personal name and permanent residence of the agent of the foreign legal person business unit .

A reporting entity shall obtain the data from paragraph 3 items 1, 2 and 3 of this Article by checking the original or certified copy of the documentation from the CBR or other appropriate public register that may not be older than three months of its issue date, or by checking the CBR or other appropriate public register. If the required data cannot be obtained by checking the documentation, the missing data shall be obtained from the original or certified copy of documents and other business files, forwarded by a legal person upon a reporting entity's request, or directly from a written statement of the agent of a legal person from paragraphs 1 and 2 of this Article.

By the way of exception to paragraphs 1, 2, 3, 4 and 5 of this Article a reporting entity shall conduct repeated control of a foreign person from Article 29 item 1 of this Law.

6. Special types of customer due diligence

Article 24

Special types of customer due diligence, in the context of this Law, shall be:

1. enhanced customer due diligence,
2. simplified customer due diligence.''

Enhanced customer due diligence

Article 25

A reporting entity shall conduct enhanced customer due diligence in cases when a reporting entity estimates that there is high risk on money laundering or terrorist financing.

Reporting entity shall conduct enhanced CDD measures in the following cases as well:

1. on entering into open account relationship with a bank or other similar credit institution, with registered office outside the EU or outside the states from the list;
2. on entering into business relationship or executing transaction from Article 9 paragraph 1 item 2 of this Law with a customer that is a politically exposed person from Article 27 of this Law,
3. when a customer is not present during the verification process of establishing and verifying the identity.

A reporting entity shall apply enhanced customer due diligence measures in cases when, in accordance with the Article 8 of this Law, a reporting entity estimates that regarding the nature of a business relationship, the form and manner of executing a transaction, business profile of the client or other circumstances related to the client, there is or there could be a high risk of money laundering or terrorist financing."

Correspondent relationships of banks with credit institutions of other countries

Article 26

When establishing a correspondent relationship with a bank or other similar credit institution that has a registered office outside the European Union or outside the states from the list, a reporting entity shall perform customer due diligence pursuant to Article 10 of this Law and obtain the following data;

1) issue date and validity of the license for providing banking services and the name and registered office of the competent state body that issued the license;
2) description of conducting internal procedures, related to detection and prevention of money laundering and terrorist financing, and in particular, client verification procedures, determining beneficial owners, reporting data on suspicious transactions and clients to competent bodies, records keeping, internal control and other procedures, that a bank or other similar credit institution has established in relation to preventing and detecting money laundering and terrorist financing;
3) description of systemic organization in the area of detecting and preventing money laundering and terrorist financing, applied in a third country, where a bank or other similar credit institution has a registered office or where it has been registered;
4) a written statement, that a bank or other similar credit institution in the state where it has a registered office or where it has been registered, under legal supervision and that, in compliance with legislation of that state, shall apply appropriate regulations in the area of detecting and preventing money laundering and terrorist financing;
5) a written statement that a bank or other similar credit institution does not operate as a shell bank;
6) a written statement that a bank or other similar credit institution has not established or it does not establish business relationships or executes transactions with shell banks.
7) a written statement that a bank or other similar credit institution has with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant data from the CDD procedure.

A reporting entity shall obtain the data from paragraph 1 of this Article from public or other available data records, or by checking documents and business files provided for by a bank or other similar credit institution that has a registered office outside the European Union or outside the states from the list.

Politically exposed persons

Article 27

A natural person that is acting or has been acting in the last year on a distinguished public position in Montenegro or in another country or on the international level, including his/her immediate family members and close associates, shall, in the context of this Law, be considered politically exposed person, as follows:

1. presidents of states, prime ministers, ministers and their deputies or assistants, heads of administration authority and authorities of local governance units, as well as their deputies or assistants and other officials;
2. elected representatives of legislative authorities;
3. holders of the highest juridical and constitutionally judicial office;
4. members of State Auditors Institution or supreme audit institutions and central banks councils;
5. consuls, ambassadors and high officers of armed forces, and
6. members of managing and supervisory bodies of enterprises with majority state ownership.

Marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters shall be deemed immediate family members of the person from paragraph 1 of this Article.

Close associates of the person from paragraph 1 shall be deemed the following:

1. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
2. any natural person who has sole beneficial ownership of a legal entity or has established business relations for the benefit of the politically exposed person.

Within enhanced customer verification from paragraph 1 of this Article, in addition to identification from Article 10 of this Law, a reporting entity shall:

1. obtain data on funds and asset sources, that are the subject of a business relationship or transaction, from personal or other documents submitted by a customer, and if the prescribed data cannot be obtained from the submitted documents, the data shall be obtained directly from a customer's written statement;

2. obtain a written consent of the person in charge before establishing business relationship with a customer, and
3. after establishing a business relationship, monitor with special attention transactions and other business activities carried out with an institution by a politically exposed person.

A reporting entity shall by an internal enactment, in accordance with the guidelines of a competent supervisory authority, determine the procedure of identifying a politically exposed person.

The list of politically exposed persons from the paragraph 1 of this Article shall be published on the website of the competent administration body.

Verifying the identity of a customer in absence

Article 28

If a client is not present during the identity verification, a reporting entity shall, within enhanced customer due diligence, in addition to the appropriate measures from Article 10 of this Law, undertake one or more additional measures, such as:

1) obtaining additional documents, data or information, on the basis of which he/she verifies client identity ;
2) verifying the submitted documents and to obtain a certificate from a financial institution or a bank performing payment operations, that the first client's payment has been made on the account held with the relevant financial institution."

New technologies
Article 28a

Banks and other financial institutions shall take measures and actions to eliminate money laundering risks that may arise from new developing technologies that might allow anonymity (internet banking, cash dispenser use, phone banking etc.).

Banks and other financial institutions shall adopt internal procedures for prevention of the new technologies use for the purpose of money laundering and terrorist financing.

Simplified customer verification
Article 29

Unless there are reasonable grounds for suspicion of money laundering or terrorist financing in relation to a customer or transaction from Article 9 paragraph 1 items 1 and 2 of this Law, a reporting entity can conduct simplified verification of a customer that is:

1. the reporting entity from Article 4 paragraph 2 items 1, 2, 4, 5, 6, 8 and 9 of this Law or other appropriate institution that has a registered office in the EU or in a state from the list of countries applying the international AML/CFT standards that are at the same level as the EU standards or higher;
2. state body or local governance body and other legal persons exercising public powers;
3. an organization whose securities are included in the trade on the organized market or stock exchange market in the EU member states or other states where the international standards that are at the same level of European Union standards or higher are applied .

The list of states from paragraph 1 of this Article shall be published on the website of the competent administration body.

Obtaining and verifying customer data
Article 30

Simplified customer verification and monitoring from Article 29 of this Law shall include obtaining data when:

1. establishing a business relationship, the data on:
   - a company and the registered office of a legal person that establishes, or on whose behalf and for whose account a business relationship is being established;
   - the personal name of an agent or authorized person that establishes a business relationship for a legal person, and
   - the purpose, nature and date of establishing a business relationship;
2. executing transactions from Article 9 paragraph 1 item 2 of this Law:
   - company and the registered office of a legal person, on whose behalf and for whose account a transaction is being conducted;
   - the personal name of an agent or authorized person conducting a transaction for a legal person;
   - date and time of executing a transaction;
   - the amount of a transaction, currency and the manner of executing a transaction, and
   - the purpose of a transaction, personal name and permanent residence, or a company and registered office of a legal person whom the transaction is intended to.

A reporting entity shall obtain data from paragraph 1 of this Article by checking the originals or certified copies of the documentation from CBR or other appropriate public register submitted by a customer or by direct check.

If the required data cannot be obtained in the manner from paragraph 2 of this Article, the missing data shall be obtained from the originals or certified copies of identification documents and other business files submitted by a customer, or from the written statement of an agent or authorized person.

Documentation from paragraphs 1, 2 and 3 of this Article may not be older than three months of its issue date.

Limitations for carrying on business with a customer

Article 31

A reporting entity may not, for a customer, open, or keep an anonymous account, a coded or bearer passbook or provide other service (banking product) that can indirectly or directly enable the concealment of a customer identity.

Prohibition of carrying on business with shell banks

Article 32

A reporting entity may not establish correspondent with a bank that operates or could operate as a shell bank or with other similar credit institution known for allowing shell banks to use its accounts.

7. Reporting obligation

Article 33

A reporting entity shall provide to the competent administration body data from Article 71 items 1, 2, 3,4, 5, 9, 10, 11 and 12 on any transaction executed in cash in the amount of at least € 15,000, immediately after, and not later than three working days since the day of execution of the transaction.

A reporting entity shall provide data from Article 71 of this Law to the competent administration body without delay when there are reasonable grounds for suspicion of money laundering or terrorist financing related to the transaction (regardless of the amount and type) or customer, before the execution of the transaction, and state the deadline within which the transaction is to be executed. The statement could also be provided via telephone, but it has to be sent to the competent administration body in a written form as well, not later than the following working day from the day of providing the statement.

A reporting entity shall provide to the competent administration body data from Article 71 of this Law after the executed transaction, when there is suspicion of money laundering or terrorist financing related to the transaction (regardless of the amount or type) or client.

Where a transaction is considered to represent money laundering or terrorist financing and when it is not possible to suspend such transaction, or when there is probability that the efforts of monitoring a client engaged into activities suspected to be related to money laundering or terrorist financing could be frustrated, reporting entities shall notify the competent administration body immediately afterwards.

The obligation from paragraph 2 of this Article shall refer to the reported transaction as well, regardless of whether it is executed later or not.

The manner and requirements of providing the data from paragraphs 1 to 5 of this Article shall be more specifically defined by the Ministry.

Unusual transactions

Article 33a

A reporting entity shall analyze all unusually large transactions which have no apparent economic or visible lawful purpose.

The findings of the analysis from paragraph 1 of this Article shall be recorded in writing by the reporting entity.

A reporting entity shall determine by an internal act its own criteria for recognizing unusual transactions.

The Guidelines on transactions that are considered as unusual shall be established by the Ministry on the basis of professional opinion of the competent administration body.

8. Applying measures of detection and prevention of money laundering and terrorist financing in business units and companies with majority ownership in foreign states

Article 34

A reporting entity shall ensure that measures of detection and prevention of money laundering and terrorist financing, defined by this Law, are applied to the same extent both in business units or companies in majority ownership of the reporting entity, whose registered offices are in other state, if that is in compliance with the legal system of the concerned state.

If the regulations of a state do not prescribe the implementation of measures of detection and prevention of money laundering or terrorist financing to the same extent defined by this Law, a reporting entity shall immediately inform the competent administration body on that and undertake measures for removing money laundering or terrorist financing risk.

9. Designating a compliance officer and his/her deputy

Performing the affairs of detecting and preventing money laundering and terrorist financing

Article 35

A reporting entity shall establish and apply appropriate rules regarding the procedures with a client, reporting, keeping of data, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

Banks, credit and other financial institutions defined by this Law shall order, conduct and supervise the application of the rules from paragraph 1 of this Article in branches and majority-owned subsidiaries in third countries.

Reporting entities that have more than three employees shall designate a compliance officer and his/her deputy for the affairs of detecting and preventing money laundering and terrorist financing.

At reporting entities' that have less than four employees the affairs of detecting and preventing money laundering and terrorist financing shall be performed by a director or other compliance officer.

If the reporting entity from Article 4 paragraph 2 of this Law does not designate a compliance officer, the authorized representative or other person managing the affairs of the reporting entities, or the reporting entity's person in charge, in accordance with the Law.

Requirements for a compliance officer

Article 36

The affairs of a compliance officer and deputy compliance officer from Article 35 of this Law can be performed by a person meeting the requirements determined by the general enactment on systematization of job positions, particularly including the following:

1. that he/she is permanently employed for carrying on affairs and tasks that are in accordance with the enactment on systematization organized in the manner ensuring fast, qualitative and timely performance of tasks defined by this Law and regulations passed on the basis of this Law;
2. that he/she has professional skills for performing affairs of preventing and detecting money laundering and terrorist financing and has professional competencies for reporting entity's operation in the areas where the risk of money laundering or terrorist financing exists, and
3. he/she has not been finally convicted of a crime act for which punishment of

imprisonment longer than six months is provided for, and which makes him/her inadequate for performing affairs of prevention of money laundering and terrorist financing.

Compliance officer's obligations

Article 37

A compliance officer from Article 35 of this Law shall perform the following affairs of:

1. taking care for establishing, functioning and developing the system of detecting and preventing money laundering and terrorist financing;
2. taking care for proper and timely data provision to the competent administration body;
3. initiating and participating in preparing and modifying operational procedures and preparing reporting entity's internal enactments related to the prevention and detection of money laundering and terrorist financing;
4. cooperating in preparation of guidelines for carrying out verifications related to the prevention of money laundering and terrorist financing;
5. monitoring and coordinating reporting entity's activity in the area of detecting and preventing money laundering and terrorist financing;
6. cooperating in establishing and developing information technology for carrying out activities of detecting and preventing money laundering and terrorist financing;
7. make initiatives and proposals to the competent administration body or managing or other body of a reporting entity for the improvement of the system for detecting and preventing money laundering and terrorist financing, and
8. preparing programs of professional training and improvement of the employed at reporting entities in the area of detecting and preventing money laundering and terrorist financing.

A compliance officer shall be directly accountable to the administration or other managing or other reporting entity's body, and functionally and organizationally shall be separated from other organizational parts of a reporting entity.

In the case of his/her absence or inability to attend to his/her duties, the compliance officer shall be substituted by the person determined by a general enactment of a reporting entity (deputy of the compliance officer).

Working conditions for a compliance officer

Article 38

A reporting entity shall provide the compliance officer particularly with the following:

1. functional connection of organizational parts with the compliance officer and to regulate the manner of cooperation between organizational units and obligations and responsibilities of the employed;

2. appropriate competencies for efficient performance of tasks from Article 38 paragraph 1 of this Law;

3. appropriate material and other conditions for work;

4. appropriate spatial and technical options ensuring an appropriate degree of protecting confidential data and information he/she manages on the basis of this Law;

5. appropriate information-technical support enabling ongoing and reliable monitoring of the activities in the area of preventing money laundering and terrorist financing;

6. regular professional improvement in relation to detecting and preventing money

laundering and terrorist financing, and

7. deputy during the absence from work.

Managing body in an organization shall provide the compliance officer with assistance and support in performing the tasks defined by this Law and inform him/her on facts significant for detecting and preventing money laundering and terrorist financing.

A reporting entity shall provide the competent administration body with data on the personal name and name of the job position of the compliance officer and the person that substitutes the compliance officer in the case of his/her absence or inability to attend to his/her duties, as well as inform the competent administration body on any change in these data, without delay, and not later than within 15 days since the day of their change.

Professional training and improvement

Article 39

A reporting entity, a lawyer, or a notary shall ensure regular professional training and improvement of employees performing affairs of detecting and preventing money laundering and terrorist financing.

A reporting entity , a lawyer, or a notary shall prepare the program of professional training and improvement of persons from paragraph 1 of this Article not later than the end of the first quarter of a business year.

10. Internal control

Article 40

A reporting entity shall ensure regular internal control of performing affairs of detecting and preventing money laundering and terrorist financing.

The method of work of compliance officer person, exercising internal control, keeping and protecting data, keeping records and the training of the employees at a reporting entity, lawyers, law offices and law firms (hereinafter: a lawyer), notaries, revision agencies, independent auditors or natural persons providing accounting or other similar services shall be specifically defined by the regulation of the Ministry.

III TASKS AND OBLIGATIONS OF LAWYERS AND NOTARIES

Tasks and obligations of lawyers and notaries

Article 41

A lawyer or a notary shall, in compliance with this Law, implement the measures of detecting and preventing money laundering and terrorist financing, when:

1. he/she assists in planning and executing transactions for a customer related to:
   - purchase or sale of real estates or a business organization,
   - managing money, securities or other property of a customer;
   - opening and managing a banking account, savings deposit or the account for dealing with securities;
   - collection of funds for founding, dealing with or managing a business organization, and
   - founding, dealing with or managing an institution, fund, business organization or other similar organization form.

2. he/she executes a financial transaction or transaction concerning real estate on behalf and for a customer.

Customer verification

Article 42

Within customer verification in the process of establishing the identity from Article 9 paragraph 1 items 1 and 2 of this Law, a lawyer or notary shall obtain data from Article 73 items 1, 2, 3, 4, 5, 6 and 11 of this Law.

Within customer verification in the process of establishing the identity from Article 9 paragraph 2 of this Law, a lawyer or notary shall obtain data from Article 73 items 1, 2, 3, 4, 7, 8, 9, 10 and 11 of this Law.

In the process of applying enhanced customer due diligence measures from Article 9 paragraph 1 items 3 and 4 of this Law a lawyer or notary shall obtain data from Article 73 items 12, 13 and 14 of this Law.

A lawyer or notary shall establish and verify the identity of a customer or his/her agent, or authorized person and obtain data from Article 73 items 1, 2 and 3 of this Law by checking the personal identification document of a customer in his/her presence, or the originals or certified copy of the documentation from the CBR or other appropriate public register, that may not be older than three months of its issue date.

A lawyer or notary shall establish the beneficial owner of a customer that is a legal person or other similar forms of organizing foreign legal persons, obtaining data from Article 73 item 4 of this Law, by checking the originals or certified copy of the documentation from the CBR or other public register, that may not be older than a month of its issue date. If the required data cannot be obtained from register, the missing data shall be obtained by checking the originals or certified copies of documents and other business documentation submitted by the agent of a legal person or other organizational form or its authorized person.

A lawyer or notary shall obtain the missing data from Article 73 of this Law by checking the originals or certified copies of documents and other business files.

If the required data cannot be obtained in the manner from paragraphs 1, 2, 3, 4, 5 and 6 of this Article, the missing data, otherwise than data from Article 73 items 12, 13 and 14 of this Law shall be obtained directly from the customer's written statement.

Reporting on customers and transactions for which there are reasons for suspicion of money laundering and terrorist financing

Article 43

If a lawyer or a notary, when performing affairs from Article 41 item 2 of this Law, establishes that there are reasonable grounds for suspicion of money laundering or terrorist financing related to a transaction or a customer, he/she shall inform the competent administration body before the execution of a transaction and in the report he/she shall state the deadline within which the transaction is to be executed. The information can be provided via telephone, but it must be sent in written form to the competent administration body not later than the following working day after the day of informing.

The obligation from paragraph 1 of this Article shall refer to planned transactions as well, regardless of whether the transaction has been executed later, or not.

If a lawyer, law office or notary in cases from items 1 and 2 of this Article cannot provide information due to the nature of transaction, due to the fact that it has not been executed or due to other justified reasons, he/she/it shall provide data to the competent administration body as soon as possible, or as soon as he/she/it finds out that there are reasonable grounds for suspicion of money laundering or terrorist financing and substantiate the reasons for not acting in the prescribed manner from paragraphs 1 and 2 of this Article.

When a customer asks for advice on money laundering or terrorist financing, a lawyer or notary shall inform the competent administration body without delay.

A notary shall, once a week, provide certified copies of the sales contracts referring to real estate trade, with the value exceeding €15,000 to the competent administration body

A lawyer, legal firm or notary shall provide data from Article 74 of this Law to the competent administration body in the manner defined by the regulation of the Ministry.

Exceptions

Article 44

By the way of exception to Article 43 paragraphs 1 and 2 of this Law, a lawyer does not need to provide the competent administration body with data he/she obtained from a customer or data on a customer when establishing his/her legal position or representing in the proceedings conducted before court, which includes providing advice on its proposing or avoiding.

Upon the competent administration body's request for providing data from Article 49 paragraphs 1 and 2 of this Law, a lawyer shall, without delay, not later than 15 days after the day of receiving the request, in written form state the reasons for which he/she did not act in accordance with the request.

A lawyer does not need to report on cash transactions from Article 33 paragraph 1 of this Law, unless there are reasonable grounds for suspicion of money laundering or terrorist financing related to a transaction or a customer.

IV LIST OF INDICATORS FOR IDENTIFYING SUSPICIOUS CUSTOMERS AND TRANSACTIONS

Applying the list of indicators

Article 45

When establishing reasonable grounds for suspicion of money laundering or terrorist financing and other circumstances related to the suspicion, a reporting entity, lawyer or notary shall use list of indicators for identifying suspicious customers and transactions.

List of indicators from paragraph 1 of this Article shall be placed in the premises of reporting entities, lawyers or notaries.

Defining the list of indicators

Article 46

The list of indicators for identifying suspicious customers and transactions shall be defined by the Ministry on the professional basis prepared by the competent administration body in cooperation with other competent bodies.

V ADMINISTRATION BODY COMPETENCIES

Affairs and tasks of the competent body

Article 47

Administration affairs related to detecting and preventing money laundering and terrorist financing defined by this Law and other regulations shall be performed by the competent administration body.

Provision of data, information and documentation to the competent administration body from paragraph 1 of this Article shall be carried out without compensation in accordance with this Law.

Data provision upon request

Article 48

The competent administration body, after estimating that there are reasonable grounds for suspicion of money laundering or terrorist financing, can request from a reporting entity to provide, in particular, the following data:

1. from the records on clients and transactions, kept on the basis of Article 70 of this Law;
2. on the state of funds and other property of a certain customer at a reporting entity;
3. on funds and asset turnover of a certain customer at a reporting entity;
4. on business relationships established with a reporting entity, and
5. information that a reporting entity has obtained or kept on the basis of law.

In the request from paragraph 1 of this Article the competent administration body shall state the data that are to be provided, legal basis, the purpose of data gathering and the deadline for their provision.

The competent administration body can also require the provision of data from paragraph 1 of this Article on the persons for whom it is possible to conclude that they have cooperated or participated in

transactions or on the business of persons for whom there are reasonable grounds for suspicion of money laundering or terrorist financing.

Upon the request of the competent administration body in cases from paragraphs 1 and 2 of this Article, a reporting entity shall provide the documentation that it keeps.

The competent administration body can require from a reporting entity to provide data, information and documentation related to performing affairs in accordance with this Law, as well as other necessary data for monitoring the fulfillment of obligations defined by this Law.

A reporting entity shall provide data, information and documentation from paragraphs 1, 2, 3, 4 and 5 of this Article to the competent administration body without delay, and not later than eight days since the day of receiving the request.

Upon the competent administration body's request for delivering data, information and documents from paragraphs 1 to 5, a reporting entity shall, in cases when the request is designated as urgent, deliver the requested data without delay, not later than 24 hours after receiving the request.

The competent administration body can, due to extensive documentation or other justified reasons, upon the reasoned request of a reporting entity, prolong the deadline from paragraph 2 of this Article or carry out data verification at a reporting entity.

Request to a lawyer or notary for submitting data on suspicious transactions or persons

Article 49

If the competent administration body estimates that there are reasonable grounds for suspicion of money laundering or terrorist financing, it can request from a lawyer or notary to provide data from Article 48 of this Law necessary for detecting money laundering or terrorist financing.

The competent administration body shall state in the request the data that are to be provided, legal basis, the purpose of data gathering and the deadline for their provision.

The competent administration body can require the provision of data from paragraph 1 of this Article on the persons for whom it is possible to conclude that they have cooperated or participated in transactions

or on business of persons for whom there are reasonable grounds for suspicion of money laundering or terrorist financing.

The competent administration body can require a lawyer or notary to provide data, information and documentation related to performing affairs in accordance with this Law, as well as other necessary data for monitoring the fulfillment of obligations defined by this Law.

Considering terms and manners of providing data from paragraphs 1, 2, 3 and 4 of this Law provisions from Article 48 paragraphs 6 and 7 of this Law shall be applied.

Request to a state authority or public powers holder for submitting data on suspicious transactions or persons

Article 50

If the competent administration body estimates that there are reasonable grounds for suspicion of money laundering or terrorist financing, it can require state authorities or public powers holders to provide data, information and documentation necessary for detecting money laundering or terrorist financing.

The competent administration body shall state in the request the data that are to be provided, legal basis, the purpose of data gathering and the deadline for their provision.

The competent administration body can also require the provision of data from paragraph 1 of this Article on the persons for whom it is possible to conclude that they have cooperated or participated in transactions or on business of persons for whom there are reasonable grounds for suspicion of money laundering or terrorist financing.

State authorities and public powers holders shall provide the requested data, information and documentation to the competent administration body without delay, and not later than eight days after the day of receiving the request, or enable, without compensation, direct electronic access to data and information stated in the request.

An order on temporary suspension of transaction

Article 51

The competent administration body may temporarily suspend transaction by written order, within 72 hours, if it evaluates that there are reasonable grounds for suspicion of money laundering or terrorism financing, and is obliged, without delay, to notify competent bodies of it.

If the deadline referred to in this paragraph occurs during non-working days, the competent state authority shall issue an order to extend such deadline for additional 48 hours.

If due to the nature of transaction or manner of executing the transaction or other circumstances, under which the transaction has been carried out, refraining from the transaction execution is impossible, an order shall be done verbally, with exemption of paragraph 1 of this Article.

Person in charge of a reporting entity should make a note on receiving verbal order from the Paragraph 1 of this article.

The competent administration body shall, without delay, provide in written form previously given verbal order.

Upon received notification of suspension of transaction, competent authorities from paragraph 1 of this Article are obliged to act urgently in accordance with their powers and within 72 hours from the beginning of the temporary suspension of transaction and shall immediately inform the competent administration body.

Termination of the measures for temporary suspension of transaction

Article 52

If the competent authority of the competent administration body, within 72 hours from the order on temporary suspension of transaction, evaluates that there is no reasonable suspicion on money laundering and terrorism financing, shall without delay inform the competent authorities and the reporting entity.

If the competent authority within 72 hours does not take measures from the Article 51 paragraph 5 of this Law, reporting entity shall immediately execute the transaction.

Request for ongoing monitoring of customer's financial operations

Article 53

The competent administration body shall request, in written form, from the reporting entity ongoing monitoring of customer's financial business, in relation to which there are reasonable grounds for suspicion of money laundering or terrorism financing, or other persons, for which may be concluded that he/she cooperated or participate in transactions or operations activity to which are grounds for reasonable suspicion of money laundering or terrorism financing are related , and shall determine deadline within which is obliged to inform and to provide required data.

Reporting entity shall provide or inform the competent administration body on data from the paragraph 1 of this Article, before carrying out the transaction or concluding the business and in report shall state deadline estimation, within which the transaction or business should be done.

If due to the nature of transaction or business or due to other justified reasons reporting entity is not able to act as it is prescribed in paragraph 2 of this Article, he/she shall forward the data to the competent administration body as soon as he/she is able to do so, but not later than next working day from the day of carrying out the transaction or concluding the business activity. The organization shall explain in the report the reasons for not acting in accordance with the provisions of paragraph 2 of this Article.

Ongoing monitoring of transactions from paragraph 1 of this Article shall not be longer than 3 months and for reasonable grounds for suspicion of money laundering and terrorism financing it shall be prolonged not later than 3 months starting from the day of submitting the request from paragraph 1 of this Article.

Collecting data upon the initiative

Article 54

If in relation to a certain transaction or a person there are reasons for suspicion of money laundering or terrorist financing, the competent administration body shall on the basis of written and grounded initiative of the Court, State Prosecutor, Police Directorate, National Security Agency, Tax Administration, Custom Directorate, Directorate for Anti Corruption and other competent state authorities, initiate the procedure for obtaining and analyzing data, information and documentation for the purpose of detecting and preventing money laundering and terrorist financing.

The written initiative from the paragraph 1 of this Article shall include the reasons for suspicion of money laundering or terrorist financing and arguments, as well as the following data:

1. name and surname, date and place of birth, permanent residence of the natural person, or the name, address and registered office for the legal person, that are related to the suspicion of money laundering or terrorist financing;
2. data on the transaction related to the suspicion of money laundering or terrorist financing (subject, amount, currency, date or period of executing the transactions or other data on transactions);

In cases the written initiative from the paragraph 1 of this Article is not argumented and does not contain the data from the paragraph 2 of this Article the competent administration body shall return such written statement to the initiator for supplementing it.

If the written statement is not supplemented within 8 days, or if it is again not argumented and contains no data from the paragraph 2 of this Article, the competent administration body shall inform the initiator, in written form, that the initiative is not valid for initiating a procedure for collecting and processing data, stating the reasons for not taking the initiative into consideration and initiating the procedure.''

Notifying on suspicious transactions

Article 55

If the competent administration body evaluates on the basis of data, information and documentation obtained in accordance with this Law, that in relation to certain transaction or certain person there are reasonable grounds for suspicion of money laundering or terrorist financing, it shall inform the competent authority in written form with necessary documentation about the reasons for suspicion.

In notification from paragraph 1 of this Article the competent administration body shall not state data on reporting entity and on person employed in the institution, that announced data unless there are reasonable grounds for suspicion that reporting entity or reporting entity's employee committed criminal act of money laundering or terrorist financing, or if those data are necessary for establishing facts in criminal proceedings and if transferring those data are required, in written form, by Court.

Information on other criminal acts

Article 56

If the Administration, on the basis of data, information and documentation, obtained in accordance with this Law, evaluates that in relation to transaction or a person there are grounds for suspicion of

committing other criminal acts that are prosecuted ex officio, shall provide, in written form, information to the competent authority.

Information Feedback

Article 57

After obtaining and analyzing data, information and documentation that are in relation to transactions or persons, for which there are reasonable grounds for suspicion of money laundering or terrorist financing or established facts, that may be connected with money laundering or terrorist financing, the competent administration body shall, in written form, give a notice to reporting entity or person that submitted the initiative, unless the competent administration body evaluates that notification may cause detrimental effects on the course and outcome of the proceeding.

International cooperation

Article 58

Before submitting personal data to the foreign competent authority for prevention of money laundering and terrorist financing, the competent administration body shall carry out a verification if the foreign competent authority to which it shall forward required data, possess arranged system for personal data protection and that used data shall be used only for required purpose, unless it is otherwise provided by the international agreement.

The competent administration body may conclude agreements on financial and intelligence data, information and documentation exchange with foreign countries competent authorities and international organizations in accordance with concluded international agreement.

Request to the competent authority of a foreign state for submitting data

Article 59

The competent administration body may request, within its jurisdiction, from the competent authority of a foreign state data, information, and documentation necessary for detection and prevention of money laundering or terrorist financing.

The competent administration body may use data, information and documentation obtained in accordance with paragraph 1 of this Article, only for purposes provided for by this Law, without previous approval of the competent authority of the foreign state from which data are obtained, may not provide or discover it to another authority, legal or natural person, or use it in purposes that are not in accordance to the conditions and limits established by commissioned competent authorities.

Providing data and information on the request of the competent authority of a foreign state

Article 60

The competent administration body can provide data, information and documentation about persons or transactions if there are reasonable grounds for suspicion of money laundering or terrorist financing on a request of competent authority of foreign state for detection and prevention of money laundering and terrorist financing, under reciprocity conditions.

The competent administration body needs not to act in accordance to the request from the paragraph 1 of this Article if :

1. on the basis of the facts and circumstances, stated in the request , evaluates that there are not enough reasons for suspicion of money laundering or terrorist financing, and,
2. providing data should jeopardize or may jeopardize the course of criminal proceeding in Montenegro or otherwise could affect interests of the proceeding.

The competent administration body shall give information in written form to the competent authority which provided request, about reasons for rejecting and shall state the reasons for rejecting.

The competent administration body may determine conditions and data usage limits from the paragraph 1 of this Article.

Self initiative data provision to the competent authority of a foreign state

Article 61

The competent administration body may self-initiatively provide data, information and documentation on a customer or transaction, for which there are reasonable grounds for suspicion of money laundering or

terrorist financing, that are obtained or processed in accordance to the provisions of this Law, and may provide data to a foreign country competent authority, under reciprocity conditions.

The competent administration body, in process of self initiative data providing may prescribe conditions and limits under which a foreign competent authority for detection and prevention of money laundering or terrorism financing, may use data from paragraph 1 of this Article.

Temporary suspension of transaction on the initiative of the competent authority of foreign state

Article 62

The competent administration body may, in accordance to this Law, under reciprocity conditions, and by reasoned written initiative of a foreign competent authority, by written order temporary suspend transaction within 72 hours.

The competent administration body is obliged to inform competent authorities about the order from the paragraph 1 of this Article.

The competent administration body may reject initiative of the competent authority of foreign state from the paragraph 1 of this Article, if based on the facts and circumstances, that are mentioned in the initiative, evaluate that given reasons are not sufficient grounds for reasonable suspicion of money laundering and terrorism financing, and shall inform in written form the authority that submitted the initiative and give the reasons for its rejection.

The initiative to a foreign competent authority for temporary suspension of transaction

Article 63

The competent administration body may, within its jurisdiction in detection and prevention money laundering and terrorist financing, submit written initiative to a foreign competent authority for temporary suspension of transaction, if evaluate that there are sufficient grounds for reasonable suspicion of money laundering or terrorist financing.

Prevention of money laundering and terrorism financing

Article 64

The competent administration body shall have the following authorities:

1. to initiate changes and amendments to regulation related to prevention of money laundering and terrorist financing;

2. to participate in consolidation of and to compile the list of indicators for identifying costumers and transactions for which there are grounds for suspicion of money laundering and terrorist financing and to submit it to persons that have duties determined by this Law;

3. to participate in training and professional improvement of reporting entity's compliance officers and competent state authorities;

3a) to publish on its website the list of countries that apply international standards in the area of preventing money laundering and terrorist financing that are at the same level as the EU standards or higher;

3b) to publish on its website the list of domestic politically exposed persons;

4. to publish on its web site the list of countries that do not apply standards in the area of detection and prevention of money laundering and terrorist financing

5. to prepare and publish recommendation or guidelines for unique implementation of this Law and regulations enacted in accordance with this Law, at the reporting entities

6. to publish statistical data related to the money laundering and terrorist financing area (the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and indicate on an annual basis the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and how much property has been frozen, seized or confiscated), at least once a year and to notify the public, in an appropriate manner, on the phenomenon of money laundering and terrorist financing.

Competent administration body is obliged upon the request of the court or state prosecutor to provide available data, information and documentation from the register of transaction and persons that are necessary for the needs of case prosecution, except the information obtained on the basis of international cooperation and for which don't have approval of the competent authority of the foreign state.

Reporting to the Government

Article 65

The competent administration body shall submit a report to the Government on its work and status, at least once a year.

VI DUTIES OF THE STATE AUTHORITIES

The administration body competent for custom affairs

Article 66

The administration body competent for custom affairs shall provide data or enable electronic access, to the competent administration body, on each money, check, bearer securities, precious metals and precious stones transport across the state border, exceeding value or amount of 10.000 € or more, within 3 days from the date of transporting.

The administration body competent for custom affairs shall provide data, from paragraph 1 of this Law, to the competent administration body on transportation or attempt of money, check, bearer securities, precious metals and precious stones transportation, in value or amount lower than 10.000€ ,if in accordance with person there are reasons for suspicion of money laundering or terrorist financing.

Exchange and clearing-deposit society

Article 67

Exchange and clearing – deposit societies shall, without delay, inform in written form the competent administration body, if during carrying out activities within the scope of its business, detect facts indicating possible connection with a money laundering or terrorist financing.

A legal persons from paragraph 1 of this article shall upon a request of the competent administration body, and in accordance with the Law, provide data, information or documentation that indicate possible connection with a money laundering or terrorist financing.

Courts, State Prosecutor and other state authorities

Article 68

For the purpose of single record keeping on money laundering and terrorist financing the Competent court, State prosecutor and other state authorities shall provide data to the competent administration body about misdemeanor and criminal offences related to money laundering and terrorist financing.

The competent state authority, from paragraph 1 of this Article, shall provide, to the competent administration body, regularly and on the request, the following information:

1. date of filing criminal charge
2. personal name, date of birth and address or company name, registered office of the company and residence of reported person
3. nature of criminal offence and place, time and manner of carrying out the activity, which has elements of a criminal offence, and
4. previous criminal offence and place, time and manner carrying out the activity, which has elements of previous criminal offence.

State prosecutor and the Competent Courts shall, at leas semiannually, provide data, to the competent administration body, referring to:

1. personal name, date of birth and address or registered office of the company, address and residence of the reported person or the person that submitted the request for court protection within misdemeanor proceeding of the Law;
2. phase of the misdemeanor proceeding and final decree;
3. legal elements of the nature of criminal offence or misdemeanor
4. personal name, date of birth and address or company name, address and residence of the person for whom is ordered temporary request for the seizure of unlawfully acquired assets or temporary confiscation.
5. date of ordering and duration of the order on temporary request for the seizure of unlawfully acquired assets or temporary confiscation;
6. the amount of the assets or property value, referring to temporary request for the seizure of unlawfully acquired assets or temporary confiscation;
7. date of issuing the order on assets and money confiscation, and
8. the amount of confiscated assets or value of the seized property

Reporting on observations and measures taken

Article 69

The Competent state authorities shall once a year, but not later than end of January of the current year for previous year, inform the competent administration body on its observation and measures taken referring to suspicious transactions on money laundering or terrorism financing, in accordance with this Law.

VII RECORDS, SAVING AND PROTECTING DATA

70. Keeping records and contents

Reporting entity's record keeping

Reporting entities shall:

1. keep records on customers, business relationships and transactions from article 9 of this law;
2. keep records from Article 33 of this Law.

Contents of reporting entity's records

Article 71

In records form Article 71 of this Law shall be kept and processed the following data:

1. name of the company, address, registered office of the company and personal identification number of the legal person, that establishes business relationship or executes transaction, or legal person for whom is established business relationship or executed transaction.
2. name, address of permanent residence or temporary residence, date and place of birth and tax ID number of a representative or an authorized person, that for a legal person or other juristic person conclude the business relationship or execute transaction, number, kind and name of the authority that issued the personal documents.
3. name, address of permanent residence or temporary residence, date and place of birth and tax ID number of an authorized person, which requires or executes transaction for a costumer, and number, kind and name of the competent body that issued the personal documents;
4. name, address of permanent residence or temporary residence, date and place of birth and tax ID number of natural person or tax ID number of its representative, entrepreneur or

natural person carrying out activities, and that establish business relation ship or execute the transaction, or natural person, for which is established business relationship or executed transaction, and number, kind and name of the competent body that issued the personal documents;

5. name, address and personal identification number , if it is assigned, of an entrepreneur or natural person carrying out business activities;
6. name, address of permanent residence or temporary residence, date and place of birth of natural person entering the casino or accessing to the safe deposit box;
7. purpose and presumed nature of business relationship, including information on customer's businesses
8. date of establishing business connections or date and time of entering the casino or accessing to safe deposit box;
9. date and time of executing transaction ;
10. the amount of transaction and foreign currency of transaction that is executed;
11. the purpose of transaction and name and address of permanent residence or temporary residence, registered office of the company and residence of the person to which transaction is intended;
12. method of executing the transaction;
13. data on assets and income sources, that are or will be the subject of transaction or business relationship;
14. reasons for suspicion of money laundering;
15. name, address of permanent residence or temporary residence, date and place of birth of the beneficiary owner- legal person or in case from the Article 19 paragraph 2 item 2 of this Law, data on the category of the person, on whose behalf is establishing and operating of the legal person or similar foreign legal person and
16. name of other juristic person and personal name, address of permanent residence or temporary residence, date and place of birth and tax ID number.

Contents of lawyer's or notary's records

Article 72

Lawyer or notary shall keep the following:

1. records on customers, business relationships and transactions from Article 9 of this Law, and
2. records on data from Article 43 paragraph 1 of this Law.

Contents of layer's or notary's records

Article 73

In records form Article 73 of this Law shall be kept and processed the following data:

1. name, address of permanent residence, date and place of birth of the entrepreneur and natural person, carrying out the business, or company name and registered office of the company and address and personal identification number of legal person or entrepreneur to whom lawyer or notary provides legal services;
2. name, address of permanent residence, date and place of birth of the agent, that establishes business relationship or executes transaction for the person from item 1 of this Article;
3. name, address of permanent residence, date and place of birth of the agent, that executes transaction for person from item 1 of this Article,
4. data from Article 72 of this Law in relation to legal person to whom lawyer or notary provides legal services;
5. purpose and presumed nature of business relationship, including information on customer's business
6. date of concluding business relationship
7. date of executing transaction
8. the amount of transaction and foreign currency of transaction that is executed
9. purpose of transaction and personal name and permanent residence or company name and residence of the person, to whom the transaction is intended
10. method of executing the transaction
11. data on assets and income sources, that are the subject of transaction or business relationship.
12. name, address of permanent residence or company name and residence of the person for which exists reasonable suspicion of money laundering and terrorist financing (amount, foreign currency or time period of executing transaction) and
13. data on transaction, for which there is reasonable ground for suspicion of money laundering or terrorist financing (amount, foreign currency or time period of executing transaction)
14. when there are reasonable grounds for suspicion of money laundering or terrorism financing.

Records kept by administrative body competent for custom services

Article 74

Administrative body competent for custom service shall keep the following records:

1. on reported and non reported transport of money, checks, securities, precious metals and precious stones across the state border, in amount and in value of 10.000€ or more, and
2. on transport or attempt of transport of money, checks, securities, precious metals and precious stones across the state border, in amount less than 10.000€, if there are reasons for suspicion of money laundering or terrorism financing.

Contents of the records of the administration body competent for customs services

Article 75

In records form Article 74 of this Law shall be kept and processed the following data:

1. name, address of permanent residence, date and place of birth and the nationality of the natural person, that transports or attempts to transport assets from Article 74 of this Law, across the state border.
2. company, address and the registered office of a legal person or personal name , address of permanent residence, nationality of the natural person, for whom the transport of assets from Article 74 of this Law across the state border is performed;
3. name, address of permanent residence and the nationality of the natural person, or company name, address and the registered office of the legal person to whom cash is provided;
4. the amount, currency and the type of cash transported across the state border;
5. source and purpose of using the cash transported across state border;
6. place, date and time of crossing or attempt of crossing the state border, and
7. reasons for suspicion of money laundering or terrorist financing

Additionally to data from paragraph 1 of this Article in the records from Article 74 item 2 of this Law, the data on whether the cash transfer has been reported to the administrative body competent for customs affairs shall also be kept.

Records kept by the competent administration body

Article 76

The competent administration body shall keep records and statistics on:

1. persons and transactions from Article 33 of this Law;
2. persons and transactions from Article 43 paragraph 1 of this Law;
3. received initiatives from Article 54 of this Law;
4. notifications and information from Articles 55 and 56 of this Law;
5. international requests from Articles 59 and 60 of this Law, and
6. criminal acts and misdemeanors from Article 68 of this Law.

Content of the records kept by the competent administration body

Article 77

In data records on persons and transactions from Article 33 of this Law data from Article 71 of this Law are kept and processed for the reasons of temporary suspension of transaction from Article 51 of this Law.

In data records on persons and transactions from Article 43 paragraph 1of this Law data from Article 71 of this Law are kept and processed for temporary suspension of transaction.

In data records from Article 76 item 3 of this Law, the following data are kept and processed:

1. name, date and place of birth, address of permanent residence, or company name, address and registered office of the person for which there are reasons for suspicion of money laundering and terrorist financing;
2. data on transaction, for which there are reasons for suspicion of money laundering or terrorist financing (amount, currency, date or period of the transaction execution);
3. reasons for suspicion of money laundering or terrorist financing

In records from Article 76 item 4 of this Law, following data are kept and processed

1. name, date and place of birth, address of permanent residence or company name and registered office of the person for which the competent administrative body forwarded notification or information.
2. data on transaction, for which there are reasons for suspicion of money laundering or terrorist financing (amount, currency, date or period of the transaction execution)
3. data on previous punishing;
4. data on the authority that received the notification or information.

In records from Article 76 item 5 of this Law, following data are kept and processed:

1. name, date and place of birth, address of permanent residence, or company, address and registered office of the person the request refers to.
2. the name of the state and requested authority, or of the authority that issued the request.

In records from Article 76 item 6 of this Law the following data are kept and processed:

1. name, date and place of birth, address of permanent residence, or company, address and registered office of the person for which data are provided out of the country;
2. the name of the state and name of the authority data are delivered to.

Content of the records on non-residents

Article 78

In data records from the Article 78 of this Law shall not be recorded data on personal identity number, tax ID number, for non residents, unless otherwise provided by this Law

Records on supervision bodies' access to data, information and documentation

Article 79

Reporting entity, lawyer or notary shall keep separate records on access of supervision bodies from Article 86 of this Law, to data, information and documentation from Article 80 of this Law.

In data records from paragraph 1 of this Article the following data are recorded:

1. name of the supervision body;
2. name of the authorized official, that checked data,
3. date and time of checking data

Reporting entity, lawyer or notary shall inform the competent authority, not later than 3 days from completed check, on any accession of supervision bodies, from Article 86of this Law , to data from paragraph 1 of this Article.

2. Data protection

Prohibition of giving information

Article 80

Reporting entitiesand reporting entity's employees, members of authorized, supervising or managing bodies, or other persons, to which data from Article 71 of this Law were available, may not reveal to a customer or third person:

1. that data, information or documentation on the customer or the transaction, from Article 33 paragraph 2, 3 and 4, Article 43 paragraph 1, Article 48 paragraph 1, 2 and 3, Article 49 paragraph 1 and 2 of this Law, are forwarded to the competent administration body ;
2. that the competent administration body on the basis of Article 51 of this Law, temporarily suspended transaction or in accordance with that gave instructions to the reporting entity;
3. that the competent administration body on the basis of Article 53 of this Law demanded regular supervision of customer's financial business;
4. that against customer or third party is initiated or should be initiated investigation for the suspicion of money laundering or terrorist financing .

An attempt to retort a client from engaging into illegal activity shall not be deemed as disclosure in the sense of paragraph 1 of this Article.

Information on facts from paragraph 1 of this Article, reports on suspicious transactions, as well as all other data, information and documentation collected by the competent administration body in accordance with this Law shall be designated the appropriate degree of confidentiality and must not be made available to third parties.

The competent administration body is not obliged to confirm or deny the existence of a confidential data.

The decision on lifting the status of confidentiality from paragraph 3 of this Article shall be made by the authorized person from the competent administration body in accordance with the Law on data secrecy.

Prohibition of giving information from paragraph 1 of this Article may not be applied on:

1. data, information and documentation, that are , in accordance with this Law obtained and kept by reporting entity, and necessary for establishing facts in criminal proceedings, and if submitting those data in written form is required or ordered by the Competent court, and
2. data from item 1 of this Article, if it is demanded by supervision body from Article 86 of this Law for the reasons of carrying out the provisions of this Law and regulations passed on the basis of this Law.

Exception to the principle of keeping confidentiality

Article 81

During the process of providing data, information and documentation to the administration, in accordance with this Law, the obligation to protect business secrecy, bank secrecy, professional and official secrecy shall not apply to reporting entitys, an organization with public authorization, state bodies, courts, lawyers or notaries and their employees.

Reporting entity, lawyer or notary and their employees shall not be liable for damage caused to their customers or third persons, if they are in accordance to this Law :

1. providing data, information and documentation on their customers, to the competent administration body
2. obtaining and processing data , information and documentation on their customers
3. carrying out the administration's order on temporary suspension of transaction, and

4. carrying out the administration's request on regular monitoring of customer's financial businesses

Reporting entity's employees, lawyers or notaries shall not be disciplinary or criminally liable for breach of obligation of keeping data secrecy, if:

1. they are providing data, information and documentation to the competent administration body, and in accordance to provisions of this Law
2. they are processing data, information and documentation, obtained in accordance to this Law, for the evaluation of customer and transaction, for which there are reasons for suspicion of money laundering and terrorism financing.

Usage of received data

Article 82

The competent administration body, state bodies and barriers of public authorities, reporting entitys or notaries and their employees are obliged to use data, information and documentation which they have received; only for the purposes they are provided for.

Keeping records

Article 83

Reporting entity shall keep records provided on the basis of Articles 9,14,15,16,17,18,19,20,21,22,23,26,27 and 30 of this Law and related documentation ten years after the termination of business relationship, executed transaction, entrance of the customer into room where special games on chance are organized or access to the safe deposit box.

Reporting entity shall keep data and supporting documents on authorized person and its deputy, professional trainings of employees and applying measures of internal control from Articles 35, 39 and 40 of this Law, for four years from dismissal of the authorized person and its deputy, or from completing professional training and internal control.

Lawyer or notary shall keep data provided on the basis of Article 42 paragraph 1 of this Law and related documentation ten years after the verification of client identity has been carried out

Lawyer or notary shall keep data and supporting documents on professional training of employees for four years after the training has been carried out.

Record keeping at the competent administration for custom services

Article 84

The competent administration for custom services shall keep data, from records from Article 75 of this Law, for 11 years from date of obtaining data and after the expiration date will be destroyed.

Record keeping in competent administration body

Article 85

The competent administration body shall keep data and information from records, kept in accordance to the provisions of this Law, for 11 years from date of obtaining and after expiration date will be destroyed.

The competent administration body shall not inform a person on information and data that it posses and which refers to that person, before the expiration of 10 years from the date of obtaining data.

The person referred to in paragraph 2 of this Article shall have the right to check its personal data after the expiration of 10 years from the date of obtaining data.

VIII SUPERVISION

Article 86

Supervision of implementation of this Law and regulations passed on the basis of this Law, within established jurisdiction, is carried out by:

1. The Central bank of Montenegro in relation to reporting entities from Article 4 paragraph 1 items 1, 2, 3,10 and 13;
2. The Agency for Telecommunication and Postal Services in relation toreporting entitys from Article 4 paragraph 1 item 4;
3. The Securities Commission in relation toreporting entitys from Article 4 paragraph 1 items 5,6 and 7;

4. The Insurance Supervision Agency in relation toreporting entitys from Article 4 paragraph 1 item 8;
5. The administration body competent for game of chance, through authorized official in accordance with the Law that defines inspection control in relation toreporting entitys from Article 4 paragraph 1 item 9;
6. The Tax authority in relation to reporting entities from Article 4 paragraph 1 item 11;
7. The Ministry competent for financial affairs in relation to reporting entitys, from Article 4 paragraph 1 item 12;

7a) Bar Association of Montenegro in relation to lawyers and law offices;

7b) Notary Chamber in relation to notaries;

8. The administration body competent for prevention of money laundering and terrorist financing through authorized official, in accordance with the Law that defines inspection control in relation toreporting entitys from Article 4 paragraph 1 items 14 and 15.

The authorities from paragraph 1 items 1-8 of this Article shall, prior to conducting the inspection, inform and consult with the competent administration body on activities of supervision they plan to carry out and, if necessary, to coordinate and harmonize its activities in performing supervision over the implementation of this Law

Article 87

If an authorized official of the competent administration body for prevention of money laundering and terrorist financing, in procedure of inspection control of thereporting entity, discover reasonable grounds for suspicion of committing criminal offence of money laundering or terrorist financing, or another criminal offence from Article 56 of this Law, can take documentation fromreporting entity and deliver it to the competent administration body

Article 88

If the competent administration body for prevention of money laundering and terrorist financing, in the procedure of processing the case, discover reasonable grounds for suspicion of committing criminal offence from Article 56 of this Law, shall provide data, information and other documentation, which implies criminal offence, to other competent bodies.

Article 89

Bodies from Article 86 of this law shall inform the competent administration body on measures taken in process of supervising in accordance with this Law, and within 8 days from the date on which the measures were taken.

The competent administration body keeps records on measures and bodies from paragraph 1 of this Article.

If the supervisory authorities from the Article 86 of this Law, during the inspection, assess that in relation to any transaction or person there is suspicion of money laundering or terrorist financing, or establish facts that can be related to money laundering or terrorist financing, shall immediately and without delay inform the competent administration body.

Article 90

On submitted request on commencing misdemeanor's procedure for the reasons of acting contrary to the propositions of this Law, the competent administrative body shall inform competent supervising body or The Bar Association in case when the request has been submitted against the lawyer.

IX MISDEMEANOR PROCEDURE

Article 91

This Article is deleted . (Official Gazette of Montenegro , No.14/12)

X PENALTY PROVISIONS

Article 92

A legal person shall be fined for misdemeanor in an amount from €2,500 to €20,000 in the following cases:

1. when it does not draft risk analysis or does not determine risk evaluation of certain groups or types of clients, business relationships, transactions or products (Article 8);

2. it does not conduct the appropriate measures from Article 10 of this Law when establishing a business relationship with a client (Article 9 paragraph 1 item 1);

3. it does not conduct the appropriate measures from Article 10 of this Law when executing one or several linked transactions in the amount of €15,000 or more (Article 9 paragraph 1 item 2);

4. it does not conduct the appropriate measures from Article 10 of this Law when the accuracy and authenticity of the obtained client identification data are doubtful (Article 9 paragraph 1 item 3);

5. it does not conduct the appropriate measures from Article 10 of this Law when there is suspicion of money laundering or terrorist financing related to a transaction or a client(Article 9 paragraph 1 item 4);

6. when it establishes a business relationship with a client without previously undertaking the prescribed measures from Article 10 paragraph 1 items 1 and 2 of this Law (Article 11 paragraph 1);

7. when it carries out the transaction without previously undertaking the prescribed measures (Article 12);

8. it does not establish and verify the identity of a natural person or their legal representative, entrepreneur or natural person that is carrying out business activities, legal person, agent of legal person, authorized person and beneficiary owner of the legal person or other foreign legal person, or does not obtain prescribed data or does not obtain them in the prescribed manner or does not provide it as it is prescribed or does not obtain a verified written copy of approval for representing (Articles 14,15,16,17 and 20);

9. it establishes and verifies client's identity by using the qualified certificate in improper way (Article 14 paragraph 5);

10. it does not establish and verify client's identity during their entrance in premises for special games of chance or during each client's approach to the safe deposit box or does not provide prescribed data or does not obtain them in the prescribed manner (Article 18);

11. does not act accordingly to the provisions of Article 21;

12. does not act accordingly to the provisions of Article 26;

13. it does not obtain data on funds and property sources, that are the subject of the business relationship or transaction, from the identification or other documents submitted by a client, and

if the required data cannot be obtained from the submitted documents, the data shall be obtained directly from the written statement of the client (Article27 paragraph 4 item 1);

14. it does not obtain a written consent of the responsible person before establishing a business relationship with a client (Article27 paragraph 4 item 2);

15. after establishing a business relationship it does not monitor carefully the transactions and other business activities carried out at the institution by a politically exposed person(Article27 paragraph 4 item 3);

16. it does not apply one or more additional measures from Article 28 of this Law within enhanced customer due diligence process;

17. it conducts simplified customer due diligence contrary to Article 29 of this Law;

18. within simplified customer due diligence it does not obtain the prescribed data on a client in the prescribed manner (Article30);

19. it opens, issues or keeps anonymous accounts, coded passbooks or passbooks on bearer for its client, or carries out other services (banking products) that directly or indirectly enable hiding client identity (Article 31);

20. it establishes, or continues correspondent relationships with a bank that carries out or could carry out business activities as a shell bank or with other similar credit institution that is known for allowing shell banks to use its accounts (Article 32);

21. it does not provide the prescribed data to the competent administration body, within the deadline defined by the Law, when there is suspicion of money laundering or terrorist financing in relation to a transaction or announced transaction or a client (Article 33);

22. it does not provide, within the prescribed deadline and in the prescribed manner, to the competent state body the required data, information and documentation, when there is suspicion of money laundering or terrorist financing in relation to a transaction or a person (Article 48);

23. it does not act accordingly to the provisions of Article 51 and Article 62 paragraph 1 of this Law;

24. it does not act upon a request of the competent administration body on current monitoring of financial business activities of a certain client (Article 53 paragraphs 1, 2 and 3).

The responsible person in a legal entity and natural person shall be fined in an amount from €300 to €2,000 for the misdemeanor from paragraph 1 of this Article.

An entrepreneur shall be fined in an amount from €500 to €6,000 for the misdemeanor from paragraph 1 of this Article.

Article 93

A legal person shall be fined in the amount from €2,500 to €15,000 for misdemeanor when it:

1. does not carry out client identification (Article10);

2. does not define, in its internal acts, the procedures of undertaking the prescribed measures (Article 10) of this Law;

3. does not obtain accurate and complete information on the originator of wire transfers and does not enter them into the form or message related to wire transfers of funds sent or received in any currency that is the subject of the wire transfer (Article 12a paragraph 1 item);

4. does not refuse to transfer the funds if the originator's data are not complete or does not require the data to be supplemented within the shortest time possible.(Article 12a paragraph 3 item).

5. does not monitor client's business activities (Article 22 paragraph 1);

6. does not carry out repeated annual control of the foreign legal person or does not obtain the prescribed data or does not obtain required data in the prescribed manner (Article 23);

7. does not define politically exposed persons identification procedures in its internal acts (Article 27 paragraph 5);

8. does not undertake measures and actions to eliminate money laundering risks that may arise from new developing technologies (Article 28a paragraph 1);

9. does not adopt internal procedures for prevention of the new technologies usage for the purpose of money laundering and terrorist financing (Article 28a paragraph 2);

10. does not provide the competent administration body, within the prescribed deadline, with the prescribed data on a transaction executed in cash and in the amount of at least €15.000 in cash (Article 33 paragraph 1);

11. does not ensure undertaking measures of detection and prevention of money laundering and terrorist financing, defined by this Law, in its business units or majority holding company, that have residence in a foreign country (Article 34 paragraph 1);

12. does not determine a compliance officer and his/her deputy for carrying out business and tasks of detecting and preventing money laundering and terrorist financing (Article 35 paragraphs 3 and 4);

13. does not provide the compliance officer with appropriate conditions from Article 38 of this Law;

14. does not keep records and documentation in accordance with Article 83 of this Law;

The responsible person in a legal entity and a natural person shall be fined in an amount from €300 to €1,000 for the misdemeanor from paragraph 1 of this Article.

An entrepreneur shall be fined in the amount from €500 to €6,000 for the misdemeanor from paragraph 1 of this Article.

Article 94

A legal person shall be fined in the amount from €1,000 to €6,000 for misdemeanor if:

1. it does not monitor client's business activities in accordance with Article 22 paragraph 2 of this Law;

2. it does not analyze all unusually large transactions that have no apparent economic or legal purpose and it does not record the results of the analysis in written form (Article 33a paragraphs 1 and 2);

3. it does not develop its internal list of criteria for recognizing unusual transactions (Article 33a paragraph 3);

4. it does not inform the competent administration body and does not undertake appropriate measures for eliminating risks of money laundering or terrorist financing (Article 34 item 2);

5. it does not ensure that the activities of an compliance officer are carried out by a person that meets the prescribed requirements (Article 36);

6. it does not deliver to the competent administration body, within the prescribed deadline, data on personal name and working position of the compliance officer and his/her deputy and information on any change of those data (Article 38 paragraph 3);

7. it does not ensure regular professional training and advanced training for employees that carry out the activities of detecting and preventing money laundering and terrorist financing pursuant to this Law (Article 39 paragraph 1);

8. it does not prepare the program for regular professional training and advanced training for detecting and preventing money laundering and terrorist financing within the prescribed deadline (Article 39 paragraph 2);

9. it does not ensure regular internal control of carrying out activities for detecting and preventing money laundering and terrorist financing pursuant to this Law (Article 40);

10. it does not use the indicator list from Article 45 paragraph 1 of this Law ,when establishing suspicion of money laundering and terrorist financing and other related circumstances;

11. it does not keep records and documentation on compliance officer and his/her deputy, advanced training of employees and undertaking measures of internal control from Articles 35, 39 and 40 of this Law, four years from discharging compliance officer and his/her deputy, completed advanced training and internal control (Article 83 paragraph 2).

The responsible person in a legal entity and a natural person shall be fined in the amount from €200 to €1,000 for misdemeanor from paragraph 1 of this Article.

An entrepreneur shall be fined in the amount from €500 to €3000 for misdemeanor from paragraph 1 of this Article.

Article 95

The person registered for qualified electronic certificate shall be fined in the amount from €3,000 to €20,000 for misdemeanor if it does not provide a copy of personal documents and other documentation

that it used for identifying and verifying client's identity upon a reporting entity's request (Article 14 paragraph 4).

The responsible person in a legal entity registered for the qualified electronic certificate shall be fined in the amount from €300 to €3,000 for the misdemeanor from paragraph 1 of this Article.

Article 96

A lawyer or notary shall be fined in the amount from €3,000 to €20,000 for misdemeanor in the following cases:

1. he/she does not act accordingly to the provisions of Article 21,

2. within client verification, he/she does not obtain all prescribed data pursuant to this Law (Article 42 paragraphs 1, 2 and 3);

3. he/she does not identify and verify client or his/her representative or authorized person or if he/she does not obtain required data in the prescribed manner (Article 42 paragraph 4, 6 and 7);

4. he/she does not inform the competent administration body, within the prescribed deadline and in the prescribed manner, that there is suspicion of money laundering and terrorist financing related to a transaction or intended transaction or certain person (Article 43 paragraph 1, 2 and 3);

5. he/she does not inform the competent administration body that a client asked for advice in relation to money laundering and terrorist financing (Article 43 paragraph 4);

6. he/she does not provide the competent administration body with certified copies of the sale contracts related to real estate trade in the amount exceeding €15 000 (Article 43 paragraph 5);

7. he/she does not inform the competent administration body on cash transactions from Article 33 paragraph 1 of this Law, when there is suspicion of money laundering or terrorist financing related to the transaction or client (Article 44 paragraph 3);

8. he/she does not appoint a compliance officer or his/her deputy for performing certain tasks of detecting and preventing money laundering or terrorist financing defined by this Law and regulations passed on the basis of this Law (Article 35 paragraphs 3 and 4 in relation to Article 41 paragraph 1);

9. he/she does not provide a compliance officer with appropriate powers, conditions and assistance for carrying out their activities and tasks (Article 38 paragraph 1 and 2 in relation to Article 41 paragraph 1);

10. he/she does not identify a beneficiary owner of a client that is a legal person or other similar form of organizing a foreign legal person, or does not obtain required data or does not obtain them in the prescribed manner (Article 42 paragraphs 5 and 7);

11. he/she does not provide the competent administration body, within the prescribed deadline and manner, with data, information and documentation from Article 49 paragraph 4 of this Law;

12. he/she does not ensure that activities of a compliance officer and his/her deputy are carried out by a person that meets the prescribed requirements (Article 36 in relation to Article 41 paragraph 1);

13. he/she does not provide the competent administration body, within the prescribed deadline, with data on personal name and job position name of the compliance officer and his/her deputy and information on any change of those data (Article 38 paragraph 3 in relation to Article 41 paragraph 1);

14. he/she does not carry out regular professional training and advanced training for employees engaged in the activities of detecting and preventing money laundering and terrorist financing pursuant to this Law (Article 39 paragraph 1 in relation to Article 41 paragraph 1);

15. he/she does not prepare program for professional training and advanced training for detecting and preventing money laundering and terrorist financing within the prescribed deadline (Article 39 paragraph 2 in relation to Article 41 paragraph 1);

16. he/she does not ensure regular internal control of the activities of detecting and preventing money laundering and terrorist financing pursuant to this Law (Article 40 in relation to Article 41 paragraph 1);

17. he/she does not provide the competent administration body with reasons for not acting in accordance with its request or does not provide them within the prescribed deadline (Article 44 paragraph 2);

18. he/she does not use the indicator list, from Article 45 paragraph 1, when establishing suspicion of money laundering and terrorist financing and other related circumstances;

19. he/she does not keep the data obtained on the basis of Article 42 paragraph 1 of this Law and related documentation for 10 years after identifying and verifying client's identity (Article 83 paragraph 3);

20. he/she does not keep data and documents on employees' advanced training for 4 years after completing the training (Article 83 paragraph 4).

Article 96a

In case of particularly serious violation or repeated violations from the Articles 92 - 96 of this Law a prohibition on performing business activities may be imposed to the legal person up to two years and a prohibition on performing business activities may be imposed to the responsible person and natural person up to two years.

XI. TRANSITIONAL AND FINAL PROVISIONS

Article 97

The regulations for implementation of this Law shall be passed within six months as of the affective date of this Law.

Until enacting regulations from paragraph 1 of this Article shall be implemented regulations enacted on the basis of the Law on the Prevention of Money Laundering ("Official Gazette of the Republic of Montenegro", No. 55/03, 58/03 and 17/05) if it is not in defiance of this Law.

Article 97a

Regulations for implementation of this Law shall be passed in the period of *six months from the date of entry into force of this Law.*

Article 97b

Reporting entities shall harmonize its business activities with the provisions of Articles 12a, 28a and 33a of this Law in the period of twelve *months from the date of entry into force of this Law* ".

Article 98

Obligors shall harmonize its business activities with the provisions of this Law within six months as of the effective date of the regulations from Article 97 of this Law.

Article 99

Procedures started in accordance with the Law on the Prevention of Money Laundering ("Official Gazette of the Republic of Montenegro", No. 55/03, 58/03 and 17/05) shall be continued in accordance with the provisions of this Law , if it is more favorable for party in misdemeanor procedure.

Article 100

On the effective date of this Law shall case to exist the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of the Republic of Montenegro", No. 55/03, 58/03 and 17/05).

Article 101

This Law shall come into effect eight days upon publishing in the "Official Gazette of Montenegro.

SU- SK No. 01-518/10

Podgorica,29th November 2007

Parliament of Montenegro,

Chairman,

Ranko Krivokapić, m.p.

C R I M I N A L   C O D E

OF MONTENEGRO

GENERAL PART

TITLE ONE
GENERAL PROVISIONS

Basis and Framework of Criminal Justice Coercion

Article 1

Protection of persons and other fundamental social values constitutes the basis and framework for defining what acts constitute statutory criminal offences, for prescribing criminal sanctions and for their application, to the extent necessary for the suppression of these offences.

Legality in Defining Statutory Criminal Offences and Prescribing Criminal Sanctions

Article 2

A punishment or other criminal sanction may only be imposed for an act which constituted a statutory criminal offence before the time of commission and for which punishment was authorized by law.

No Punishment without Guilt

Article 3

A punishment or any of the warning measures may be imposed only on a perpetrator who is guilty of having committed a criminal offence.

Criminal Sanctions and Their General Purpose

Article 4

(1) Criminal sanctions shall include the following: punishments, warning measures, security measures, and correctional measures.

(2) Criminal sanctions shall be prescribed and imposed for the general purpose of suppressing the acts which violate and threaten the values protected by criminal legislation.

TITLE TWO
CRIMINAL OFFENCE

2. Attempted Criminal Offence and Voluntary Abandonment

Attempt

Article 20

(1) Anyone who commences the commission of a criminal offence with wrongful intent but does not complete it shall be punished for attempted criminal offence punishable under law by a prison term of five years or longer, whereas other attempted criminal offences shall only be punishable where it is explicitly provided for by law that the punishment also applies to an attempt.

(2) Also considered to be the commencement of a crime is the use of a specific tool or the application of a specific method of commission provided that they are defined by law as elements of the crime.

(3) A perpetrator shall be punished for an attempt by the punishment laid down for the criminal offence, but may also receive a lighter punishment.

Inappropriate Attempt

Article 21

Where a perpetrator attempted to commit a criminal offence with an inappropriate tool or against an inappropriate object punishment may be remitted.

Voluntary Abandonment

Article 22

(1) Where a perpetrator attempted to commit a criminal offence but has voluntarily abandoned its commission punishment may be remitted.

(2) Where a perpetrator voluntarily abandoned the commission of a criminal offence, he shall receive punishment for the acts that constitute another separate criminal offence which is not covered by the criminal offence that the perpetrator abandoned.

3. Complicity in Criminal Offence

Principal and Co-principal

Article 23

(1) A principal shall be a person who commits a criminal offence himself or a person who carries out the crime through another person provided that this other person can not be considered to be the principal.

(2) Where several persons jointly take part in the commission of a crime with wrongful intent or by negligence, or where they follow their prior arrangement and jointly act with wrongful intent and thus make a significant contribution to the commission of the criminal offence, each person shall receive a punishment prescribed for the crime in question.

Instigation

Article 24

(1) Anyone who acts with wrongful intent to instigate another person to commit a criminal offence shall receive a punishment as if he committed the crime by himself.

(2) Anyone who acts with wrongful intent to instigate another person to commit a criminal offence which carries a five year prison term or a more severe punishment but does not even attempt commission shall receive the punishment laid down by law for the attempted criminal offence.

Aiding

Article 25

(1) Anyone who acts with wrongful intent to aid another in the commission of a criminal offence shall be punished as if he committed it himself, but may receive a lighter punishment.

(2) The following, in particular, shall be considered as aiding in the commission of a criminal offence: giving counsel or instructions on how to commit the crime, supplying the perpetrator with the means for commission of the crime, creating conditions or removing obstacles to the commission of crime as well as promising one prior to the commission to conceal the crime, a perpetrator, the means by which the crime was committed, any traces of the crime, or the proceeds of crime.

Limits of Liability and Punishment of Accomplices

Article 26

(1) Co-principal liability is defined by his wrongful intent or negligence, and instigator and aider liability by their wrongful intent.

(2) Where a co-principal, instigator or an aider voluntarily prevented the commission of a criminal offence, punishment may be remitted.

(3) Personal relations, capacity and circumstances for which the law excludes culpability or allows for the remission of punishment and which serve as ground to qualify an offence as serious or minor, or have an impact on the punishment imposed, may apply only to the principal, co-principal, instigator or aider with whom such relations, capacity and circumstances exist.

Punishment of Instigator and Aider for
Attempt and for Minor Criminal Offence

Article 27

(1) Where the commission remains incomplete, the instigator and aider shall receive a punishment for an attempt.

(2) Where the principal commits a minor criminal offence than the one that instigation or aiding refers to and which would have been contained in it, the instigator and aider shall receive punishment for the criminal offence committed.

(3) The provision of para. 2 hereof shall not apply if the instigator would receive a more severe punishment under Art.24, para. 2, hereof.

Special Provisions on Liability for Criminal Offences Committed through Media

Liability of Editor-in-chief

Article 28

(1) Liability for criminal offences committed through media shall be borne by the editor-in-chief or a person replacing him at the time of publication of the information provided that:

1) until the end of the main hearing before a first instance court the author remains unknown,

2) the information was published without the consent of the author,

3) at the time when the information was published there existed, and still exist, factual or legal obstacles to prosecuting the author.

(2) An editor-in-chief or a person replacing him shall not be liable if for justified reasons he had no knowledge of the circumstances referred to in para. 1, subparagraphs 1 through 3 hereof.

Liability of Publisher, Printing-entity and Producer

Article 29

(1) Provided that the requirements referred to in Art.28 above are met, liability shall be borne by the following:

1) publisher – for a criminal offence committed through regular press publications, and where the publisher does not exist or where there are factual or legal obstacles to his prosecution, then liability shall be borne by the printing-entity which had knowledge of it,

2) producer – for a criminal offence committed through a compact disc, phonograph record, magnetic tape and other audio means, film intended for public or private reproduction, slides, videos or other similar means of communication intended for wider audience.

(2) Where the publisher, printing-entity or producer is a legal person or a state authority, liability shall be borne by the officer responsible for publishing, printing or production.

Application of Provisions from Articles 28 and 29

Article 30

The provisions on liability of the persons referred to in Articles 28 and 29 hereof shall only apply where under the general provisions of this Code these respective persons may not be considered to be a perpetrator of a criminal offence.

5. Criminal Liability of Legal Persons

Article 31

(1) Criminal liability of legal persons and sanctions to be applied thereto shall be laid down by law.

TITLE THREE

PUNISHMENT

Concurrence of Criminal Offences

Article 48

(1) Where a perpetrator by one or more acts committed several criminal offences for which he is tried at the same time, the court shall first pronounce the punishment for each of the respective criminal offences, and then impose a cumulative punishment for all the offences.

(2) A cumulative punishment shall be imposed by the court subject to the following rules:

1) where for one of the concurrent criminal offences the court pronounced a forty year prison term, the court shall impose that punishment only;

2) where for concurrent criminal offences the court pronounced prison terms, the court shall increase the most severe punishment fixed, provided that the cumulative punishment is shorter than the sum of individual punishments fixed and that it does not exceed twenty year prison term;

3) where all of the respective concurrent criminal offences carry a prison term of up to three years, the cumulative punishment may not exceed ten year prison term;

4) where for concurrent criminal offences the court pronounced only fines, the court shall impose a cumulative fine which amounts to the sum of individual fines provided that it does not exceed twenty thousand euros, or a hundred thousand euros where one or more criminal offences were committed out of greed; and where the court pronounced only daily fines, they may not exceed the amount of three hundred and sixty thousand euros;

5) where for concurrent criminal offences the court pronounced community work as the only punishment, the court shall impose a cumulative punishment of community work which amounts to the

sum of hours of work to be served, provided that the punishment does not exceed three hundred and sixty hours and that the period within which the community work must be done does not exceed six months;

6) where for some concurrent criminal offences the court pronounced prison terms and fines for other concurrent criminal offences, the court shall impose a cumulative prison term and a single fine, under the provisions of subparagraphs 2 through 4 of this paragraph.

(3) The court shall impose a fine as an accessory punishment provided that it was pronounced as punishment for at least one of the concurrent criminal offences, and where the court pronounced more than one fine, it shall impose a cumulative fine under the provision of para. 2, subpara. 4 hereof.

(4) Where the court pronounced prison terms and juvenile prison terms for concurrent criminal offences, the court shall impose a cumulative prison term under the rules laid down in para. 2, subparagraph 2 hereof.

TITLE FIVE
SECURITY MEASURES

Purpose of Security Measures

Article 66

Within the general purpose of criminal sanctions (Art.4, para. 2), the purpose of security measures shall be to eliminate the situations or conditions which might influence a perpetrator to reoffend.

Types of Security Measures

Article 67

A perpetrator may receive any of the following security measures:

1) mandatory psychiatric treatment and placement in a medical institution;
2) mandatory psychiatric outpatient treatment;
3) mandatory medical treatment of drug addiction;
4) mandatory medical treatment of alcoholism;
5) disqualification from a profession, activity or duty;
6) driving prohibition;
7) confiscation of objects;
8) expulsion of a foreign national from the country;
9) publication of the judgment;
10) restraining order; and
11) eviction from home or other residence.

Imposition of Security Measures

Article 68

(1) The court may impose one or more security measures against a perpetrator provided that the requirements for their imposition as set by this Code are met.

(2) Mandatory psychiatric treatment and placement in a medical institution and mandatory psychiatric outpatient treatment are measures which are imposed as individual measures on a mentally incapacitated perpetrator. In addition to these measures, the court may order disqualification from a profession, activity or duty, driving prohibition and confiscation of objects.

(3) The measures referred to in para. 2 above may be imposed on a perpetrator whose mental capacity has been significantly diminished provided that he has already received a punishment or suspended sentence.

(4) Mandatory medical treatment of drug addiction, mandatory medical treatment of alcoholism, disqualification from a profession, activity or duty, driving prohibition, confiscation of objects and publication of the judgment may be imposed if the perpetrator has already received punishment, suspended sentence or judicial admonition or if his punishment has been remitted

(5) The measure of expulsion of a foreign national from the country may be imposed provided that the perpetrator has already received punishment or suspended sentence.

(6) Restraining order and eviction from home or other residence may be imposed on perpetrators who have received a prison term or a fine.

(7) A security measure shall be imposed for concurrent criminal offences provided that it was pronounced for at least one of the concurrent criminal offences.

Confiscation of Objects

Article 75

(1) The objects which were used or intended for use in the commission of a criminal offence or which resulted from the commission of a criminal offence may be confiscated provided that they are owned by the perpetrator.

(2) The objects referred to in para. 1 above may be confiscated even if they are not owned by the perpetrator if so required for reasons of security of people or property, or for moral reasons, but also where there is still a risk that they may be used for the commission of a criminal offence notwithstanding however the rights of third persons to claim damages from the perpetrator.

(3) Mandatory confiscation and the requirements to be met for confiscation of objects may be laid down by law.

(4) Mandatory destruction of confiscated objects may be laid down by law.

TITLE SEVEN

CONFISCATION OF PECUNIARY GAIN

Article 112

(1) No person may retain pecuniary gain[2] originating from an unlawful act which is established by law as a criminal offence.

(2) The pecuniary gain referred to in para. 1 above shall be liable to confiscation under the conditions laid down by the present Code and a court decision.

Requirements for Confiscation of Pecuniary Gain

Article 113

(1) Money, property of value and any other pecuniary gain originating from a criminal offence shall be confiscated from the perpetrator, and where such confiscation is not possible, the perpetrator shall pay the equivalent amount in money.

(2) Also liable to confiscation from the perpetrator shall be pecuniary gain for which there is reasonable suspicion to believe that it originates from criminal activity unless the perpetrator makes it probable to believe that its origin is legitimate (extended confiscation).

(3) The confiscation of pecuniary gain referred to in para. 2 above may apply if the perpetrator has been convicted under a final judgment of any of the following:

1) any of the criminal offences committed through a criminal organization (Art.401a);
2) any of the following criminal offences:
- crime against humanity and other values protected under international law and committed out of greed;
- money laundering;
- unauthorized production, possession and distribution of narcotics;
- criminal offences against payment operations and economic activity and criminal offences against official duty, which were committed out of greed, and which carry eight year prison term or a more severe punishment.

(4) Pecuniary gain shall be liable to confiscation if it was obtained in the period before and/or after the commission of any of the criminal offences under para. 3 hereof until the finality of judgment, and if the court establishes that the time when the pecuniary gain was obtained and other circumstances of the case in question justify the confiscation of the pecuniary gain.

(5) Also liable to confiscation shall be pecuniary gain originating from a criminal offence where it has been transferred to other persons free of charge or where such persons knew, could have known, or were obliged to know that the pecuniary gain originated from a criminal offence.

(6) Where pecuniary gain was obtained for another person, such gain shall also be liable to confiscation.

Protection of Injured Party

[2] *pecuniary gain* as used here refers to a gain of monetary value, i.e. anything the value of which can be expressed in money and which serves as impetus for the commission (translator's note)

Article 114

(1) Where the injured party has been awarded his claim for damages in criminal proceedings, the court shall order the confiscation of pecuniary gain only insofar as such pecuniary gain exceeds the adjudicated claim of the injured party.

(2) The injured party which has been referred by the criminal court to bringing his claim for damages in a civil action may request to be reimbursed from confiscated pecuniary gain, provided that he brings a civil claim within six months from the final decision directing him to bring a civil action and under the further condition that he claims reimbursement from the confiscated pecuniary gain within three months from the final decision awarding his claim.

(3) Any injured party who has not brought his claim for damages in the course of the criminal proceedings may request to be reimbursed from confiscated pecuniary gain provided that he instituted a civil action for the purpose of establishing his claim within three months of the date he learnt of the judgment ordering confiscation of pecuniary gain, but not later than within three years of the date of final decision ordering confiscation of pecuniary gain and provided further that he requests, within three months of the date of decision awarding his claim for damages, to be reimbursed from the confiscated pecuniary gain.

TITLE THIRTEEN
MEANING OF TERMS

Meaning of Terms Used in this Code

Article 142

(1) The territory of Montenegro shall mean land, territorial sea, and water areas within its borders, as well as air space above them.

(2) Criminal legislation of Montenegro shall mean this Code, and all other criminal provisions contained in other laws of Montenegro.

(3) A public official shall mean:

1) a person who performs official duties in a state authority;

2) an elected, appointed or designated person in a state authority, local self-government authority or a person who performs on a permanent or temporary basis official duties or official functions in these authorities;

3) a person in an institution, business organization or other entity who is delegated authority to carry out public functions, a person who decides the rights, obligations or interests of natural and legal persons or public interest;

4) and any other person performing official duties under a law, regulations adopted pursuant to laws, contracts or arbitration agreements, as well as a person who is entrusted with the performance of certain official duties or affairs;

5) a military person, with the exception of provisions of Chapter Thirty Four of this Code.

5a) a person performing in a foreign state legislative, executive, judicial or other public function for a foreign state, a person who performs official duties in a foreign country on the basis of laws, regulations adopted in accordance with a law, contract or arbitration

agreement, a person performing official duty in an international public organization and a person performing judicial, prosecutorial or other office in an international tribunal.

(4) A responsible officer is understood to mean the owner of a business organisation or other entity, or a person in a business organisation, institution or other entity who is entrusted by virtue of his function the funds invested or his authority, with a range of duties with respect to property management, production or other activity or with activities or their supervision or is tasked with the discharge of certain affairs. Also considered to be a responsible officer shall be a public official where he is designated as the principal of any of the criminal offences which are are not included in the chapter of this Code governing criminal offences against official duties, or as criminal offences against a public official.

(5) A military person is understood to mean the following: professional military person (soldiers under contract, non-commissioned officers, non-commissioned officers under contract, officers and officers under contract), members of the reserve forces (reserve soldiers, reserve non-commissioned officers and reserve officers), civilians performing a specific military duty and persons who in state of war or emergency are subject to military service.

(6) Where a public official, a responsible officer or a military person is designated as a principal of specific criminal offences, persons referred to in paras 3, 4 and 5 above may be principals of these acts unless the elements of an individual offence or an individual regulation imply that the principal may be only one of these persons.

(7) A child is understood to mean a person who has not reached the age of fourteen.

(8) A juvenile is understood to mean a person who has reached the age of fourteen, but not yet the age of eighteen.

(9) A minor is understood to mean a person who has not reached the age of eighteen.

(10) A perpetrator is understood to mean principal, co-principal, instigator and aider.

(11) A victim is understood to mean a person against whom an unlawful act was committed which constitutes a crime by law and who as a result has suffered physical or mental pain, or suffering, property damage or violation of human rights and freedoms.

(12) Pecuniary gain originating from a criminal offence is understood to mean pecuniary gain obtained directly from a criminal offence which consists in an increase or prevention of a decrease of the gain resulting from the commission of the crime, the property for which pecuniary gain obtained directly from a criminal offence is replaced or into which it is converted, as well as any other benefit obtained from the pecuniary gain directly obtained from the criminal offence irrespective of whether it is located in or outside of the territory of Montenegro.

(13) Bribe, as used in this code, is understood to mean a gift or other undue material or non-material advantage, irrespective of the value.

(14) Force is understood to mean the use of hypnosis or overpowering agents with the purpose of bringing someone against his will to the state of unconsciousness or inability to give resistance.

(15) Elections are understood to mean the elections to the Parliament of Montenegro, President of Montenegro, local self-government authorities and other elections called for and conducted on the basis of the Constitution and law.

(16) Referendum is understood to mean the expression of citizens' will whereby they decide the issues as set by the Constitution and law.

(17) Narcotic drugs are understood to mean substances and preparations declared as narcotics in accordance with regulations based on law.

(18) A movable object is understood to also mean every generated or collected energy for production of light, heat or movement, a telephone impulse, as well as a computer data and a computer program.

(19) A computer system is understood to mean every device or a group of mutually connected or conditioned devices, of which one or several, depending on the programme, perform automatic data processing.

(20) A computer data is understood to mean any presentation of facts, data or concepts in the form that is suitable for processing in a computer system, including programmes by which a computer system performs its functions.

(21) A computer programme is understood to mean a set of ordered computer data on the basis of which a computer system performs its functions.

(22) A computer virus is understood to mean a computer programme which threatens or alters the functions of a computer system and alters, jeopardizes or uses computer data without authorization.

(23) Computer traffic data are understood to mean all computer data generated by computer systems, which make a chain of communication between two computer systems that communicate, including themselves.

(24) Protected natural good is understood to also mean a good which enjoys previous protection under regulations on the protection of natural good.

(25) A cultural good is understood to also mean a good which under regulations on the protection of cultural good enjoys previous protection, as well as a part of cultural good and the protected surrounding of an immovable cultural good.

(26) Money is understood to mean both metal coins and paper banknotes or money made of some other material which by law is a legal tender in circulation in Montenegro or in a foreign country.

(27) Tokens of value are understood to also include foreign tokesn of value.

(28) A motor vehicle is understood to mean every engine powered means of transport used in road, waterborne and air transport.

(29) A document is understood to mean any object which is suitable or designated to serve as evidence of a specific fact of relevance to legal relations, as well as a computer data.

(30) A file, letter, parcel and a document may also be in an electronic form.

(31) A family or family community is understood to also mean former spouses, cousins and relations through full adoption in a direct line without limitation, and in a collateral line conclusively with the fourth degree, relatives through incomplete adoption, relatives through marriage conclusively with the second degree, persons who live in the same household and persons that parent a child or a child on the way, even where such persons have never shared a household.

(32) The expression “shall not be punished” means that there exists no criminal offence in that case.

(33) When an imperfective verb is used to define the act of a criminal offence, the offence shall be understood to have been committed provided that the act has been committed once or more times.

SPECIAL PART

TITLE FOURTEEN

CRIMINAL OFFENCES AGAINST LIFE AND LIMB

Aggravated Homicide

Article 144

Punished by a prison term of not less than ten or over forty years shall be a person who:

1) takes life of another person in a cruel or insidious manner,

2) takes life of another person behaving carelessly and violently,

3) takes life of another person and thereat acts with wrongful intent to endanger life of another person,

4) takes life of another person out of greed, in order to commit or conceal other criminal offence, out of unscrupulous revenge or other base motives,

5) takes life of a public official or military person while serving or in relation to serving an official duty,

6) takes life of a child or pregnant woman,

7) takes life of a member of his own family or a family community who he has previously abused,

8) acts with wrongful intent to take life of several persons, where such acts do not constitute manslaughter, killing a child at birth, or taking life out of mercy.

TITLE TWENTY-THREE

CRIMINAL OFFENCES AGAINST PAYMENT TRANSACTIONS

AND BUSINESS OPERATIONS

Smuggling

Article 265

(1) Anyone who takes goods across the customs line evading customs control or who by evading customs control takes goods across customs line armed, in a group or using force or threats shall be punished by a prison term from six months to five years and by a fine.

(2) Whoever, by avoiding customs control, transfers across the customs line a large quantity of weapons or ammunition or weapons the possession of which is prohibited to citizens or other goods the production or trade of which is restricted or prohibited shall be punished by a prison term from one to eight years and by a fine.

(3) Anyone who sells, distributes or conceals uncleared goods or organizes a network of dealers or middlemen for distribution of such goods shall be punished by a prison term from one to eight years and by a fine.

(4) The goods which are the object of the offences under paragraphs 1, 2 and 3 above shall be confiscated.

(5) A vehicle with hidden compartments which was used for the transport of the goods which represent the object of the offences under para. 1 above or intended for commission of these criminal offences may be confiscated when the owner or user of vehicle knew, could have known or should have known thereof, or when the value of the goods which are the object of the criminal offence exceeds one third of the value of the means of transport at the time of commission of the criminal offence.

Money Laundering

Article 268

(1) Anyone who converts or transfers money or other property knowing that they are derived from criminal activity for the purpose of concealing or disguising the origin of the money or other property or who acquires, possesses or uses money or other property knowing at the time of receipt that they are derived from criminal activity, or who conceals or misrepresents the facts on the nature, origin, place of deposit, movement, disposal or ownership of money or of other property knowing they are derived from criminal activity shall be punished by a prison term from six months to five years.

(2) The punishment under para. 1 above shall apply to the principal of the offence under para. 1 above if he was at the same time the principal or the accomplice in the commission of the criminal offence by which the money or property referred to in para. 1 above was acquired.

(3) Where the amount of money or value of the property referred to in paras 1 and 2 above exceed forty thousand euros, the perpetrator shall be punished by a prison term from one to ten years.

(4) Where the offences under paras 1 and 2 above were committed by several persons who associated for the purpose of committing such offences, they shall be punished by prison term from three to twelve years.

(5) Anyone who commits the offence under paras 1 and 2 above and could have known or should have known that the money or property was derived from criminal activity shall be punished by a prison term up to three years.

(6) The money and property referred to in paras 1, 2 and 3 above shall be confiscated.

Misuse of insider information

Article 281

(1) Anyone who with the intent to obtain for himself or another pecuniary gain or cause damage to another reveals or otherwise makes accessible insider information to an unauthorised person or who by using insider information buys or sells for himself or another directly or indirectly securities or other financial instruments that the insider information relates to, or who recommends to another or induces another to buy or sell securities or other financial instrument that the insider information relates to shall be punished by a fine or a prison term up to three years.

(2) The punishment under paragraph 1 above shall also apply to an unauthorised person for using the information obtained in the manner described in paragraph 1 above.

(3) Where the offence referred to in paragraph 1 above was committed by a person who is a member of the board of directors or of supervisory board of the issuance authority or a person who has a share in its capital, such person shall be punished by a prison term from six months to five years.

(4) Where the offence under paragraphs 1, 2 and 3 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from one to eight years.

(5) Where the offence under paragraphs 1, 2 and 3 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to ten years.

(6) An attempted offence under paragraph 1 shall be subject to punishment.

Manipulation in the stock market and market in other financial instruments

Article 281a

(1) Anyone who with the intention to obtain for himself or another pecuniary gain or cause harm to another acts in violation of the regulations governing stock market by taking any of the following actions:

1) effects any transaction or enters an order for a transaction which creates or may create a false or misleading appearance with respect to the supply, demand or the price of securities or other financial instruments, or by which either alone or with one or more other persons one fixes the price levels for one or more securities or for other financial instruments at an unrealistic level;
2) when effecting or entering an order for a transaction, fixes, raises, depresses, or causes volatility of market prices for securities and other financial instruments by the use of purchase or sale or by effecting a fictitious transaction which involves no change in the beneficial ownership of such security or other financial instrument;
3) disseminates or circulates, by the use of media, internet or otherwise, false or misleading information that is likely to create a misleading appearance with respect to the securities or other financial instruments knowing that such information is false or misleading and that it may mislead the party using such information, shall be punished by a prison term from six months to five years and by a fine.

(2) Where the offence under paragraph 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to ten years and by a fine.

TITLE TWENTY-FIVE

CRIMINAL OFFENCES AGAINST ENVIRONMENT AND SPATIAL PLANNING

Taking hazardous substances

in and out of the country

Article 313

1) Anyone who in breach of the regulations exports, to takes abroad, or imports, or takes into Montenegro nuclear or radioactive material or other hazardous matter or hazardous waste, or anyone who transports such substances across the territory of Montenegro shall be punished by a prison term up to three years.
2) Anyone who allows or enables other by misusing his office or authority to export or take abroad or import or take into Montenegro the substances, material, or waste referred to in paragraph 1 above, shall be punished by a prison term from six months to five years.
3) Where the offences under paragraphs 1 and 2 above resulted in serious harm to the quality of air, water or soil or in extinction or serious harm or flora or fauna, the perpetrator shall be punished by a prison term from one to eight years.
4) Where the offences under paragraphs 1 and 2 above resulted in a serious bodily injury or serious harm to health of one or more persons, the perpetrator shall be punished by a prison term from two to ten years.
5) Where the offences under paragraphs 1 and 2 above resulted in the death of one or more individuals, the perpetrator shall be punished by a prison term from three to twelve years.
6) An attempt of the offence under paragraph 1 shall be subject to punishment.

Unlawful use, production, processing, possession, disposal, and storage

of hazardous substances

Article 314

(1) Anyone who in breach of regulations uses, produces, processes, possesses, disposes, collects, stores or dispatches nuclear or radioactive substances or other hazardous substances or hazardous waste shall be punished by a prison term up to three years.

(2) Anyone who, by misuse of his office or authority, allows or enables the use, production, processing, possession, disposal, collection, storage or dispatch of substances, material or waste referred to in paragraph 1 above shall be punished by a prison term from six months to five years.

(3) Where the offence in paragraphs 1 and 2 above resulted in serious harm to air, water, and soil quality or in extinction or serious harm to flora and fauna, the perpetrator shall be punished by a prison term from one to eight years.

(4) Where the offences under paragraphs 1 and 2 above resulted in a serious bodily injury or serious harm to health of one or more persons, the perpetrator shall be punished by a prison term from two to ten years.

(5) Where the offences under paragraphs 1 and 2 above resulted in the death of one or more persons, the perpetrator shall be punished by a prison term from three to twelve years.

(6) An attempted offence under paragraph 1 shall be subject to punishment.

(7) Where a suspended sentence is imposed for the offences under paragraphs 1 to 4 above, the court may order the perpetrator to take the measures prescribed for the protection, preservation and improvement of the environment.

TITLE TWENTY-SIX

CRIMINAL OFFENCES AGAINST GENERAL SAFETY OF PEOPLE AND PROPERTY

Endangering Safety with Nuclear Substances

Article 337

(1) Anyone who threats to use a nuclear material to endanger the safety of humans shall be punished by a prison term from six months to five years.

(2) Where the offence under para. 1 above was committed with the intention to force another person to act or refrain from acting, the perpetrator shall be punished by a prison term from one to eight years.

(3) Where a perpetrator of the offences under paras 1 and 2 above realized his threat thus inflicting a serious bodily injury causing damage to a property exceeding forty thousand euros, the perpetrator shall be punished by a prison term from two to ten years.

(4) Where a perpetrator of the offences under paras 1 and 2 above realized his threat thus causing the death of one or more persons, the perpetrator shall be punished by a prison term from three to fifteen years.

Endangering Security of Air and Maritime Traffic or of Fixed Platform

Article 342

(1) Anyone who uses violence against persons on an aircraft, ship or fixed platform in the epicontinental shelf, or who endangers the security of air traffic, maritime navigation or a fixed platform by setting up or bringing into an aircraft, ship or fixed platform explosive or other dangerous devices or substances, or who destroys, damages or interferes with navigation devices or causes other damage to the aircraft, ship or fixed platform shall be punished by a prison term from two to ten years.

(2) Where the offence under para. 1 above results in serious bodily injury on another person or a damage exceeding forty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years.

(3) Where the offence under para. 1 above results in the death of one or more persons, the perpetrator shall be punished by a prison term from five to fifteen years.

Hijack of Aircraft, Ship or Other Means of Transport

Article 343

(1) Anyone who uses force or threats of using force to take over the control of an aircraft during flight or of a ship or other means of public transport while in motion shall be punished by a prison term from two to ten years.

(2) Anyone who commits the offence under para. 1 above against a fixed platform in the epicontinental shelf shall be punished by a prison term from one to eight years.

(3) Where the offence under paras 1 and 2 above resulted in a serious bodily injury of another person or damage exceeding forty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years.

(4) Where the offence under paras 1 and 2 above resulted in the death of one or more persons, the perpetrator shall be punished by a prison term from five to fifteen years.

TITLE THIRTY-ONE

CRIMINAL OFFENCES AGAINST JUDICIARY

Assistance to Perpetrator after Commission of Criminal Offence

Article 387

(1) Anyone who conceals a perpetrator or assists a perpetrator by hiding the means or traces of a criminal offence, or otherwise assists him to avoid detection, and who conceals a convicted person or takes any other measures with the intention to avoid the enforcement of an imposed

punishment, a security measure, or placement with a community-based correctional institution or correctional home shall be punished by a fine or a prison term up to two years.

(2) Anyone who assists a perpetrator of an offence punishable under law by a prison term exceeding five years shall be punished by a prison term from three months to five years.

(3) Anyone who assists a perpetrator of an offence punishable under law by a forty year prison term shall be punished by a prison term from one to eight years.

(4) The punishment imposed for the criminal offence under para. 1 above shall not be more severe in terms of its type or duration than the punishment prescribed for the criminal offence committed by the person who has been provided assistance.

(5) The punishment for the offences under paras 1 to 3 above shall not apply to the persons to whom the perpetrator is a spouse or a partner in a durable customary marriage, direct blood relative, brother or sister, adoptive parent or adopted child, or a spouse to one of the above mentioned persons, or a person living with one of such persons in a durable customary marriage.

TITLE THIRTY-TWO

CRIMINAL OFFENCES AGAINST PUBLIC LAW AND ORDER

Conspiracy to Commit a Crime

Article 400

Anyone who conspires with another to commit a criminal offence punishable by a prison term of five years or longer shall be punished by a fine or a prison term up to one year.

Criminal Association

Article 401

(1) Anyone who organizes a group or other association with a view to commit criminal offences punishable by a prison term of one year or longer shall be punished by a prison term up to three years.

(2) Where the offence under para. 1 above refers to an association that aims to commit criminal offences punishable by a prison term of five years or longer, the mastermind of the association shall be punished by a prison term from one to eight years, and a member of the association by a prison term up to two years.

(3) Where the offence under para. 1 above refers to an association that aims to commit criminal offences punishable by a fifteen year prison term, the mastermind of the association shall be punished by a prison term from two to twelve years, and a member of the association by a prison term up to three years.

(4) Where the offence under para. 1 above refers to an association that aims to commit criminal offences punishable by a twenty year prison term or a forty year prison term, the mastermind of the association shall be punished by a prison term not shorter than ten years or a thirty year prison term, and a member of the association by a prison term from six months to five years.

(5) The mastermind of the association referred to in paras 1 to 4 above who reveals the association or otherwise prevents the commission of criminal offences for which the association was founded shall be punished by a prison term up to three years, and his punishment may also be remitted.

(6) Punishment may also be remitted where a member of the association referred to in paras 2, 3 and 4 above reveals the association and contributes to its revelation.

(7) The organizer and a member of the association who commits a criminal offence as a member of association shall be punished for that criminal offence as well.

Establishment of Criminal Organization

Article 401a

(1) Whoever organizes a criminal organization aimed at committing criminal offences punishable by law by a prison term of four years or a more severe punishment shall be punished by a prison term from three to fifteen years.

(2) A member of the criminal organization referred to in para. 1 above shall be punished by a prison term from one to eight years.

(3) The mastermind of a criminal organization who prevents the commission of criminal offences for the purpose of which the organization was created by revealing the criminal organization or otherwise shall be punished by a prison term from three months to three years and his punishment may also be remitted.

(4) A member of a criminal organization who reveals the criminal organization or contributes to it being revealed shall be punished by a prison term up to one year, and his punishment may also be remitted.

(5) The mastermind and a member of a criminal organization who commits a criminal offence as a member of criminal organization shall be punished for that offence as well.

(6) The criminal organization referred to in para. 1 above shall be considered to include the organization composed of three or more persons which has as its objective the commission of criminal offences punishable by law by a four year prison term or a more severe punishment for the purpose of obtaining unlawful gain or power, provided that minimum three of the following conditions are met:

1) that each member of the criminal organization had a predefined or obviously definable task or role;

2) that activities of the criminal organization have been planned for a longer period of time or for an unlimited period;

3) that the activities of the criminal organization are based on the application of certain rules of internal control and member discipline;

4) that the activities of the criminal organization are planned and implemented in international proportions;

5) that activities of the criminal organization include the application of violence or intimidation or that there is readiness for their application;

6) that activities of the criminal organization include the use of economic or business structures;

7) that activities of the criminal organization include laundering of money or illicit proceeds or

8) that there is an influence of the criminal organization or its part upon the political authority, media, legislative, executive or judicial powers or other important social or economic factors.

TITLE THIRTY-FIVE

CRIMINAL OFFENCES AGAINST HUMANITY AND OTHER VALUES GUARANTEED BY INTERNATIONAL LAW

Terrorism

Article 447

(1) Anyone who, with the intention to seriously intimidate the citizens or to coerce Montenegro, a foreign state or an international organization to act or refrain from acting, or to seriously endanger or violate the basic constitutional, political, economic or social structures of Montenegro, foreign state or of international organization, commits any of the following offences:

1) attack on the life, body or freedom of another,

2) abduction or hostage taking,

3) destruction of state or public facilities, traffic systems, infrastructure, including information systems, fixed platforms in the epicontinental shelf, public good or private property that may endanger the lives of people or cause considerable damage to the economy,

4) hijack of aircraft, vessel, means of public transport or transport of goods that may endanger the lives of people,

5) development, possession, procurement, transport, provision or use of weapons, explosives, nuclear or radioactive material or devices, nuclear, biological or chemical weapons,

6) research and development of nuclear, biological and chemical weapons,

7) emission of dangerous substances or causing fires, explosions or floods or taking other generally dangerous actions that might harm the lives of people,

8) obstruction or termination of water supply, electric energy or another energy generating product supply that might endanger the lives of people shall be punished by a prison term not shorter than five years.

(2) Anyone who threatens to commit the criminal offence under para. 1 above shall be punished by a prison term from six months to five years.

(3) Where the offence under para. 1 above resulted in the death of one or more persons or a large-scale destruction, the perpetrator shall be punished by a prison term not shorter than ten years.

(4) Where during the commission of the offence under para. 1 above the perpetrator killed one or several persons with wrongful intent, he shall be punished by a prison term not shorter than twelve years or by a forty year prison term.

Public Call for the Commission of Terrorist Acts

Article 447a

Anyone who publicly calls for or otherwise instigates the commission of the criminal offence under Art.447 hereof shall be punished by a prison term from one to ten years.

Recruitment and Training for Commission of Terrorist Acts

Article 447b

(1) Anyone who for the purpose of committing the offences under Art.447 hereof recruits another person to commit or participate in the commission of that offence or to join a group of people or a criminal association or criminal organization in view of participating in the commission of that criminal offence shall be punished by a prison term from one to ten years.

(2) The punishment under para. 1 above shall also apply to anyone who, with the intention to commit the criminal offence under Art.447 hereof, gives instructions on the manufacture and use of explosive devices, firearms or other weapons or harmful or dangerous substances or who trains another person for the commission of or participation in the commission of that criminal offence.

Use of Lethal Device

Article 447c

(1) Anyone who, with the intention to kill another person, inflict a serious bodily injury, or destroy or significantly damage a state or public facility, public traffic system or another facility of great significance for the security or supply of citizens, or for the economy or operation of public services, manufactures, transfers, keeps, gives to another, sets up or activates a lethal device

(explosive, chemical devices, biological devices or poisons or radioactive material) in a public location or in a facility or next to that facility shall be punished by a prison term from one to eight years.

(2) Where in the commission of any of the offences under para. 1 above the perpetrator inflicted with wrongful intent a serious bodily injury to another person or destroyed or significantly damaged a facility, he shall be punished by a prison term from five to fifteen years.

(3) Where in the commission of any of the offences under para. 1 above the perpetrator killed with wrongful intent one or more persons, he shall be punished by a prison term not shorter than ten years or by a forty year prison term.

Destruction or Damage of Nuclear Facility

Article 447d

(1) Anyone who, with the intention to kill another person, inflict a serious bodily injury, endanger the environment or cause significant property damage, destroys or damages a nuclear facility in a manner which results or could result in the emission of radioactive material shall be punished by a prison term from two to ten years.

(2) Where in the commission of any of the offences under para. 1 above the perpetrator inflicted with wrongful intent a serious bodily injury to another person or destroyed or significantly damaged a nuclear facility, he shall be punished by a prison term from five to fifteen years.

(3) Where in the commission of any of the offences under para. 1 above the perpetrator killed with wrongful intent one or more persons, he shall be punished by a prison term not shorter than ten years or by a forty year prison term.

Endangering Persons under International Protection

Article 448

(1) Anyone who commits abduction or other type of violence against a person under international legal protection shall be punished by a prison term from two to twelve years.

(2) Anyone who attacks the official premises, private apartment or vehicle of a person under international legal protection in a manner that endangers his safety and personal freedom shall be punished by a prison term from one to eight years.

(3) Where the offences under paras 1 and 2 above resulted in the death of one or more persons, the perpetrator shall be punished by a prison term from five to fifteen years.

(4) Where in the course of commission of the offences under paras 1 and 2 above the perpetrator killed another person with wrongful intent, he shall be punished by a prison term not shorter than ten years or by a forty year prison term.

(5) Anyone who endangers the safety of the person referred to in para. 1 above by a serious threat to attack him, his official premises, private apartment or a vehicle shall be punished by a prison term from six months to five years.

Terrorism Financing

Article 449

(1) Anyone who procures in any manner or raises funds for the purpose of using them partly or wholly to finance criminal offences under Articles 447, 447a, 447b, 447c, 447d and 448 hereof, or to finance organizations which have set the commission of these offences as their aim, or the members of such organizations or an individual whose aim is to commit such offences shall be punished by a prison term from one to ten years.

(2) The funds referred to in paragraph 1 above shall be understood to mean all funds, material or non-material, movable or immovable, irrespective of the way in which they were obtained or the form of the document or certificate, including electronic or digital forms, by which one proves ownership or a share in such funds, including bank loans, travellers cheques, securities, letters of credit and other funds.

(3) The funds referred to in paragraph 1 above shall be confiscated.

Terrorist Association

Article 449a

(1) Where two or more persons mutually associate for a longer period to commit the criminal offences under Articles 447, 447a, 447b, 447c, 447d, 448 and 449 hereof, they shall be punished by the punishment prescribed for the offence for the exercise of which the association has been organized.

(2) The perpetrator of the offence under para. 1 above prevents the commission of the criminal offences under para. 1 above by revealing the association or otherwise, or who contributes to its revelation shall be punished by a prison term up to three years, and his punishment may be remitted.

THE CRIMINAL PROCEDURE CODE

(Official Gazette of Montenegro, no. 57/09, 49/10)

Part one

GENERAL PROVISIONS

Chapter I
BASIC RULES

Scope and Objective of the Code
Article 1

The present Code sets forth the rules with the objective to enable a fair conduct of the criminal proceedings and ensure that no innocent person be convicted and that a criminal sanction be imposed on a criminal offender under the conditions provided for in the Criminal Code and on the basis of legally conducted proceedings.

Principle of Legality
Article 2

(1) A criminal sanction may be imposed on the perpetrator only by the competent Court in the proceedings initiated and conducted in compliance with the present Code.
(2) Freedom and other rights of the accused person may be limited prior to the rendering of the final judgment, only under the conditions set forth in the present Code.

Presumption of Innocence and *in dubio pro reo*
Article 3

(1) A person shall be considered innocent of a crime until his/her guilt has been established by the final judgment.
(2) Public authorities, media, associations of citizens, public figures and other persons shall respect the rule referred to in paragraph 1 of the present Article and shall not violate other procedural rules, rights of the accused person and the injured party and the principle of independence of judiciary by their public statements regarding the criminal proceedings that is in progress.
(3) The court shall render a decision that is more favourable for the accused person if once all available evidence are provided and presented in the criminal proceedings, only a suspicion remains with respect to the existence of a significant feature of a criminal offence or as regards facts on which depends an application of a provision of the Criminal Code or the present Code.

::::

Definition of Terms
Article 22

Certain terms used in the present Code shall have the following meaning:

1) *suspects* are persons against whom the competent public authority has undertaken an action because there are grounds for suspicion that they had committed a criminal offence, but order for initiation of investigation has not yet been issued or a direct indictment has not been filed against them;

2) *accused persons* are persons against whom an order on the conduct of investigation, indictment, bill of indictment or private action was issued or person against whom a special procedure was initiated for the enforcement of security measures of mandatory psychiatric treatment and confinement in a medical institution and mandatory psychiatric treatment while at freedom; the term accused person may be used in the criminal proceedings as a general term for the accused, defendant and convicted person;

3) *defendants* are persons against whom the indictment has entered into force;

4) *convicted* persons are persons whose criminal liablility for a particular criminal offence was established by a final verdict or a final ruling on punishment;

5) *injured parties* are persons whose personal or property right of some type was violated or endangered by a criminal offence;

6) *prosecutors* are State Prosecutors, private prosecutors and subsidiary prosecutors;

7) *parties* are the prosecutor and the accused person;

8) *organized crime* implies the existence of grounds for suspicion that a criminal offence punishable under law by an imprisonment sentence of four years or a more severe sentence is a result of the action of three or more persons joined into a criminal organization, i.e. criminal group, acting with the aim of committing serious criminal offences in order to obtain illegal proceeds or power, in case when at least three of the following conditions have been met:

a) that every member of the criminal organization, i.e. criminal group has had an assignment or a role defined in advance or obviously definable;

b) that actions of the criminal organization, i. e. criminal group have been planned for a longer period of time or for an unlimited period;

c) that activities of the criminal organization, i. e. group have been based on the implementation of certain rules of internal control and discipline of its members;

d) that activities of the criminal organization, i.e. criminal group have been planned and performed in international proportions;

e) that activities of the criminal organization, i.e. criminal group include the application of violence or intimidation or that there is readiness for their application;

f) that activities of the criminal organization, i.e. criminal group include economic or business structures;

f) that activities of the criminal organization, i.e. criminal group include the use of money laundering or unlawfully acquired gain;

i) that there is an influence of the criminal organization, i.e. criminal group or its part upon the political authorities, media, legislative, executive or judiciary authorities or other important social or economic factors.

::::

1. PROVISIONAL SEIZURE OF OBJECTS, PROPERTY GAIN AND PROPERTY

Provisional Seizure of Objects and Property Gain

Article 85

(1) Objects which have to be seized according to the Criminal Code or which may be used as evidence in the criminal procedure, shall, at the proposal of a State Prosecutor**,** and by way of a court ruling, be provisionally seized and delivered for safekeeping to the court or their safekeeping shall be secured in another way.

(2) The ruling on the provisional seizure of objects shall contain:

1) the name of the court rendering the ruling,

2) legal grounds for the seizure of objects,

3) indication and description of objects that are to be provisionally seized, and

4) the first and the last name of the person from whom the object is provisionally seized and the place at or in which a certain object should be provisionally seized.

(3) Anyone who is in possession of objects referred to in paragraph 1 of this Article shall hand them over. Persons refusing to hand over the objects may be punished by a fine of up to €1.000, and in case of further rejection, they may be detained. Detention shall last until the object is handed over or until the criminal procedure is completed, and at the longest for two months. The procedure as regards a person in an official capacity or a responsible person in a public authority, enterprise or another legal entity shall be the same.
(4) Provisions of paras. 1 and 3 of this Article shall be applied to the data saved in devices for automatic or electronic data processing and media wherein such data are saved, which shall, upon the request of the court, be handed over in a legible and comprehensible form. The court and other authorities shall abide by the regulations on maintaining data secrecy.
(5) The following objects cannot be provisionally seized:

1) papers and other documents of public authorities, publication of which would violate the obligation to keep data secret in terms of regulations laying down data secrecy, until the competent authority decides otherwise;

2) the accused persons' letters to their defense attorney or the persons referred to in Article 109, paragraph 1, items 1, 2 and 3 of the present Code unless the accused decide to hand them over voluntarily;

3) recordings, extracts from the register and similar documents that are in possession of persons referred to in Article 108, item 3 of the present Code and that are made by such persons in relation to the facts obtained from the accused person while performing their professional service, if publication thereof would constitute violation of the obligation to keep a professional secret.

(6) The prohibition referred to in paragraph 5, item 2 of this Article shall not apply to the defense attorney or persons exempted from the duty to testify pursuant to Article 109, paragraph 1 of the present Code if reasonable doubt exists that they aided the accused parties in committing the criminal offence or they helped them after the criminal offence was committed or if they acted as accomplices by virtue of concealment.
(7) The ruling referred to in paragraph 3 of this Article shall be made by the investigative judge during the investigation and by the Chair of the Panel after an indictment has been brought.
(8) The panel referred to in Article 24, paragraph 7 of the present Code shall decide on the appeal against a ruling referred to in paras. 2 and 3 of this Article. An appeal against the ruling on imprisonment shall not stay the execution.
(9) Authorized police employees may seize objects referred to in paragraph 1 of this Article when proceeding pursuant to Articles 257 and 263 of the present Code or when executing a court warrant.
(10) When seizing objects it shall be indicated where they were found and they shall be described, and where appropriate, their identity shall be established in another way as well. A receipt shall be issued for the seized objects.
(11) Measures referred to in paragraph 3 of this Article may not be enforced against the suspects or accused parties or persons relieved of duty to testify.
(12) Provision of Article 481 of the present Code shall be applied on the provisional seizure of property gain.

::::::

Provisional Seizure of Property Gain and Financial Investigation for the Purpose of Extended Seizure of Property
Article 90

(1) In the procedure conducted for the criminal offence for which the Criminal Code provides for a possibility of extended seizure of property from the sentenced persons, their legal successors or persons to whom the sentenced persons have transfered their property who are not able to prove the legality of its origin, and grounds of suspicion exist that the property in question was illicitly acquired, the court may, at the proposal of a State Prosecutor, order the property to be provisionally seized.
(2) The State Prosecutor shall initiate a financial investigation by way of an order against the suspects or accused persons for the criminal offence referred to in paragraph 1 of this Article, their legal successors or persons to whom the suspects or accused persons have transfered certain property.
(3) During the financial investigation, evidence shall be collected on the property and revenues of suspects or accused persons, their legal successors or persons to whom the accused persons have transferred property that was acquired in the period prescribed by the Criminal Code.
(4) In the procedure of provisional seizure of property referred to in paragraph 1 of this Article, provisions of the law regulating enforcement proceedings shall be applied accordingly, if provisions of the present Code do not prescribe otherwise.

Contents of the Request and Decision Making on the Request for Ordering Seizure of Objects, Property Gain or Property
Article 91

(1) The provisional seizure of objects, property gain or property shall be decided by the investigative judge immediately or within eight days as of the receipt of request, or the Chair of the Panel before which the main hearing is conducted. The panel referred to in Article 24, paragraph 7 of the present Code shall decide on appeals filed against such rulings.
(2) The State Prosecutor shall institute proceedings for ordering the provisional seizure of objects, property gain or property referred to in paragraph 1 of this Article.
(3) The request of the State Prosecutor referred to in paragraph 2 of this Article shall contain the following: a description of objects, property gain and property ; information on the person who is in possession of those objects, property gain or property; reasons for suspicion that the objects, property gain and property were illicitly acquired and reasons to believe that by the time criminal proceedings are completed it would be significantly difficult or hardly possible to confiscate objects or property gain or property obtained through the commission of a criminal offence.
(4) If the court rejects the request referred to in paragraph 1 of this Article, the ruling on rejection shall not be furnished to the person referred to in paragraph 3 of this Article.

Contents of the Ruling on the Provisional Seizure of Objects, Property Gain and Property and Appeal against the Ruling
Article 92

(1) In the ruling on the provisional seizure of objects, property gain and property, the court shall specify the type and value of the objects, property and the amount of property gain, as well as the period for which they shall be seized.
(2) In the ruling referred to in paragraph 1 of this Article, the court may decide that the provisional seizure does not cover objects, property gain or property which should be excluded by virtue of the rules on innocent title transferees.
(3) An appeal against the ruling referred to in paragraph 1 of this Article shall not stay execution.
(4) The ruling with a statement of reasons referred to in paragraph 1 of this Article, shall be delivered by the court to the persons to whom the ruling refers, to the bank or other organization competent for payment transactions, and, where appropriate, to other persons and public authorities.

Scheduling a Hearing and Decisions on Appeal
Article 93

(1) When an appeal against the ruling on the provisional seizure of objects, property gain or property is filed, the panel referred to in Article 24, paragraph 7 of the present Code shall schedule a hearing and summon the person to whom the ruling relates to, his/her defense attorney and the State Prosecutor.

(2) The hearing referred to in paragraph 1 of this Article shall be held within 30 days from the date of the filing of the appeal. Summoned persons shall be heard at the hearing. Their failure to appear shall not preclude holding of the hearing.
(3) The panel shall revoke the ruling referred to in paragraph 1 of this Article if the suspect or the accused proves the lawfulness of the origin of objects, property gain or property by plausible documents, or if, in the absence of plausible documents, s/he presents *prima facie* evidence that the objects, property gain or property were lawfully acquired.
(4) The panel shall reverse the ruling referred to in paragraph 1 of the present Article if, in line with paragraph 3 of this Article, proof has been produced or *prima facie* evidence established that the object, a part of property gain or property that were provisionally seized are of lawful origin.

Duration of the Provisional Seizure of Objects, Property Gain and Property
Article 94

(1) The provisional seizure of objects, property gain or property may last at the most until the panel referred to in Article 24, paragraph 7 of the present Code renders a decision on the request of the State Prosecutor referred to in Article 486 of the present Code.

(2) If the provisional seizure referred to in paragraph 1 of this Article is ordered during the preliminary investigation, it shall be revoked *ex officio* if the investigation has not been instituted within a term of six months as of the date of issuing the ruling on provisional seizure.
(3) The ruling on the provisional seizure of objects, property gain or property may be revoked before the lapse of the period of time referred to in paragraphs 1 and 2 of this Article, by the court's virtue of an office or upon request of the State Prosecutor or the interested party if it is proved that the measure is not needed or justifiable taking into consideration the gravity of the criminal offence, financial situation of the person the measure is imposed on or the situation of persons s/he is legally bound to support, as well as the circumstances of the case which indicate that seizure of objects, property gain and property will not be prevented or considerably aggravated until the completion of the criminal proceedings.

Enforcement of the Ruling on the Provisional Seizure of Objects, Property Gain and Property
Article 95

(1) The ruling on the provisional seizure of objects, property gain and property shall be enforced by the court competent for conducting the enforcement, in line with the law regulating the enforcement proceedings.
(2) The court referred to in paragraph 1 of this Article shall be competent to decide on disputes in connection with enforcement.
(3) On the date of opening of bankruptcy proceedings against a legal person who is in possession of objects, property gain or property that was provisionally seized, terms shall be met to file an interpleader in respect to these objects, property gain or property, as on mature amounts.

Temporary Administration of Property and Assets
Article 96

The competent public authority shall manage the provisionally seized property and assets in accordance with the law regulating the care on provisionally seized and confiscated property.

Return of Provisionally Seized Objects

Article 97

The objects which were provisionally seized in the course of criminal procedure shall be returned to the owner or holder if the procedure is discontinued and grounds for their seizure referred to in Article 477 of the present Code do not exist. The objects shall be returned to the owner or holder even before the completion of the criminal procedure if reasons for their seizure cease to exist.

::::

9. MEASURES OF SECRET SURVEILLANCE

Types of Measures of Secret Surveillance and Conditions for Their Application
Article 157

(1) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of the present Code and evidence cannot be obtained in another manner or their obtaining would request a disproportional risk or endangering the lives of people, measures of secret surveillance may be ordered against those persons:

1) secret surveillance and technical recording of telephone conversations i.e. other comunication carried out through devices for distance technical communication, as well as private conversations held in private or public premises or at open;

2) secret photographing and video recording in private premises;

3) secret supervision and technical recording of persons and objects.

(2) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of the present Code and circumstances of the case indicate that evidence shall be collected with a minumum violation of the right to privacy, measures of secret surveillance may be ordered against those persons:

1) simulated purchase of objects or persons and simulated giving and taking of bribe;

2) supervision over the transportation and delivery of objects of criminal offence;

3) recording conversations upon previous informing and obtaining the consent of one of interlocutors;

4) use of undercover investigators and collaborators.

(3) Measures referred to in paragraph 1, item 1 of this Article may be also ordered against persons for whom there are grounds for suspicion that they have been conveying to the perpetrator or from the perpetrator of criminal offences referred to in Article 158 of the present Code messages in connection to the criminal offence, or that the perpetrator has been using their telephone lines or other electronic communication devices.

(4) Enforcement of measures referred to in paragraph 2, items 1, 3 and 4 of this Article shall not constitute incitement to commit a criminal offence.

Criminal Offences for Which Measures of Secret Surveillance May Be Ordered

Article 158

The measures referred to in Article 157 of the present Code may be ordered for the following criminal offences:

1) for which a prison sentence of ten years or a more severe penalty may be imposed;

2) having elements of organized crime;

3) having elements of corruption, as follows: money laundering, causing false bunkruptcy, abuse of assessment, passive bribery, active bribery, disclosure of an official secret, trading in influence, as well as abuse of authority in economy, abuse of an official position and fraud in the conduct of an official duty with prescribed imprisonment sentence of eight years or a more serious sentence.

4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings.

5) against the security of computer data.

Competence for Ordering Measures of Secret Surveillance and Their Duration

Article 159

(1) Measures referred to in Article 157, paragraph 1 of the present Code shall be ordered via a written order by the investigative judge at the motion of the State Prosecutor containing a statement of reasons. Measures referred to in Article 157, paragraph 2 of the present Code shall be ordered via a written order by the State Prosecutor at the motion of police authorities containing a statement of reasons. The motion containing a statement of reasons shall be delivered in a closed envelope bearing the designation MSS - Measures of Secret Surveillance.

(2) The motion and the order referred to in paragraph 1 of this Article shall contain: the type of measure, data on the person against whom the measure is enforced, grounds for reasonable suspicion, the manner of measure enforcement, its goal, scope and duration. If it is a measure of engagement of an undercover agent and collaborator, the motion and the order shall also contain the use of false documents and technical devices for the transfer and recording of voice, image and video, participation in the conclusion of legal affairs, as well as the reasons justifying the engagement of a person who is not a police officer as an undercover agent and cooperative witness.

(3) The motion and the order for ordering measures shall become an integral part of the criminal file and should contain available data on the person against whom they are ordered, the criminal offence because of which they are ordered, facts on basis of which the need to undertake them originates, duration deadline that needs to be suitable to achiving the objective of measure, manner, scope and place for the measures to be implemented

(4) By way of exception, if the written order can not be issued in time and risk of delay exists, application of measure referred to in Article 157 of the present Code may begin on basis of a verbal order of the investigative judge, i.e., State Prosecutor. In that case, a written order must be obtained within 12 hours following the issue of the verbal order.

(5) Measures referred to in Article 157, paragraphs 1 and 2, items 2, 3 and 4 of the present Code may last only as long as necessary, at the longest four months, although for valid reasons they may be prolonged for three more months. The motion for undertaking the measure referred to in Article 157, paragraph 2, item 1 of the present Code may refer only to one simulated act, and all subsequent motions for the application of this measure against the same person shall contain a statement of reasons justifying the repeated application of this measure. The application of measure shall be terminated as soon as reasons for its application cease.

(6) In addition to the order for the application of measure referred to in Article 157, paragraph 1, item 1 of the present Code, the investigative judge shall issue a separate order containing solely the telephone number or e-mail address and the duration of the measure in question, and this order shall be delivered to enterprises referred to in paragraph 6 of this Article during the course of the application of the measure by the police authorities.

(7) Postal agencies, other enterprises and legal entities registered for transmission of information shall enable the police authorities to enforce the measure referred to in Article 157, paragraph 1 of the present Code. Persons acting in an official capacity and responsible persons involved in the process of passing the order and enforcement of the measures referred to in Article 157 of the present Code shall keep as secret all the data they have learned in the course of this procedure.

(8) If, during the enforcement of measures of secret surveillance, data and notifications are registered referring to some other persons for whom grounds for suspicion exist that s/he had committed the criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of the material shall be copied and forwarded to the State Prosecutor, and it may be used as evidence only for criminal offences referred to in Article 158 of the present Code.

(9) The State Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorised persons, the suspects or their defence attorney to establish the identity of persons who have enforced the measures referred to in Article 157 of the present Code, as well as undercover agent and cooperative witness. If such persons are to be heard as witnesses, the court shall act in the manner prescribed in Articles 120-123 of the present Code.

Enforcement of Measures of Secret Surveillance

Article 160

(1) The measures referred to in Article 157 of the present Code shall be enforced by the police authorities in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible.

(2) Undercover agent and collaborator may be an authorized police officer, employee in another public authority, authorized police officer of another state or, by way of exception, if the measure can not be enforced in another manner, some other person.

(3) Undercover agents and cooperative witnesses can not be persons for whom reasonable suspicion exists that they were or that they currently are members of a criminal organization or group or persons who have been sentenced for criminal offences referred to in Article 22, item 8 of the present Code.

(4) Undercover agent and cooperative witness may participate in legal dealings by using false documents, and in collecting information they may use technical devices for the transfer and recording of sound, image and video.

(5) Authorised police officer enforcing the measure shall keep records on each measure undertaken and report periodically to the State Prosecutor, that is, investigative judge on the enforcement of measures. If the State Prosecutor, i.e., investigative judge ascertains that the need for enforcement of the ordered measures does not exist any more, s/he shall issue and order on their discontinuation.

(6) Upon the enforcement of measures referred to in Article 157 of the present Code the police authorities shall submit to the State Prosecutor a final report and other material obtained by the enforcement of measures.

(7) Should the State Prosecutor decide not to initiate a criminal procedure against a suspect, s/he shall forward to the investigative judge the material obtained through the application of Article 157 of the present Code, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be

destroyed in the presence of the State Prosecutor and the investigative judge. The investigative judge shall compose a record thereon.
(8) The investigative judge shall proceed in the manner described in paragraph 7 of this Article if the State Prosecutor orders that investigation be conducted against the suspect who was subjected to measures of secret surveillance, when the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings.
(9) In cases referred to in paras. 7 and 8 of this Article, data shall be considered as classified within the meaning of regulation prescribing data secrecy.

Legally Invalid Evidence
Article 161

(1) If the measures referred to in Article 157 of the present Code were undertaken in contravention to the provisions of the present Code or in contravention to the order of the investigative judge or the State Prosecutor, the judgment may not be founded on the collected information.
(2) Provisions of Article 211 paragraph 1, Article 293 paragraph 5, Article 356 paragraph 4, and Article 392 paragraph 4 of the present Code shall be applied accordingly with regard to the recordings made in breach of the provisions of this Article and Article 157 of the present Code.

Rendering Information to Persons Against Whom Measure of Secret Surveillance Was Enforced When a Criminal Procedure Is Not Initiated
Article 162

(1) Before the material obtained through the enforcement of measures of secret surveillance in cases referred to in Article 160, paragraphs 4 and 5 of the present Code is destroyed, the investigative judge shall inform the person against whom the measure was undertaken, and that person shall have the right to examine the collected material.
(2) If there is a reasonable concern that rendering information to the person referred to in paragraph 1 of this Article or examination of the collected material by such person could constitute a serious threat to the lives and health of people or could engender any investigation underway or if there are any other justifiable reasons, the investigative judge may, based on an opinion of the State Prosecutor, decide that the person against whom the measure was undertaken not be informed and allowed to examine the collected material.

:::::

Part Three

SPECIAL PROCEEDINGS

::::

2. PROCEEDINGS FOR THE CONFISCATION OF PROPERTY GAIN

General Provisions on Confiscation of Property Gain
Article 478

(1) Property gain obtained as a result of the commission of a criminal offence shall be established as such in the investigatory proceedings, preliminary proceedings and at the trial by virtue of an office.

(2) In the course of the investigatory proceedings, preliminary proceedings and at the trial, the court and other authorities shall obtain evidence and investigate circumstances that are relevant to the establishment of property gain.
(3) If the injured party submits a property law claim regarding the recovery of items acquired in consequence of the commission of a criminal offence or regarding the amount which corresponds to the value of the items, the property gain shall only be established for the part which exceeds the property law claim.

Confiscation of Property Gain from Third Persons who have been Transferred the Property Gain

Article 479

(1) When the confiscation of property gain obtained as result of the commission of a criminal offence from other persons is being considered, the person to whom the property gain was transferred or the person for whom it was obtained, or the representative of the legal entity shall be summoned for interrogation in the pre-trial proceedings and at the trial. The summons shall contain an admonition that the proceedings will be held even in his/her absence.
(2) The representative of the legal entity shall be heard at the trial after the interrogation of the accused person. The court shall proceed in the same manner regarding other person referred to in paragraph 1 of this Article, unless s/he is summoned as a witness.
(3) The person to whom the property gain was transferred or the person for whom it was obtained or the representative of the legal entity is entitled to propose presentation of evidence concerning the establishment of the property gain and, upon the authorization of the Chair of the Panel, to pose questions to the accused person, witnesses and expert witnesses.

(4) Exclusion of the public from the trial shall not relate to the person to whom the property gain was transferred or for whom it was obtained or the representative of the legal entity.
(5) If the Court establishes that the confiscation of property gain comes into consideration while the trial is in progress, it shall recess the trial and summon the person to whom the property gain was transferred or for whom it was obtained, or the representative of the legal entity.

Determining the Amount of Property Gain by Free Evaluation
Article 480

The amount of property gain shall be determined at the discretion of the court if its assessment entails disproportionate difficulties or a significant delay in the proceedings.

Imposing Provisional Security Measures
Article 481

When the conditions for the confiscation of property gain are met**,** the court shall, by virtue of an office or upon the proposal of the State Prosecutor, impose provisional security measures, pursuant to the provisions governing the enforcement proceedings. In such a case, the provisions of Article 243 of the present Code shall accordingly apply.

Imposing Confiscation of Property Gain
Article 482

(1) Court may order the confiscation of property gain by a conviction, by a penal order issued without trial, by a ruling on a judicial admonition or by a ruling on the application of a corrective measure, as well as by a ruling on the imposition of a security measure of compulsory psychiatric treatment and confinement in a medical institution, or compulsory psychiatric treatment out of the institution.
(2) In the pronouncement of the judgement or the ruling the court shall state which valuable item, money amount, or other property gain is to be confiscated.

(3) A certified copy of the judgement or the ruling shall also be delivered to the person to whom the property gain was transferred or for whom it was obtained, as well as to the representative of the legal entity, provided that the court orders the confiscation of property gain from such a person or a legal entity.

Request for Retrial Regarding the Confiscation of Property Gain

Article 483

The person referred to in Article 479 of the present Code may submit a request for retrial regarding the decision on the confiscation of property gain.

Appropriate Application of Provisions Regulating an Appeal
Article 484
The provisions of Article 383, paragraphs 2 and 3 and Articles 391 and 395 of the present Code shall be applied accordingly in regard to an appeal filed against the decision on the confiscation of property gain.

Appropriate Application of other Provisions of the present Code
Article 485
Unless otherwise provided by the provisions of this Chapter, in regard with the implementation of security measures or the confiscation of property gain, other provisions of the present Code shall be applied accordingly.

3. CONFISCATION OF PROPERTY WHOSE LEGAL ORIGIN HAS NOT BEEN PROVED

Request for Confiscation of Property and Contents of Request
Article 486
(1) After the finality of the judgement finding the accused person guilty of the criminal offence for which the Criminal Code prescribes the possibility of extended confiscation of property from the convicted person, his/her legal successor or the person to whom the convicted person has transferred the property and who cannot prove the legality of its origin, the State Prosecutor shall, at the latest within one year, submit the request for the confiscation of the property of the convicted person, his/her legal successor or a person to whom the convicted person has transferred the property for which there is no evidence on the legality of its origin.
(2) The request from paragraph 1 of this Article shall contain the data on the convicted person, his/her legal successor or the person to whom the convicted person has transferred the property, indication of property to be confiscated, evidence on the property owned by the convicted person, his/her legal successor or the person to whom the property has been transferred, and on their legal proceeds, as well as circumstances indicating the obvious discrepancy between the total property and the legal proceeds of the convicted person, his/her legal successor and the person to whom the convicted person has transferred the property.
(3) The request from paragraph 1 of this Article shall be served without delay to the convicted person, his/her legal successor or the person to whom the convicted person has transferred the property, along with a warning stating that s/he shall prove the legal origin of the property at the Panel session referred to in Article 24, paragraph 7 of the present Code, as well as that the property will be confiscated if its legal origin has not been proved.

Deciding on the Request for the Confiscation of Property
Article 487
(1) Pursuant to Article 314 of the present Code, the Panel referred to in Article 24, paragraph 7 of the present Code shall decide on the request referred to in Article 486 of the present Code at the session from which the public may be excluded.
(2) The following shall be invited to the Panel session: State Prosecutor, convicted person, his/her legal successor or a person to whom the convicted person has transferred his/her property, and his/her proxy.
(3) If the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property does not prove by plausible documents or in absence of plausible documents, in some other manner, the legal origin of the property, the Panel shall issue a ruling on the confiscation of the property.
(4) If the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property proves by plausible documents or in some other manner the legality of the property origin or of the part of property, the Panel shall issue a ruling on total or partial dismissal of the request referred to in Article 486, paragraph 1 of the present Code.
(5) The panel referred to in Article 24, paragraph 7 of the present Code shall dismiss the request if it was submitted after the expiry of the deadline referred to in Article 486, paragraph 1 of the present Code.

Contents of the Request on Confiscation of Property

Article 488

(1) The ruling referred to in Article 487, paragraph 3 of the present Code shall contain the data on the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property, on the property being confiscated, and the decision on the costs of safekeeping and administration of the provisionally seized property referred to in Article 96 of the present Code. If the confiscation of the property would bring into question the sustenance of the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property or the persons who they are legally obliged to support, the ruling shall indicate that a portion of the property is exempted from confiscation.

(2) The ruling on property confiscation shall be delivered to the convicted person, his/her legal successor or the person to whom the convicted person has transferred his/her property, his/her proxy, State Prosecutor, and the state authority which, pursuant to the law, shall administrate the confiscated property.

Appeal against the Ruling on Confiscation of Property

Article 489

(1) Convicted person, his/her legal successor of the person to whom the convicted person has transferred his/her property and his/her proxy may appeal against the ruling referred to in Article 487, paragraph 3 of the present Code within eight days; the State Prosecutor may appeal against the ruling referred to in Article 487, paragraph 4 of the present Code.

(2) An immediately superior court shall decide on the appeal referred to in paragraph 1 of this Article.

LAW ON CRIMINAL LIABILITY OF LEGAL ENTITIES

(Published in the "Official Gazette of the Republic of Montenegro",

Nos. 2/2007 and 13/2007)

I. BASIC PROVISIONS

Subject Matter of the Law

Article 1

This Law shall govern the conditions of criminal liability of legal entities, criminal sanctions applied against legal entities, and criminal procedure in which such sanctions are imposed.

Exclusion and Limitation of Liability

Article 2

(1) The Republic of Montenegro (hereinafter referred to as "Montenegro") state authorities and local government authorities may not be liable for a criminal offence.

(2) Legal entity vested with public powers shall not be liable for a criminal offence committed in the performance of such powers.

Criminal Offences for Which Legal Entities are Liable

Article 3

Legal entities may be held liable for criminal offences referred to in the special section of the Criminal Code and for other criminal offences provided for under a separate law, if the conditions of liability of a legal entity prescribed by this Law have been fulfilled.

Definitions

Article 4

The terms used in this Law shall have the following meanings:

1) **legal entity** means a company, foreign company and foreign company branch, public enterprise, public institution, domestic and foreign non-governmental organizations, investment fund, other fund (except for the fund exercising solely public powers), sports organization, political party, as well as other association or organization which continuously or occasionally gains or acquires assets and disposes with them within the framework of their operations;

2) **responsible person** means a natural person entrusted with certain duties in a legal entity, a person authorized to act on behalf of the legal entity and a person who can be reasonably assumed to be authorized to act on behalf of the legal entity. A natural person acting on behalf of the legal entity as a shareholder shall also be considered to be a responsible person;

3) **effective, necessary and reasonable measures** mean those measures which the legal entity has undertaken with the aim to reveal and prevent criminal offences and encourage the employees to act in accordance with the law, other regulations and good business customs by which that aim is realized, and in particular:

- adoption of standards and procedures with the aim to reveal and prevent criminal offences;

- adoption of the programme for implementation of the standards and procedures referred to in indent 1 above, including the provision of necessary financial and other resources, as well as the obligation of certain persons in the legal entity to monitor constantly the implementation of those standards and procedures and to report periodically thereof to the superior officer in the legal entity and to the management bodies;

- carrying out supervision with respect to the application of the standards and procedures referred to in indent 1 above by the management bodies;

- prohibition to perform the management function to each person who is reasonably suspected of carrying out illegal actions;

- implementation of an effective programme of training of responsible persons on the standards and procedures referred to in indent 1 above;

- undertaking appropriate actions for the implementation of the standards and procedures referred to in indent 1 above by all employees, such as periodical assessments of effectiveness, providing guidelines with the aim of avoiding perpetration of criminal offences, establishing mechanisms for anonymous and confidential reporting of criminal offences, monitoring the application of the standards and procedures, control of business books and other documents;

- conducting disciplinary proceedings for violations of the standards and procedures referred to in indent 1 above, as well as giving rewards for consistent application of those standards and procedures;

- undertaking adequate measures after the criminal offence is revealed, including conducting full internal investigation and, if necessary, changing the programme referred to in indent 2 above so as to prevent future criminal offences.

II. GENERAL PROVISIONS

1. Conditions for Liability of a Legal Entity for a Criminal Offence

Grounds for Liability of a Legal Entity

Article 5

A legal entity shall be liable for a criminal offence of a responsible person who acted within his/her authorities on behalf of the legal entity with the intention to obtain any gain for the legal entity.

Limits of Liability of Legal Entity for Criminal Offences

Article 6

(1) Under the conditions referred to in Article 5 above, the legal entity shall be held liable for a criminal offence even if the responsible person who committed such criminal offence has not been convicted of such criminal offence.

(2) Liability of a legal entity shall not exclude criminal liability of a responsible person for the criminal offence committed.

(3) Subjective elements of a criminal offence that exist only with the responsible person shall be taken into account with respect to the legal entity if the grounds for liability referred to in Article 5 above exist.

2. Sanctions

Types of Sanctions

Article 12

Legal entity may be imposed the following sanctions for the criminal offence:

1) punishment;

2) suspended sentences;

3) security measures.

1) Punishments

Types of Punishments

Article 13

(1) Legal entity may be imposed the following punishments:

1) a fine;
2) dissolution of legal entity.

(2) Fine and dissolution of legal entity may be imposed only as principal punishments.

Fine

Article 14

(1) A fine shall be determined depending on the amount of the damage caused or illicit material gain obtained, and if these amounts are different the higher amount shall serve as a basis for the determination of fine.

(2) Fine may not be less than two-fold amount of the damage caused or illicit material gain obtained or higher than 100-fold amount of the material damage caused or illicit material gain obtained.

(3) If by a criminal offence no material damage was caused or no illicit material gain was obtained, or if it is difficult to determine the amount of such damage or material gain within a reasonable period of time due to the nature of the criminal offence committed and other circumstances, the court shall mete out the fine in a fixed amount which may not be less than one thousand euros or higher than five million euros.

Amounts of Fines

Article 15

Legal entity shall be punished by a fine in the amount of:

1) two-fold to five-fold amount of the damage caused or illicit material gain obtained or from one thousand to ten thousand euros for the criminal offences punishable by imprisonment for a term of up to one year or a fine;
2) five-fold to ten-fold amount of the damage caused or illicit material gain obtained or from ten thousand to twenty thousand euros for the criminal offences punishable by imprisonment for a term of up to three years;
3) ten-fold to fifteen-fold amount of the damage caused or illicit material gain obtained or from twenty thousand to fifty thousand euros for the criminal offences punishable by imprisonment for a term of up to five years;

4) fifteen-fold to twenty-fold amount of the damage caused or illicit material gain obtained or from fifty thousand to one hundred thousand euros for the criminal offences punishable by imprisonment for a term of up to eight years;
5) twenty-fold to fifty-fold amount of the damage caused or illicit material gain obtained or from one hundred thousand to two hundred thousand euros for the criminal offences punishable by imprisonment for a term of up to ten years;
6) minimum fifty-fold amount of the damage caused or illicit material gain obtained or minimum two hundred thousand euros for the criminal offences punishable by imprisonment for a term of more than ten years.

Dissolution of Legal Entity

Article 22

(1) The penalty of dissolution of a legal entity may be ordered if the business conducted by the legal entity was wholly or considerably in the function of committing the criminal offence.
(2) The liquidation proceeding shall be conducted in companies along with the imposing of the penalty of dissolution of a legal entity.
(3) A legal entity shall be dissolved upon deletion from the Central Registry of the Commercial Court in Podgorica or another registry kept by the competent state authority.
(4) If the penalty referred to in paragraph 1 above was imposed, dissolved assets of the company and assets of another legal entity shall be confiscated for the benefit of Montenegro.

LAW ON THE STATE PROSECUTOR'S OFFICE

(Published in the Official Gazette of the Republic of Montenegro 69/2003

and the Official Gazette of Montenegro 40/2008, 39/2011 and 46/2013)

I GENERAL PROVISIONS

Subject matter of the Law

Article 1

The present Law shall regulate establishment, organisation, jurisdiction and other issues of significance for the work of the State Prosecutor's Office, as well as issues of significance for the work of the Special Prosecutor for Suppression of Organised Crime, Corruption, Terrorism and War Crimes.

Constitutionality and Legality

Article 2

The State Prosecutor's Office shall perform its function based on the Constitution, laws and ratified international treaties.

Autonomy and Independence

Article 3

The State Prosecutor must not exercise his/her office under anybody's influence and nobody shall influence the State Prosecutor in the exercise of his/her office, except in cases provided for by the present Law.

Managers and State Prosecutors

Article 4

The State Prosecution Service shall be headed by the Chief State Prosecutor.

Basic and high state prosecutor's offices shall be headed by managers of state prosecutor's offices, whereas the Chief State Prosecutor's Office shall be headed by the chief state prosecutor.

A manager of a state prosecutor's office and state prosecutor shall perform their duties in the state prosecutor's office they have been elected or seconded or transferred to in accordance with this Law.

Special tasks of the State Prosecutor Service shall be performed by the Special prosecutor for suppression of organised crime, corruption, terrorism and war crimes (hereinafter referred to as "the Special Prosecutor") in accordance with the law.

Deputy

Article 5

- repealed-

Impartiality and Objectiveness

Article 6

The position of manager of a state prosecution office and a state prosecutor is performed in the public interest for the purpose of ensuring implementation of law, while at the same time ensuring observance and protection of human rights and freedoms.

The position of manager of a state prosecutor's office and state prosecutor must be performed impartially and objectively.

Code of Ethics

Article 7

A manager of a state prosecutor's office and a state prosecutor shall observe the Code of Prosecution Ethics in the performance of their duties.

The Code of Prosecution Ethics shall be passed by the Conference of State Prosecutors.

The Conference of State Prosecutors shall appoint a Commission to monitor the implementation of the Code of Prosecution Ethics (hereinafter referred to as "the Commission for the Code of Prosecution Ethics). The Commission shall have a chair and two members.

A chair of the Commission shall be proposed by the Prosecutorial Council from among its members who are not state prosecutors, one member shall be proposed by the extended session of the Chief State Prosecutor's Office and the other member shall be the President of the State Prosecutors' Association of Montenegro.

The Commission for the Code of Prosecution Ethics shall be appointed for a period of four years.

The Commission for the Code of Prosecution Ethics shall submit a report on its work to the Prosecutorial Council at a minimum once a year, no later then 31st March of a current year for the preceding year.

The Commission for the Code of Prosecution Ethics shall adopt Rules of Procedure to regulate in more detail the methods of its work and decision-making.

Conference of State Prosecutors

Article 7a

The Conference of State Prosecutors shall be made up of all managers of state prosecutor's offices and all state prosecutors.

In addition to the tasks referred to in Article 7 of this Law, the Conference of State Prosecutors shall elect and dismiss members of the Prosecutorial Council from the ranks of state prosecutors.

The Conference of State Prosecutors shall be convened and chaired by the Chief State Prosecutor.

The Conference of State Prosecutors may take place when no less than two thirds of Conference members are present.

The Conference of State Prosecutors shall make decisions by a majority vote of attending managers of state prosecution offices and state prosecutors.

The method of work and decision-making of the Conference of State Prosecutors shall be laid down in more detail by the Rules of Procedure of the Conference.

Administrative support to the Conference of State Prosecutors shall be provided by Chief State Prosecutor's Office staff, in accordance with the act on internal organization and systematization.

II ESTABLISHMENT AND JURISDICTION

1. Establishment

Structure of the State Prosecutor's Office

Article 13

The Chief State Prosecutor’s Office, high state prosecutors’ offices, and basic state prosecutors’ offices shall be established within the State Prosecution Service.

The Chief State Prosecutor’s Office shall be established for the territory of Montenegro, with the seat in Podgorica.

The High State Prosecutor’s Office shall be established for the territory of the High Court.

The Basic State Prosecutor’s Office shall be established for the territory of one or more Basic Courts.

Chief State Prosecutor

Article 14

The Chief State Prosecutor’s Office shall proceed before the Supreme Court of Montenegro, the Appellate Court of Montenegro and the Administrative Court of Montenegro, other courts and other state authorities, in accordance with the law.

The Chief State Prosecutor’s Office shall, in accordance with the law, file a petition for protection of legality.

The Chief State Prosecutor’s Office shall also exercise other duties, which are not defined as falling within the competence of the High State Prosecutor’s Office and the Basic State Prosecutor’s Office.

High State Prosecutor’s Office

Article 15

High State Prosecutors’ Offices are established as:

1) The High State Prosecutor’s Office in Bijelo Polje, to proceed before the High Court of Bijelo Polje and the Commercial Court of Bijelo Polje.
2) The High State Prosecutor’s Office in Podgorica, to proceed before the High Court of Podgorica and the Commercial Court of Podgorica.

The High State Prosecutor’s Office shall have jurisdiction to proceed in criminal matters before High Courts.

Basic State Prosecutor’s Office

Article 16

Basic State Prosecutors’ Offices are established as:

1) The Basic State Prosecutor's Office in Bar, for the territory of the Basic Court of Bar;
2) The Basic State Prosecutor's Office in Berane, for the territory of the Basic Court of Berane;
3) The Basic State Prosecutor's Office in Bijelo Polje, for the territory of the Basic Court of Bijelo Polje;
4) The Basic State Prosecutor's Office in Kolasin, for the territory of the Basic Court of Kolasin;
5) The Basic State Prosecutor's Office in Kotor, for the territory of the Basic Court of Kotor;
6) The Basic State Prosecutor's Office in Niksic, for the territory of the Basic Court of Niksic;
7) The Basic State Prosecutor's Office in Plav, for the territory of the Basic Court of Plav;
8) The Basic State Prosecutor's Office in Pljevlja, for the territory of the Basic Court of Pljevlja and the Basic Court of Zabljak;
9) The Basic State Prosecutor's Office in Podgorica, for the territory of the Basic Court of Podgorica and the Basic Court of Danilovgrad;
10) The Basic State Prosecutor's Office in Rozaje, for the territory of the Basic Court of Rozaje;
11) The Basic State Prosecutor's Office in Ulcinj, for the territory of the Basic Court of Ulcinj;
12) The Basic State Prosecutor's Office in Herceg Novi, for the territory of the Basic Court of Herceg Novi;
13) The Basic State Prosecutor's Office in Cetinje for the territory of the Basic Court of Cetinje.

The Basic State Prosecutor's Office shall also proceed before the authorities in charge of petty offences and other state authorities from within its district.

The Basic State Prosecutor's Office shall be authorised to carry out all actions falling within its competence before the court which has subject matter and territorial jurisdiction and before authorities in charge of petty offences or other state authorities, except for those actions which fall within the exclusive competence of the Chief *i.e.* High State Prosecutor and actions undertaken by them.

2. Jurisdiction

General Jurisdiction

Article 17

The State Prosecutor's Office shall perform the tasks of prosecution of perpetrators of criminal offences and other punishable offences prosecuted *ex officio*, file legal remedies falling within its jurisdiction and perform other affairs as prescribed by law.

Subject Matter and Territorial Jurisdiction

Article 18

The State Prosecutor's Office shall proceed within the limits of his/her subject matter and territorial jurisdiction, unless otherwise provided by the law.

Authority to undertake measures

Article 19

In order to perform the function of prosecution of perpetrators of criminal offences and other offences punishable by law, the State Prosecutor’s Office shall have the authority to determine and undertake measures requisite for detection of criminal and other offences punishable by law and their perpetrators, in co-operation with competent authorities.

1. General and Special Requirements

General Requirements

Article 24

Candidates for managers of state prosecution offices and state prosecutors must meet the following requirements:

- be nationals of Montenegro:
- be in good health;
- have a law faculty (university education totalling 240 CSPK credits, VII-1 level of qualification in education);
- have passed the Bar exam.

Pursuant to Article 95 item 3 of the Constitution of Montenegro, I hereby issue the

DECREE

PROMULGATING THE LAW ON INTERNAL AFFAIRS

I hereby promulgate the **Law on Internal Affairs** passed by the 24rd Parliament of Montenegro at the eight sitting of the first ordinary (spring) session in 2012 on 26 July 2012.

No 01-986/2

Podgorica, 30 July 2012

The President of Montenegro

Filip Vujanović

Pursuant to Article 82 paragraph 1 item 2 and Article 91 paragraph 2 of the Constitution of Montenegro, the the 24rd Parliament of Montenegro at the eight sitting of the first ordinary (spring) session in 2012 on 26 July 2012, adopted the following

LAW

ON INTERNAL AFFAIRS

1. Collection and Processing of Personal and other Data

Collection of Personal and Other Data

Article 37

Police may collect personal and other data (hereinafter referred to as the “data”) in the extent necessary to perform police duties and use police powers to prevent and suppress crime and maintain public peace and order.

Manner of Data Collection

Article 38

As a rule, data shall be collected directly from the person they refer to.

Without prejudice to paragraph 1 of this Article, data may be collected from other state authorities, state administration bodies, local self-government bodies, organisations, institutions or other legal or natural persons, if it is not possible to collect data directly from the person they refer to, or if such collection would jeopardise use of police powers.

Data may be collected in a special manner if performance of a concrete police duty or activity is prejudiced.

Request for Collection of Data

Article 39

Authorities and legal and natural persons referred to in Article 38 paragraph 2 of this Law, which under the law, within their jurisdictions keep data records, shall upon the police request provide the information necessary to carry out statutory duties and powers under its scope of work or jurisdiction.

The request referred to in paragraph 1 of this Article shall include: the legal basis for using the data, which data is needed, for what purpose, sufficient number of data needed to establish identity of a person or subject, and to what point the right of the person to know that his/her data is being used is restricted.

Special Manners to Collect Data

Article 40

The Police may collect data in a special manner in accordance with this Law only if:

1) a life or body is threatened, as well as freedoms and rights of an individual or a citizen, or a property of a significant values which preservation is of public interest;
2) commission of a serious crime is thus prevented, which is committed by a group or a criminal organisation, and crime prevention was not otherwise possible.

Measures to Collect Data in a Special Manner
Article 41

Collecting data in a special manner shall be done by applying the following measures:

1) surveillance of a person in duration of up to 24 hours continually, or in interrupted intervals in duration of 2 days, and;
2) covert recording and use of video recordings, and recording of non-private conversation in duration of no longer than 30 days.

Order to Apply Measures to Collect Data
Article 42

Application of measures referred to in Article 41 of this law upon justified proposal of the Director shall be approved by the Minister's order.

The order referred to in paragraph 1 of this Article shall be in written and justified.

The order referred to in paragraph 1 of this Article for application of measures referred to in Article 41 of this Law shall be issued based on court decision and it shall contain the decision itself.

Application of measures referred to in Article 41 of this law can be extended till the objective due to which measures are applied is reached, and for each prolongation of measures the order is issued in accordance with paragraphs 1,2 and 3 of this Article.

Data obtained in special manner can be used for the purpose they are collected, unless they are necessary to prevent commission of a crime the secret surveillance measures can be ordered for in accordance with law.

Internal Control Activities
Article 115

Internal control activities shall include: control of lawfulness of performance of the police activities, in particular in regard to compliance and protection of human rights when performing police tasks and exercising police powers; implementation of counter-intelligence procedures and other control relevant for efficient and legal work.

In accordance with Article 88 Item 2 of the Constitution of the Republic of

Montenegro I hereby pass the

ENACTMENT ON PROCLAMATION OF

THE LAW ON FOREIGN CURRENT AND CAPITAL OPERATIONS

("Official Gazette of RoM", No. 45/05 as of 28th July 2005)

This is a proclamation of the Law on Foreign Current and Capital Operations,

adopted by the Parliament of the Republic of Montenegro at the fourth meeting of the

first regular session in the year 2005, on 21st July 2005.

Number: 01-763/2

Podgorica, 25th July 2005

President of the Republic of Montenegro

Filip Vujanov, signed

LAW ON FOREIGN CURRENT AND CAPITAL OPERATIONS

IV Physical Import and Export of Financial Means

Reporting on Physical Import and Export of Financial Means

Article 10

For the purpose of monitoring of the Projection the Balance of Payments of the Republic, and control against money laundering and terrorism financing, resident and non-resident is obliged to declare physical import and export of means of payment at the point of entry or departure to or from the Republic.

The declaration from paragraph 1 of this Article shall be submitted to administration body in charge of customs affairs at a border crossing point.

The administration body from paragraph 2 of this Article shall perform control over physical import and export of means of payment.

The Central Bank shall prescribe the amount of cash which residents or nonresidents may import into the Republic or export from the Republic without declaring it to the body from paragraph 2 of this Article.

Administration body in charge of customs affairs shall keep records on performed controls.

Ministry of Finance shall determine more specific contents of the records from paragraph 5 of this Article.

Article 15

A pecuniary fine in the amount of 50 fold to 300 fold of the minimum labor price in the Republic shall be imposed on a legal entity and entrepreneur who do not declare physical import or export of means of payment from Article 10 paragraph 1 of this Law.

A pecuniary fine in the amount of 10 fold to 20 fold of the minimum labor price in the Republic shall be imposed on a responsible person in the legal entity for the offence from paragraph 1 of this Article.

A pecuniary fine in the amount of 10 fold to 20 fold of the minimum labor price in the Republic shall be imposed on a physical person for the offence from paragraph 1 of this Article.

Pursuant to the Article 10 Paragraph 6 of the Law on Foreign Current and Capital Operations (Official Gazette of the Republic of Montenegro 45/05 and Official Gazette of Montenegro 62/08), the Ministry of Finance has adopted the following

R U L E B O O K

ON DETAILED EVIDENCE ON PERFORMED CONTROLS OF PHYSICAL ENTRY AND EXIT OF MEANS OF PAYMENT ACROSS STATE BORDER

Article 1

This Rulebook closely defines the contents of evidence on performed controls of physical entry and exit of means of payment at locations of entry of exit to/out of Montenegro.

Article 2

Means of payment, in terms of this Rulebook are:

- Cash (bills and coins) circulating as the means of payment;

- Payment instruments (including cheques, bonds and transfer orders), payable to the bearer, endorsed without limitations, issued to a name of fictitious beneficiary or in some other form and incomplete signed instruments (cheques, bonds and transfer orders), without noting the name if the beneficiary.

Article 3

Evidence on performed controls of physical entry and exit of means of payment, in the amount of 10 000 Euro and more, or in equivalent in currency other than Euro, at locations of entry of exit to/out of Montenegro, shall be made in the Declaration form, which is the integral part of this Rulebook.

Notification on method of declaring physical entry and exit of means of payment, referred to Paragraph 1 of this Article, shall be posted at visible location at border crossing point.

Article 4

Data from evidence of performed controls of entry and exit of means of payment to/out of Montenegro can be a matter of exchange with the EU member countries and third countries.

Article 5

This Rulebook shall come into force on the eight day after its publication in the Official Gazette of Montenegro.

No: 02-7991

Podgorica, 11 July 2011

Minister,

Milorad Katnić, PhD, signed

Pursuant to Article 20 of the Code of Ethics of Civil Servants and State Employees ("Official Gazette of Montenegro 20/12), the Director of Customs Administration announces:

CODE OF ETHICS

FOR CUSTOMS OFFICERS AND ADMINISTRATION EMPLOYEES

1. Keeping official secrets, confidentiality and use of official information

Article 5

The customs officer shall maintain the documents, files, data and information constituting official secret accessible to him/her in course of performing his/her duties and tasks, and use them for professional purposes when performing duties.

The customs officer must not remove or destroy official data, documents or files. The customs officer may change the official data solely where that is directly connected with performing professional duties aimed at ensuring accurate and reliable official data in line with prescribed procedure.

Decision on Nomination and Appointment, Termination of Term of Office and Revocation
Article 55

Decision on appointment, termination of office and revocation of a person belonging to senior management staff in state administration authority and service established by the Government, shall be adopted by the Government.

The person referred to in paragraph 1 of this Article shall be appointed for the period of five years and may be reappointed upon the expiration of that period of time.

The decision on nomination and appointment, termination of term of office and revocation of the person referred to in paragraph 1 of this Article in another state authority shall be adopted by that authority, in accordance with a separate law or another regulation.

Termination of Term of Office and Revocation
Article 56

Term of office shall terminate to a person belonging to the senior management staff:
- **By expiration of the term of office;**
- **Upon personal request;**
- **By termination of employment in accordance with Article 123, paragraph 1, item 1, of this Law;**
- **In case referred to in Article 133 of this Law;**
- **By revocation.**

The person referred to in paragraph 1 of this Article shall be revoked, if:
- **He is convicted to an unconditional imprisonment;**
- **He is convicted of a criminal offence making him unworthy to perform the duties;**
- **He is imposed in the form of a final decision a disciplinary measure instituting termination of employment.**

The person, whose term of office terminated under paragraph 1, items 1 and 2 of this Article, may be reassigned within the same or another state authority to a job position corresponding to his qualifications and skills.

The person, who cannot be reassigned under paragraph 3 of this Article, within a year from the day of termination of term of office, shall be entitled to receive during that period of time the compensation in the amount of the wage he received for the last month of performing the service, with appropriate adjustment. Exceptionally, the right to compensation may be extended for one additional year, if within that period of time the person acquires the right to pension.

The senior management staff shall acquire the right referred to in paragraph 4 of this Article on the basis of a personal request to be submitted to a competent working body of the Government or another competent body within 30 days from the day of termination of term of office.

Nomination of Head of Administration Authority

Article 57

A person may be nominated as a head of administration authority if he has VII1 level of qualifications and at least three years of work experience in management jobs or other appropriate jobs requiring autonomy in work.

Upon publishing a public competition for nominating a head of administration authority, the Human Resources Management Authority, on the basis of timely, complete and proper documentation, shall prepare a list of candidates meeting the requirements referred to in paragraph 1 of this Law.

The Human Resources Management Authority shall submit the list referred to in paragraph 2 of this Article to a respective Minister who, based on the interviews with all candidates from the list, proposes nominations to the Government.

Persons who manage the legal entities referred to in Article 3, paragraph 2 of this Law shall be nominated in accordance with the law regulating the area that such legal entities have been established for.

Obligation to Safeguard and Protect Secret and Personal Data

Article 64

Civil servant and state employee shall be obliged to provide, in the course of their work, the free access to information, in accordance with law and other regulations.

Civil servant and state employee shall be obliged to ensure the protection and safeguard of secret and personal data in accordance with law, regardless of the manner of learning about such data.

Civil servant and state employee shall be obliged to keep the secrecy of the data referred to in paragraph 2 of this Article also upon the termination of employment with state authority, and for the period not exceeding five years from the day of termination of employment, unless otherwise determined by a separate law.

Head of state authority may release a civil servant and/or state employee from the obligation to keep the data referred to in paragraphs 2 and 3 of this Article in a court procedure, if such data are necessary to determine in such a procedure the facts and adopt a lawful decision.

Integrity, Conflict of Interest and Protection of Civil Servant and State Employee Reporting Suspicion of Corruption (Whistleblowers)

Integrity of Civil Servant and State Employee

Article 67

For the purpose of creating and maintaining trust of citizens in good-faith and responsible performance of tasks in a state authority, civil servant and state employee must conduct in a manner not to diminish their reputation and reputation of a state authority, and not to compromise their impartiality in their work, as well as to eliminate suspicion regarding the occurrence and development of corruption.

Integrity Plan

Article 68

A state authority shall adopt an integrity plan on the basis of assessment of susceptibility of certain job positions for occurrence and development of corruption and other forms of partial actions of civil servants and state employees regarding certain job positions, which shall include measures preventing and eliminating the possibilities for corruption occurrence and development, in accordance with the guidelines of administration authority in charge of anti-corruption activities.

The state authority shall determine a civil servant who is responsible for preparing and implementing the integrity plan.

Avoiding Conflict of Interest

Article 69

In performance of tasks, civil servant and state employee shall be obliged to avoid situations wherein their private interest affects or may affect their impartial and objective performance of tasks of their job positions.

Private interest shall mean ownership and other material or non-material interest of a civil servant and state employee.

Obligation to Report Potential Conflict of Interest

Article 70

Civil servant and/or state employee shall be obliged to inform in writing an immediate manager about the following:

- Private interest that he or his related person may have in relation to activities within the competency of a state authority wherein he participates;
- Ownership of shares and bonds or other financial and other interests in business organizations within competency of a state authority he is working for;
- Physical persons and legal entities that he had contractual or business relation with, two years prior to entering employment with a state authority, and which are within competency of the state authority he is working for.

Related person, under this Law, shall mean a relative of a civil servant and/or state employee in the first direct line and in the collateral line up to the second degree of kinship, relative-in-law up to the first degree of kinship, spouse and out-of-wedlock partner, adoptive parent and adoptee.

In case of the existence of the circumstances referred to in paragraph 1 of this Article, a head of state authority shall make a decision on exempting the civil servant and/or state employee from working on certain tasks, in accordance with the law regulating general administrative procedure.

The data on potential conflict of interest referred to in paragraph 1 of this Article, as well as the decision referred to in paragraph 3 of this Article, shall be entered in personal file of civil servant and/or state employee.

Prohibition of Abuse of Authorizations and Use of Assets

Article 71

Civil servant and state employee must not use his authorizations in state authority to influence the realization of private interest or interest of his related physical person or legal entity.

Civil servant and state employee must not, for the purpose of realizing private interest or interest of his related physical person or legal entity, use State assets and data available to him while performing the tasks.

Prohibition to Receive Gifts

Article 72

Civil servant and/or state employee must not receive money, securities or precious metal, regardless of their value.

Civil servant and/or state employee must not receive gifts, except for appropriate gifts of smaller value.

The appropriate gift referred to in paragraph 2 of this Article shall be considered to be a gift worth up to 50 euro.

Civil servant and state employee shall be obliged to report the received gift referred to in paragraph 3 of this Article to a state authority he is working for, on the prescribed form.

State authority shall keep the records of gifts referred to in paragraph 4 of this Article.

The Ministry shall determine the contents and the manner of keeping the records referred to in paragraph 5 of this Article, as well as the contents of the form referred to in paragraph 4 of this Article.

Refusal of Gifts

Article 73

Civil servant and/or state employee, who is offered a gift that he must not accept, shall be obliged to refuse the offer.

If a civil servant and/or state employee could not refuse the gift, or return the gift to the gift maker, he shall be obliged to deliver the gift to the state authority he is working for.

Outside Employment

Article 74

Civil servant and/or state employee may, outside working hours, following prior approval of a head of state authority, perform activities or provide services to a physical person or legal entity, only if the state authority that he is working for does not supervise such activities or work, or if such a work is not

prohibited by a separate law, and if it does not represent a conflict of interest or obstacle to proper performance of regular tasks, and if it does not damage reputation of the state authority.

With a prior notification of a head of state authority, civil servant and state employee may perform work in scientific, research, pedagogic, humanitarian, sports activity, as well as publish professional papers and act as lecturer at professional seminars and conferences.

Prohibition to Establish Business Organizations

Article 75

Civil servant and state employee must not establish a business organization or engage in entrepreneurial activities.

Restrictions of Membership in Bodies of Legal Entities

Article 76

Civil servant and state employee must not be a chairman or member of management or supervisory body of a business organization.

Civil servant and state employee may be a chairman or member of management or supervisory body of a public company, public institution or another legal entity, wherein the State or municipality is the owner, as well as of management and supervisory body of scientific, humanitarian and sports associations.

Restriction upon Termination of Employment

Article 77

Civil servant and/or state employee, within the period of two years upon termination of employment with state authority, cannot:

- Enter employment in the capacity of director, manager or consultant in business organization or another legal entity where a state authority, which used to employ civil servant and/or state employee, carried out audit- or control-related activities;

- Enter into contractual relations or other form of business cooperation with the state authority that he was employed with;
- Use, for the purpose of acquiring benefit for himself or his related person, knowledge and information he acquired while working for the state authority.

Application of Regulations on Preventing the Conflict of Interest of Public Functionaries

Article 78

Provisions of Articles 72, 73 and 77 of this Law shall not apply to civil servants that the law regulating the prevention of conflict of interest of public functionaries applies to.

Protection of Civil Servants and State Employees Reporting Suspicion of Corruption (Whistleblower Protection)

Article 79

Civil servant and/or state employee, having made denunciation to a competent authority, after he learnt, in the course of performing the tasks, that a criminal offence against official duty or criminal offence or act with elements of corruption was committed, shall be obliged to inform his immediate manager in writing about denunciation.

The immediate manager referred to in paragraph 1 of this Article shall be obliged to take all measures to ensure the anonymity, protection against all forms of discrimination, suspension, and restriction or denial of the rights determined by this Law, as well as against termination of employment, of the civil servant and/or state employee who acted in accordance with paragraph 1 of this Article.

Burden of Proof

Article 80

In case of conducting litigation due to the violation of any of the rights of civil servant and/or state employee referred to in Article 79 of this Law, the burden of proof shall be on the authority that made a decision violating the employee’s rights.

V LIABILITY OF CIVIL SERVANT AND STATE EMPLOYEE

1) **Disciplinary Liability of Civil Servant and State Employee**

Ground for Disciplinary Liability

Article 81

Civil servant and state employee shall be disciplinary liable for violations of official duty arising from employment that may be minor and severe.

The issues of disciplinary liability and disciplinary procedure for certain civil servants and state employees may be regulated otherwise by law.

Liability for criminal offence or misdemeanour offence shall not exclude disciplinary liability.

Termination of Employment by Operation of Law
Article 123

Employment of civil servant and/or state employee shall terminate by operation of law:

- When he turns 67 years of age and at least 15 years of contributing to insurance – on the day of submitting the final decision to the civil servant and/or state employee;
- If the working capacity is lost – on the day of submitting the final and non-appealable decision on determining the loss of working capacity;
- If he does not pass the professional examination for work in state authorities within one year from the day of entering employment or from the day of reassignment;
- If it is determined that he does not meet general requirements for entering employment with a state authority – on the day of determining it;
- In the cases referred to in Article 131, paragraph 3, and Article 132, paragraph 1 of this Law;
- If he fails to show satisfactory performance during trial period;
- If he gets two consecutive times an unsatisfactory grade, in accordance with Article 110, paragraph 6 of this Law;
- If a measure of termination of employment is imposed on him in the disciplinary procedure;
- If upon cessation of reasons for suspension of labour-based rights referred to in Article 62 of this Law, he fails to start working within 30 days;
- If he refuses reassignment or fails, unjustifiably, to start working at a job position that he is reassigned to, on a day the decision becomes final;
- If he is forbidden, in accordance with law, by final and non-appealable court decision or decision of another authority, to perform certain activities, and he cannot be reassigned to other activities - on the day of submitting a final and non-appealable decision;
- If he is sentenced by a final and non-appealable judgment to an imprisonment sentence of at least six months - on the day the judgment becomes final and non-appealable;
- If a safety measure, corrective or protective measure is imposed on him, lasting more than six months, due to which he must be absent from work –on the day this measure starts to apply.

Termination of Term of Office of Person belonging to Senior Management Staff
Article 133

Term of office of a person belonging to senior management staff shall terminate, if a state authority is abolished or some tasks not assumed by another state authority are abolished or if his job position is abolished by the adoption of a new internal organization and systematization act or amendments thereto.

In the case referred to in paragraph 1 of this Article, a person belonging to senior management staff shall exercise the rights referred to in Article 56, paragraphs 3 and 4 of this Law.

BANKING LAW
(OGM 17/08 and 44/10)

Scope and Purpose of the Law
Article 1

This Law governs foundation, management, operations and supervision of banks and micro-credit financial institutions and credit unions and it governs the conditions and supervision of operations of parties involved in credit and guarantee operations with the purpose of establishing and maintaining safe and sound banking system that provides protection of interests of depositors and other creditors.

Qualified Participation in a Bank
Article 9

No legal or natural person may acquire qualified participation in a bank without prior approval of the Central Bank.
A party with qualified participation may not further increase participation in capital or voting rights in a bank, on the basis of which it acquires 20%, 33%, or 50% or more of participation in voting rights or in capital of the bank, without the prior approval of the Central Bank.
A group of related parties related pursuant to Article 3 point 8) indents 1 to 5 of this Law, shall be deemed as one acquirer of participation in a bank capital and/or voting rights..

Legal Consequences of Illegal Acquisition of Qualified Participation
Article 14

A party referred to in article 13 paragraph 3 of this Law may not exercise voting rights above the level of voting rights which the party has had prior to the acquisition or increase of qualified participation in a bank nor exercise the right to dividend payment on the basis of the shares acquired in such way until it obtains appropriate approval of the Central Bank.

The Central Bank shall order a party, which does not submit request for granting the appropriate approval within the timeframe referred to in article 13 paragraph 3 of this Law, or the request for granting the approval is denied, to dispose of shares within the timeframe that may not be shorter than three or longer than six months, on the basis of which such party would exercise rights above the level of qualified participation for which it has had appropriate approval of the Central Bank.
If illegal acquirer of shares does not alienate the shares within the time period specified in the decision of the Central Bank, such illegally acquired shares shall become shares carrying no voting rights until their alienation.
If shares referred to in paragraph 2 above are alienated, the new legal acquirer of such shares shall acquire all rights on the basis of these shares.

Application for a Bank License
Article 21

The bank founders shall submit to the Central Bank the application for a bank license, supported by the following documents:

1) authorization for a person which will cooperate with the Central Bank in the procedure of discussions on the application for a bank license;
2) proposal of the bylaws;
3) statement of the founders on the financial amount of the founding capital and evidences on sources of these funds;
4) documents and information on legal persons with qualified participation in a bank, which specifically contain a statement of registration or other appropriate statement from public register, financial reports for the last three years with authorized external auditor opinion, bank related parties and their connected interest, including data on parties that have significant influence based on ownership, or in any other way, on the operations of such group of related parties;

5) appropriate document of the supervisory authority that there are on obstacles for a foreign bank or other financial institution to be founder of a bank;
6) documents, data and information on natural persons with qualified participation in a bank, which specifically contain their names and addresses of permanent or temporary place of residence and other identification data, appropriate evidence on sources of financial amount of founding capital, bank related parties and their connected interest;
7) biography data on proposed members of the board of directors that as a minimum contain the following: information on identification, professional qualifications and working experience and information on their achieved and planned education;
8) business plan of the bank for the first three years, which specifically contains an overall strategy of a bank, expected targeted market, projections of the balance sheet and income statement and cash flow projections;
9) proposal of a strategy for capital management and strategy for risk management in a bank;
10) documentation on technical capabilities and organizational structure, which specifically contains evidence on the use of business premise and equipment required for the performance of projected activities, proposal of rules and regulations on organization and job position scheme, and detailed description of organization of accounting and IT support.

Besides the documentation referred to in paragraph 1 of this article the Central Bank may require the bank to submit additional information and data.

Deadline for Deciding
Article 27

The Central Bank shall reach its decision on the approvals referred to in this law within 60 days as of the day the application for obtaining approval has been orderly submitted, unless other timeframes has been stipulated by this law.

The Central Bank shall prescribe in its regulation the documentation that is submitted together with the application for obtaining approval referred to in paragraph 1 above, and which is not prescribed in accordance with this Law.

Board of Directors
Article 30

The Board of Directors shall govern a bank and oversee its business activities.

Foreign citizens may be elected members of the Board of Directors.

The Board of Directors shall have at least five members, provided that at least two members of the Board of Directors must be persons independent from the Bank.

A person independent from the bank shall be considered a person:
1) not holding a qualified participation in the bank or in a superior company in the banking group to which the bank belongs;
2) that has not been employed in that bank or its subsidiary in the last three years.

Employees of the bank may not be members of the Board of Directors.

By way of exception from paragraph 5 of this Article, executive directors of the bank may be members of the Board of Directors, provided that the total number of the executive directors in the Board of Directors may not exceed one third of the total number of the members of the Board of Directors.
Chairman of the Board of Directors shall be elected by the Board of Directors from among their members.
Executive director cannot be elected chairman of the Board of Directors.
The chairman and members of the Board of Directors shall be elected for the period of four years and they may be re-elected.

A member of the Board of Directors may only be a person holding a university degree, of recognized personal reputation and professional qualifications, professional ability and experience in managing a bank by applying the rules of prudent business, unless otherwise restricted by provisions of Article 31 of this law.
The Central Bank shall prescribe detailed requirements under paragraph 10 of this Article.

Executive Directors
Article 36

A bank shall have at least two executive directors, of which one shall be the Chief Executive Officer.
Only a person holding a university degree, of recognized personal reputation and professional qualifications, professional ability and experience at managerial positions in a bank or in the financial sector may be elected executive director, provided that there are no obstacles set out in Article 31 hereof to his/her election.
Foreign citizens may be elected executive directors, and at least one executive director must speak the language that is in official use in Montenegro.
Executive directors shall be full-time employees of the bank.

Approval for the Executive Director Election
Article 37

A person that has obtained prior approval of the Central Bank may be elected executive director.
The evidence to prove the meeting of the election requirements under Article 36 of this law must be submitted together with the request for granting the approval for the election of the executive director.
When deciding on granting the approval for the election of the executive director, the Central Bank may require the prospective candidate to submit the presentation on managing bank’s operations.
The Central Bank shall issue approval under paragraph 1 above if, based on the evidence under paragraph 2 above, presentation under paragraph 3 above and other information available, it evaluates that the prospective candidate meets the requirements for his/her election as the executive director of the bank.
The approval of the Central Bank under paragraph 1 above shall be the condition for the registration in the CRCC.
The Central Bank shall revoke the approval under paragraph 1 above if it has been issued on the basis of incorrect data or if the executive director does not meet the requirements based on which the approval has been issued.
The approval referred to in paragraph 1 above shall cease to be valid if:

1) the approved person is not elected within 30 days following the approval, or the approved person has not started to perform its function;
2) on the day of the termination of the executive director function;
3) an executive director’s employment contract with a bank expires as of the day of the contract expiry.

Entities Subject to Supervision
Article 105

In the performance of its supervisory role, the Central Bank shall supervise:
1) banks;
2) foreign bank branches;

3) micro-credit financial institutions and credit unions and other parties licensed by the Central Bank, and
4) parties involved in credit and guarantee operations

Responsibilities for Performing Supervision

Article 106

The Central Bank shall perform the supervision of the banks' operations, in accordance with the law and internationally accepted standards of efficient bank supervision, with a view to establishing and maintaining a sound banking system and protecting depositors and other creditors of banks, by evaluating their capacity to manage risks and compliance of their operations with the law and the Central Bank's regulations.

The members of the Council of the Central Bank, authorized examiners and other employees in the Central Bank as well as agents, interim administrators, external auditors and any party retained by the Central Bank in connection with the exercise of its functions under this law shall not be held liable for damage that might incur during the performance of duties in accordance with the law and regulations enacted on the basis of the law, unless it has been proved that the particular action has been performed deliberately or by negligence.

The expenses of the court protection of the persons referred to in paragraph 2 above shall be covered by the Central Bank for all disputes arising from the execution of duties referred to in paragraph 1 above.

Cooperation with Other Institutions

Article 107

In performing its supervisory function, the Central Bank shall cooperate with representatives of foreign institutions responsible for bank supervision and with domestic authorities and institutions responsible for the supervision of financial operations, with which it has concluded appropriate cooperation and confidentiality agreements regarding the exchange of information.

The exchange of information referred to in paragraph 1 above shall not be considered as revealing a secret

Methods of Supervision

Article 109

The Central Bank shall perform the supervision referred to in Article 105 above by:

1) analyzing the reports, information and data that the banks deliver to the Central Bank in accordance with the law and the Central Bank regulations, information and data that the banks deliver at the Central Bank's request and other data on banks' operations available to the Central Bank;
2) direct review of business books, accounting and other documentation in banks and their counterparts in the supervised transactions.

Authorized Examiners

Article 110

The bank supervision shall be performed by employees of the Central Bank, authorized for the conduct of such duties by the Central Bank.

Notwithstanding paragraph 1 above, the Central Bank may also hire non-employees of the Central Bank to perform individual duties in the process of bank supervision.

Examination Notice

Article 111

The Central Bank shall inform a bank of a planned direct – on site examination, as a rule, ten working days before the examination commences.

Notwithstanding paragraph 1 above, if the reports and information held by the Central Bank indicate that there are irregularities that may be relevant to the safe and sound operations of the bank, an on-site examination may start without a prior notice.

Bank's Obligations during Examination Procedure
Article 112

The bank shall enable the Central Bank's authorized examiners a free insight in business books, other business documentation and records, insight in the functioning of information technology and computer database, and it shall provide, upon the request of authorized examiners, copies of business books, other business documentation and records, in hard and/or electronic copy.

Process of Imposing Measures against Bank
Article 115

If a bank fails to submit objections to the examination report within the prescribed time frame or fails to provide reasonable grounds for its objections to the report or addition to the report that states irregularities in the bank's operations, the Central Bank shall impose measures for removal of the irregularities against that bank.

The irregularities in a bank's operations, within the meaning of this Law, shall be considered:

1) inadequate managing of risks to which the bank is exposed in its operations;
2) bank's action and/or failure to act which is not in accordance with the law and regulations passed on the basis of the law;
3) applying unsafe or unsound banking practices.

Unsafe or unsound banking practice referred to in paragraph 2 point 3) above shall mean every action or failure to act which is contrary to the generally accepted standards of prudent banking operations and the consequences of which, in case of a continuing risk, could result in loss or damage to the bank.

Notwithstanding paragraph 1 above, the Central Bank may impose measures for the removal of the found irregularities during an on-site examination, if:

1) the bank has been found to violate the law or other regulations to the extent that necessitates urgent removal of those irregularities;
2) the bank's financial condition is assessed as threatening the bank's further existence.

Types of Measures
Article 116

If the Central Bank establishes irregularities in the bank's operations, it may take one of the following measures:"

1) warn the bank in writing about the irregularities found and request the bank to undertake one or more activities to remove the irregularities;
2) conclude a written agreement with the bank making the bank bound to remove the irregularities found within a specified time;
3) issue an order imposing one or more of the following measures:
    - order the bank to remove the irregularities found in its operations and/or undertake other activities to improve the condition in the bank;
    - order the bank to scale down or cease one or more of the activities that, as the Central Bank has established, caused losses for the bank or are contrary to best banking practices;
    - order the bank to establish stricter limits in operations than prescribed by the Central Bank or the bank's policies;
    - order a bank classification of assets based on the exposure to credit risk in riskier group,
    - order a bank to establish adequate reserves for losses based on country risk;
    - order the bank to increase the amount of own funds, ensure higher solvency ratio and/or other capital adequacy indicators than those prescribed if one or more conditions under Article 71 above are met;
    - order a bank to discharge a member of the Board of Directors, an executive director or an official with special powers and responsibilities and set the timeframe for conducting the procedure of their relieving of duty and, as a rule, prohibit these persons to further perform their functions until the completion of the ordered procedure;

- revoke the previously granted approval to a board of directors member;
- order the bank to prepare capital restoration plan acceptable to the Central Bank, within 60 days;
- order the bank to reduce overhead expenses, including the imposing of restrictions to salaries and other benefits of the bank's executive directors and other officials with special powers and responsibilities;
- order that all deposit interest rates do not exceed market prevailing interest rates for comparable amounts and maturities;
- order the bank to require from its subsidiary to reduce the intensity of or cease the activity which is deemed by the Central Bank to have caused significant losses for the bank or to represent a large risk to the bank;
- prohibit or restrict the growth of the bank's assets;

- order the bank to sell a part of its assets;

- prohibit further investments in other legal persons;

- order the bank to terminate an outsourcing agreement that poses a high operational risk to the bank.

- temporarily prohibit the performance of certain or all activities

- temporarily prohibit or restrict the opening of new organisational units or the introduction of new products,

- temporarily prohibit the acceptance of new deposits and other repayable funds,

- temporarily prohibit dividend or any other profit payment,

- order the bank to discontinue applying unsafe or unsound banking practices,

- order the bank to conduct measures aimed at ensuring safe and efficient payment system, including the prohibition of disposing of funds in an account and measures of prohibiting crediting or debiting the account;

- order the bank to pass and enforce measures for: improving the procedure of collection of due claims, proper evaluation of balance sheet and off-balance sheet items, improve its accounting and information system and/or improve the system of internal controls and internal audit."

4) pass a decision ordering the bank to prepare a plan to improve the condition of the bank, which must contain detailed measures and activities taken by the bank to provide adequate management of risks the bank is exposed to in its operations and/or to remove the identified irregularities, as well as timeframes for their implementation."

5) institute interim administration in the bank in accordance with Article 120 of this Law.

6) revoke the bank's license.

The bank shall submit to the Central Bank for its approval the plan for the improvement of the bank condition prepared in accordance with provisions under paragraph 1 point 4) above.

In the course of the procedure of granting the approval under paragraph 2 above, the Central Bank may require the bank to make amendments to the plan.

If the bank's own funds, solvency ratio and/or other indicators of the bank's capital adequacy are below the prescribed levels, the Central Bank may, before taking other measures provided in this law, prohibit the bank, by way of an order, to engage in one or more activities specified in the respective bank licence or approval issued by the Central Bank.

The provisions of Article 114 above shall not apply in the procedure of imposing measures referred to in paragraph 4 above.

.

Assumptions for Choosing Measures against Banks

Article 117

In deciding which measures will be undertaken towards a bank, the following shall be considered:

1) the assessment of impact of the found irregularities on:
   - the current and future financial position of the bank;
   - the bank's exposure to individual types of risks;
2) number and degree of difficulty of the found irregularities, and number, frequency and duration of irregularities found in previous operations of the bank;
3) the assessment of readiness and capability of the bank's bodies and management to remove the found irregularities based on the evaluation of:
   - the capability of the bank's bodies and management to manage risks in the bank's operations;
   - efficiency of internal control systems in the bank;
   - efficiency of the bank's bodies and management in the removal of earlier irregularities found in the bank's operations;
   - degree of cooperation of the bank's management with authorized examiners during the bank's examination;
4) the assessment of the degree of impact of the found irregularities on the financial discipline, safety and stability of the banking system.

Request for Granting Approval for Branch Operations
Article 140

Request for granting the approval for branch operations shall be submitted to the Central Bank.
The following documents shall be submitted with the request referred to in paragraph 1 above:

1) statement from appropriate register of a country in which head office of a foreign bank is located, which cannot be older than 30 days;
2) bylaws or other appropriate documents of a foreign bank;
3) policies and procedures of the foreign bank on risk management;
4) information on members of board of directors and other foreign bank bodies;
5) financial statements of a foreign bank for the last three years with external auditor's opinion;
6) evidence on long-term credit rating of a foreign bank, determined by an internationally recognized rating agency;
7) description of operations that a branch will conduct and a business plan for the following three years of operations;
8) information on foreign bank owners;
9) documents and information on foreign bank shareholders, legal entities owning more than 5% of voting stock, which specifically contain a statement of registration or other appropriate statement from public register, bank related parties and their connected interest;
10) documents, data and information on foreign bank shareholders, natural persons owning more than 5% of voting stock, which specifically contain their names and addresses of permanent or temporary place of residence and other identification data, bank related parties and their connected interest;
11) evidence that a foreign bank is included in a deposit protection system and information on the amount of protected deposit, as well as an evidence that a branch will be included in the deposit

protection system in the country of a foreign bank to the level and extent of coverage prescribed for banks operating in Montenegro, but it will not exceed such level;

12) document of supervisory authority of a country in which head office of a foreign bank is located, which gives approval to a foreign bank to start with operations in Montenegro through a branch or appropriate document of such authority that such approval is not required pursuant to the regulations of that country;
13) data and information on persons who will conduct branch operations;
14) documentation on business premise and technical capabilities for branch operation.

The Central Bank may request a foreign bank to submit additional data and information in the procedure of issuing the approval referred to in paragraph 1 above.

Operations and Supervision of Branch Operations
Article 148

The provisions of this law governing banking secret (articles 84 through 86), protection of clients (articles 87 through 92) and the manner and procedure of bank supervision (articles 108 through 114) shall be also applied to foreign bank branches.

Measures against MFI
Article 154

If it determines that an MFI has acted contrary to the regulations or acts of its business policy, or has entered into unsafe and unsound operations, the Central Bank may:

1) warn the MFI in writing;
2) conclude a written agreement with the MFI which will oblige the MFI to eliminate the found irregularities within a specified period of time;
3) order the MFI to eliminate the irregularities found and comply its operations with the regulations;
4) order temporary suspension for a member of the bodies, a body or management of the MFI.

The resolution referred to in paragraph 1 point 3 above shall be final.

The administrative proceedings may be brought against the resolution referred to in paragraph 1 point 3 above.

Revoking a License
Article 155

The Central Bank shall revoke a license of an MFI:

1) when the MFI fails to start its operations within six months as of the date of its registration with the CRCC;
2) when the MFI fails to act under the orders referred to in Article 154, point 3 below;
3) when the MFI has been included in illegal activities;
4) when the authorized examiners of the Central Bank are hindered in their examination of the MFI or the submission of the requested documentation is disabled or avoided;
5) when the MFI submits false statements of its operations to the Central Bank.

The Central Bank shall revoke a license of an MFI when it finds that the license was issued on the basis of false data.

The resolution on revoking the license of an MFI shall be final and shall be published in the "Official Gazette of Montenegro".

The administrative proceedings may be brought against the resolution referred to in paragraph 3 above.

Operations and Supervision of MFI

Article 157

Provisions of this law governing granting a license to a bank (articles 21 through 24), banking secret (articles 84 through 86), protection of clients (articles 87 through 92) and the manner and procedure of bank supervision (articles 108 through 114) shall also be applied to MFIs.
Minimum standards for risk management in MFI shall be prescribed by the Central Bank regulation.

Operations and Supervision of Credit Unions

Article 163

The provisions of this Law relating to the operations and supervision of banks shall also apply to the credit unions, unless otherwise prescribed by a Central Bank's regulation.

Conditions for Performing Credit and Guarantee Operations

Article 164

Legal persons that obtain appropriate approval of the Central Bank for performing the credit and guarantee operations may engage in such operations.

The Central Bank shall reach a decision on the request for granting the approval referred to in paragraph 1 above within 120 days after its submission.

The conditions for granting the approval referred to in paragraph 1 above, as well as the minimum founding capital, operations, supervision and revoking the approval referred to in paragraph 1 above shall be prescribed in the regulation of the Central Bank.

Pursuant to Article 88, item 2 of the Constitution of the Republic of Montenegro I hereby pass the

DECREE
PROMULGATING THE LAW ON BUSINESS ORGANIZATIONS

I hereby promulgate the Law on Business Organizations adopted by the Parliament of the Republic of Montenegro at the sitting of the first extraordinary session in 2002, held on 29 January 2002.

Number: 01-265/2
Podgorica, 31 January 2002
President of the Republic of Montenegro
Milo Djukanovic, m.p.

LAW ON BUSINESS ORGANIZATIONS

(Official Gazette of the Republic of Montenegro 06/02 of 8 February 2002, Official Gazette of Montenegro 17/07 of 31 December 2007, 80/08 of 26 December 2008, 40/10 of 22 July 2010, 36/11 of 27 July 2011)

Concept and Constitution
Article 6

(1) General partnership shall mean the relationship which subsists between persons carrying on a business in common with a view of gain. All partnerships that are not limited partnerships shall be general partnerships.
(2) A general partnership may arise by operation of law, may be based upon the facts and conduct of the individuals.

(3) Persons who have entered into partnership with one another shall be called partners and collectively a firm.
(4) A general partner may be natural or legal person.
(5) A general partner shall have unlimited joint and several liability.
(6) A general partnership shall be registered by submitting a registration statement with the Central Registry for statistical purposes; however, the existence of a partnership is not conditioned on the registration. The registration statement shall state the name of the general partnership, the names of partners, their addresses and personal identification numbers (JMBG). The partnership agreement, if any, may be filed by the partners with the Central Registry.

Initial Registration of Limited Partnership
Article 12

(1) The registration of a limited partnership shall be done by submitting to the Central Registry a statement or contract signed by all partners containing the following data:
1) The partnership name and indication that the partnership is established as limited partnership;
2) The registered office of the partnership;
3) The term, if any, for which the partnership is entered into, and the date of its commencement;
4) The first name, last name and personal identification number, or name of each of the partners;
5) The name of every limited partner as such;
6) The sum contributed by each limited partner, and whether paid in cash or otherwise.

Initial Registration
Article 21

(1) The following documents and data must be submitted to the Central Registry for the first registration of a joint stock company:
1) The foundation agreement;

2) The charter and a special act, if the charter does not contain the data referred to in Article 19, paragraph 3 of this Law;
3) A list of members of the Board of Directors:
4) The first and land names, and in case of change of firs/last name any former name of the member of the Board of Directors, and dates and places of their birth;
5) Their personal identification numbers;
6) Permanent or temporary residence of the members of the Board of Directors;
7) Statements of the members of the Board of Directors indicating their citizenship;
8) Business occupation of the members of the Board of Directors;
9) Data on any other directorships or positions held in Montenegro or elsewhere and the place of registration of such companies if not in Montenegro;
10) Name and address of the Executive Director, Secretary of Company, and auditor;
11) The name of the company and the address of its registered office or address for receiving official notices;
12) The signed consent of the members of the Board of Directors, the Executive Director, the Secretary of Company, and the auditor to their appointments;
13) The Decision of the Securities Commission approving the prospectus for initial offering of shares as well as the decision of the Securities Commission confirming the successfulness of the issue, or the decision of the Securities Commission on recording the initial issue of shares in the case of a private joint stock company;
14) The proof of the payment of the appropriate fee.
(2) The registration documents shall indicate whether persons authorized to represent the company either as a body or as individuals may act alone or jointly.
(3) The company shall acquire the status of a legal person on the day of its registration with the Central Registry. The registration is evidenced by the issuance of a registration certificate.
(4) The Central Registry shall publish in the Official Gazette of Montenegro the data on company's name and registered office, the names of the members of managing bodies, Executive Director, Secretary of Company, auditor, as well as the date of concluding the foundation agreement, the date of adopting the charter, and the date of registration.

Obligation to Submit Data and Inform the Public
Article 28

(1) Joint-stock company shall submit to the Central Registry, which shall submit to the Official Gazette of Montenegro for publication, the following documents and data, in accordance with paragraph 2 of this Article:
1) any amendments to the charter, a special act referred to in Article 19, paragraph 3 of this Law if the charter does not contain the data from that act, the foundation agreement and any extension of the duration of the company;
2) any change in the company name and the registered office or address for receiving official notices;
3) the appointment, termination of office and data about the persons who are authorized to represent the company in dealings with third parties, as well as the data whether the persons authorized to represent the company may do so jointly or alone;
4) the appointment, termination of office and data of the Executive Director, Secretary of Company, and the auditor;
5) the decision of the general meeting of shareholders on liquidation of the company;
6) the decision on appointment of a liquidator, his identity, qualifications and powers other than those set out in this Law or in the charter;
7) the financial reports, including the auditor's report.

(2) In the Official Gazette of Montenegro, in addition to the data, names of the documents shall be published which also contain the notice that the documents are filed in the Central Registry.
(3) Joint stock company shall be obliged to submit to the Central Registry all amendments made to the foundation agreement, the charter or any other document or data determined by the provisions of this

Law within 7 business days from the day of their adoption. The Secretary of Company shall be responsible for the submission of the aforementioned documents and data.
(4) After every amendment to the charter or the foundation agreement, the complete text shall be submitted to the Central Registry. Amendments to the charter or the foundation agreement shall be valid only when registered.
(5) The documents and data shall be binding upon the company towards third persons from the day of their publication in the Official Gazette of Montenegro, unless the company proves that the third parties had knowledge of them. The documents and data shall not be binding upon good faith third parties regarding transactions executed within 16 days from the day of publication of the documents and data, who can prove that they did not know or could not have known about their publication.
(6) There must not be any discrepancy between what is published and what has been filed in the Central Registry. If there is such a discrepancy, the text on file at the Central Registry shall be controlling. The published text may not be asserted by the company as a defense against third parties relying on the text in the Central Registry. However, third parties may rely on such published text unless the company proves that they had knowledge of the text filed in the Central Registry.

Shares
Article 52

(1) A share shall mean an equity interest in a company consisting of a right to participate in the distribution of its gain and other rights defined by this Law and a company‟s charter. In Montenegro shares shall be issued, transferred and kept in dematerialized form and shall exist in electronic form in the information system of the Central Depositary Agency (hereinafter referred to as: the CDA).
(2) The issuance of and trading in shares of a joint-stock company shall be carried out in accordance with the Law on Securities.
(3) A share shall not be divisible into smaller parts. If a share is held by several persons, all its holders shall be considered as a single shareholder. The rights carried by the share shall be exercised by one of the holders by a general agreement. All holders of a share shall be, without limit, severally and jointly liable for the shareholders‟ obligations.
(4) The initial, i.e. nominal as well as market value of a share shall be denominated in Euro.
(5) Shares of joint-stock companies shall be issued in the name of the holder and must be registered with the Securities Commission and the CDA.
(6) It is possible to acquire the shares of a company in bankruptcy proceedings.
(7) Shares shall be classified by the rights they carry. The rights shall be specified in the charter of the company or in a separate legal document which is adopted when new shares are issued.
(8) Subscription, issuance, registration, ownership, proof of ownership, public offering and transfer of shares, insider trading or security market abuses shall be regulated by the Law on Securities.

Membership in the Limited Liability Company
Article 65

(1) One or more persons may found a limited liability company.
(2) A limited liability company must limit the maximum number of its members to 30.
(3) The charter of a limited liability company shall restrict the transfer of its parts. A limited liability company shall not have the right to issue a public invitation subscription of any of its parts.

Initial Registration
Article 70

(1) The following documents and data shall be submitted to the Central Registry and published at the first registration of a limited liability company:
1) the foundation agreement;
2) the charter;

3) a list of founders, members of the company, managers and members of the Board of Directors, if appointed, including--
a) the first and last names and former names in case of change of the first/last name;
b) the date and place of birth of members of the Board of Directors, their personal identification number, or passport number if a foreign national;
c) the permanent or temporary residence of the members of the Board of Directors;
d) the statement of the members of the Board of Directors regarding their citizenship;
e) data on any other company memberships, directorships or other functions held in Montenegro or elsewhere, as well as the place of registration of such companies if not in Montenegro;
4) the name of the Executive Director;
5) the name of company, the address of the registered office and address of place for receipt of official notices, if different;
6) persons authorized to represent the company either jointly or individually;
7) the signed consent of the members of the Board of Directors to their appointments, if any;
8) a document confirming payment of the registration fee.
(2) The company shall acquire the status of a legal person on the day of its registration. The issuance of a registration certificate by the Tax Administration shall be the evidence of registration.
(3) The Central Registry shall publish in the Official Gazette of Montenegro the data on company's name and registered office, name of Executive Director, names of members of the Board of Directors, if appointed, date of adoption of foundation agreement and charter, as well as date of the registration.
(4) Publication of documents in the Official Gazette of Montenegro shall be by reference to the document in question.
(5) All amendments to the foundation agreement, the charter or any other documents or data which a limited liability company is obliged to file, in accordance with this Law, with the Central Registry shall be submitted within seven working days from the day the amendments have been made. The submission of data shall be within the competence of the Executive Director or another designee.
(6) After every amendment of the charter or the foundation agreement, the complete text as amended shall be submitted to the Central Registry. Amendments to the charter or the foundation agreement shall come into force on the day of their registration.
(7) The documents and data submitted to the Central Registry shall be binding on the company in relation to third parties from the day of their publication in the Official Gazette of Montenegro, unless the company proves that the third parties had knowledge of them. With regard to transactions taking place within sixteen days following the publication of documents and data, the documents and data shall not be binding on good faith third parties who can prove that they did now know and could not have known about their publication.
(8) There must not be discrepancy between what is published and what has been filed in the Central Registry. If there is a discrepancy the published text cannot be relied on as against third parties. Third parties may, however, rely on such text unless the company proves that they had knowledge of the text filed in the Central Registry.

Transfer of Parts
Article 74

(1) The parts of a limited liability company may be transferred only in accordance with the provisions established in the charter. These parts shall not be registered with the Securities Commission and the CDA.
(2) A part may be transferred among members of the company without restriction in conformity with the charter.
(3) Where a member of the company intends to transfer his part, other members of the company and the company itself shall have a preemptive right to purchase the part, in accordance with the charter. Where no agreement to purchase the part is reached between the transferor of the part and other members of the company, the part shall be divided among them proportionately to their current parts in the company, unless otherwise provided in the charter. Where the members and the company itself have declined to purchase the part proposed to be sold within 30 days from the day on which the part was offered, the part may be transferred to a third party under terms no less favorable than the terms offered to the existing members or the company.

(4) If the part is being sold by enforcement procedure, the court shall notify thereof the members of the company and the company. If the members of the company and the company itself fail to express their interest to buy the part within 15 days from the day of receiving the notice, such part shall be sold in accordance with the provisions on enforcement procedure.
(5) In the event of death of natural person or dissolution of a legal person, his part shall be transferred to his heirs or legal successors, unless otherwise provided by the charter. Where the charter prohibits transfer of a part, the charter shall provide that such part be bought by members of the company or the company itself. Where the members of the company or the company itself do not buy the part, the part shall be withdrawn in conformity with the provisions of this Law relating to the reduction of the share capital.
(6) In the event of a part being transferred, the transferor and transferee shall be, without limit, jointly and severally liable to the limited liability company for obligations associated with membership. A part shall be transferred by written agreement.

Central Registry (CRPS)
Article 83

(1) The Tax Administration shall keep the Central Registry,
(2) The Central Registry shall be located in Podgorica.
(3) The Tax Administration shall make registrations in the Central Registry based on the Registration Application, attached thereto shall be the documents set forth by this Law.
(4) The registration application may be lodger in regional offices of the Tax Administration.
(5) The data and documentation submitted to the Central Registry shall be kept in a single, information database.
(6) The Central Registry database may be inspected six hours per day on each business day.
(7) During the inspection period, any person may view, transcribe, or copy the abstract from the Registry and the documents submitted to the Central Registry.
(8) The Tax Administration shall be obliged to issue registration decisions, and certificates of registration expiry, and to receive company constitutional and other documents being registered in accordance with this Law even during the time envisaged for the inspection period.
(10) Inspection of the Central Registry‟s data shall also be possible through electronic means of communication including its website.

CENTRAL BANK OF MONTENEGRO LAW
(Official Gazette of Montenegro 44/10, 46/10, 6/13)

Definitions
Article 2

Terms and definitions used in this Law shall have the following meanings:
1) **"bank"** is a legal person which performs banking operations with the permission or the approval of the Central Bank of Montenegro (hereinafter: the Central Bank) to perform such operations;
2) **"financial institution"** is a microcredit financial institution, credit union or a party pursuing credit-guarantee operations and which was licensed or authorized by the Central Bank;
3) **"deposit"** is money deposited in an account, with or without interest or other expenses, which is paid on demand or at certain maturity date, depending on the conditions agreed at the time of depositing the funds;
4) **"loan"** is the obligation of a lender to provide funds to a borrower, for a specified or unspecified period of time, earmarked or non-earmarked, and the borrower is obliged to repay the agreed interest and the received amount of funds to the bank at the agreed time and in the agreed manner;
5) **"fiscal agent"** is the function of the Central Bank where it performs operations involving securities issued by Montenegro, the payment of principal, interest and other expenses associated with those securities and other related operations;
6) **"Council of the Central Bank"** is the governing body of the Central Bank in accordance with Article 44 above;
7) **"Governor of the Central Bank"** is the managing body of the Central Bank in accordance with Article 45 hereof;
8) **"Audit Committee"** is the permanent body of the Council of the Central Bank;
9) **"Chief Internal Auditor"** is the person managing the internal audit of the Central bank.

Central Bank Independence
Article 7

The Central Bank shall be independent in pursuing the objectives and exercising the functions under this law.
The Central Bank, members of its bodies and employees in the Central Bank shall be independent in the performance of their functions and their activities established under this and other laws and they may not receive or seek any instruction from the government and other bodies and organisations or any other entities.
The state and other bodies and organizations and other persons may not exert any influence on the performance and decision-making of members of the Central Bank bodies.

International Cooperation
Article 9

The Central Bank may cooperate with other central banks, international financial institutions and organisations (hereinafter: international financial institutions), which scope of activities is related to the objectives and functions of the Central Bank, and it may be a member of international institutions and participate in their work.

Measures against Banks and Financial Institutions
Article 30

In case a bank or a financial institution fails to manage risks to which it is exposed in accordance with the law or in case it acts contrary to the regulations, the Central Bank may impose measures against, and

other obligations on, such a bank or financial institution, including pecuniary fines, in accordance with the law.
The Central Bank may disclose the information on imposed measures referred to in paragraph 1 above.

Submission of Central Bank Report

Article 39

The Central Bank shall submit, as needed, but at least annually and by 30 April of the current year, the report on its prior year's operations to the Parliament of Montenegro (hereinafter: the Parliament) for its consideration.

The report on the Central Bank's operations shall contain information on the economic environment during the reporting year, including the assessment of economic trends in the following year, emphasizing the Central Bank's policy objectives and the condition of the financial system, as a whole. The report shall also include the review and assessment of the Central Bank's policies followed during the reporting year and the description and explanation of the Central Bank's policies to be followed during the following year.

The Central Bank shall also publish reports on financial system stability and price stability matters which it shall submit to the Parliament and to the Government for information purposes, as needed, and at least once a year up to 30 June of the current year for the previous year.

Council Composition
Article 46

The Council shall consist of seven members.
Members of the Council shall be the Governor, the Vice-Governor for the banking system supervision, the Vice-Governor for financial stability and payment systems and four members.
The Governor shall chair the Council meetings.

Article 47

The Vice-Governor for the banking system supervision shall perform operations related to the supervision of the banking system.
In exercising his powers, the Vice-Governor under paragraph 1 above shall propose to the Governor decisions and other acts during the supervision of banks and financial institutions.

Article 48

The Vice-Governor for financial stability and payment systems shall perform operations related to the financial stability and payment system.
In exercising his powers, the Vice-Governor under paragraph 1 above shall propose to the Governor respective decisions and other acts.

Term of Office of Council Members
Article 49

Members of the Council shall be appointed for the period of six years and may not serve more than two terms, in accordance with this law.
A member of the Council whose term of office has expired shall continue to perform his/her function until the appointment of a new member.

Appointment of Council Members
Article 50

Members of the Council shall be appointed by the Parliament.
The Governor shall be appointed by the Parliament, upon the proposal of the President of Montenegro.

The Vice-Governors shall be appointed by the Parliament, upon the proposal of the Governor.
Four members of the Council shall be appointed by the Parliament, upon the proposal of the working body of the Parliament responsible for financial affairs.

Eligibility to Serve on the Council and Incompatibility of Functions
Article 51

A member of the Council must be a person having Montenegrin citizenship, holding a university degree, having a recognized personal reputation and professional experience in economics, banking, finances or law.
A member of the Council may not be a member of a political organisation, a member of the Parliament, a member of the Government or person performing another function or duty as designated by the Parliament or the Government, except a function or a duty in international financial institutions, and he/she may not be performing a function or a duty in any local authority or trade union bodies.
A member of the Council may not be a member of a body, an employee or external associate of a bank, a financial institution, or another legal person subject to supervision of the Central Bank.
A member of the Council may be a person engaged in scientific or research activity, except a person whose work or activity could affect his/her independence or conflict the interests of the Central Bank.
A member of the Council may not hold 5% or more shares or stake in a bank or a financial institution and any other legal person subject to the Central Bank supervision, nor may he/she hold 5% or more shares or stake in an audit firm.
A member of the Council may not be a person for whom it has been established that he/she is subject to provisions of Article 53 hereof prescribing the conditions for the relieving of duty a Council member.

Prevention of Conflict of Interest
Article 52

A member of the Council is obliged to perform his/her function in the Central Bank in the manner so that he/she shall not put his/her personal interest or interests of parties related with him/her before the interests of the Central Bank.

The Council members shall report to the Council on the acquiring of direct or indirect financial interests and those of the related parties, in the manner to be prescribed by the Central Bank.
The Council members shall submit written statements to the Council presenting the facts under Article 51 paragraphs 2 to 6 herein and the report under paragraph 2 above within 15 days following his/her appointment and once a year by the end of February in the current year for the previous year.
When a member of the Council is in any way connected with the subject matter of deciding or if he/she is indirectly or directly interested in that subject matter, the member concerned shall disclose his/her interest at the beginning of the discussion and shall not participate in the discussion and deciding on such a matter, but his/her presence shall be accounted for the purpose of constituting a quorum at the relevant meeting.
Any rights and obligations of the Council members not specified in this law or the Statute shall be subject to provisions of the law governing the prevention of conflict of interest.

Relieving of Duty
Article 53

A member of the Council shall be relieved of duty prior to the expiry of his/her term of office if:
1) it has been established, after his/her appointment, that he/she had been appointed based on inaccurate and/or incorrect information or if any of the circumstance under Article 51 paragraphs 2 to 5 hereof has occurred;

2) he/she has been sentenced to unconditional prison term or convicted of offence which makes him/her unworthy of performing the function of the Council member or if he/she has been subject to the prohibition of further conduct of work or duty imposed by the competent authority;
3) he/she has deliberately or by gross negligence made a serious omission in performing his/her function;
4) he/she has requested the relieving of duty personally;
5) he/she has become a debtor in the bankruptcy proceedings.
A member of the Council may be relieved of duty if he/she has failed to perform his/her duties for a consecutive period of more than three months without the approval of the Council, if he/she has been unable to perform the function because of illness for a consecutive period of more than six months or if he/she has failed to submit or submits a false statement and the report referred to under Article 52 paragraph 3 herein.

A member of the Council may not be relieved of duty for reasons other than those specified under paragraphs 1 and 2 above.

Regulations and Other Acts of the Central Bank
Article 77

The Central Bank shall have the power to pass regulations necessary for the exercising of its functions granted to it under this Law or other laws.
The Central Bank shall pass regulations under paragraph 1 of this Article in the form of decisions.
The Central Bank may also issue binding individual acts.
The Central Bank shall keep records on passed regulations and other acts.

Obligation of Keeping Confidential Information and Data
Article 84

A member of the Council and employees of the Central Bank shall be obliged to keep confidential the information and data which are considered secret in accordance with the law or another act.
The confidentiality obligation under paragraph 1 above shall last after the termination of function and/or of employment in the Central Bank.
Notwithstanding paragraph 1 of this Article, members of the Council and employees may disclose information and data to third parties outside the Central Bank in accordance with the procedure established in the special act of the Central Bank, provided that:
1) the person to whom the information relates has given his/her explicit consent;
2) it represents the provision of assistance to the competent authorities in their enforcement of the law and at a court’s order;
3) they are submitted to the external auditor of the Central Bank;
4) they are given to supervisory authorities of foreign banks and financial institutions and representatives of international financial institutions for the performance of their official duties;
5) the interest of the Central Bank in court proceedings requires the disclosure of such information and data.

Rights and Obligations of Employees
Article 87

General labour regulations shall apply to the rights and obligations of employees of the Central Bank, unless otherwise specified under this law.
The Governor shall decide on the employment in the Central Bank.
Employees of the Central Bank may not perform any activity for another employer, except based on a special approval of the Governor and provided that it is not contrary to the interests of the Central Bank.
Employees may not be guided by their political affiliations in performing their operations.
The Central Bank may open accounts for its employees.
The Central Bank may grant loans to its employees in accordance with the general act.

CLASSIFIED INFORMATION LAW

Article 12

Grounds for deciding on level of classification of information shall be its content and its importance for the security of Montenegro or its political or economical interests

A TOP SECRET classification shall be applied to classified information the disclosure of which would do irreparable damage to the security and interests of Montenegro;

A SECRET classification shall be applied to classified information the disclosure of which could seriously harm the security or interests of Montenegro;

A CONFIDENTIAL classification shall be applied to classified information the disclosure of which could harm the security or interests of Montenegro;

A RESTRICTED classification shall be applied to classified information the disclosure of which could harm the performance of tasks of an Body.

Article 14

Authorised persons for deciding on level of classification of information »TOP SECRET« are: President of Montenegro, President of Parliament of Montenegro, Prime Minister and members of Government of of Montenegro, director of the state administration agency competent for police affairs, director of state administration of state for loudry many, director of state administration Agency competent for national security affairs (hereinafter : Agency), supreme state prosecutor and president of the supreme court .

Pursuant to Article 88 paragraph 2 of the Constitution of the Republic of Montenegro, I hereby pass the

DECREE ON PROMULGATION

OF THE LAW ON GAMES OF CHANCE

(“Official Gazette of the Republic of Montenegro”, No. 52/04 of 2 August 2004

and “Official Gazette of Montenegro”, No. 13/07 of 18 December 2007)

This is to promulgate the Law on Games of Chance, adopted by the Parliament of the Republic of Montenegro at the seventh meeting of its first regular session in the year 2004, held on 28 July 2004.

Number: 01-074/2

Podgorica, 30 July 2004

President of the Republic of Montenegro

Filip Vujanović, signed

LAW ON GAMES OF CHANCE

Article 4

Individual expressions used in this Law shall have the following meanings:

1) lottery games of chance shall be the games organized by public drawings with a pre-defined winning fund;

2) lottery shall be the game in which a player holds a lottery ticket issued by the game operator, which, in line with the game rules, has a pre-printed number. The lottery ticket shall be a winning one if a certain part of the number or the entire number appearing on the lottery ticket is drawn in a public lottery draw held at a pre-defined date;

3) express lottery shall be the game in which a player has a lottery ticket issued by the game operator, which, in line with the game rules, has a pre-printed type and amount of prize or a certain number, covered by a protective screen. The lottery ticket shall be a winning one if it bears the prize, symbol or number, which, in line with the game rules, indicates the reward;

4) instant lottery shall be the game in which a player holds an instant lottery ticket issued by the game operator, which, in line with the game rules, has a pre-printed type and value of the prize, or a certain number or a symbol, covered by a protective wrapping or a protective screen, which the player removes by opening the wrapping or scratching off the screen. The instant lottery ticket shall be a winning one if it shows the prize or the number or the symbol previously designated as the winning one, in line with rules of the game;

5) sports pool shall be the game in which a player takes part by filling in a ticket, issued by the game operator, with pre-printed pairs of opponents in matches and guesses the results of the matches on the ticket for each pair, using symbols defined by the game rules. The ticket shall be a winning one if the player guessed well all the results or as many results as required by the game rules, and if the symbols have been properly filled in or the required result symbols crossed on the ticket, or the coupon, and if other conditions set by the game rules have been met;

5a) toto shall be the game in which a player takes part by filling in a ticket, issued by the game operator, with pre-printed pairs of opponents in matches, and guesses the results of football matches on the ticket for each pair, using symbols or designations defined by rules of the game. The ticket shall be a winning one if the player guessed well all the results or as many results as required by rules of the game, and if the symbols have been properly filled in or the required result symbols crossed on the ticket, or the coupon, and if other conditions set by rules of the game have been met;

6) lotto, keno and similar games shall be the games in which a player fills in a ticket, issued by the game operator, with pre-printed numbers, in line with rules of the game, with the intention to guess a certain group of numbers, crossing them at his own choice. The ticket shall be a winning one if all the numbers or some of the numbers crossed on the ticket match the numbers drawn in a public draw and if other conditions set by rules of the game have been met;

7) bingo and TV tombola shall be the games in which a player has a tombola card with pre-printed numbers, in line with rules of the game, and the numbers are drawn in a public draw broadcasted by TV at a pre-set date, at the pre-set time, in line with the game rules;

8) tombola held on the premises shall be the game of chance in which a player has a tombola card with pre-printed numbers, in line with the game rules. The player shall win a prize if the numbers printed on the card have been drawn in a draw, which cannot be broadcasted by public media;

9) video lottery shall be the game played at video lottery terminals, where the terminals have been linked into an electronically controlled network, within which the players may lay stakes at various games and jackpot games, in line with rules of the game, having a possibility of multiple stakes and winnings. Whenever the player lays a stake in a jackpot game, certain percentage of his stake goes into the jackpot prize fund. The rules of the game shall define the conditions for winning a jackpot;

10) fonto and similar games shall be the games played over the telephone, Internet and similar media, where a player is assigned or a player chooses himself a certain number or other unique symbol, by a telephone call and after meeting other conditions, if they are foreseen by the game rules. The player shall win a prize if the given number or other unique symbol is drawn in a public draw, in line with the game rules;

11) special games of chance shall be the games where a player competes against another player or the operator and expects winnings depending on the money paid and rules of the game;

12) games organized in casinos shall be the games where the players play against the casino or against each other in line with international rules at gaming tables using:

- small balls (roulette, boulle, etc.);
- dice (craps and alike);
- cards (baccarat, trente-quarante, blackjack, punto banco, mini punto banco, shemin de fer, Caribbean poker and alike);

13) betting games shall be the games where the players, in line with rules of the game, place bets on the results of various sports and other events:

- betting on results of single or group sports events,
- betting on results of dancing, singing, music and similar events
- other betting;

14) games of chance played on slot machines shall be the games organized on automatic machines, electronic roulettes and other machines with multiple stakes and winnings (multiplayer) and on a system of automatic machines, where a larger number of automatic machines are connected for the purpose of forming a single jackpot with the same and simultaneous chances for all players (progressive);

15) automatic machines for the games with multiples stakes and winnings (multiplayer) shall be mechanical, electronic and similar devices on which the players, by payment of a certain amount (chips, coins and direct payment to the cashier or on the machine), have the possibility of winning.

Article 9

Operating Internet gaming or games played via other means of telecommunication shall only be allowed to business organizations granted a concession for operating games of chance, upon obtaining approval from the administrative authority competent for games of chance (hereinafter: the Competent Authority).

Business organizations referred to in paragraph 1 above shall connect their information system for Internet gaming to the information system of the Competent Authority and provide it with access to data and system notes at any time.

For the organization of game of chance referred to in paragraph 1 above, a concession fee shall be determined in the amount of EUR 10,000 per month, to be paid by the 15th day in a month for the current month.

Article 14

The concession for organizing games of chance shall be withdrawn from the operator if:

1) the concession has been granted on the basis of untrue data;

2) the concessionaire has not started to operate within the commencement deadline determined in the concession contract;

3) the concessionaire stopped the operation in violation to the provisions of this Law;

4) the concessionaire fails to meet the prescribed technical, IT and other conditions any longer;

5) the concessionaire breaches the rules of the games of chance;

6) the concessionaire fails to pay obligations stipulated in this Law or fails to pay winnings to players;

7) the concessionaire does not allow or otherwise prevents the supervision prescribed by this Law or makes the supervision difficult;

8) the concessionaire presents the realized turnover incorrectly;

9) the concessionaire lends money to players;

10) the concessionaire breaches the provisions of the concession contract;

11) the facts have occurred due to which the concession would not have been granted.

Article 36

Applications for concession for organizing games of chance in casinos must be supported by the following:

1) data on the name and head-office of the company;

2) proof of registration;

3) the incorporation charter;

4) the three-year business plan;

5) proof of core capital;

6) proof of ownership or the right to use appropriate premises and of the size of premises in which the games of chance will be organized;

7) indication of the type and scope of the games;

8) rules for each type of game of chance that will be organized, conditions for participating in the game, the amount of stake, price of a token or credit point for the games on slot machines, description of the method of recording in the total-register of slot machines and deadline for the collection of payment for participating in the game;

9) data on individuals managing the business and proof of their education and qualification for carrying out activities in the casino;

10) rules of the casino;

11) data on type and number of gambling machines and gambling aids, with detailed description for their identification;

12) proof that the authorized persons have not been convicted for criminal offences against the payment system and commercial operations and that there are no pending criminal proceedings for such offences;

13) proof of deposit or a bank guarantee.

For the opening of the first casino, the operator who was granted a concession must submit the proofs referred to in paragraph 1, bullets 6 and 13 above, within not later than 6 (six) months from the date of issuing the concession granting decision.

Pursuant to Article 88 paragraph 2 of the Constitution of the Republic of Montenegro, I hereby issue the

DECREE

PROMULGATING THE LAW ON INSPECTION SUPERVISION

(Official Gazette of Montenegro 39/03 of 30 June 2003, Official Gazette of Montenegro 76/09 of 18 November 2009)

I hereby promulgate the Law on Inspection Supervision, passed by the Parliament of the Republic of Montenegro at the second sitting of the first ordinary session in 2003 on 25 June 2003.

No 01-331/2

Podgorica, 26 June 2003

The President of the Republic of Montenegro

Filip Vujanovic

LAW ON INSPECTION SUPERVISION

Conduct of inspection supervision
Article 4

An inspector shall conduct inspection supervision. Inspector is an officer with special authorizations and responsibilities.

A Head of inspection body may determine that inspector conducts inspection supervision in another administrative area that is within competencies of such body.

Exceptionally, when special circumstances require due to increased load of work or in the event of absence or longer prevention of Inspector, Head of inspection body may authorize an individual civil servant who fulfills prescribed requirements to conduct on a temporary basis the work of inspection supervision with all authorizations of Inspector, while such circumstances exist.

Inspector's obligations
Article 13

When conducting inspection supervision Inspector shall be obliged to:

1) Review a request for commencement of inspection supervision procedure and to inform a person who submitted the request;
2) Inform responsible person of entity subject to supervision on initiation of inspection review, unless there is an opinion that the notification would decrease efficiency of inspection supervision;

3) Inform an entity subject to supervision on his rights which he can exercise in inspection supervision proceedings;
4) Track the record on conducted inspection review, as well as other prescribed records;
5) Act lawfully and promptly and in accordance with the Code of Ethics of Civil Servants.

Obligations and authorizations for elimination of irregularities
Article 15

In order to eliminate determined irregularities, Inspector shall be entitled and obliged to:

1) Indicate determined irregularities to the entity subject to supervision and prescribe the term for their elimination;
2) Order undertaking of appropriate measures and actions in determined term;
3) Prohibit the conduct of activity and other actions on a temporary basis;
4) Take away objects or means on a temporary basis by which a criminal act was caused, until termination of the proceedings;
5) Pronounce a fine in accordance with the Law and other regulations;
6) Submit the request for initiating of misdemeanor procedure;
7) Initiate criminal or other appropriate procedure; and
8) Exercise other powers and obligations in accordance with regulations.

Obligations of entity subject to supervision in proceedings
Article 21

Entity subject to supervision shall be obliged to provide to inspector free conduct of inspection supervision, to provide information and to make available papers or data necessary for the conduct of control.

Entity subject to supervision shall be obliged to provide the inspector with conditions necessary for free work and establishing of factual situation.

Upon the request or order of Inspector and within a prescribed deadline, entity subject to supervision shall be obliged to submit or prepare accurate and full data, documents or other material necessary for the conduct of inspection.

Duties of other persons
Article 24

In proceedings, a person who is not entity subject to supervision shall be obliged to permit the conduct of inspection review when there is reasonable doubt that in the facility or premises there is activity or objects subject to supervision.

If the person referred to in the paragraph 1 of this Article does not permit the conduct of inspection review, inspector shall enforce the same authorizations he has for entity subject to supervision.

Indication
Article 36

If inspector determines irregularities in the course of inspection supervision proceedings, he shall indicate all irregularities to entity subject to supervision and determine the reasonable term for their removal.

Inspector shall proceed according to the manner referred to in the paragraph 1 of this Article if the entity subject to supervision approves it or state that it does not require issuing of a decision.

Irregularities, actions and measures, approval, i.e. statement of the entity subject to supervision and the term for their removal shall be included in report.

Entity subject to supervision shall be obliged to inform inspector in writing on undertaken actions and measures within 7 days from the date of expiry of the deadline for removal of irregularity.

Inspector shall suspend proceedings by the conclusion if it is determined by subsequent review that entity subject to supervision completely removed irregularity indicated by inspector within the prescribed term. Inspector shall order removal of irregularity by decision if entity subject to supervision did not remove irregularity within the prescribed term.

Execution of fine
Article 59

If entity subject to supervision is obliged to do or bear something by ordered measure, but it proceeds opposite to that obligation and the imposed measure cannot be fulfilled through other persons or by direct compulsion, Inspector shall impose a fine to entity subject to supervision ranging from € 500 to € 5,000 for a legal entity and from € 50 to € 500 for a physical entity. Inspector shall indicate that fine shall not be collected if entity subject to supervision fulfills its obligation within the prescribed term.

Fine can be imposed again until fulfillment of obligation.

Fine shall be imposed through the conclusion against which an appeal is allowed.

Cooperation of the bodies
Article 63

When conducting inspection supervision, inspection bodies shall be obliged to ensure mutual cooperation as well as to cooperate with other authorities and organizations.

Upon a request of Inspector, public authorities, local self-government authorities and other authorities and organizations shall be obliged to submit requested data and information necessary for the procedure of inspection supervision.

Pursuant to Article 88, item 2 of the Constitution of the Republic of Montenegro I hereby issue the

DECREE PROMULGATING THE INSURANCE LAW

(Official Gazette of the Republic of Montenegro, No 78/06 of 22 December 2006, 19/07 of 2 April 2007: Official Gazette of Montenegro, No 53/09 of 7 August 2009, 73/10 of 10 December 2010, 40/11 of 8 August 2011, 45/12 of 17 August 2012, 06/13 of 31 January 2013)

I hereby promulgate the Insurance Law, adopted by the Constituent Parliament of Montenegro at the fifth sitting of the second regular session in 2006 on 11 December 2006.

Number: 01-1547/2

Podgorica, 15 December 2006

The President of Montenegro

Flip Vujanović, m.p.

INSURANCE LAW

Approval for Qualifying Holding

Article 23

A person who intends to acquire, directly or indirectly, a qualifying holding in an insurance company shall be obliged to obtain a prior consent for acquisition of such shares from the regulatory authority.

A person who intends to increase the size of a qualifying holding which would reach or exceed 20%, 33% or 50% of the capital or shares with voting rights, or so acquires 100% of holding in capital or voting rights in an insurance company shall be obliged to obtain a prior consent for such acquisition from the regulatory authority.

Consents referred to in paragraphs 1 and 2 of this Article shall cease to be valid if the applicant fails to acquire the shares for which the consent was issued within six months as of the day of issuing the consent.

The qualifying holder who intends to sell or otherwise dispose of the shares below the level for which it has received the consent, shall be obliged submit a prior notification thereof to the regulatory authority.

Insurance company shall be obliged to notify the regulatory authority forthwith on any change in qualifying holding in the capital of the company.

Rejection of Application for Obtaining Qualified Participation Approval

Article 26

In the procedure upon a request for acquiring qualifying holding, the regulatory authority shall assess the eligibility of the applicant based on:

1) business reputation, as well as of legal status or financial standing of the applicant;
2) reputation and professional qualification of persons holding managing position, in case of applicants who are legal persons;
3) financial stability of the applicant, considering the type of business it carries out;
4) possibility of efficient supervision of the company which is acquiring the holding upon possible issuing of the consent;
5) in terms of that acquisition, possibility of making possible money laundering and terrorism financing or if it was made or attempted to do so.

The regulatory authority shall reject the application for issuing the consent for acquiring the qualifying holding if based on the criteria referred to in paragraph 1 of this Article it assess that:

1) due to the business or activities currently performed or actions taken in pursuit of the insurance business by the applicant for acquisition of qualifying holding or its related party, the operations of the insurance company might be jeopardized;
2) due to the business or activities of the applicant for acquisition of qualifying holding or its related party or because of the nature of their relation, the insurance company supervision might be impossible or difficult;
3) the acquisition of the qualifying holding would be against the conditions stipulated by the law governing the securities market;
4) in terms of that acquisition, possibility of making possible money laundering and terrorism financing or if it was made or attempted to do so.

Prior to rendering the decision referred to in paragraph 2 of this Article, the regulatory authority shall be obliged to enable a period not exceeding 15 days for the applicant, within the deadline referred to in Article 25 paragraph 5 of this Law, to make statement about facts that may serve to reject the application.

Loss of Voting Rights

Article 27

A person that acquires qualifying holding in an insurance company without a consent of the regulatory authority shall not have voting rights in the management of the insurance company, for the shares so obtained and shall be obliged to divest them within 30 days as of the day of acquisition.

Approval of Appointment of Members of Board of Directors

Article 49

Only a person who received consent of the regulatory authority may be appointed as a member of the board of directors.

Along with the request for obtaining the consent referred to in paragraph 1 of this Article, the insurance company shall submit evidence of meeting the conditions referred to in Article 30 of this Law.

Application for Insurance Brokerage License

Article 56

An application for obtaining a license for pursuit of insurance brokerage activities shall be submitted to the regulatory authority by founders of the insurance brokerage company or, on their behalf, by a person authorized by them.

The following documents shall be submitted along with the application referred to in paragraph 1 of this Article:

1) memorandum of association;
2) proposed articles of association;
3) list of shareholders, or owners of holdings, with the data referred to in Article 30 paragraph 2 items 6, 7 and 8 of this Law;
4) evidence that natural persons nominated as members of a board of directors and executive director meet the conditions referred to in Article 30 of this Law ;
5) evidence on at least two persons to be employed in the company, having authorisation for pursuit of insurance brokerage activities, with pre-contract on employment and with personal data of persons to be responsible for insurance brokerage activities;
6) statement on relation with respect to holding in capital or voting rights of insurance companies, reinsurance companies, insurance brokerage or insurance agency companies;
7) evidence on liability insurance for damages which may result from pursuit of business in the amount of at least EUR 200,000 for each damage or EUR 250,000 on aggregate level for one year;
8) business plan for the following three years, including data and evidence on personnel and technical capacity of the company;
9) other evidence and data as may be requested by the regulatory authority.

Entities Subject to Supervision

Article 115

The regulatory authority shall exercise supervision, in accordance with this Law and Core Principles for Efficient Insurance Supervision, over the operations of insurance companies, branches of foreign insurance companies, insurance brokerage companies, insurance agency companies, entrepreneurs-insurance agents, ancillary insurance service providers and the legal persons referred to in Article 80 of this Law.

The regulatory authority may inspect business records of legal persons which are related to the insurance company, as well as the business records of all participants in a transaction that is subject to supervision if so is considered necessary in order to supervise the insurance company's operations.

In cases when another supervisory body is responsible for supervising legal persons referred to in paragraph 2 of this Article, the regulatory authority will exercise supervision in collaboration with the competent supervisory body.

Manner of Performing Supervision

Article 118

Supervision of operations of insurance companies shall be performed by:

1) collecting, monitoring and analysing reports, data and notices that the insurance company is obliged to submit to the regulatory authority by operation of law;
2) on-site examination of the operations of the insurance company;
3) following up implementation of measures imposed in accordance with this Law and by bringing charges to competent authorities if there is reasonable doubt that the illegality and irregularities found have the characteristics of a criminal offence, commercial violation or minor offence.

Authorizations in a Control Procedure

Article 120

In carrying out on-site insurance supervision, the authorized person shall have right to:

1) inspect general acts, business policies and procedures acts and business books of the company, as well as to inspect all other acts, documentation and data relating to the company's operations;
2) demand from members of the board of directors. internal auditor, authorised actuary and person with special authorizations to give information and explanations within their scope of work regarding operations of the company;
3) temporarily revoke documents that indicate the existence of actions having the characteristics of a criminal offence, commercial violation or minor offence.

Obligations of Insurance Company

Article 121

An insurance company shall be obliged to provide the following to the authorized person upon his/her request:

1) enable supervision of the company's operations in its head office and other premises in which the company, or other person under its authorization, performs the business activity and operations supervised by the regulatory authority;
2) enable examination of business and other documents, accuracy and correctness of business and other books and other records, accuracy and correctness in compiling financial reports and annual

reports on the company's operations, as well as reports and notifications submitted to the regulatory authority;
3) provide access to accounting and other documents, business books or parts of business books and other records;
4) data extracts on a media chosen by the authorized person, as well as enable full access to the electronic data processing system for accounting records.

The authorized person shall be obliged to perform supervision in such manner to minimize the disruption to the regular operations of the company.

Cooperation with Other Supervisory and Regulatory Authorities

Article 128

The regulatory authority shall cooperate with other supervisory and regulatory authorities, in order to carry out its supervisory and regulatory role efficiently, with the objective to encourage a harmonised development of a network for supervision of financial institutions, in accordance with agreements concluded.

Supervisory or regulatory authorities may convey information obtained from the regulatory authority to other regulatory authority only upon prior approval of the regulatory authority.

Exchange of information in accordance with concluded agreements referred to in paragraph 1 of this Article, in the process of cooperation of the regulatory authority with other supervisory and regulatory authorities shall not be considered as disclosure of confidential information.

Types of Supervisory Measures

Article 129

In exercising supervision over operations of an insurance company, the regulatory authority may:

1) warn the insurance company in writing and request for irregularities established in operation to be corrected within a specified deadline;
2) order measures to correct illegalities and irregularities;
3) order special measures against responsible persons in the company;
4) order transfer of insurance portfolio to the another insurance company;
5) introduce interim administration in the company;
6) revoke a license for pursuit of specific or all insurance activities.

The regulatory authority shall impose measure referred to in paragraph 1 item of this Article on the insurance company if irregularities established in operation:

- do not affect directly and substantially financial operations of the company and rights of insured persons or insurance contract beneficiaries;
- could have a substantial effect on financial operations of the company and rights of insured persons or insurance contract beneficiaries.

Measures referred to in paragraph 1 items 2 to 6 of this Law shall be imposed by way of a decision.

Decision imposing measures referred to in paragraph 1 items 5 and 6 of this Article shall be published in the “Official Gazette of Montenegro”.

Actions to Correct Illegalities and Irregularities

Article 130

The regulatory authority, shall order the insurance company to correct illegalities and irregularities in operations, by way of decision, if establishes the following:

1) company stops to meet any of requirements prescribed for pursuit of insurance activities;
2) company performs activities, which under this Law cannot be performed;
3) company acts contrary to the rules of keeping business books and preparing business reports, or rules on internal audit, or audit of financial reports;
4) company fails to act in line with reporting and information requirements of the regulatory authority;
5) member of the board of directors or executive director of the company fails to meet prescribed requirements;
6) company acts contrary to law, other regulations and general acts which govern the insurance company operations;
7) company acts towards insured persons and other insurance beneficiaries contrary to the rules of insurance profession, good business practice and business ethics;
8) company breaches rules on risk management referred to in Article 100 of this Law.

If the regulatory authority establishes that the insurance company breached risk management rules referred to in paragraph 1 item 8 of this Article, the regulatory authority shall, by way of its decision on correcting illegalities and irregularities, order to the insurance company to ensure:

1) co-insurance and reinsurance of excess risks above the self-insured retention;
2) payment of claims, contracted insured sums and execution of the insurance related obligations;
3) capital in the prescribed amount;
4) stipulated technical provisions;
5) liquidity of the company;
6) depositing and investing technical provisions funds in line with prescribed amount and structure;
7) depositing and investing capital funds in line with prescribed amount and structure;
8) alignment of capital and the solvency margin or guaranteed capital and solvency margin;
9) meeting of obligations pertaining to risk management established under this Law.

In addition to measures referred to in paragraph 2 of this Article, the regulatory authority may:

1) prohibit entering of new insurance contracts for specific or all classes of insurance and expansion of undertaken obligations;
2) order termination of insurance contract, insurance brokerage or insurance agency contract, if application thereof would cause damage to the company;
3) limit risk level to be assumed by the company;
4) prohibit execution of certain payments;

5) prohibit transactions with specific shareholders, members of managing bodies of the company, related parties or other legal persons;
6) order appointment of an adviser for segment of operations where illegalities and irregularities are established;
7) order change of organisation of work;

8) order collection of receivables;
9) prohibit or limit temporarily disposal of assets;
10) order updating of business books, inventory of assets and liabilities, reconciling receivables and liabilities and assessment of balance and off-balance items;
11) order the improvement of electronic data processing system;
12) order the improvement of organization and manner of carrying out the internal audit;
13) order undertaking of other activities in accordance with law.

By way of a decision on imposing measures referred to in paragraphs 1, 2 and 3 of this Article, the regulatory authority shall also determine the deadline for removal of identified illegalities and irregularities.

The insurance company shall be obliged to correct the established irregularities within the deadline referred to in paragraph 4 of this Article and report to the regulatory authority on the implementation of the ordered measures.

The decision of the regulatory authority referred to in paragraphs 1, 2 and 3 of this Article shall be final.

Governing Provisions

Article 147

The provisions of this Law on supervision of the insurance business shall apply accordingly to supervision of operations of insurance brokerage companies, or insurance agency companies or entrepreneurs - insurance agents and ancillary insurance services providers.

Status

Article 176

The activities of the regulatory authority determined by this Law shall be performed by the Insurance Supervision Agency (hereinafter referred to as: the Agency), which shall have the status of a legal person.

The Agency shall be independent in carrying out activities within its scope of work.

The Agency shall perform the activities referred to in paragraph 1 of this Article primarily in order to protect interests of insured persons and other insurance beneficiaries, provide stability and development on the insurance business based on sound competition and equal operating conditions.

Montenegro is the founder of the Agency.

The Council of the Agency shall exercise the rights of founders on behalf of Montenegro, in accordance with law.

Composition and Appointment of the Council of the Agency

Article 180

The Council of the Agency shall consist of a president and two members.

The Parliament shall appoint and dismiss the president and members of the Council of the Agency.

President and one member of the Council of the Agency shall be appointed at the proposal of the working body of the Parliament competent for elections and appointments, whereas one member at the proposal of the Government.

President and members of the Council of the Agency shall be appointed for the period of five years and may be reappointed. President and members of the Council of the Agency shall be responsible for their work to the Parliament.
President of the Council of the Agency shall discharge his office as a professional, while members of the Council shall discharge their office on part-time basis.

Conditions for Appointment of the President and Members of the Council of the Agency

Article 181

A person to be appointed as a President or a member of the Council of the Agency shall meet the following requirements:

1) is a citizen of Montenegro;
2) holds university degree;
3) has professional experience in the field of insurance, law or economics of at least three years;
4) during the three years prior to the appointment was not a member of a management body in a legal entity under liquidation or bankruptcy proceedings.

Dismissal of President and Members of the Council of the Agency

Article 184

President or member of the Council of the Agency may be dismissed prior to expiration date of the term in the office:

1) upon a personal request;
2) due to permanent loss of working capacity to discharge the office;
3) if circumstances referred to in Article 192 of this Law occur;
4) if violates the obligation of keeping confidential data.

Director of the Agency

Article 187

The director of the Agency shall be appointed by the Council of the Agency based on a public competition, for the four-year period.

A person to be appointed as the director of the Agency shall meet the requirements for appointment of a member of the Council of the Agency determined by Article 181 of this Law, in addition to the general requirements.

A person who cannot be appointed as a member of the Council of the Agency pursuant to this Law, as well as a person who does not have a permanent residence in Montenegro, cannot be appointed as the director of the Agency.

Keeping Confidential Data

Article 189

The President and members of the Council of the Agency, the Director of the Agency and employees of the Agency, shall be obliged to keep as confidential data on persons over which the Agency exercises supervision, as well as other data in accordance with this Law and the Agency's Statute, except for the data which are disclosed according to the provisions of this Law and which are available for review by interested parties.

Confidential data, within the meaning of this Law, shall be considered to be, *inter alia*, data from the supervision procedure and data on imposed supervision measures under this Law.

The obligation referred to in paragraph 1 of this Article shall continue for three years after termination of their office or employment in the Agency.

Funds for Operation of the Agency

Article 190

Funds for operation of the Agency shall be provided from:

1) fees determined in accordance with this Law;
2) funds allocated by the companies under Article 4 paragraphs 1 and 2 of this Law, up to 1% of gross insurance premium;
3) other revenues of the Agency, in accordance with the law.

Excess of revenues over expenditures of the Agency shall be the revenue of the Budget of Montenegro.

Reporting

Article 193

After being adopted by the Agency, the reports and statements referred to in Article 185 items 4 and 5 of this Law shall be submitted to the Parliament for adoption.

Pursuant to Article 95 item 3 of the Constitution of Montenegro I hereby issue the

DECREE ON PROCLAMATION OF THE LAW ON INVESTMENT FUNDS
("Official Gazette of Montenegro", No. 54/11 of 17November, 2011)

I hereby promulgate the Law on Investment Funds, adopted by the Parliament of Montenegro at its second sitting of the second regular (fall) session in 2011, held on November 1st, 2011.

Number: 01-1294/2

Podgorica, November 14th, 2011

The President of Montenegro,

Filip Vujanović, manu propria

Pursuant to Article 82 paragraph 1 item 2 and Article 91 paragraph 2 of the Constitution of Montenegro, the Parliament of Montenegro at its second sitting of the second regular (fall) session in 2011, held on November 1st, 2011has adopted

LAW ON INVESTMENT FUNDS

Conditions for owners and employees
Article 91

The following persons may not be owners of management companies, supervisory board members or employees of the respective company:

1) persons who, in the period of three years prior to acquiring membership interest in the management company, had not less than 10% share in the registered capital of the management company, bank or other institution authorized for carrying on tasks of the depositary, closed-ended investment fund, brokerage company or a bank authorized for purchasing and selling securities, insurance company or privately-owned pension fund, if the company was revoked authorization during that period;
2) persons who no longer hold membership in a professional association on grounds of infringement of association rules, or against whom the competent authority has imposed a measure of withdrawing the authorization for carrying on securities-related activities,

3) persons punished for a criminal offence of causing bankruptcy by negligent operations, violation of liability to keep business books, causing damage to creditors or privileging them, abuse in bankruptcy proceedings, unauthorized disclosure and gaining knowledge of professional secrecy, as well as for a criminal offence of fraud, in the period of five years following the date the sentence has become final, where the time of serving the sentence is not calculated in this period,
4) persons against whom the safety measure has been imposed of prohibiting the pursuit of business, activity or duty which is completely or partially included in the objects of the management company's operations in the period the prohibition is in effect,
5) persons punished for a criminal offence or the offence stipulated by the law regulating securities-related operations in the period of five years following the date the sentence has become final;
6) persons who have been declared incapacitated,
7) persons holding a valid license granted by the Commission, for a broker, dealer or investment manager, i.e. the appropriate approval of the competent authority of other state and who effectively perform those tasks as employees of a brokerage company or a bank authorized for securities transactions,

Application for issue of the authorization
Article 93

(1) The management company shall submit to the Commission the application for issue of the authorization.
(2) Along with the application referred to in paragraph 1 of this Article the following documents shall be submitted:
1) Instruments of incorporation of the management company;
2) Business plan for the first three years of performing business operations of the management company which shall contain: the planned volume of investment funds which the management company intends to market, the organizational chart of the company, as well as the data concerning the employees' structure;
3) A list of the management company members (first and last names, address, i.e. company's name and registered office), nominal value of shares, as well as percentage of each founder in the registered capital of the company;
4) A list of persons related to the management company;
5) Evidence on personnel and technical - organizational capacity of the company;
6) Other documents in accordance with the Law.
(3) The Commission is obliged to decide within sixty days following the date of submitting the application.
(4) The authorization shall cease to be valid for a management company if it fails to establish the fund within one year following the date of issue of the license.
(5) Conditions for personnel and technical - organizational capacity of the company and the content and procedure for issue of authorizations shall be determined by the rules of the Commission.

Supervision over business operations
Article 100

(1) The Commission shall perform supervision of business operations of a management company branch office established in Montenegro.
(2) The Commission may submit the request to the competent authority of the Member State in which the management company performs its business operations, to perform the supervisory procedure over the operation of the management company branch office in the respective Member State, if in this manner the supervisory procedure is going to be expedited and simplified, in accordance with the principles of efficacy, cost-efficiency and taking action within a reasonable time period.
(3) Persons authorized by the Commission may take part in the supervisory procedure carried by the supervisory body of the respective Member State.

Direct pursuit of business operations in Montenegro
Article 106

(1) The management company having the registered office in a Member State that intends to carry out directly fund management activities in Montenegro is obliged to notify the Commission and the competent home Member State thereof.
(2) Along with notification referred to in paragraph 1 of this Article, the following information shall be submitted:

1) activities plan;

2) data and documents referred to in Article 104 of this Law.

(3) The competent authority of the home Member State, along with notification submitted to the Commission, shall also notify the management company.

(4)Along with notification referred to in paragraph 2 of this Article, the following information shall be submitted to the Commission:

1) data on the amount of registered capital of the management company;

2) statement that every fund to which the notification referred to in paragraph 2 of this Article relates, meets the stipulated requirements.

(5) The management company is obliged to notify the Commission and the competent authority of a home Member State on any change in particulars referred to in paragraph 1 of this Article, within the period of 30 days prior to implementation of planned changes.

Authorization withdrawal and termination of the management company
Article 108

The management company shall be withdrawn the authorization by the Commission if:

1) the management company fails to start business operations within the period of one year following the date of authorization granting;

2) the management company requests termination of authorization validity;

3) the management company has not carried on the activity of investment fund management for six or more months, in accordance with this Law;

4) the authorization has been granted on the basis of false or misleading information;

5) it fails to meet conditions for granting the authorization;

6) the authorized person has seriously or systematically infringed this Law.

Operations of the company from a Member State

Article 113

(1) The management company that performs the activity of collective portfolio management on a cross-border basis, by establishing a branch office or under the freedom to provide services, is obliged to operate in accordance with the provisions of this Law in relation to: the organization of the management company, transfer of management activities to third parties, procedures for risk management, prudential rules and supervision systems referred to in Article 119 of this Law and the provisions regulating the obligation of reporting.

(1) Supervision of organization and business operations of the management company referred to in paragraph 1 of this Article shall be carried out by the Commission.

(2) The company referred to in paragraph 1 of this Article is obliged to operate in accordance with the regulations of the home Member State in which the investment fund is located, and which relate to:

1) establishment and granting of authorization to the investment fund ;

2) investment unit issue and redemption;

3) investment and limitations policies, including calculation of the total exposure and indebtedness;

4) limitation of indebtedness, credit granting and sale without the collateral;

5) property valuation and accounting of the investment fund;

6) calculation of a price during issue, redemption and errors in the calculation of net asset value and the compensation of investors;

7) distribution or reinvestment of income;

8) disclosure and reporting of the investment fund, including the prospectus, the key information for investors and periodical reports;

9) agreements on trade;

10) relationship with the unit-holders;

11) merger and restructuring of the investment fund;

12) termination of business operations and winding-up of the investment fund;

13) content of unit-holders' register;

14) fees related to the issue of the authorization and supervision of the investment fund;

15) exercise of voting rights of unit-holders and other holders' rights with regard to items 1 to 15 of this Article.

Powers of the Commission

Article 141

(1) The Commission shall supervise the management company and investment fund by giving approval to their regulations and by control of their operations in accordance with this Law.

(2) The Commission may also perform control of the depositary under the activities it performs in accordance with this Law.

(3) The Commission may, without limitation, to examine documents, business books, records and other documentation of the management company regarding operations of the respected company and the investment fund.

Remedying illegalities and irregularities

Article 144

(1) Where the Commission, in the course of supervision, reveals illegalities or irregularities in the management company and investment fund's operations, it shall order by its decision remedying of the foregoing illegalities, i.e. irregularities within a determined period.

(2)The management company is obliged to, within the term ordered, remedy revealed illegalities, i.e. irregularities and to notify the Commission on measures taken.

Measures

Article 145

(1) In case the management company fails to remedy revealed illegalities, i.e. irregularities within a determined period and to notify the Commission thereof along with the submission of appropriate evidence, the Commission may take the following measures:

1) give order for dismissal of investment fund supervisory board's members, and management and governing bodies of the management company;
2) give order for the change of the management company;
3) give a written warning, temporary suspend or withdraw the license to an investment manager;
4) temporary prohibit use of the management fund and investment fund's assets;
5) withdraw the management company's authorization;
6) take other measures required for remedying revealed illegalities and irregularities in operations of the management company and the investment fund.

(2)The Commission may impose one or more measures referred to in paragraph 1 of this Article, depending on nature and importance of irregularities revealed.

(3)Detailed conditions, a manner and procedure of supervision shall be established by the Commission.

Announcement of imposed measures

Article 146

The Commission may announce measures imposed in the oversight procedure, except when such announcement would seriously jeopardize financial market, investors' interests or cause disproportionate damage to parties involved.

Keeping of business secret
Article 148

The persons employed in the Commission are obliged to keep, in accordance with law, confidential information received in the course of their duties determined by this Law.

The rules of the Commission
Article 190

Rules of the Commission shall establish in detail:
1) a content of the management agreement and transformation of an existing fund;
2) methodology for calculation of net asset value of an existing fund in the transformation process;
3) a manner of reporting on holding of monetary assets of an existing fund in the transformation process;
4) conditions and a manner of promotion an existing fund's operations in the transformation process;
5) a manner of publication of the report and content of the report of both management company's operations and the fund in the transformation process;
6) conditions, manner and procedure of enforcement of supervision over investment funds' management companies and funds in the transformation process;
7) a manner of calculation and charge of compensations for management companies in the transformation process;
8) a period in which the value, at which investment units of open-end fund in the transformation process are issued and redeemed, is established;

XVI. PENALTY PROVISIONS

Article 191

(1) The management company shall be punished for a committed misdemeanor with a pecuniary penalty amounting from EUR 5,000 to EUR 40.000 in case:

1) the costs and expenses that are not determined by the rules on fund management are paid out of its assets. (Article 6 paragraph 2);
2) of the issue of investment units before the payment of net amount of the price at which investment units are issued in the stipulated term and manner (Article 8 paragraph 2);
3) evaluates the fund's assets contrary to Article 8 paragraph 3 of this Law;
4) it fails to redeem investment units of the fund at the request of unit-holder. (Article 9 paragraph 1)
5) it fails to redeem investment units at the value which is calculated in the manner laid down in Article 8 of this Law, with deduction of all costs and fees. (Article 9 paragraph 2);
6) it charges the mutual fund, i.e. the investor charges and expenses other than those stipulated by Article 9 paragraph 3 indent 3 of this Law (Article 9 paragraph 4);
7) it issues or redeem investment units at a price which is not determined in accordance with Article 9 of this Law (Article 10 paragraph 1)
8) fails to pay assets after the redemption of investment unit to a unit-holder, under conditions established by the rules on management (Article 10 paragraph 3).

9) fails to make calculation of ongoing charges and fails to publish the exact amounts of ongoing charges in the key investor information (Article 11 paragraph 1 item 1);
10) fails to make calculation of ongoing charges in accordance with the methodology referred to in Article 12 of this Law (Article 11 paragraph 1 item 2)
11) fails to keep register of all accounts of ongoing charges and to keep information from the register for at least five years from the date of entry into the register (Article 11 paragraph 1 item 3);
12) pays costs that are not determined by the rules on fund management, out of the fund's assets (Article 11 paragraph 4);
13) pays, out of the fund's assets, fees relating to advertizing or promotion of the fund's investment units sale or fees to funds' sales representatives (Article 11 paragraph 5);
14) fails to notify the Commission and unit-holders, without delay, on its decision to suspend investment units redemption (Article 13 paragraph 2);
15) fails to notify the Commission, within three days from the date of commencement of the period of investment units suspension, on measures taken in order for remedying reasons that caused the suspension of investment units (Article 13 paragraph 3);
16) fails to notify the unit-holders on withdrawal of the management company's decision on suspension of the fund's investment units redemption in the manner laid down in the rules on management (Article 13 paragraph 6);
17) issues new investment units or redeems the fund's investment units within the period of suspension of the fund's investment units (Article 13 paragraphs 8 and 9);
18) fails to redeem investment units at a price determined in accordance with this Law on the date when the suspension of the fund's investment units is terminated (Article 13 paragraph 10);
19) fails to make payments of interest to unit-holders out of its assets in case referred to in Article 13 paragraph 11 indents 1 and 2 of this Law (Article 13 paragraph 12);
20) fails to notify, without delay, the competent authorities of other Member States where mutual fund's investment units are marketed, on its decision to suspend the redemption of investment units (Article 13 paragraph 13);
21) issue and redemption of investment units is being made when the fund does not have a management company or the depositary (Article 13 paragraph 14 indent 1);
22) issue and redemption of investment units is being made at the time when winding-up or bankruptcy procedures are initiated over the management company or the depositary (Article 13 paragraph 14 indent 2);
23) fails to establish the rules on the fund's management (Article 14 paragraph 1);
24) fails to exercise the rights arising from securities of the mutual fund's portfolio (Article 15 paragraph 3);
25) fails to act with a care of a prudent businessman in the course of management of the mutual fund's assets in accordance with the highest professional standards. (Article 16 paragraph 1);
26) fails to act objectively and in the best interests of unit-holders in exercising the rights and obligations established by this Law and the agreement (Article 21 paragraph 1);
27) performs task and activities both as the management company and the depositary (Article 21 paragraph 2);
28) performs its functions towards the mutual fund in case of termination of the agreement by the management company, providing that a new management company is designated(Article 22 paragraph 1 item 1);
29) performs its functions towards the mutual fund in case of mutual consent of the agreement or termination of the agreement with the depositary by the management company; (Article 22 paragraph 1 item 2);
30) performs its functions towards the mutual fund in case when winding-up or bankruptcy procedures, i.e. receivership, are initiated over the management company (Article 22 paragraph 1 item 3);
31) performs its functions towards the mutual fund in case when the supervisory body withdraws authorization to the management company (Article 22 paragraph 1 item 4);
32) performs its functions towards the mutual fund contrary to the rules on fund's management (Article 22 paragraph 1 item 5);
33) issues the fund's investment units after occurrence of conditions for initiation of the winding-up procedure of the mutual fund (Article 23 paragraph 2);
34) charges an exit fee in case of the fund's winding-up regardless the ground for initiation of the winding-up procedure (Article 23 paragraph 4);
35) invests more than 10% of its assets in transferable securities or money market instruments, other than securities and instruments (Article 25 paragraph 2 item 1);
36) acquires precious metals or certificate representing them (Article 25 paragraph 2 item 2);

37) derogates from its investment objectives established by the rules on fund's management, instruments of incorporation or the prospectus (Article 26 paragraph 3);
38) fails to provide that its overall exposure relating to derivative instruments does not amount more than the total net asset value of its portfolio (Article 26 paragraph 4);
39) invest more than 10% of its assets in transferable securities or money market instruments of the same issuer; (Article 27 paragraph 1 indent 1);
40) invest more than 20% of its assets in deposits with the same entity (Article 27 paragraph 1 indent 2);
41) risk exposure of the counterparty in transactions in over the-counter derivatives is higher than 10% of its assets when the other counterparty is a credit institution referred to in Article 25 paragraph 1 item 4 of this Law (Article 27 paragraph 2 indent 1);
42) risk exposure of the counterparty in transactions in over the-counter derivatives is higher than 5% of its assets in other cases (Article 27 paragraph 2 indent 2);
43) the total value of transferable securities and money market instruments held by open-end fund in issuers in which it separately invests more than 5 % of its assets exceeds 40% of the open-end fund's value (Article 27 paragraph 3);
44) limitation referred to in Article 27 paragraph 3 of this Law applies to deposits or transactions in over-the-counter derivatives with financial institutions that are subject to prudential supervision (Article 27 paragraph 4);
45) if more than 20% of its assets is invested in the same company, by combining investments in transferable securities and money market instruments issued by that company (Article 27 paragraph 5 indent 1);
46) if more than 20% of its assets is invested in the same company, by combining deposits with that company (Article 27 paragraph 5 indent 2);
47) if more than 20% of its assets is invested in the same company, by combining exposures arising from transactions in over-the–counter derivatives in which the respected company is involved (Article 27 paragraph 5 indent 3);
48) invests more than 5% of its assets in bonds referred to in Article 27 paragraph 7 of this Law issued by the same issuer, and the total value of such investments exceeds 80% of open-end fund's assets value (Article 27 paragraph 9);
49) invests more than 5% of its assets in transferable securities and money market instruments in accordance with Article 27 paragraphs 6 and 7 and takes into account such transferable securities when applies limitations referred to in Article 27 paragraph 2 of this Law. (Article 27 paragraph 10)
50) investments in transferable securities and money market instruments issued by the same issuer, or investments in deposits or derivatives of the same issuer carried out in accordance with Article 27 paragraphs 1 to 8 of this Law, in aggregate exceed 35% of open-end fund's assets (Article 27 paragraph 11);
51) invests more than 30% of its total assets in the securities of a single issue (Article 29 paragraph 2);
52) investments in shares of collective investment undertakings, which are not open-ended funds, in the total amount of an open-end fund's assets, are greater than 30% (Article 30 paragraph 3);
53) calculates a subscription or redemption fee of open-end fund in the investment units of another open-end fund or collective investment undertaking (Article 30 paragraph 4);
54) fails to publish, in its prospectus, the highest amount of management fee that can be calculated for that and for another open-end fund or to a collective investment undertaking in which it intends to invest, and if, in its annual financial report, it fails to specify the highest amount of management fees calculated to that and to another open-end fund or a collective investment undertaking in which it invests its assets (Article 30 paragraph 5);
55) the prospectus and marketing communication do not contain a clear statement that warns of the investment policy, if an open-end fund mainly invests in property referred to in Article 25 of this Law (Article 31 paragraph 3);
56) borrows in the name and on behalf of the fund (Article 34 paragraph 1)
57) sells with no collateral transferable securities, money market instruments or other financial instruments referred to in Article 25 paragraph 1 items 3, 4 and 5 of this Law (Article 35)
58) fails to inform the Commission, in writing, on change of the data which are relevant for trade or change of class of shares that will be traded (Article 36 paragraph 3);
59) by acts referred to in Article 38 paragraph 4 of this Law stipulates as the required majority more than 75% of the votes of shareholders present or represented at the shareholders meeting (Article 38 paragraph 7);
60) fails to submit to the Commission the documentation referred to in Article 39 paragraph 2 of this Law in the Montenegrin language (Article 39 paragraph 3);

61) fails to develop a common draft of merger conditions that contains the elements set out in Article 42 of this Law (Article 42 paragraph 1);
62) fails to engage an independent auditor in order to evaluate and confirm the criteria for valuation of assets and liabilities at the date of the calculation of exchange relation, in accordance with Article 48 paragraph 1 of this Law (Article 44 paragraph 1 item 1);
63) fails to engage an independent auditor in order to evaluate and confirm money compensation per investment unit, if money compensation is paid (Article 44 paragraph 1 item 2);
64) fails to engage an independent auditor in order to evaluate and confirm the method of calculation of an exchange ratio, as well as a real exchange ratio established on the date set for the calculation of this relation, in accordance with Article 48 paragraph 1 of this Law (Article 44 paragraph 1 item 3);
65) fails to submit notifications with adequate information and accurate data on the proposed merger to unit-holders, in order to evaluate the impact of the proposed merger to their investment, after approval of the Commission for the proposed merger referred to in Article 39 of this Law (Article 45 paragraph 1);
66) fails to inform the Commission and other competent authorities involved in the merger and to publish the entry into force of the merger in at least one daily paper media distributed in the territory of Montenegro and in the electronic media whose program is available within the entire territory of Montenegro, as well as on its website (Article 48 paragraph 3);
67) fails to inform in writing the depositary of the receiving fund that the transfer of assets and liabilities of the acquired fund is completed, if the fund is managed by the management company. (Article 49 paragraph 4);
68) in order to maintain its overall exposure within the limits laid down in Article 26 paragraph 3 of this Law, fails to calculate its risk exposure on financial derivative instruments, by combining its immediate exposure according to Article 51 paragraph 2 item 2 of this Law with the actual exposure of the master fund per financial derivative instruments, proportionally to share of the feeder fund in the master fund; or by total maximum potential exposure of the master fund per financial derivative instruments, established by the master fund's management rules or by the instruments of incorporation, in proportion to share of the feeder fund in the master fund (Article 51 paragraph 3);
69) fails to submit the documents stipulated in Article 52 paragraph 3 of this Law;
70) fails to enable the feeder fund to redeem or pay the investment units held in the master fund, prior to the enforcement or division of the master fund, except in case referred to in paragraph 53 paragraph 10 item 1 of this Law (Article 53 paragraph 12);
71) invests in the master fund's investment units until conclusion of the agreement referred to in Article 54 paragraph 1 of this Law. (Article 54 paragraph 2);
72) fails to inform, without delay, the depositary of the feeder fund on irregularities related to the master fund which may have a negative impact to the feeder fund (Article 54 paragraph 3);
73) invests in the master fund's investment units until conclusion of the agreement referred to in Article 55 paragraph 1 of this Law (Article 55 paragraph 2);
74) fails to submit to the Commission the prospectus and the key investor information referred to in Article 161 of this Law, as well as their amendments and annual and half-yearly reports of the master fund (Article 56 paragraph 3).
75) fails to emphasize the information in all marketing communication, that it permanently invests 85% or more of its assets in the master fund (Article 56 paragraph 4);
76) fails to monitor continually and effectively operations of the master fund, based on information and documentation received by the master fund or by the management company, depositary and auditor and in any other appropriate manner (Article 58 paragraph 1);
77) fails to inform the Commission on the name and registered office of the feeder fund which invests in master fund's investment units (Article 59 paragraph 1);
78) calculates fees for subscription, redemption or sale of investment units to the feeder fund (Article 59 paragraph 3);
79) fails to provide access to information in accordance with the rules on management or articles of association of the feeder fund or a management company , to the Commission and the competent authorities, the depositary and the auditor of the feeder fund (Article 59 paragraph 4);
80) carries out the winding-up and transformation of the master and feeder fund, without the prior approval of the Commission (Article 60 paragraph 4);
81) invests more than 20% of its net assets in any company for investment of the initial capital (Article 62 paragraph 2);
82) fails to provide that management bodies' members of the management company that manages the investment fund may only be the persons who have relevant professional experience in managing this type of fund (Article 62 paragraph 6 item 1);

83) fails to provide that the annual and half-yearly reports of the investment fund includes information and data on the development of companies in which the assets are invested provided that, in case of sale of securities from the fund's portfolio, the amount of loss or profit per each investments shall be obligatorily stated (Article 62 paragraph 6 item 2);
84) fails to ensure that the financial statements of the investment fund report on the existence of potential conflict of interest between bodies of the management company and interests of the fund (Article 62 paragraph 6 item 3);
85) fails to provide that the prospectus contains a detailed description of investment risks of the proposed investment fund's investment policy and a possible conflict of interest between the management company's bodies and interests of the fund (Article 62 paragraph 6 item 4);
86) fails to provide that the prospectus contains a statement that investment into the investment fund involves risk above the average and is suitable for investment of entities that can afford such a risk to and that the average investor is recommended to invest only part of the assets it intends to invest for the long run (Article 62 paragraph 6 item 5);
87) fails to provide that management bodies' members of the investment fund management company may only be the persons who have relevant professional experience in the management of this type of the fund (Article 63 paragraph 3 item 1);
88) fails to provide that the annual and half-yearly reports of the investment fund contains information about each category of options and futures that are marketed, the amount of profit or loss that has been made by each of the contracts (Article 63 paragraph 3 item 2);
89) fails to provide that financial statements contain an indication of the amount of commissions paid to brokers and the fees paid on the basis of management, as well as other fees (Article 63 paragraph 3 item 3);
90) fails to provide that the prospectus contains a detailed description of trading strategy in derivative securities and investment risks that accompany such investment policy (Article 63 paragraph 3 item 4);
91) fails to provide that the prospectus contains an indication that the securities market is extremely variable and that there is a significant risk of loss, as well as an indication that investment into the investment fund involves risk above the average and is suitable for people who can afford such a risk (Article 63 paragraph 3 item 5);
92) fails to reach the minimum amount of net assets within a year following the date of its establishment (Article 65 paragraph 3);
93) issues preference shares (Article 68 paragraph 3);
94) costs and fees relating to the establishment that are paid at the expense of the fund's assets are higher than 3,5% of total cash funds raised by issuing shares (Article 71 paragraph 3);
95) fails to manage the investment fund in the best interests of shareholders of the fund (Article 79 paragraph 2);
96) has a controlling influence or a controlling stake in a brokerage company or bank authorized to conduct transactions in securities (Article 85 paragraph 1);
97) has a stake in the depositary (Article 85 paragraph 2);
98) is organizationally related with the depositary and those positions are occupied by the same persons (Article 85 paragraph 3);
99) directly or through related persons acquires shares of the fund during the fund management (Article 85 paragraph 4);
100) the capital of the company amounts less than one-fourth of the costs of the management company incurred in the previous year (Article 87 paragraph 3);
101) fails to submit to the Commission the request for approval of the certified auditor appointment (Article 94 paragraph 1);
102) fails to comply with the principles of good faith in establishing contractual relations, and exercising the rights and obligations arising from such contractual relations (Article 95 paragraph 1 item 1);
103) fails to act with the utmost care in carrying out the obligations of the management company, according to professional standards and good business practice (Article 95 paragraph 1 item 2);
104) fails to meet timely all outstanding liabilities (liquidity principle), or is permanently able to meet all its liabilities (solvency principle) (Article 95 paragraph 1 item 3);
105) fails to provide and to be responsible for timely, conscientious and efficient exercise of all rights and obligations under this Law, the prospectus and the fund's articles of association (Article 95 paragraph 1 item 4);
106) fails to keep information on shareholders, unit-holders, payments and compensations as a professional secrecy in accordance with law (Article 95 paragraph 1 item 5);
107) fails to follow execution of activities and tasks entrusted to third parties (Article 95 paragraph 1 item 6);

108) with the approval of the competent authority, fails to issue rules on prevention of conflict of interest with investment funds it manages, as well as with unit-holders in mutual funds, i.e. shareholders in closed-end investment funds, and with persons engaged in investment advising (Article 95 paragraph 1 item 7);
109) fails to provide supervision systems that allow reliable monitoring of all decisions, orders and transactions in the fund's assets in accordance with law (Article 95 paragraph 1 item 8);
110) fails to ensure that all advertising and promotional content, notifications, as well as reports to shareholders or unit-holders are clear, accurate and not misleading (Article 95 paragraph 1 item 9);
111) fails to provide sale of investment fund's units and shares in accordance with Article 84 of this Law (Article 95 paragraph 1 item 10);
112) fails to purchase the property on its behalf and for the account of the mutual investment fund it manages, as well as on behalf and for the account of a closed-end investment fund (Article 95 paragraph 1 item 11);
113) fails to submit to the depositary photocopies of documents related to transactions in investment fund's assets (Article 95 paragraph 1 item 12);
114) fails to keep its assets, liabilities, claims, income and expenditures separately from assets, liabilities, claims, income and expenditures of the investment fund it manages, i.e. separately by funds (Article 95 paragraph 1 item 13);
115) fails to keep business books and other documentation in accordance with law (Article 95 paragraph 1 item 14);
116) fails to publish the data on the funds it manages (Article 95 paragraph 1 item 15);
117) fails to submit to the Commission periodical and annual financial reports in accordance with the Commission's rules (Article 95 paragraph 1 item 16);
118) fails to inform the Commission on any change of management and supervisory board's members, i.e. change in the membership of a management company, as well as on any change of the capital, ratio or participation in the initial capital in relation to the status approved by the Commission; (Article 95 paragraph 1 item 17);
119) fails to comply with other requirements envisaged by this law and the Commission's rules (Article 95 paragraph 1 item 18);
120) fails to enter into agreement in accordance with this Law; (Article 95 paragraph 1 item 19);
121) fails to ensure that his employees and each person the contract on sale of shares or investment units has been entered into with, do not act in accordance with this Law and other regulations (Article 95 paragraph 1 item 20);
122) fails to manage the fund in accordance with its investment policy(Article 95 paragraph 1 item 21);
123) fails to give orders to the depositary for exercise of the rights related to the fund's assets (Article 95 paragraph 1 item 22);
124) fails to provide that evaluations of the fund's assets are accurate and that the price of investment units is correctly determined (Article 95 paragraph 1 item 23);
125) fails to establish a risk management system that allows daily measurement and monitoring of risk of individual instruments in the fund's portfolio, as well as the overall portfolio of the fund and accurate and independent determination of financial derivatives' value marketed on other regulated markets (Article 96 paragraph 1);
126) for each fund, fails to report to the Commission on the types of financial derivatives in the fund's portfolio, associated risks, quantitative limits and the methodology applied to measure risks related to positions and transactions in those derivatives, in accordance with the Commission's regulations (Article 96 paragraph 2);
127) fails to inform the Commission and to submit a request for mediation with the competent authority of the Member State where it intends to open a branch office (Article 98 paragraph 1);
128) fails to inform the Commission in case of changing the data laid down in Article 98 paragraph 2 of this Law, within the period of 30 days before implementation of this change (Article 98 paragraph 7);
129) fails to inform the Commission of its intention to carry out directly the fund's management activities in a Member State, indicating the Member State where it intends to commence a direct performance of the fund's management activities (Article 99 paragraph 1);
130) opens a branch office abroad without a prior permission of the Commission (Article 101 paragraph 1);
131) fails to submit to the Commission, along with a request, a certificate of home Member State's competent authority that the fund meets the requirements stipulated by the regulations of a Member State (Article 102 paragraph 1 item 1);
132) fails, along with a request, to submit to the Commission the articles of association or other general act of the fund (Article 102 paragraph 1 item 2);

133) fails, along with a request, to submit to the Commission the prospectus and the abbreviated prospectus (Article 102 paragraph 1 item 3);
134) fails, along with a request, to submit to the Commission the last half-yearly and annual financial statements (Article 102 paragraph 1 item 4);
135) fails, along with a request, to submit to the Commission information on how to offer its investment units or other appropriate shares on the market in Montenegro (Article 102 paragraph 1 item 5);
136) fails, along with a request, to submit information on the place where the investors in Montenegro may obtain the prospectus, articles of association, reports and other information about the fund, as well as information on the place where the investors in Montenegro will be able to purchase and sell investment units of the fund (Article 102 paragraph 1 item 6);
137) fails to inform the Commission and the competent authority of a home Member State on its intention to carry out directly activities of the funds' management in Montenegro (Article 106 paragraph 1);
138) fails to inform the Commission and the competent authority of a home Member State on changes referred to in Article 106 paragraph 1 of this Law, within the period of 30 days before the intended change of the data (Article 106 paragraph 5);
139) fails to notify all unit-holders in that fund on the transfer of management, within not less than 90 days prior to transfer of management140 (Article 109 paragraph 3);
140) calculates and charges the exit fee to unit-holders who, within the stipulated period, express the intention to exit the Fund (Article 109 paragraph 4);
141) performs mediation activities in purchase and sale of securities (Article 111 paragraph 1 item 1);
142) alienates securities or other assets of the fund or acquires the same from the fund for its own account nor for the account of related persons (Article 111 paragraph 1 item 2);
143) purchases, out of the fund's assets, the property that is not envisaged by its articles of association and its prospectus (Article 111 paragraph 1 item 3);
144) performs transactions which violates the provisions of of this Law and Commission's rules, including provisions on limitations of investments in funds it manages (Article 111 paragraph 1 item 4);
145) alienates the closed-end investment fund's assets and assets that make a mutual investment fund without the appropriate compensation for the fund (Article 111 paragraph 1 item 5);
146) alienates or acquires property on behalf of funds it manages at a price less favorable than the market price or the estimated value of the respected property (Article 111 paragraph 1 item 6);
147) in its own name and for the account of a mutual investment fund, i.e. on behalf of a closed-end investment fund borrows funds contrary to the this Law (Article 111 paragraph 1 item 7);
148) grants loans out of the fund's assets (Article 111 paragraph 1 item 8);
149) uses the fund's assets as a collateral for performance of management company or third parties' obligations or to enable the management company, its employees or related entities the business startup under favorable conditions (Article 111 paragraph 1 item 9);
150) arranges the sale, purchase or transfer of assets between two funds it manages, under conditions other than market conditions or conditions under which it favors one fund in relation to the another one (Article 111 paragraph 1 item 10);
151) assumes the obligations regarding the assets, which, at the time of taking these obligations, is not the property of the investment fund with a public offering (Article 111 paragraph 1 item 11);
152) acquires or alienates, for its own account, investment units in the mutual investment fund under its management (Article 111 paragraph 1 item 12);
153) issues other securities of the mutual investment funds, other than their investment units (Article 111 paragraph 1 item 13);
154) invests the fund's assets in securities or other financial instruments it issues (Article 111 paragraph 1 item 14);
155) fails to perform activities of the collective portfolio management on cross-border basis, by establishing branch offices or under the freedom to provide services in accordance with provisions of this Law (Article 113 paragraph 1);
156) by submitting the request for investment fund management to the competent authorities of a home Member State, fails to submit a written agreement entered into with the depositary and information on the arrangement of transformation of investment management function and administration (Article 114 paragraph 1);
157) fails to inform the competent authority of an open-end fund's home Member State on any change of the documents referred to in Article 114 paragraph 1 (Article 114 paragraph 4);

158) fails to enable the competent authorities of an open-end fund's home Member State to obtain directly from the management company the information referred to in Article 115 paragraph 1 of this Law (Article 115 paragraph 2);
159) fails to establish and implement decision-making procedures and organizational structures that clearly and documentary determine specific reporting procedures and rights and obligations of the persons involved in the procedure (Article 117 paragraph 1 item 1)
160) fails to provide for the authorized persons to be familiar with the procedures to be implemented in order to fulfill its obligations; (Article 117 paragraph 1 item 2)
161) fails to establish and implement adequate internal control systems to ensure compliance at all levels of a management company; (Article 117 paragraph 1 item 3)
162) fails to establish and maintain effective internal reporting systems at all levels of decision-making of a management company as well as a procedure of informing the third parties; (Article 117 paragraph 1 item 4)
163) fails to keep records on its operations and internal organization (Article 117 paragraph 1 item 5);
164) fails to establish and maintain systems and procedures that are adequate to ensure the security, integrity and confidentiality of information according to the nature of information; (Article 117 paragraph 2 indent 1);
165) fails to establish a business continuity policy in order to ensure maintenance of key data and functions and maintenance of services and activities in case of system failure and procedures or timely recovery of such data and functions and re-performing of business and activities; (Article 117 paragraph 2 indent 2);
166) fails to establish and maintain accounting policies and procedures that enable, at the request of the Commission, timely providing of financial reports that accurately and fairly reflects financial positions that are in accordance with accounting rules and procedures; (Article 117 paragraph 2 indent 3);
167) fails to monitor and evaluate, on a regular basis, adequacy and effectiveness of internal control systems and the contracts concluded in accordance with provisions of this Article and to take appropriate measures to eliminate shortcomings (Article 117 paragraph 2 indent 4);
168) fails to meet the conditions for carrying out activities referred to in Article 118;
169) fails to establish an appropriate system of electronic data exchange that enables timely and adequate registration of each transaction from the fund's portfolio or subscription orders or redemption of investment units (Article 119 paragraph 1);
170) fails to establish accounting policies and procedures in accordance with accounting rules of the open-end fund's home Member State in order to ensure accurate calculation of the net asset value of open-end fund's investment and redemption of units per investment unit net value (Article 120 paragraph 1);
171) fails to keep separate accounts for each investment compartment (Article 120 paragraph 3);
172) fails to determine the person authorized to supervise the implementation of policies and measures to remedy deficiencies in acting in accordance with this Law, the internal auditor and the person authorized for the risk management (Article 122 paragraph 1);
173) fails to keep register of all transactions on behalf and for the account of an open-end fund, that contains the data necessary to monitor transactions at any time (Article 123 paragraph 1);
174) fails to register the investment units upon receipt of orders for their subscription and redemption (Article 124 paragraph 1);
175) fails to keep register referred to in Article 124 paragraph 1 of this Law at least five years after the termination of operations or withdrawal of the authorization (Article 124 paragraph 2);
176) fails to identify transactions that represent a conflict of interest between the company and open-end fund's investors (Article 125 paragraph 1);
177) fails to establish the adequate and effective rules for exercising the voting right on financial instruments from the open-end fund's portfolio in the sole interest of the open-end fund (Article 126 paragraph 1);
178) fails to provide equal treatment to all unit-holders (Article 127 paragraph 1 item 1);
179) fails to act in a manner that ensures market stability and integrity (Article 127 paragraph 1 item 2);
180) fails to provide an evaluation system that is fair, accurate and transparent in order to provide acting in the best interest of the unit-holder (Article 127 paragraph 1 item 3);
181) fails to provide implementation of procedures and decision-making procedures in accordance with objectives, investment policy and risk limits stipulated for an open-end fund (Article 127 paragraph 1 item 4);
182) fails to implement risk management policy which requires, before any investments of the fund's assets, analyzing of contribution of transaction to the fund's portfolio, liquidity and risk profiles of the fund (Article 127 paragraph 1 item 5);

183) fails to act with the utmost care when entering or termination of contracts with third parties relating to the performance of risk management obligations (Article 127 paragraph 1 item 6);
184) fails to act with the care of a prudent businessman in the management of fund assets in accordance with professional standards in the interests of shareholders and the fund's unit-holders (Article 128);
185) does not have the authorization issued in accordance with this Law (Article 130 paragraph 1)
186) fails to publish a prospectus, annual report for each financial year and half-yearly financial report covering the first six months of the financial year for each mutual and closed-end fund it manages (Article 152 paragraph 1);
187) fails to provide the Commission with the fund's prospectus, potential amendments and half-yearly reports (Article 157 paragraph 1);
188) fails to publish the price of its investment units in the issue procedure, sale, redemption or payment each time it issues, sells, purchases or pays investment units, and at least once a month (Article 159 paragraph 2);
189) fails to make a brief document containing key investor information for each mutual fund it manages (Article 161 paragraph 1);
190) a document referred to in Article 161 paragraph 1 of this Law does not contain the indication: "the key investor information" or, if the fund is established in Montenegro or its investment fund units are marketed in Montenegro, the wordings "key investor information" are not specified in the Montenegrin language (Article 161 paragraph 2);
191) fails to communicate the key investor information regarding the fund to each mutual fund under its management, and which are sold by the investment fund directly or through another person or entity acting on its behalf and under its full and unconditional responsibility, in a timely manner before the proposed date of investment units subscription (Article 163 paragraph 1);
192) for each mutual fund it manages, and which does not sell the fund directly or through another natural or legal person acting on its behalf and under his responsibility, to submit key investor information to derivatives producers who sell products or advise investors about a possible investment in such a fund or in derivatives that provide exposure to such a fund, at their request (Article 163 paragraph 2);
193) the key investor information are not delivered on a durable medium or available on the website (Article 164 paragraph 1);
194) fails to provide key investor information and all amendments thereto to the Commission (Article 165 paragraph 1);
195) the management rules or instruments of incorporation of the investment fund, do not contain explicit indication of a possibility to the investment fund to be made up of more than one compartment and indication of the rules on management of each individual compartment (Article 167 paragraph 5);
196) grants authorization to the investment compartment, which did not meet the requirements of this Law (Article 167 paragraph 11);
197) is transformed into other forms of business organizations, other than conditions and manner provided for by this Law (Article 168 paragraph 2);
198) fails to implement the transformation in accordance with Article 168 of this Law (Article 169 paragraph 1);
199) disposes of an existing fund's assets or takes other legal actions on behalf and for the account of an existing fund, following the date of entry into force of this Law, until the date of granting the Commission's approval for the transformation, except in case of taking urgent and immediate measures necessary for the protection of fund's assets and interests of shareholders, upon the prior approval of the fund's supervisory board or upon supervisory board's order (Article 172);
200) fails to report to the Commission, the supervisory board of the fund and the depositary on taking measures, actions and procedures to implement the investment program of restructuring in accordance with paragraph 1 of Article 179 (Article 175 paragraph 11);
201) fails to submit to the Commission a request for approval of the transformation program in accordance with Article 177 of this Law, within eight days following the date of conclusion of the contract on management (Article 178 paragraph 1);
202) commences implementation of a transformation program without the prior approval of the Commission (Article 178 paragraph 2);
203) fails to harmonize investments and operations of an open-end fund resulting out of the transformation with the provisions of this Law governing the mutual fund operations and the regulations made under this Law within two years following the date of the Commission's decision approving the transformation program (Article 180 paragraph 1);
204) fails to transfer a management function to another management company, directly or indirectly, until the Commission's decision referred to in Article 184 paragraph 4 of this Law (Article 182 paragraph 2);

205) unilaterally terminates the management and transformation contract until the Commission's decision referred to in Article 184 paragraph 4 of this Law, which states that the transformation is complete (Article 182 paragraph 3);
206) upon expiration of two-year period following the date of the receipt of the Commission's decision on approval for the transformation program, fails to propose to the supervisory board and shareholders of the transformed closed-end fund the development program of the fund and organize the shareholders meeting in order to decide on the proposed program (Article 184 paragraph 1);
207) within the term stipulated, fails to submit to the Commission a report on harmonization of operations (acts, organization and investment) of a transformed closed-end fund and the open-end fund created in the transformation process and the auditor's report, stating that the transformed closed-end fund's investments and investments of the open-end fund in transformation process are in accordance with this Law (Article 184 paragraph 3);
208) fails to pay out the shareholders referred to in Article 185 paragraph 2 of this Law within the term of one year following the date of submission of the payment request (Article 185 paragraph 3);

(2) The responsible person in the management company shall be punished for the offense referred to in paragraph 1 of this Article, with a fine in the amount of EUR 500 to 4,000.

Article 192

(1) A depositary shall be punished for an administrative offence with a fine in the amount of EUR 5,000 to 40,000 if:

1) it does not have a registered office or if not established in Montenegro (Article 18 paragraph 2);
2) fails to perform activities of the depositary without prior approval of the Central bank of Montenegro (Article 18 paragraph 3);
3) does not fulfill conditions regarding solvency and that is not under the constant supervision of operations in accordance with the Commission's regulations (Article 18 paragraph 4);
4) fails to inform the Commission, without delay, on identity of members of management and governing bodies of the depositary and the persons replacing them in performance of management and governing body member's function (Article 18 paragraph 6);
5) fails to submit to the Commission, at the written request, all data obtained during performance of its duty, necessary for the Commission in order to enforce permanent control of operations of a mutual fund (Article 18 paragraph 7);
6) fails to provide that trade, issue, redemption and cancellation of investment units of a mutual fund, for the account of the fund or by a management company, are not performed in accordance with this Law and rules on the fund's management (Article 19 paragraph 2 item 1);
7) the value of mutual fund's investment units is not calculated in accordance with this Law and rules on fund's management (Article 19 paragraph 2 item 2);
8) fails to act in accordance with instructions and orders of the management company, except when instructions and orders of the management company are not in accordance with the law and/or rules on fund management (Article 19 paragraph 2 item 3);
9) fails to ensure that, after transaction in fund's assets is made, a transaction fee is paid to the account of the fund within stipulated or regular period (Article 19 paragraph 2 item 4);
10) fails to ensure that the income of mutual fund is collected in accordance with rules on fund management (Article 19 paragraph 2 item 5);
11) fails to conclude the agreement in written form, on the manner of exchange of data necessary for performance of depositary's activities when a home Member state of the management company is not a home Member State of a mutual fund (Article 19 paragraph 3);
12) fails to act objectively and in the best interest of unit-holders (Article 21 paragraph 1);
13) fails to perform his functions towards a mutual fund in case of termination of contract by the management company provided that a new management company has been designated(Article 22 paragraph 1 item 1);
14) fails to perform his functions towards a mutual fund in case of mutual termination of the agreement or termination of the agreement with the depositary by the management company (Article 22 paragraph 1 item 2);
15) fails to perform his functions towards a mutual fund when winding-up or bankruptcy procedure, i.e. receivership, has been initiated over the depositary (Article 22 paragraph 1 item 3);

16) fails to perform his functions towards a mutual fund in case that supervisory board withdraws authorization to the depositary (Article 22 paragraph 1 item 4);
17) fails to perform all urgent tasks for the purpose of protection of the fund's unit-holders until the appointment of the new depositary, and latest within 60 days following the date of termination of the contract (Article 22 paragraph 2);
18) takes loans on behalf and for the account of the fund (Article 34 paragraph 1);
19) fails to enter into information-sharing agreement for the purpose of performing tasks and activities established by this Law (Article 54 paragraph 1);
20) is organizationally related to a management company; those tasks and activities are carried out by the same persons (Article 85 paragraph 3);

(2) Responsible person in the depositary shall be punished for an administrative offence referred to in paragraph 1 of this Article with a fine in the amount of EUR 500 to 4,000.

Article 193

(1) Certified auditor shall be punished for an administrative offence with a fine in the amount of EUR 500 to 4,000 if:

1) it fails to enter into information-sharing agreement in order to fulfill the obligations of both auditors (Article 55 paragraph 1);
2) fails to make a report as of the date on which the auditor's report of the feeder fund is made (Article 55 paragraph 4);
3) fails to specify in its report, irregularities found in the auditor's report of the master fund and the impact of these irregularities to the feeder fund (Article 55 paragraph 5);
4) fails to inform the Commission about the facts he found or becomes aware of in the course of audit of financial statements or the management company's annual report on operations, concerning operations of the management company or the investment fund, if it proves to be contrary to the law or jeopardizes regular and continuous operations of the management company or a company that contributes to its business activities; or result in rejection of financial statements or express reservation to the auditor's opinion (Article 94 paragraph 5);
5) fails to inform the Commission about the facts he found or became aware during the audit of financial statements of the company related to the fund or organization that contributes to its business activities, and if it is contrary to this Law; (Article 94 paragraph 6 indent 1);
6) fails to inform the Commission, without delay if, in the course of the audit, he found that the information contained in reports or other documentation that was submitted to investors or the Commission by the management company, does not fully and accurately represent the financial status, assets and liabilities of the management company. (Article 94 paragraph 6 indent 2);

Article 194

(1) President or supervisory board's member shall be punished for an administrative offence with a fine in the amount of EUR 500 to 4,000 if:

1) receives compensation from the issuer of securities in which the fund invests its assets (Article 77);
2) fails to convene a shareholders meeting within 120 days following the date of entry into force of this Law and to organize holding of the shareholders meeting of an existing funds within the period of 180 days following the date of entry into force of this Law, in order to decide on issues referred to in Article 170 paragraph5 of this Law. (Article 170 paragraph 1)
3) fails to publish a notification on convening the shareholders meeting in order to decide on the transformation of an existing fund at least twice in two paper media that are distributed within the whole territory of Montenegro and on the website of the fund (Article 170 paragraph 2);
4) fails to organize and ensure that, no later than 90 days following the date of entry into force of this Law, the evaluation of an existing fund's assets and liabilities is made in accordance with the law (Article 170 paragraph 3);

5) fails to exercise the supervision over liabilities of the management company provided for in this Law, transformation program and the management agreement in the course of transformation of the fund (Article 174 paragraph 1);
6) fails to report periodically the shareholders meeting of a transformed closed-end fund (Article 174 paragraph 2);
7) fails to submit the decision to the management company, along with the proposal to amend the management agreement, after the shareholders meeting adopts a draft proposal (Article 174 paragraph 4 indent 2)
8) fails to provide shareholders with the draft proposal of transformation is for inspection in management company's registered office, 30 days prior to the date of holding of shareholders meeting (Article 175 paragraph 6)
9) fails to enter into the contract with the management company whose program has won the highest number of votes of an existing fund in accordance with the decision of the shareholders meeting. (Article 176 paragraph 1)
10) fails to take measures for ensuring execution of urgent and priority tasks necessary for the protection of fund's assets and interests of fund's shareholders, if the management company fails to prepare a transformation program. (Article 176 paragraph 2)
11) within ten days following the date of submission of offers referred to in paragraph 1 of Article 187, fails to provide the existing fund's shareholders with submitted offers for the conclusion of the management agreement; (Article 187 paragraph 2 indent 1)
12) fails to organize the shareholders meeting in order to decide on offers referred to in Article 187 paragraph 2 indent 1, within the period of 30 days following the date of submission of offers (Article 187 paragraph 2 indent 2).

Article 195

(1) Legal person shall be punished shall be punished for an administrative offence with a fine in the amount of EUR 5,000 to 40,000 if:

1) performs depositary activities without the approval of the Central Bank of Montenegro (Article 18 paragraph 3);
2) uses a type or description misleading that the entity is established and / or operates in accordance with provisions of this Law, which is not authorized in accordance with this Law (Article 167 paragraph 1);

(2) Responsible person in the legal person shall be punished with the fine in the amount of EUR 500 to 4,000 for the offence referred to in paragraph 1 of this Article.

(3) Natural person shall be punished with the fine in the amount of EUR 500 to 4,000 for the offence referred to in paragraph 1 of this Article.

Article 196

Natural person shall be punished for an administrative offence with a fine in the amount of EUR 500 to 4,000 if performs activities that could lead to conflict of interest (Article 122 paragraph 2);

Pursuant to Article 82 paragraph 1 item 2 and Article 91 paragraph 1 of the Constitution of Montenegro, the 24th Parliament of Montenegro, at the seventh sitting of its second regular session in 2010, on 22 December 2010, issued the following

LAW ON MISDEMEANORS

Fine

Article 24

(1) A fine may be prescribed within a specific range or in a fixed amount.

(2) A fine may be prescribed within the following ranges:

1) For natural and responsible persons in an amount ranging from 30 euro to 2 000 euro;

2) For entrepreneurs in an amount ranging from 150 euro to 6 000 euro;

3) For legal entities in an amount ranging from 500 euro to 20 000 euro.

(3) For minor misdemeanours a fine in a fixed amount may be prescribed as follows:

1) For natural and responsible persons in an amount up to 200 euro;

2) For entrepreneurs in an amount up to 400 euro;

3) For legal entities in an amount not exceeding 2 000 euro.

(4) Notwithstanding paragraph 2 of this Article, for misdemeanours in the area of domestic violence protection, health protection, environmental protection, consumer protection, protection of market competition, cultural assets, construction, public information, workplace safety, public revenue, customs, foreign trade and foreign exchange dealings, services and securities trade, a fine that may not exceed double the maximum amount set forth in paragraph 2 of this Article.

(5) For the most severe misdemeanours provided for in paragraph 4 of this Article a fine between 1-10% of the protected value injured as a result of the misdemeanour may be prescribed, and the special minimum and maximum percentage must be indicated.

(6) For the most severe misdemeanours in the area of preventing, limiting and undermining competition a fine may be prescribed in the range between 1-10% of the total annual income of the market participants, gained in the financial year preceding the year the misdemeanour was committed.

(7) For misdemeanours committed for gain, and as a result of which material gain was acquired, the offender may receive a heavier penalty, but no more than double the amount of the fine prescribed for that particular misdemeanour.

Concurrence

Article 29

(1) Should an offender, by a single act or a number of acts, commit several misdemeanours, for which he is simultaneously tried before a court, the court shall first determine the sentences for each individual misdemeanour, and then impose a single aggregate sentence.

(2) The aggregate sentence shall be imposed in accordance with the following rules:

1) If a sentence of imprisonment has been determined as the penalty for all of the concurrent misdemeanours, an aggregate sentence of imprisonment that may not exceed 60 days shall be imposed;

2) If a fine has been determined as the penalty for all of the concurrent misdemeanours, an aggregate fine equal to the sum of all of the individually determined fines shall be imposed, but the aggregate fine may not exceed the maximum level of such penalties as provided by this Law;

3) If a sentence of imprisonment has been determined as the penalty for some of the concurrent misdemeanours, and a fine for the others, one term of imprisonment and one fine shall be imposed in accordance with items 1 and 2 of this paragraph;

4) If community service has been determined as the penalty for all of the concurrent misdemeanours, an aggregate sentence of community service that may not exceed 80 hours shall be imposed.

Types of Protective Measures

Article 42

(1) The following protective measures may be set for misdemeanours:

1) Seizure of items;

2) Prohibition to practice a profession, business activity or duty;

3) Suspension of driver's license;

4) Mandatory alcohol addiction treatment;

5) Mandatory drug addiction treatment;

6) Mandatory psychiatric treatment and internment in a health care institution;

7) Mandatory psychiatric outpatient treatment;

8) Public announcement of decision;

9) Deportation of foreign nationals from Montenegro.

(2) Other protective measures and the conditions and time limits for imposing such measures may be established in laws regulating misdemeanours.

(3) The protective measures prescribed by this Law and by other laws may, unless otherwise provided in this Law, be prescribed and applied for a period of time that may not be shorter than 30 days or longer than two years.

(4) The protective measure "seizure of items" shall be permanent.

Public Announcement of Decision

Article 47

(1) The court shall impose the protective measure of public announcement of the decision if it finds that it would be beneficial for the public to be acquainted with the decision, and in particular if publication of the decision would help eliminate a threat to the lives or health of people or help safeguard the trade of goods and services or the economy.

(2) Depending on the significance of a misdemeanour, the court shall decide whether the decision shall be announced in the press, on radio or television or in more than one of the aforementioned mass media, as well as whether the Statement of Reasons shall be announced in full or in part, thereby taking care to ensure that the manner of announcement allows the decision to be noted by all those in whose interest it should be made public.

(3) Public announcement of a decision may be carried out no later than 30 days from the date it took effect as final and legally binding.

(4) The law prescribing a misdemeanour may provide for the mandatory imposition of the protective measure of public announcement of a decision.

(5) The costs of public announcement of a decision shall be borne by the convicted person.

Register of Fines

Article 54

(1) The Register of Fines is an electronic database into which data on all fines imposed for misdemeanours and costs awards (costs of proceedings, legal costs) are entered.

(2) A court that rendered a decision or the authorised body that issued the Misdemeanour Order shall, without delay and in appropriate form, enter information on the imposed fines and costs awards into the Register of Fines.

(3) A court that receives a Petition for Court Adjudication, provided for in Article 150 of this Law, shall without delay and in appropriate form, enter that information into the Register of Fines, and delete the imposed fine and costs award.

(4) Fines and costs awards imposed by means of a final and enforceable Misdemeanour Order or a final and legally binding Misdemeanour Decision shall without delay be entered into the Register of

Fines as debt and remain recorded in the database until the convicted person, or sentenced person, effects payment of the full amount of the fine and the costs of proceedings.

(5) The Ministry responsible for judicial affairs shall administer the work of the Register of Fines and ensure its functioning.

(6) The contents and manner of managing the Register of Fines shall be prescribed by Ministry responsible for judicial affairs.

Limitation Period for Initiating and Conducting Misdemeanour Proceedings

Article 59

(1) Misdemeanour proceedings cannot be initiated or conducted in the event one year has passed from the date the misdemeanour was committed.

(2) The running of the period of limitations for the prosecution of a misdemeanour shall be suspended for any time during which, by law, the prosecution cannot be instituted or continued.

(3) The running of the period of limitations shall be interrupted and suspended by every procedural action taken by the competent body for the purpose of prosecuting the person that committed the misdemeanour.

(4) The running of the period of limitations shall resume after any interruption.

(5) In exceptional cases, for misdemeanours in the area of health protection, environmental protection, protection of competition, construction, customs, foreign trade and foreign exchange dealings, public revenues, political party funding and fundraising for elections, movement of goods and services and securities trade, a longer period of limitations for initiating and conducting misdemeanour proceedings, which may not exceed three years, may be provided by a separate law.

(6) The period of limitations set for the prosecution of a misdemeanour expires whenever twice the time set forth in the statute of limitations for misdemeanour prosecution has elapsed.

Submitting a Petition

Article 143

Misdemeanour proceedings may be initiated on the basis of:

1) A Petition for Court Adjudication of the Misdemeanour Order, or

2) A Petition to Initiate Misdemeanour Proceedings.

Misdemeanour Order

Article 144

(1) An authorized body shall issue a Misdemeanour Order if it is determined in any of the following ways that a misdemeanour that is within its jurisdiction has been committed:

1) Direct observation of an authorized officer while conducting inspection, supervision or review, as well as while performing an inspection of the official records of a competent body;

2) On the basis of information obtained by means of supervision or measurement devices;

3) In the course inspecting documentation, premises and goods or through other legal means;

4) On the basis of the accused person's admission that he committed the misdemeanour, given before an authorized body at the scene or at another court or administrative proceeding.

(2) A Misdemeanour Order shall be issued pursuant to the conditions set forth in paragraph 1 of this Article when a penalty is prescribed in a fixed amount. A Misdemeanour Order may also be issued pursuant to the conditions set forth in paragraph 1 of this Article when a fine is prescribed in a range or when a fine is determined using a mathematical formula.

(3) If the fine is prescribed in a range, the authorized body shall impose the minimum prescribed fine in the Misdemeanour Order.

(4) Apart from a penalty, only a protective measure prohibiting the offender from driving a motor vehicle for the shortest provided length of time and a protective measure ordering seizure of items, as well as penalty points, may be imposed in a Misdemeanour Order.

(5) If a person commits a number of concurrent misdemeanours, an authorized body may, by a Misdemeanour Order, impose an aggregate fine that is equal to the sum of all of the individual fines imposed in their minimum amounts, and if a protective measure was prescribed for one or more of the committed misdemeanours, it also may impose a protective measure ordering seizure of items or protective measure prohibiting the offender from driving a motor vehicle for the shortest provided length of time.

(6) If the authorised body, instead of issuing a Misdemeanour Order as provided in paragraph 2 of this Article, filed a Petition to Initiate Misdemeanour Proceedings for a misdemeanour punishable by a fixed fine, the court shall issue a decision rejecting the Petition.

Accepting Responsibility

Article 147

(1) The accused may accept responsibility for a misdemeanour by paying the fine and fulfilling all other obligations set forth in the Misdemeanour Order within the specified deadline, or by notifying the authorized body that he accepts the sanction set forth in the in the Misdemeanour Order.

(2) In the event the accused accepts responsibility pursuant to paragraph 1 of this Article, the Misdemeanour Order shall become final and enforceable.

THE LAW ON MUTUAL LEGAL ASSISTANCE

IN CRIMINAL MATTERS

(Official Gazette of Montenegro, No. 04/2008 and 36/2013)

Article 2

(1) Mutual legal assistance shall be provided in accordance with an international agreement.

(2) If there is no international agreement or if certain issues are not regulated under an international agreement, mutual legal assistance shall be provided in accordance with this Law, provided that there is reciprocity or that it can be expected that the foreign state would execute the letter rogatory for mutual legal assistance of the domestic judicial authority.

Article 4

(1) Domestic judicial authority shall forward letters rogatory for mutual legal assistance to foreign judicial authorities and receive the letters rogatory for mutual legal assistance of the foreign judicial authorities through the ministry responsible for the judiciary (hereinafter referred to as the "Ministry").

(2) In cases where there is no international agreement or reciprocity, the Ministry shall deliver and receive letters rogatory for mutual legal assistance through diplomatic channels.

(3) Exceptionally, in cases when provided for under an international agreement or where there is reciprocity, the national judicial authority may deliver directly or indirectly to the competent foreign judicial authority and receive letters rogatory for mutual legal assistance of the foreign state, with the obligation to deliver copy of letter rogatory to the Ministry.

(4) In urgent cases, provided that there is reciprocity, letter rogatory for mutual legal assistance may be delivered and received through the National Central Bureau of the Interpol.

(5) The courts and the state prosecutors' offices shall be responsible for provision of mutual legal assistance in accordance with the law.

Article 6

(1) Unless otherwise has been provided for by an international agreement or this Law, the letter rogatory for mutual legal assistance of the domestic or of the foreign judicial authority shall be accompanied with the translation of the letter rogatory into the language of the requested state, or one of the official languages of the Council of Europe, if the requested state accepts it. The replies to the letters rogatory of the foreign judicial authorities do not need to be translated.

(2) Domestic judicial authority shall also proceed upon the letter rogatory for mutual legal assistance of the foreign judicial authority if the letter rogatory has been presented electronically or by some other means of telecommunication providing delivery receipt, if it may verify its authenticity and if the foreign judicial authority is prepared to deliver the original of the letter rogatory within 15 days at latest.

II. EXTRADITION OF ACCUSED AND SENTENCED PERSONS

Article 10

The extradition of the accused or sentenced persons shall be requested and enforced in accordance with this Law unless otherwise has been provided for under an international agreement.

Article 11

(1) The conditions for the extradition upon the request of the Requesting State shall be as follows:

1) that the person claimed is not a national of Montenegro;

2) that the offence for which extradition is requested was not committed in the territory of Montenegro, against Montenegro or its national;

3) that the offence motivating the request for extradition is a criminal offence both under the domestic law and under the law of the country in which it was committed;

4) that the criminal prosecution or enforcement of criminal sanction has not been barred by the lapse of time under the domestic law before the person claimed has been detained or examined as an accused;

5) that the person claimed has not been already convicted by a domestic court for the same offence or he has not been acquitted of the same offence by the domestic court in a final and legally binding manner, except if the requirements prescribed by the Criminal Procedure Code for retrial have been met; or criminal proceedings have not been instituted in Montenegro for the same offence committed against Montenegro or a national of Montenegro; or the security for the fulfilment of property law claim of the victim has been provided if the proceedings have been instituted for the offence committed against a national of Montenegro;

6) that the identity of the person claimed has been established;

7) that the requesting state presented facts and sufficient evidence for a grounded suspicion that the person claimed committed the criminal offence or there is a final and legally binding judicial decision;

Article 12

(1) The extradition shall not be allowed for a political criminal offence, an offence connected with a political criminal offence or a military criminal offence within the meaning of the European Convention of Extradition (hereinafter referred to as "political and military criminal offences").

(2) Prohibition referred to in paragraph 1 above shall not apply to the criminal offences of genocide, crime against humanity, war crimes and terrorism.

Article 13

(1) The extradition shall not be granted for the criminal offence punishable under the domestic law and the law of the Requesting State by imprisonment for a term of up to one year or a fine.

(2) If the extradition of the sentenced person is requested to serve the sentence, his extradition shall not be granted if the duration of the imposed imprisonment sentence or the remaining portion thereof which is yet to be served does not exceed four months.

(3) If the extradition request is related to the accused or convicted of various offenses, of which conditions for extradition for one criminal offense were met, pursuant to paragraphs. 1 and 2 of this Article, extradition may be allowed for the crimes for which these conditions have not been met.

Article 14

If the law of the requesting state prescribes death penalty for the offence for which the extradition is requested, extradition may be granted only if that state gives assurance that the death-penalty will not be imposed or carried out.

Article 15

(1) The procedure for extradition of the accused or sentenced person shall be initiated upon the letter rogatory of the Requesting State, or by determining detention on the grounds of the international arrest warrant.

(2) Letter rogatory for extradition shall be delivered to the Ministry.

(3) The following shall be enclosed to the letter rogatory:

1) means required to establish the identity of the accused and/or of the sentenced person (accurate description, photographs, fingerprints and the like);

2) certificate or other information on the nationality of the person claimed;

3) indictment, verdict or detention order, or any other document equivalent to indictment, verdict or detention order, in the original or certified copy, which shall contain the forename and surname of the person claimed and other information necessary to establish his identity, description of the offence, legal qualification of the offence and evidence for a grounded suspicion;

4) excerpt from the wording of the criminal law of the requesting country which is to be applied or which has been applied against the accused for the offence for which extradition is requested, and if

the offence was committed in the territory of a third country, the excerpt from the wording of the criminal law of that country as well.

(4) If the information and documents referred to in paragraph 3 above were submitted in a foreign language, they shall be accompanied by a certified translation into the Montenegrin language.

Article 16

(1) The Ministry shall deliver letter rogatory for the extradition to the investigating judge of the court within the jurisdiction of which the person claimed resides or within the jurisdiction of which the person claimed happens to be.

(2) If the domicile or residence of the person claimed is unknown, his domicile or residence shall be established through the state administration authority competent for affairs relating to domicile and residence.

(3) If the letter rogatory was submitted in accordance with Article 15 above, the investigating judge shall issue the order to detain the person claimed, if there is a danger that the person shall avoid the procedure of extradition, or if other reasons referred to in the Criminal Procedure Code exist, and/or he shall undertake other measures to ensure his presence, unless it is obvious from the letter rogatory and delivered information and documents that the conditions for extradition have not been met.

(4) Detention referred to in paragraph 3 above may last until the decision on extradition is enforced at latest but no longer than six months.

(5) Upon a reasoned request of the Requesting State, the panel of the competent court may extend the duration of detention referred to in paragraph 3 above in justified cases for additional two months.

(6) The investigating judge shall, after he establishes the identity of the person claimed, inform him without delay why and based on which evidence his extradition is requested and the investigating judge shall ask him to present his defence.

(7) The record shall be made of examination and presenting of defence. The investigating judge shall be obliged to inform the person claimed immediately that he may engage a defence attorney, or that a defence attorney ex officio may be appointed for him if the defence is mandatory for the criminal offence in question pursuant to the Criminal Procedure Code.

Article 17

(1) Detention aimed at extradition may be ordered under conditions referred to in Article 15 of this Law even before the letter rogatory of the Requesting State is received, if requested by it, or if there is a grounded suspicion that the person claimed committed the criminal offence for which he can be extradited to the requesting state.

(2) Investigating judge shall release the person claimed when the reasons for detention terminate or if the letter rogatory has not been submitted within the period of time he determined while taking into consideration all circumstances, and which cannot exceed 40 days from the date of detention. The

detention ordered pursuant to paragraph 1 above may be revoked if the letter rogatory has not been submitted within 18 days from the date of detaining the person claimed.

(3) The Ministry shall inform the Requesting State about the deadlines determined by the investigating judge without delay. Without prejudice to the above, if there are justified reasons, the investigating judge may extend the duration of detention for additional 30 days at most, if requested by the Requesting State.

Article 18

(1) Upon hearing by the state prosecutor and the defence attorney, the investigating judge shall undertake other actions, if necessary, to determine if the conditions for extradition and/or surrender of the items on which or by which the criminal offence was committed, if these had been confiscated from the person claimed, are fulfilled.

(2) After the actions referred to in paragraph 1 above have been completed, the investigating judge shall deliver the case files to the competent panel along with his opinion.

(3) If the criminal proceedings are underway before a domestic court against the person claimed for the same or another criminal offence, the investigating judge shall note that in the case files.

Article 19

(1) If the Chamber of the competent court finds that the conditions for extradition prescribed by this Law have not been met, it shall make a decision to reject the letter rogatory for extradition.

(2) The order referred to in paragraph 1 above shall be submitted by the court ex officio directly to the higher court which may confirm, repeal or reverse the decision after it hears the state prosecutor.

(3) If the person claimed is held in detention, the Chamber of the competent court may decide that he remain in detention until the decision rejecting his extradition becomes final and legally binding.

(4) Final and legally binding decision rejecting the extradition shall be submitted to the Ministry which shall inform the requesting state thereof.

Article 20

(1) If the Chamber of the competent court finds that the conditions for extradition prescribed by this Law are met, it shall confirm this by passing a decision.

(2) The person claimed shall have right to complain against the decision referred to in paragraph 1 above directly to the court of higher instance within three days after the receipt thereof.

Article 21

If the court of second instance confirms the decision referred to in Article 20 above, or if the complaint has not been lodged against the decision of the court of first instance, the case shall be delivered to the minister competent for judiciary (hereinafter referred to as the Minister), in order to make decision whether to grant extradition.

Article 22

(1) In the event referred to in Article 21 above, the Minister shall pass the decision granting or refusing the extradition.

(2) When he grants the extradition, the Minister may make a decision to postpone the extradition because criminal proceedings are underway before a domestic court for another criminal offence against the person claimed or because this person is serving the imprisonment sentence in Montenegro.

(3) The Minister shall not grant the extradition of the person who enjoys the right of asylum in Montenegro or where it can be reasonably assumed that the person claimed shall be subjected to prosecution or punishment because of his race, religion, nationality, belonging to a specific social group or for his political beliefs, or that his status would be made more difficult for one of these reasons.

(4) The Minister shall refuse the extradition if the person claimed has not been given the possibility to have a defence attorney in the criminal proceedings preceding the extradition.

Article 23

1) When extradition approved, the person claimed whose extradition has been approved, may not be prosecuted for another criminal offence committed prior to the extradition; the punishment for another criminal offence committed prior to the extradition cannot be enforced against the person claimed; nor a punishment more severe than the one to which he has been sentenced can be enforced against the person claimed, without the approval of the competent authority of Montenegro.

2) The approval referred to in paragraph 1 of this Article shall not be required if the person whose extradition was allowed during the extradition proceedings before the investigating judge issued a statement that he/she did not oppose the prosecution, the execution, the application of severe punishment or extradition to a third country for another before extradition committed criminal offense (hereinafter referred to as the waiver).

(3) A statement of waiver is given on the record before the competent court in accordance with the Criminal Procedure Code in a way that guarantees that the person whose extradition is requested voluntarily gave the statement and was aware of its consequences. The given statement of waiver cannot be revoked.

(4) The limitation of paragraph 1 of this Article or statement of waiver shall be noted in the decision granting the extradition.

Article 24

(1) The requesting state shall be notified of the decision concerning extradition through diplomatic channels.

(2) The decision granting extradition shall be submitted to the administration authority competent for police affairs which shall escort the person claimed to the border crossing where at an agreed place he will be surrendered to the authorities of the requesting state.

Article 25

(1) The requesting state shall take over the person the extradition of whom has been granted within 30 days as of the date of delivery of the decision on extradition.

(2) The Minister may extend the deadline referred to in paragraph 1 above for additional 15 days upon reasoned request of the requesting state.

(3) If the person the extradition of whom has been granted has not been taken over upon the expiry of the deadline referred to in paragraphs 1 and 2 above, he shall be immediately released, and the Minister may refuse repeat extradition request for the same criminal offence.

Article 26

If the extradition of the same person is requested by more than one country, either for the same offence or for different offences, the decision shall be taken having regard to seriousness of the criminal offences, the place of commission, the respective dates of the requests, the nationality of the person claimed, the possibility of subsequent extradition to another state, and other circumstances.

Article 27

(1) If the extradition is requested by a foreign state from another foreign state and the person claimed would have to be escorted through the territory of Montenegro, transit may be granted by the Minister upon the letter rogatory by the requesting state provided that the person concerned is not a national of Montenegro and that the extradition is not enforced for political or military criminal offence.

(2) Letter rogatory for transit of the person through the territory of Montenegro shall contain the information and documents referred to in Article 15 paragraph 3 of this Law.

(3) In the case of transit of the person through the territory of Montenegro by air transit, if no landing is expected, it shall not be necessary to obtain permit referred to in paragraph 1 above.

(4) The requesting state shall notify the Ministry of transit referred to in paragraph 3 above. The notification shall contain information such as: the name of the person escorted through the territory of Montenegro, the state to which the person is extradited, the criminal offence for which the person is extradited, and the time of air transit.

Article 28

(1) At the request of the requesting state, the competent court shall seize and surrender, in accordance with the domestic law, items which may serve as evidence materials or that resulted from the commission of criminal offence.

(2) The items referred to in paragraph 1 above shall be surrendered even in case when an already approved extradition may not be enforced due to the death or escape of the person claimed.

(3) If the items referred to in paragraph 1 above are subject to seizure or confiscation in the territory of Montenegro, they may be temporarily retained or surrendered provided that they are returned in connection with the ongoing criminal proceedings.

(4) The items referred to in paragraph 1 above, to which Montenegro and third persons have rights, shall be returned to Montenegro as soon as possible after the hearing is completed. The costs of returning of items shall be borne by the requesting state.

Article 29

(1) The person for the extradition, if the conditions for extradition prescribed by this Law have been met, may be extradited within a summary procedure if the person claimed consented.

(2) The consent referred to in paragraph 1 above shall be entered for the record before a competent court in accordance with the Criminal Procedure Code, in a way ensuring that the consent has been given voluntarily and that the person claimed has been aware of all consequences of such consent. The consent once given cannot be revoked.

(3) In the case where the process of extradition of the accused or convicted was instituted by the imposition of custody at an international arrest warrant, the Requesting State shall be notified within 10 days of the consent referred to in paragraph 1 of this Article and the statement of waiver, with note that it is not required to submit the letter rogatory.

(4) The decision on extradition in a summary procedure shall be passed by a competent court, which shall without delay inform the Ministry, and the Ministry shall further notify the Requesting State.

(5) The extradition within a summary procedure shall have the same force and effect as the extradition within an ordinary procedure.

Article 30

The costs of extradition incurred outside the territory of Montenegro shall be incurred by the requesting state**.**

Article 31

(1) If criminal proceedings are underway in Montenegro against a person located in a foreign state or if the person located in a foreign state has been sentenced by a competent Montenegrin court, the Minister may submit the letter rogatory for extradition.

(2) The letter rogatory shall be submitted to the requested state through diplomatic channels and it shall be accompanied by documents and information referred to in Article 15 of this Law.

Article 32

(1) If there is danger that the person claimed will flee or hide, the Minister may request to order to detain that person temporarily or to undertake other measures required to prevent his escape even before the actions are taken in accordance with Article 31 of this Law.

(2) The letter rogatory for temporary detention shall contain specifically the information on the identity of the person claimed, the name of the criminal offence for which the extradition is requested, indictment, verdict or detention order, date, place and name of the authority ordering detention, and/or information about the validity of verdict, as well as the statement that the extradition shall be requested through regular channels.

Article 33

(1) If the person claimed is extradited, he may be criminally prosecuted and/or the punishment may be enforced against him only for the criminal offence for which the extradition has been granted, unless he has waived this right.

(2) If the extradition has been granted under certain conditions with respect to the type or duration of sanction which may be imposed and/or enforced and if it has been accepted under such conditions, the court shall be bound by such conditions when pronouncing a sentence; while if the enforcement of an already imposed sentence is the subject of the extradition, the court adjudicating in the highest instance shall reverse the verdict and impose the punishment in accordance with the conditions of extradition.

(3) If the person extradited had been held in detention in a foreign country for the criminal offence for which he has been extradited, the time spent in detention shall be accounted for in the imprisonment sentence.

III. TRANSFER AND ASSUMING OF CRIMINAL PROSECUTION

Article 34

(1) If a foreigner whose place of residence is in a foreign state committed a criminal offence in the territory of Montenegro, that state can be surrendered the criminal files for the purpose of criminal prosecution and trial if the foreign state does not object to it.

(2) Before confirmation of the indictment, the decision to transfer criminal prosecution shall be taken by the competent state prosecutor; and after the confirmation of the indictment the decision to transfer criminal prosecution shall be taken by the panel of the competent court composed of three judges.

(3) If the victim is a national of Montenegro, the transfer of criminal prosecution shall not be allowed if the victim opposes to it, unless a security for the settlement of his property law claim has been provided.

Article 35

The competent court or the state prosecutor shall deliver the letter rogatory for the transfer of the criminal prosecution accompanied with the decision on the transfer of criminal prosecution and the case files to the Ministry.

The Ministry shall deliver the letter rogatory for the transfer of the criminal prosecution to the competent authority of the requested state, in accordance with Article 4 of this Law.

Article 36

(1) Upon letter rogatory of the Requesting State for Montenegro to assume the criminal prosecution of a national of Montenegro or a person whose residence is in Montenegro for the criminal offence committed abroad, the competent authority in Montenegro may assume the criminal prosecution:

1) when extradition is not allowed;

2) if the competent authority of the Requesting State states that upon the final decision of the competent authority in Montenegro it will not prosecute the defendant for the same offense.

(2) The letter rogatory referred to in paragraph 1 of this Article shall be submitted with the documents to the competent public prosecutor in whose territory the person resides.

(3) If the property law claim has been lodged with the competent authority of the Requesting State, action shall be undertaken as if it were presented to the competent court.

(4) The Requesting State shall be informed of the refusal to assume criminal prosecution as well as of the final and legally binding decision passed within the criminal proceedings, in accordance with Article 4 of this Law.

Article 37

(1) If the criminal prosecution has been assumed upon the letter rogatory referred to in Article 36 of this Law, domestic law shall apply.

(2) Procedural action taken under the regulations of the Requesting State is equated with procedural action taken against the Montenegrin legislation, unless it is contrary to the fundamental principles of the domestic legal order and international standards on the protection of human rights and fundamental freedoms.

(3) The law of the foreign state shall apply in case when it is more lenient for the accused.

IV. ENFORCEMENT OF FOREIGN CRIMINAL VERDICT

Article 38

(1) Competent Montenegrin court shall, to enforce final and legally binding criminal verdict of a foreign court if this has been prescribed under an international agreement or if there is reciprocity, make a decision on the imposition of criminal sanction, or a decision ordering the suspension or revocation of property obtained by criminal activity, in accordance with domestic law.

(2) In the case referred to in paragraph 1 above, the competent court shall pass the decision within a panel composed of three judges without presence of the parties.

(3) Territorial jurisdiction of the court shall be defined according to the last place of residence of the sentenced person in Montenegro and if the sentenced person has never reported his place of residence in Montenegro – according to the place of birth. If the sentenced person neither has had his place of residence nor was born in Montenegro, the Supreme Court of Montenegro shall identify one of the courts having subject-matter jurisdiction before which the proceedings shall be conducted.

(4) In the operative part of the verdict referred to in paragraph 2 of this Article, the court shall insert full wording of the operative part and the name of the court from the verdict of the foreign court and it shall pronounce the sentence upon letter rogatory. In the particulars of judgement, the court shall state reasons it took into account in the pronouncement of the sanction and refer to the reasons of the foreign court the verdict of which is to be enforced.

(5) State prosecutor and the sentenced person or his defence attorney may lodge a complaint against the verdict.

Article 46

Mutual legal assistance shall not be provided if the letter rogatory concerns military criminal offence.

Article 47

Mutual legal assistance referred to in Article 42 of this Law may be refused:

1) if the letter rogatory of the requesting state concerns political criminal offences;

2) if the execution of the letter rogatory of the requesting state is likely to prejudice the sovereignty, constitutional order, security or other essential interests of Montenegro.

LAW ON NATIONAL PAYMENT OPERATIONS

(OGM 61/08, 40/11, 31/12)

Definition of Transfer of Funds

Article 3

(1) Transfer of funds (hereinafter: the transfer) shall be a transfer of monetary assets executed at the originator's order by the performing institution referred to in Article 4 of the Law hereof.

(2) A postal transfer executed through a post office shall not be considered a transfer within the meaning of this Law.

Performing Institution

Article 4

Performing institutions within the meaning of this Law shall be:

1) the Central Bank;
2) banks, foreign bank branches and other legal entities licensed or approved by the Central Bank to execute transfers.

Transfer Execution Account

Article 11

(1) The transfer execution account (hereinafter: the account) shall be opened in line with a contract concluded between the performing institution and a client.

(2) A client may have several accounts in one performing institution and accounts with several performing institutions.

(3) The account shall be closed under conditions stipulated in the Law or other applicable regulation or the contract referred to in paragraph 1 of this Article.

(4) The account of the client that is frozen based on a decision of the competent authority cannot be closed, unless otherwise stipulated by the law.

(5) The Central Bank shall prescribe the structure of the account and more detailed conditions and the manner of opening and closing the account.

Registry of Accounts
Article 12

(1) The Central Bank shall maintain the Central Registry of Accounts as a unique information database on the accounts and their holders.

(2) The data in the Central Registry of Accounts shall be confidential, unless otherwise stipulated by the law.

(3) The performing institution is obliged to maintain the registry of accounts of its clients.

(4) The performing institution shall furnish the Central Bank with information on opened accounts, changes in information on the account and information referring to the closing of the account no later than by the end of the banking day when the account has been opened, closed or when the change has occurred.

(5) The Central Bank shall prescribe the contents of the Central Registry of Accounts.

Filing and Safekeeping of Documentation
Article 16

The performing institution shall be obliged to archive the documentation on executed transfers and store them for five years, and to keep the electronic data on executed transfers for ten years from the date of the execution of the transfer.

Pursuant to Article 82 paragraph 1 item 2 and Article 91 paragraph 2 of the Constitution of Montenegro, the 24th Parliament of Montenegro, at the eleventh sitting of the first ordinary (spring) session in 2011, on 22 July 2011, has adopted

LAW ON NON-GOVERNMENTAL ORGANIZATIONS

Foreign Non-Governmental Organization

Article 4

Foreign non-governmental organization (hereinafter: foreign organization) may operate on the territory of Montenegro in order to achieve goals and interests which are not prohibited by the Constitution and law.

Foreign organization, in the meaning of this Law, is a non-governmental organization with the legal entity status, whose head office is in a different state, and which is established in line with the regulations of that state aiming at achieving common or general goals and interests.

Law Application

Article 5

This Law shall not apply to political parties, trade unions, business association, other organizations and foundations established by the state, as well as other forms of association, which are established by separate law or on the basis of separate law, except for the issues not regulated by those separate laws.

Founding Act

Article 11

Non-governmental organization shall be established by the founding act which shall consist of the following:

1) Information on its founders:

- personal name or founder's title;

- unique master citizen number of its founder, and if its founder is a foreign national, travel document number and the name of the state issuing the travel document;

- tax ID number and official seal if its founder is a legal person;

- signature of its founder, i.e. authorized person in legal entity, if its founder is legal person;

2) Information on non-governmental organization:

- name;

- address and its head office;

- goals and activity;

- personal name, unique master citizen number, address and signature of the person authorized to represent the organization, and if that person is a foreign national, his/her personal name, travel document number and the name of the state that issued the travel document, as well as his/her signature.

Apart from the information from paragraph 1 of this Article, the founding act also includes information on the president and the members of the managing board, as well as information about the initial assets of the foundation, if the foundation has initial assets.

If the foundation is established by a testament, the testament must have information on founders, goals and foundation activities, as well as the information on the person authorized to undertake all the activities necessary for establishment and registration of the foundation.

Statute

Article 12

Non-governmental organization shall have a statute.

The statute of non-governmental organization regulates the following:

- name and head office of the organization, its goals and activities, as well as the bodies of the non-governmental organization;

- authorization of the governing bodies and their composition, manner of election, recall, work and convening sessions of the governing bodies, quorum and decision making process, as well as the mandate of the governing bodies’ members;

- manner of election and recall of person authorized for representation and his/her mandate;

- manner of statute amendments and manner of adopting other general acts of the organization;

- manner of conducting activities in a transparent way;

- manner of financing, as well as the commercial activity that the non-governmental organization will perform if it opts for that;

- assets management, including management of assets in case of termination of non-governmental organization activities;

- seal form and content;

- termination of work;

- other issues important for work and operations of non-governmental activity.

The statute of association also regulates the following:

- conditions for acquiring and losing member status;

- rights and obligations of members, including the way of exercising right to convene assembly when it has not been convened within the deadline determined by the statute;

- manner of keeping records of the members.

The foundation statute may also regulate special rights of founders towards the foundation, as well as the issues on foundation's initial assets, if the foundation has initial assets.

Jurisdiction

Article 14

Association, foundation and foreign organization register in written and electronic form shall be kept by the state administration body competent for public administration (hereinafter: the Ministry).

The ministry shall prescribe the content and the manner of keeping registers, as well as the application forms for registration.

Register Availability

Article 16

Information from the registers from Article 14 paragraph 1 of this Law shall be public and shall be published on the web site of the Ministry, unless otherwise prescribed by a separate law.

Change of facts and information

Article 19

Non-governmental organization or the branch office of a foreign organization shall submit to the Ministry, via person authorized to represent them, the notification on any change of facts and information entered into the register, within 30 days from the day the change has occurred.

In addition to the notification from paragraph 1 of this Article, non-governmental organization shall submit the decision of the body in charge of non-governmental organizations, on the change of facts and information, i.e. the minutes from the assembly session or managing board of that organization or some other evidence on the change of facts and information.

Change of facts and information from paragraph 1 of this Article shall not produce any legal consequences for third persons if it is not entered into the register, unless the third person knew or must have known about the change.

Foreign Organization's Activity

Article 20

Foreign organization may have its activities on the territory of Montenegro if it has registered its branch office with the Ministry.

Registration of the branch office from paragraph 1 of this Article shall be performed on the basis of application which shall contain:

- proof of legal entity status in the state where that organization has its head office;

- certificate from the founding act or statute which lay down the aims of the foreign organization;

- personal name and address of the person authorized for representation of the foreign organization's branch offices in Montenegro;

- information on the head office of the foreign organization branch office on the territory of Montenegro.

Foreign organization branch office shall not have the status of a legal entity.

Assets

Article 28

Non-governmental organization shall acquire assets from membership fee, voluntary contributions, gifts, donations, estate, investment interests, dividends, rent, and income from commercial activities and in other ways not prohibited by law.

Performance of Commercial Activities

Article 29

Non-governmental organization may directly perform a temporary commercial activity stipulated by the statute if it is registered in the business entity register for the performance of that activity.

If the commercial activity income in the current year exceeds the amount of 4.000 EUR, non-governmental organization shall not directly perform a commercial activity until the end of the year.

By way of exception to paragraph 2 of this Article, non-governmental organization may continue to perform the commercial activity until the end of the year provided that the income from that activity in the current year does not exceed 20% of the overall annual income from the previous calendar year.

Profit gained by performance of the commercial activity shall be used on the territory of Montenegro with the aim of reaching the goals for which the non-governmental organization has been established.

Non-governmental organization shall perform commercial activities in line with special regulations which lay down the conditions for performing that kind of activity.

Income generated by the non-governmental organization which exceeds the amount from paragraphs 2 and 3 of this Article shall be paid in the budget of Montenegro.

Publishing Report

Article 37

Non-governmental organization which has generated income of more than 10.000 EUR during a calendar year on all grounds shall publish the annual financial report, adopted by the organization’s competent body, on its web page, within 10 days from the day of the adoption of the report.

Inspection Control

Article 41

Inspection control over the implementation of this Law shall be performed by the inspection bodies, in line with law.

Misdemeanors

Article 42

Non-governmental organization shall be fined with 500 to 800 EUR for misdemeanor, if:

1) it fails, within 30 days, to submit to the competent body the change of facts and information entered into register (Article 19 paragraph 1);

2) it uses, in legal transactions, a name under which it is not registered (Article 13);

3) it does not use the assets in line with this Law (Article 30);

4) it does not publish the annual financial report adopted by the organization’s competent body on its web page within ten days from the day of its adoption (Article 37).

For misdemeanor from paragraph 1 of this Article, the responsible person in the non-governmental organization shall be fined with 30 to 100 EUR.

The responsible person in the association shall be also fined with the fine from paragraph 1 of this Article if he/she does not keep updated records on its members (Article 21 paragraph 2).

Foreign non-governmental organization’s branch office and the responsible person shall be fined with fine from paragraph 1 and 2 of this Article if it starts its activities before registration (Article 20 paragraph 1).

Misdemeanors related to Commercial Activities Performance

Article 43

Non-governmental organization shall be fined with 500 to 4,000 EUR for misdemeanor if within the current calendar year it continues to directly perform a commercial activity after the exceeded amount of 4,000 EUR or 20% of the overall annual income (Article 29 paragraph 2 and 3).

The responsible person in the non-governmental organization shall be also fined with 50 to 500 EUR for the misdemeanor from paragraph 1 of this Article.

PAYMENT SYSTEM LAW

(«OG MNE», No. 62/13)

Payment services

Article 2

(1) Payment services shall include:

1) Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;

2) Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;

3) Execution of payment transactions, including transfers of funds on a payment account of the payment service user held with payment service provider or with another payment service provider:

- execution of direct debits, including one-off direct debits,
- execution of payment transactions through a payment card or a similar device,
- execution of credit transfers, including standing orders.

4) Execution of payment transactions where the funds are covered by a credit line for a payment service user:

- execution of direct debits, including one-off direct debits,
- execution of payment transactions through a payment card or a similar device,
- execution of credit transfers, including standing orders;

5) Issuing and/or acquiring of payment instruments;

6) Money remittance; and

7) Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

Payment service providers

Article 4

(1) Payment services in Montenegro may be provided by:

1) banks and other credit institutions having their head offices in Montenegro;

2) a payment institution having its head office in Montenegro;

3) an electronic money institutions having its head offices in Montenegro;

4) a branch of a third-country credit institution having its head office in Montenegro;

5) the Central Bank of Montenegro (hereinafter: the Central Bank);

6) the state of Montenegro and local authorities when not acting in their capacity as public authorities.

(2) Payment services in Montenegro may be provided only by payment service providers under in paragraph (1) above.

(3) Payment service providers under paragraph (1) 1) and 4) above may provide payment services subject to their competencies specified under laws regulating the taking up and pursuit of their respective businesses.

(4) Payment service providers under paragraph (1) 2) and 3) above may provide payment services pursuant to their authorities specified herein.

(5) Rights of payment service providers under paragraph (1) 5) and 6) to provide payment services shall be specified in the law regulating their operations.

Definitions

Article 9

For the purpose of this Law, the following definitions shall apply:

1) payment transaction means an act, initiated by the payer or by the payee, of placing, withdrawing or transferring funds, irrespective of any underlying obligations between the payer and the payee;

2) payer means a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

3) payee means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;

4) payment service user means a natural or legal person making use of a payment service in the capacity of payer and/or payee;

5) credit institution means an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account;

6) consumer means a natural person who, in payment service contracts covered by this Law, is acting for purposes other than his trade, business or profession;

7) money remittance means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of

transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee;

8) funds means cash (banknotes and coins), funds in accounts, and electronic money;

9) payment order means any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction;

10) value date means a reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account;

11) reference exchange rate means the exchange rate which is used as the basis to calculate any currency exchange and which is made available by the payment service provider or comes from a publicly available source;

12) reference interest rate means the interest rate which is used as the basis for calculating any interest to be applied and which comes from a publicly available source which can be verified by both parties to a payment service contract;

13) unique identifier means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously the other payment service user and/or his payment account for a payment transaction;

14) payment instrument means any personalised device and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order;

15) acceptance of payment instruments is a payment service where the payment service provider enables the execution of a payment transaction initiated by the payer to the benefit of the payee, using a specified payment instrument;

16) payment card means a payment instrument enabling its holder to make payments for goods and services either at an accepting device or remotely, and/or to withdraw cash and/or use other services at an automated teller machine or another self-service device;

17) means of distance communication refers to any means which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment services contract;

18) durable medium means any instrument which enables the payment service user to store information addressed personally to him in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;

19) business day means a part of the day on which the relevant payment service provider of the payer or the payment service provider of the payee involved in the execution of a payment transaction is open for business and enables the execution of a payment transaction to its payment service user;

20) credit transfer means a payment service where the payer instructs the payment service provider to initiate the execution of a payment transaction or several payment transactions, including the issuing of a standing order;

21) direct debit means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider;

22) branch of a payment institution means a place of business other than the head office which is a part of a payment institution, which has no legal personality and which carries out directly some or all of the transactions inherent in the business of a payment institution; all the places of business set up in the same Member State by a payment institution with a head office in another Member State shall be regarded as a single branch within the meaning of this law;

23) group means a group of undertakings, which consists of a parent undertaking and its subsidiaries within the meaning of the law regulating company business, as well as the entities in which the parent undertaking or its subsidiaries have a holding, as well as undertakings linked to each other by a relationship in the manner that they are managed on a unified basis pursuant to a contract concluded or provisions in the articles of association of those undertakings and/or articles of incorporation or undertakings interconnected in the manner that the management bodies consist for the major part of the same persons in office during the financial year and until the consolidated accounts are drawn up;

24) qualifying holding means a direct or indirect holding on the basis of which an investor, whether a natural or legal person, acquires 10 percent or more of the capital or of the voting rights of another legal person, or a holding of less than 10 percent of the capital or of the voting rights of that legal person which makes it possible to exercise a significant influence over the management of that legal person;

25) good reputation means the reputation of a person who:

- has by his/her former professional work and personal integrity achieved good results and earned respect in the previous working environment;
- has not been convicted by a final judgment of a crime that would make him/her unworthy of performing the function or relevant work and/or who has not been appointed member of the management board at the time the undertaking has been the subject to bankruptcy or liquidation proceedings, and/or
- is not subject to investigation or criminal proceedings for a crime prosecuted ex officio;

26) connected parties means two or more legal and/or natural persons connected in at least one of the following ways:

- one party either has a direct or indirect participation in capital or voting rights of the other party of no less than 20%,
- one party has a controlling share in another party, or
- two or more parties are controlled by a third party,

whereby the expressions indirect participation and control have the meaning specified in the law regulating the taking up and pursuit of the banking business;

27) outsourcing means a contractual agreement by which the performance of certain operational activities of a payment institution, an e-money institution or a payment system operator, which would otherwise be performed by them, is entrusted to third parties;

28) Member State means a member state of the European Union or a signatory to the Agreement on the European Economic Area;

29) home Member State means the Member State in which the registered office of the payment service provider is situated or, if the payment service provider has, under its national law, no registered office, the Member State in which its head office is situated;

30) host Member State means the Member State other than the home Member State in which a payment service provider has a branch or an agent or provides payment services;

31) third country means, until Montenegro's accession to the European Union, any foreign country, and after the accession, any country other than the Member State;

32) national payment transaction means a payment transaction provided by a payer's payment service provider and/or a payee's payment service provider in the territory of Montenegro;

33) cross-border payment transaction means a payment transaction the execution of which involves two payment service providers of which one payment service provider provides this service in the territory of Montenegro and the other payment service provider provides the same service in the territory of another Member State, as well as a payment transaction provided by one payment service provider to a payment service user in the territory of Montenegro as well as to the same or another payment service user in the territory of another Members State;

34) international payment transaction means a payment transaction the execution of which involves two payment service providers of which one payment service provider provides this service in the territory of Montenegro and the other provides the same service in the territory of a third country, as well as a payment transaction provided by one payment service provider to a payment service user in the territory of Montenegro as well as to the same or another payment service user in the territory of the third country;

Provision of payment services through agents

Article 77

(1) A payment institution shall provide payment services through an agent in accordance with Article 6 herein and paragraphs (2) to (7) below.

(2) A payment service provider shall apply to the Central Bank for the listing of the agent in the register of payment institutions.

(3) The agent may not commence its operations before it has been listed in the register under paragraph (2) above.

(4) The Central Bank may refuse to list the agent in the register under paragraph (2) above if it has established that the submitted documents contain incomplete or inaccurate information.

(5) The Central Bank may remove the agent from the register under paragraph (2) above if it no longer meets the prescribed requirements and/ors if it has established that the listing in the register had been made on the basis of incorrect information or documents.

(6) When the agent has been removed from the register under paragraph (2) above, documentation and funds related to outstanding liabilities and unresolved relationships connected to payment transactions performed by the agent shall be submitted to the payment service provider on whose behalf the agent has been acting.

(7) The Central Bank shall prescribe detailed requirements for agent operations and the information and documents required for their listing in the register.

(8) Provisions under paragraphs (1) to (7) above shall apply mutatis mutandis to the listing of agents of other payment service providers under Article 4 herein in the relevant registers.

Register of payment institutions

Article 89

(1) The Central Bank shall maintain a register of payment institutions authorised to provide payment services, and their branches and agents (hereinafter: the register of payment institutions) and update it as appropriate.

(2) The register of payment institutions shall include a list of payment services which the individual entities under paragraph (1) above are authorised to provide and their registration number.

(3) The register of payment institutions shall be publicly available and accessible on the website of the Central Bank.

(4) The Central Bank shall prescribe the manner of keeping the register and the information contained therein to be made available.

Exchange of information between the Central Bank and competent authorities of Member States

Article 105

(1) The Central Bank shall cooperate with the competent authorities of the Member States and, where appropriate, with the European Central Bank and the national banks of the Member States and other relevant competent authorities by submitting information and notifications.

(2) The submission of the information and notifications referred to in paragraph (1) above shall not constitute the violation of confidentiality.

Pursuant to Article 95 item 3 of the Constitution of Montenegro I hereby pass the

D E C R E E

PROMULGATING THE POSTAL SERVICES ACT

I hereby promulgate the **Postal Services Act**, adopted by the Parliament of Montenegro in its 24th convocation, at the fifth session of the second regular (autumn) sitting in 2011, on November 17, 2011.

Number: 01-1330/2

Podgorica, on November 23, 2011

The President of Montenegro,

Filip Vujanović, sgd.

Pursuant to Article 82 paragraph 1 item 2 and Article 91 paragraph 2 of the Constitution of Montenegro, the Parliament of Montenegro in its 24th convocation, at the fifth session of the second regular (autumn) sitting in 2011, on November 17, 2011, passed the

POSTAL SERVICES ACT

3. The Agency

Article 65

The Agency shall:

1) determine the criteria based on which prices of universal postal service are set;
2) prepare expert basis for development of regulations passed by the Ministry in accordance with this Act;
3) issue and revoke special licenses and licenses for provision of universal postal services;
4) maintain the register of postal operators (hereinafter referred to as: the Register);
5) set the prices of reserved postal services;
6) cooperate with the bodies and authorities of the Universal Postal Union and the European Union and carry out exchange of data and regular informing of those authorities in accordance with this Act and international obligations;
7) cooperate with the regulatory authorities of the European Union member states and other countries;
8) participate in the work of administrative bodies and task forces of the relevant European and international organizations and institutions in the field of postal services;
9) verify the calculation of net costs of universal postal service;
10) determine fulfillment of conditions for obtaining of a special license and license for provision of

postal services;

11) monitor implementation of the prices of postal services;
12) provide approval of the general terms and conditions for provision of postal services of postal operators;
13) monitor development of postal services;
14) provide approval of the conditions and prices of access to the Universal Service Operator network;
15) settle disputes between operators with regard to access to the Universal Service Operator network;
16) decide upon appeals of users of postal services;
17) perform expert supervision over the work of postal operators;
18) monitor the situation and development of the postal services market and take measures to ensure competitiveness in the postal services market;
19) provide expert opinions regarding implementation of this Act;
20) publish acts of the Universal Postal Union on its website;
21) perform other tasks in accordance with this Act.

Cooperation of the Agency
Article 66

The Agency shall cooperate with postal operators and other authorities and organizations with regard to protection of consumers and postal services market.

Inspection and expert supervision tasks
Article 106

Inspection supervision over implementation of this Act and other rules regulating provision of postal services shall be carried out by the Ministry, or another relevant administration authority.

Expert supervision over implementation of this Act shall be carried out by the Agency.

Authorities and organizations carrying out inspection and expert supervision shall establish necessary coordination, communication and cooperation in supervision tasks.

Expert supervision of the Agency
Article 109

The Agency shall carry out expert supervision over implementation of this Act, regulations passed based on the Act and the general terms and conditions of postal service provider, regulating provision of postal services, quality of universal postal services, network access, prices, accounting of postal service provider, acting within given authorizations and supervision over implementation of individual acts passed within its competence.

The Agency may carry out expert supervision only over legal and natural persons listed in the register of postal operators.

Authorized employee of the Agency
Article 110

Expert supervision tasks shall be carried out by authorized employees of the Agency in a manner set out by a regulation of the Agency.

An authorized employee must possess an authorization while carrying out tasks of expert supervision.

The form and content of the authorization and the procedure of expert supervision, as well as other matters relating to expert supervision shall be regulated by the relevant body of the Agency.

DECREE PROMULGATING THE SECURITIES LAW (OGRM 59/00, 10/01, 43/05, 28/06, OGM 53/09, 73/10, 40/11, 06/13)

The Securities Law is hereby promulgated, which has been adopted by the Parliament of the Montenegro at the second sitting of the second ordinary session in 2000, on 22 December 2000.

Number: 01-2913/2 Podgorica, 26
December2000

President of the Montenegro Milo
Đukanović, m.p.

SECURITIES LAW

Confidentiality

Article 18

Members or former members, and employees or former employees of the Commission, shall be obliged to keep information obtained during their work in the Commission, or otherwise, that are considered, in accordance with regulations, as business secret.

Prohibition referred to in paragraph 1 of this Article shall cease to be valid once the denotation business secret is removed from the information, in accordance with criteria established by a legal document of the Commission.

Persons referred to in paragraph 1 of this Article must not give advice related to investment in securities or give opinion on favourable and unfavourable purchase or sale of securities.

Prohibition referred to in paragraph 3 of this Article shall cease to be valid after termination of the performance of function or operations in the Commission.

Persons referred to in paragraph 1 of this Article shall be obliged to keep privileged information until the information loses its privileged capacity^

Cooperation of the Commission with other Regulatory Authorities

Article 18a

At the request of competent state body or foreign body competent for supervision of trade in securities, the Commission shall be obliged to submit necessary data and information.

Exchange of data and information referred to in paragraph 1 of this Article shall not be considered as disclosure of business secret.

Definition of Securities Markets

Article 45

The trade of securities is conducted on the securities markets that are established for the purpose of creating the conditions for matching the demand and offer of securities.

Stock Exchanges conduct securities market business.

Notwithstanding paragraph 1 of this Article, trading in securities shall not be carried out on securities markets in the following cases:

1) when securities, in accordance with Articles 44a and 44b of this Law, are offered through the closed offering;

2) in the case of implementation of the public offering for taking over a joint stock company in accordance with special regulations;

3) in the case of implementation of trade in block securities, in accordance with special regulations; and

4) when the Commission allows by its rules trade in short-term debt securities

Eligibility for Licensing

Article 66

A broker's license may only be granted to a legal person which shall at all times employ at least 2 individuals who are licensed as broker's representatives under the rules of the Commission.

A dealer's license may only be granted to a legal person which shall at all times employ at least 2 individuals who are licensed as dealer's representatives under the rules of the Commission.

An investment manager license may only be granted to a legal person which shall at all times employ at least 2 individuals who are licensed as investment manager representatives under the rules of the Commission.

Broker, dealer and investment manager activities may be carried out only by persons who acquired adequate title for performance of such activities, in accordance with more detailed requirements determined by the Commission.

By the way of exception to article 63, paragraph 1 above, in the case of a bank a securities business license may be granted by the Commission only to a bank that obtained a license from the Central Bank of Montenegro and which has a special organisational part that is exclusively engaged in securities business.

Application for License

Article 68

An application for a securities business license shall be submitted in the form and manner determined by the Commission and shall be accompanied by the prescribed fee.

The application set forth in paragraph 1 above shall include the following information:

1) information about the services which the applicant intends to provide;

2) information about the business which the applicant proposes to carry on and to which the application relates, and about any person whom the applicant proposes to employ or with whom the applicant intends to be associated in the course of carrying on the business;

3) specific location of all premises at which the review of technical equipment for the business for which the application can be made.

In order to obtain the license, licensees - legal persons shall, in addition to the application, provide the Commission with the following:

1. a foundation chart (contract);
2. the statute;
3. a job description and the work plan for the following two years;
4. information on individuals with special powers and responsibilities;
5. information and evidence regarding the share capital and fulfilment of other conditions depending on the type of activity, personnel, technical, financial and organizational capability of the company applying for the license.

Grant of License

Article 69

The Commission may grant a license to a licensee subject to such conditions as prescribed by this law.

Where the applicant is a legal person, the Commission shall take into account any circumstances relating to its majority shareholder.

A majority shareholder shall mean a person having shares in a legal person whose number is equal or greater than 25% of the total number of shares with voting right.

Power of Commission

Article 71

The Founding Agreement, Statute and Rules of licensees are subject to approval of the Commission. The Commission shall also approve the appointment of executive director of licensees.

The Commission may, amend or cancel any condition attached to the license or impose further conditions to a licensee.

Revocation and Suspension of Licenses

Article 74

The Commission may revoke a license granted to a licensee - legal person if:

1) it ceases, on a permanent basis, to carry on the business for which it is licensed;

2) the decision on bankruptcy or liquidation has been passed;

3) it fails to comply with any condition applicable in respect of the license;

4) it contravenes the provisions of this law.

The Commission may revoke a license granted to a licensee - natural person if such natural person:

1) becomes incapable of performing the activities to which the license relates;

2) ceases, on a permanent basis, to carry on the business for which he is licensed;

3) fails to comply with any condition applicable in respect of the license;

4) contravenes the provisions of this law;

5) is convicted with an unconditional custodial sentence or of an offence which disqualifies him from engaging in the business for which he has been licensed.

The Commission may, suspend the license for such specified period, to a licensee pending a hearing and determination by the Commission.

The revocation decision made by the Commission shall establish the date as of which the licensee shall stop its operations.

The Commission shall submit the revocation decision to a competent Court.

The suspension or revocation of a license does not influence on:

1) realisation of transactions with securities concluded by the person whose license has been suspended or revoked, where one party is a person with suspended or revoked license;

2) any right, obligation, or liability arising from such transactions.

Power of Commission to Call for Information

Article 108

The Commission may require, by notice in writing, licensees to furnish it with such information as it may reasonably require for the exercise of its functions under this Law within such reasonable time and verified in such manner as it may specify.

Power of Commission to Inspect

Article 110

For the purpose of ascertaining whether a person who is, or at any time has been, a licensee is complying or has complied with any provision of or requirement under this Law, Rules made under this Law or the terms and conditions of its license, the Commission may inspect the business to which the license applies without prior notice.

The Commission may appoint a person (hereinafter referred to as the "authorised person") to exercise the powers of the Commission under this Article.

The person that is subject to inspection shall afford an authorised person access to the records or other documents as may be reasonably required for the inspection and ensure that his employees provide required information.

Period of application

Article 124a

The provision of Article 20 paragraph 2 of this law will apply until 1st of January 2016.

Pursuant to Article 88, point 2 of the Constitution of the Republic of Montenegro I adopt

DECREE

ON PROCLAMATION OF THE LAW ON VOLUNTARY PENSION FUNDS

("Official Gazette of the Republic of Montenegro", No. 78/06 dated December 22, 2006, No. 14/07 dated March 12, 2007 and No. 40/11 dated August 8, 2011)

The Law on Private Pension Funds adopted by the Parliament of the Republic of Montenegro at its fifth session of the second regular convening in 2006 is proclaimed on December 12, 2006.

No: 01-1538/2

Podgorica, December 15, 2006

President of the Republic of Montenegro

Filip Vujanović

LAW

ON VOLUNTARY PENSION FUNDS

Contents of the Law

Article 1

This Law shall govern the conditions for establishing pension fund managing company (hereinafter: the management companies) and organizing voluntary pension funds based on individual capitalized savings (hereinafter: pension funds) and their operating.

Trade Name

Article 5

The trade name of the Management Company must include a words: “Pension Fund Management Company”.

The trade name of the Voluntary Fund must include a word: “Voluntary Pension Fund”.

Business organizations including in their trade name the following words cannot be entered in the court register: “Pension fund Management Company”, “Pension Fund”, or other words with similar meaning unless founded in compliance with provisions of this Law, neither can they use these trademarks in the legal transactions and/or trade name.

Implementation of the Law

Article 7

Provisions of the law governing legal status of business organizations shall apply to the Pension Fund Management Company and Pension Fund unless stipulated otherwise by this Law.

Provisions of the law governing securities shall apply to securities operations under this Law unless stipulated otherwise by this Law.

Head Office

Article 8

Head office of the Pension Fund Management Company founded and operating in compliance with this Law must be on the territory of the Republic of Montenegro (hereinafter: the Republic).

Capital and Shares

Article 11

The cash amount of the initial capital of the Management Company cannot be lower than €250,000.

The initial capital set under the paragraph 1 of this Article shall be fully paid before the registration of Management Company in the Central Register of the Commercial Court.

In the course of operations the Management Company shall be obliged to have at all times available the overall capital in the amount set under paragraph 1 of this Article at minimum.

Management Company shall without delay inform Securities Commission about every decrease of initial capital below the amount stipulated under the paragraph 1 of this Article.

Should in the term specified by the Securities Commission, that shall not be longer than six months, the initial capital is not reaching the prescribed level, Securities Commission shall withdraw the Management Company license.

By-laws

Article 12

The by-laws of Management Company are: Statute, Rules on Managing and other general acts.

Limitations To Prevent Conflict Of Interest

Article 15

Member of the Board of Directors or Executive Director of Management Company cannot be the person who is the member of Board of Directors or Executive Director of:

1) other Management Company;
2) Custodian;
3) The person related to the persons stipulated under the item 1 and 2 of this paragraph.

Request for Obtaining License for Management Company Operations

Article 18

The Management Company must obtain the permission from the Commission for performing activities of Pension Fund management (hereinafter: the license).

The Management Company shall submit the request for obtaining the license to the Commission after the foundation General Meeting.

In addition to the request under paragraph 2 of this Article the Managing Company shall submit:

1) Foundation Charter of the Management Company,
2) Statute of the Management Company,
3) Proposal of a Rules on Managing of Pension Fund;
4) Proves of the founders that they paid the amount of the cash part of the initial capital prescribed by this Law;
5) Evidence on staff, technical and organizational capacity of the Management Company;
6) Proposal for appointment of members of Board of Directors and Executive Director with their statements on accepting performing of these functions;
7) Proves on intent to employ two investment managers;
8) Other data and evidence.

The contents of requests and documentation as well as evidence that are attached to the request for obtaining the license shall be set by the Commission in its rules.

Separate Keeping of Assets

Article 20

The Pension fund is managed, in accordance with this Law and Rules on managing pension funds, by the Pension Fund Management Company.

Assets, liabilities, claims, revenues and expenditures and other rights of the Management Company shall be kept separately from the assets, liabilities, claims, revenues and expenditures and other rights of the Pension Fund.

The Management Company managing more funds shall separately keep the assets, liabilities, claims, revenues and expenditures and other rights for each Pension Fund.

Representation in Legal Transactions

Article 23

In legal transactions performed for the Pension Fund, the Management Company shall act on behalf and for the account of the Pension Fund in compliance with this Law and Rules on Managing of Pension Fund.

Liability of the Custody

Article 48

Custody shall be responsible to the Pension Fund Management Company for any inflicted

damage resulting from non - performing or inappropriately performing the activities

specified in the contract, in compliance with this Law.

The liability of the Custody shall not be limited nor terminated by the Contract.

The Pension Fund Management Company shall be authorized to, in its name and on its behalf, and in the name and behalf of the Members of the Pension fund, initiate an action against custody for damage compensation.

If the Pension Fund Management Company fails to initiate action against Custody in accordance with the paragraph 3 of this Article, within 30 days from the date of delivering of written notification from the Member of the Pension Fund, the action for damage compensation may be filled by the Pension Fund Member himself/herself.

In accordance with Article 88 Item 2 of the Constitution of the Republic of Montenegro I hereby pass the

ENACTMENT ON PROCLAMATION OF

THE LAW ON FOREIGN CURRENT AND CAPITAL OPERATIONS

(“Official Gazette of RoM”, No. 45/05 as of 28th July 2005)

This is a proclamation of the Law on Foreign Current and Capital Operations, adopted by the Parliament of the Republic of Montenegro at the fourth meeting of the first regular session in the year 2005, on 21st July 2005.

Number: 01-763/2

Podgorica, 25th July 2005

President of the Republic of Montenegro

Filip Vujanović, signed

LAW ON FOREIGN CURRENT AND CAPITAL OPERATIONS

Foreign Payment Operations

Article 4

Foreign payment operations shall be performed through the Central Bank of Montenegro (hereinafter: the Central Bank), banks and other payment services providers that are issued approval by the Central Bank to perform foreign payment operations.

Exchange Operations

Article 8

Exchange operations may be performed by legal entities and entrepreneurs, which have contract with a bank, and are registered for performing exchange operations.

The Central Bank shall prescribe more specific terms and manner of performing exchange operations.

THE GUIDELINES ON DEVELOPING RISK ANALYSIS WITH A VIEW TO PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

September 2009

In relation to the Article 8 paragraph 3 of the Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 14/07) and Article 2 of the Rulebook on developing risk analysis guidelines with a view of preventing of money laundering and terrorist financing**, (Official Gazette of Montenegro No.20, from 17th March 2009)**

The Administration for the Prevention of Money Laundering and Terrorist Financing established

The Guidelines on developing risk analysis with a view of preventing of money laundering and terrorist financing

LEGAL FRAMEWORK

Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 14/07)

Rulebook on manner of work of the compliance officer, the manner of conducting the internal control, data keeping and protection, manner of record keeping and employees professional training (Official Gazette of Montenegro No. 80 from 26th December 2008)

Rulebook on the manner of reporting cash transactions exceeding €15,000 and suspicious transactions to the administration for the prevention of money laundering and terrorist financing (Official Gazette of Montenegro 79, from 23rd December 2008).

Rulebook on developing risk analysis guidelines with a view of preventing of money laundering and terrorist financing (official gazette of Montenegro, no. 20, from 17th March 2009)

This guidelines shall define closer risk factors based on which the level of risk of a client, group of clients, business relationship, transaction or production relation to which the reporting entity shall design internal procedure on risk analysis.

The APMLTF shall, in accordance with the Article 86, paragraph 1, item 8 of the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the Law), conduct supervision on implementation of

the Law and its regulations, within its established competences, in accordance with the law on inspection control and in relation to reporting entities from Article 4, paragraph 1, items 15:

16) humanitarian, nongovernmental and other non-profit organizations, and
17) other business organizations, legal persons, entrepreneurs and natural persons engaged in an activity or business of:

- sale and purchase of claims;
- factoring;
- third persons' property management;
- issuing and performing operations with payment and credit cards;
- financial leasing;
- travel organization;
- real estate trade;
- motor vehicles trade;
- vessels and aircrafts trade;
- safekeeping;
- issuing warranties and other guarantees;
- crediting and credit agencies;
- granting loans and brokerage in loan negotiation affairs;
- brokerage or representation in life insurance affairs, and
- Organizing and conducting biddings, trading in works of art, precious metals and precious stones and precious metals and precious stones products, as well as other goods, when the payment is made in cash in the amount of € 15.000 or more, in one or more interconnected transactions.

Basic principles of the fight against money laundering and terrorist financing

1. *Establishing and verifying client's identity*

Before establishing the business relationship or executing the business transaction, reporting entities are obliged to collect necessary data on a client or to carry out client's identification.

The client's identification is a procedure which includes:

1) establishing client's identity, or if the client's identity has been previously confirmed, to conduct verification of client's identity based on authentic, independent and objective sources;

2) collecting data on a client, of if these data are collected, verification of collected data based on authentic, independent and objective sources.

The reporting entity shall, for a client who is a natural person, or its legal representative, entrepreneur or natural person performing activities, establish and verify client's identity, by insight into the personal identification documents, in client's presence and collect data from Article71, item 4 of the Law. If the required

data can not be established from the submitted personal documentation the missing data are collected from other relevant public document submitted by a client.

The client's identity from paragraph 1 of this Article can also be established on the basis of client's qualified electronic certificate issued by a certificate service provider in accordance with the regulation on electronic signature and electronic business.

The reporting entity shall, within procedure of establishing and verifying client's identity, in accordance with the manner prescribed by paragraph 2 of this Article, register data on a client from the qualified electronic certificate into data records from Article 70 of the Law. The data, which can not be collected from client's qualified electronic certificate, shall be collected from the copy of personal documentation which a client submits, in written form, to the reporting entity or in electronic form and if in this manner all required data can not be obtained, the missing data shall be obtained directly from the client.

The electronic service providers, from paragraph 2 of this Article, which issued the qualified electronic certificate, shall upon the reporting entity's request, without delay, provide data on the manner in which they established and verified the identity of the client who possess the qualified electronic certificate.

Establishing and verifying client's identity by usage of qualified electronic certificate is not allowed in the following cases:

1) in the process of opening account at the reporting entities from Article4, paragraph 2 items 1 and 2 of the Law, except when the client is opening temporary depository account for depositing the nominal capital;

2) If there are suspicions that the qualified electronic certificate is misused, or if the reporting entity establishes that the circumstances, which can significantly influence on the certificate's validity, has changed.

If the reporting entity in the process of verifying and establishing client's identity suspect the validity of the collected data or authenticity of documents from which the required data are obtained, than the reporting entity is obliged to require the written statement from the client.

The reporting entity establishes and verifies client's identity from Article 71 item 1 of the Law with insight into original or verified copy of the document from the Central Register of the Commercial Court (hereinafter: CRCC)or other available public registry, which are submitted by an authorized representative and on behalf of the legal person.

The document from paragraph 1 of this Article shall not be older than three months since the issuance date. The reporting entity can establish and verify identity of a legal person and obtain data from Article 71 item 1 of the Law and with insight into CRCC or other available public registry. The reporting entity shall, on the certificate from the registry, which has been viewed, write date and time and personal number of a person which had insight into documentation. The certificate from the business register shall be kept in accordance with the Law.

The reporting entity shall obtain data, from Article 71 items 2, 7, 9, 10, 11, 12, 13 and 14 of this Law, with insight into original documents or verified copies of the documents and other business documentation. If it is not possible to establish data with insight into certificates and documentation, the missing data shall be obtained directly from the representative or authorized person.

If the reporting entity in the process of verifying and establishing client's identity suspects the validity of the collected data or authenticity of certificates and other business documentation from which the required data

are obtained, than the reporting entity, before establishing business relationship or before executing the transaction, is obliged to require the written statement from the representative or authorized person.

If the client is a foreign legal person, performing business activities in Montenegro through its subsidiary, than the reporting entity shall establish and verify the identity of the foreign legal person and its subsidiary.

The reporting entity shall establish and verify the identity of the legal representative and obtain data from Article 71 item 2 of the Law. The data shall be obtained with insight into the personal certificate of the legal representative and in the presence of the legal representative. If it is not possible to establish data with insight into personal certificate of the legal representative, the missing data shall be obtained from other public documents submitted by the legal representative or authorized person.

If the reporting entity in the process of verifying and establishing identity of the legal representative suspects the validity of the collected data, than the reporting entities obliged to require the written statement from the legal representative.

In case when the client's identity can not be established or verified, the reporting entity can not conclude the business relationship or execute the transaction. The reporting entity shall cease all current business relationships with this client.

2. Implementation of the Law and standards

The reporting entities, in the process of performing business activities for which they are registered, are obliged to act in accordance with the adopted laws and by laws that regulate the area of disclosure and prevention of money laundering and terrorist financing. Also, the reporting entities shall ensure that required measures are incorporated into reporting entities performances at all levels.

The legislation in the area of the prevention of money laundering and terrorist financing in Montenegro is harmonized with the relevant regulations in the area of the prevention of money laundering and terrorist financing.

1. Council Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (91/308/EEC)

2. Directive 2001/97/EC of the European Parliament and of the Council

Of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

3. Directive 2005/60/EC of the European Parliament and of the Councilor 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

4. FATF Recommendations (40+8+1)

5. The United Nations Convention against Corruption (UNCAC)

The Council of Europe through its MONEYVAL Committee also accepts the mentioned documents as referent in its evaluations.

3. Cooperation with the Administration for the Prevention of Money Laundering and Terrorist Financing

In accordance with the Law, reporting entities are obliged to ensure the full cooperation with the supervisory bodies. The obligation related to cooperation between the reporting entities and supervisory bodies is very significant in cases of providing required data, information and documentation, that refer to the clients or transactions for which there are reasons to suspect in money laundering or terrorist financing. Also, the cooperation is necessary in case of giving information related to behavior or circumstances that could be connected to ,money laundering or terrorist financing and that could harm the safety, stability and reputation of the financial system of Montenegro.

Due to that the realization of the internal procedures can not, in any case, directly or indirectly, limit the cooperation between the reporting entities and the APMLTF or in any other manner influence on the cooperation efficiency.

4. Adoption of internal procedure

The reporting entities shall adopt the unique policy of risk management in combating money laundering and terrorist financing , and due to that adopt the internal procedures, particularly in the area of: client's verification, risk analysis, recognizing clients and transactions for which there are reasons to suspect in money laundering and terrorist financing. It is particularly important that all employees are informed about the procedures, to act in accordance with the procedures and to use them in their daily work.

The content of internal procedures developed by the reporting entities:

A) manner of establishing client's acceptability;

b) risk assessment of groups and clients;

c) the manner of establishing the risk of product and services, with the view of the prevention of money laundering and terrorist financing;

d) manner of client's identification;

e) client's accounts and transactions supervision;

f) managing risks to which the reporting entities are exposed, in the area of the prevention of money laundering and terrorist financing;

h) training programs for employees.

5. Professional training

The reporting entity is obliged to provide, on regular basis, professional training and qualification of all employees that directly or indirectly perform activities of prevention or concealing money laundering and terrorist financing.

RISK ASESSMENT

1. The purpose of risk assessment

In accordance with the Law, the risk on money laundering and terrorist financing is the risk that the client is going to misuse the financial system of Montenegro for money laundering and terrorist financing or that a certain business relationship, transaction or product is going to be directly or indirectly used for money laundering and terrorist financing.

The reporting entity shall, in accordance with the Law and in order to prevent exposure to money laundering and terrorist financing, make risk assessment through which the level of client, business relationship, product or transaction's exposure to risk will be determined

The risk analysis preparation is a necessary precondition for performing the prescribed client's verification measures. The classification of the client, business relationship or transaction in one risk category depends on the type of client's verification which the reporting entity is obliged to perform in accordance with the Law (enhanced customer due diligence , simplified customer due diligence and simplified customer due diligence)

2. Risk management policy and risk analysis

The reporting entity or its management can, for the necessity of more efficient implementation the provisions of the Law and Guideline, before the risk analysis preparation, adopt adequate risk management policy for the prevention of money laundering and terrorist financing. The purpose for adopting this policy is primary to determine, 0n the level of reporting entities, the areas of business activities that are, due to possibility of

misuse for money laundering or terrorist financing, more or less critical, or for the reporting entities to establish and determine the main risks in this areas and measures for their solution. The reporting entities shall, during the process of developing the starting basis for adoption the policy for money laundering or terrorist financing risk management, take into consideration the following criteria that , in the process of designing the policy, defines details on:

1. the purpose and aim of money laundering and terrorist financing risk management and its connection with the reporting entities' business aims and strategy,
2. the reporting entities' areas and business processes that are exposed to money laundering and terrorist financing risks,
3. money laundering and terrorist financing risks in all key business areas of the reporting entities,
4. measures for resolving money laundering and terrorist financing risks,
5. the role and responsibility of the reporting entities management in the process of performing and adoption of money laundering and terrorist financing risk management.

3. Risk analysis preparation

Risk analysis is a procedure in which the reporting entity defines:

- evaluation of probability that the reporting entities' business activities can be misused for money laundering and terrorist financing
- criteria, based on which the certain client, business relationship, product or transaction will be classified in to category of clients that are more or less exposed to money laundering and terrorist financing clients,
- establishing consequences and measures for efficient managing of these risks.

The reporting entity shall, in the process of risk analysis preparation, take onto consideration the following criteria:

1. the reporting entity is obliged to develop the risk criteria so that the specific client, business relationship, product or transaction is determined in one risk category.
2. the reporting entity can, in the process of determine risk category, in accordance with its risk management policy, classify, on their own, the certain client, business relationship, product or transaction category as the category exposed to high risk of the money laundering and terrorist financing and perform enhanced due diligence,
3. the reporting entity may not, in the process of determining the certain client, business relationship, product or transaction risk category, that are in accordance with the Law and Guidelines determined as high risk clients, classify as middle(average)or low risk clients.

4. Preparation of risk evaluation

4.1. Početno utvrđivanje rizičnosti

The reporting entity shall, based on risk analysis, prepare the risk evaluation of each customer-client, business relationship, product or transaction; before closing business relationship or executing business transaction it is necessary:

1. To establish client's identification through obtained data that are required on client, business relationship, product or transaction and other data which the reporting entity is obliged to obtain.
2. to evaluate obtained data with the view of risk criteria for money laundering or terrorist financing (risk establishment)
3. to determine the evaluation of the risk of the client, business relationship, product or transaction, which must be based on previously established risk analysis, through the classification of the costumer, business relationship, product or transaction into one of the risk categories
4. performs measures of enhanced customer risk analysis (enhanced CDD, simplified CDD and usual CDD)

4.2. Subsequent risk assessment

The reporting entity shall, within measures of regular supervision of the business relationship with the costumer, verify, again, basis for the initial evaluation of the costumer or business relationship, by which the reporting entity evaluated the costumer and if it is necessary, the reporting entity shall define the new risk assessment (or subsequent risk assessment). The reporting entity shall subsequently assess the initial risk evaluation of a certain customer or business relationship in the following cases:

1. if the circumstances , on which the evaluation of a certain customer or business relationship is based, has changed significantly; or if the circumstances, that significantly influence on the classification of costumer or business relationship into risk category , change,
2. If the reporting entity suspects the validity of data, based on which a certain costumer or business relationship has been classified into the specific risk category.

5. Criteria for defining customer risk category

The reporting entity shall, in the process of defining risk evaluation of a customer, business relationship, product or transaction, take into account the following criteria:

1. type, business profile and structure of client
2. geographical origin of the customer

3. the nature of business relationship, product or transaction
4. Previous experiences of the reporting entity in relation to a client.

In the process of defining customer risk category, the reporting entity can, besides the mentioned criteria, observe other criteria for defining the level of risk for a certain costumer, product or transaction:

1. size, structure and business activity of the costumer, including the scope, structure and complexity of business activities which costumer carries out on the market ,
2. status and ownership structure of costumer
3. costumer's presence during the process of closing business activity or executing transaction,
4. source of assets that are subject of the business relationship or transaction in case if the costumer is, in accordance with criteria prescribed by the Law, defined as politically exposed person
5. purpose of closing business relationship or execution of business transaction,
6. costumer's knowledge on product and its experience or knowledge on this area,
7. other information showing that costumer, product or transaction could have high risk.

6. Costumer risk categories

In relation to risk categories costumer, business relationship, products and transactions can be classified into 4 main risk categories, as follows:

1. extremely high risk, due to which the business with costumer is prohibited,

2. high risk,

3. Medium (average) risk

4. Low risk.

6.1. Prohibition on conducting business activities with a customer

Conducting business activities with the following costumers is prohibited due to direct and high risk on money laundering or terrorist financing:

1. customers (legal and natural persons and other subjects) that are listed as persons against whom UN Security Council or European Union measures are taken- these relevant measures are: financial sanctions that include freezing assets on the account and /or prohibition on assets usage (economical sources), military embargo which means prohibition on arms trafficking with the mentioned subject etc.
2. customers with the residence or head office inanities that are not subject to the international law or not internationally recognized sovereign states (these entities give the possibility of fictive registration for legal persons , allow issuing fictive identification documents etc.)

Prohibition on executing transactions and closing business relationship with a customer is applied in the following cases:

1. transactions were intended to be sent to persons or subjects against which UN Security Council or European Union imposed measures
2. transactions that customer would execute on behalf of person or subject against which UN Security Council or European Union imposed measures
3. business relationships that would be concluded on behalf of a person or subjects that are listed as persons against whom UN Security Council or European Union imposed measures

6.2. **High risk of money laundering or terrorist financing**

6.2.1. Type, business profile and structure of customer

The high risk of money laundering and terrorist financing costumers is as follows:

Natural persons:

Customer is politically exposed person or person that is acting or has been acting in the last year on a prominent public position in a state, including his/her immediate family members and close associates, as follows:

1. presidents of states, prime ministers, ministers and their deputies or assistants, heads of administration authority and authorities of local governance, as well as their deputies or assistants and other officials;
2. elected representatives of legislative authorities;
3. holders of the highest juridical and constitutionally judicial office;
4. members of State Auditors Institution or supreme audit institutions and central banks councils;
5. consuls, ambassadors and high officers of armed forces, and
6. members of managing and supervisory bodies of enterprises with majority state ownership

Marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters shall be deemed immediate family members of the politically exposed person.

A natural person that has a common profit from the asset or established business relationship or other type of close business contacts shall be deemed a close assistant of the politically exposed person.

Legal persons:

a. customer is a foreign legal person that does not conduct or is not allowed to conduct trade, production pr other business activities in the country in which it is registered (legal person with head office in the state that is known as off shore financial center and for which there are a certain limitations when performing direct business registration in that country)
b. customer is fiduciary (trust) or other similar company of the foreign legal person with unknown or disguised owners or management team (company of foreign legal person that provides conducting business activities for third persons i.e. companies established on the basis of legal agreement between founder and manager that governs the founder's property, on behalf of certain persons that are users or beneficiaries or for other purposes(from private gained assets to general assets that are not gained),
c. customer has a complicated status structure or complex ownership chain (complicated ownership structure or complex ownership chain disables or does not allow establishment of the beneficiary owner of legal person),
d. customer is organization that, for conducting its business activities does not need or is not obliged to get license from the competent supervising body; or in accordance with the national legislation customer is not subject to measures of detection and prevention of money laundering and terrorist financing,
e. customer is non profitable organization (institution, company or other legal person or entity established for publicly useful, charity purposes, religious communities, association, foundation, non profit association and other persons that do not perform economic activity) and fulfils one of the following conditions:

1. has a registered office in the state known as off shore financial center
2. has a registered office in the state know as financial or tax paradise
3. has a registered office in the non EU member state or did not sign EU pre accession agreement
4. among its members or founders is a natural or legal person which is resident of any of the states mentioned in the previous item.

6.2.2. Geographical position of customer

The customers that present high risk from money laundering and terrorist financing are included in customers with the permanent residence or registered office:

1. in the state that is non EU member state or did not sign EU pre accession agreement,
2. in the state that is , based on assessment of the competent international organizations, known for production or well organized drug trafficking (Middle and Far East countries known for heroin production: Turkey, Afghanistan, Pakistan and golden triangle countries (Myanmar, Laos, Thailand), South American Countries known for cocaine production Peru, Columbia and neighbor countries, Middle and Far East Countries , Central American Countries known for Indian hemp production: Turkey, Lebanon, Afghanistan, Pakistan, Morocco, Tunis, Nigeria and neighbor countries , Mexico),
3. state that is , based on assessment of the competent international organizations , known as country with high level of organized crime due to corruption, arm trafficking, human trafficking or human rights violation,
4. state that is , based on assessment of the international organization FATF (Financial Action Task Force) classified in to the non cooperative countries or territories (that are countries and territories that , according to FATF assessment, do not have relevant legislation in the area of prevention and detection of money laundering or terrorist financing, the state supervision of financial institutions does not exist or it is not relevant, establishing and acting of the financial institutions is possible without state certificates or registration at the competent authorities,

state supports opening anonymous accounts or other anonymous financial instruments, the system of recognizing and reporting suspicious transactions is inappropriate , the establishing beneficial owner is not an obligation prescribed by the law, international cooperation is not efficient or does not exists at all)

5. country against which UN or EU measures are imposed, including complete or partial break up of economic relations, ***railways***, ***waterways***, ***post***, telephone lines, ***telegraph*** lines, ***radio*** and other communicational relations, breakup of diplomatic relations , military embargo, travel embargo etc.
6. country which is known as financial or tax paradise (for these countries it is particularly important that they enable complete or partial tax free obligation, or tax rate is significantly lower than tax rate in other countries. These countries usually do not have concluded agreements for the avoidance of double taxation, or if they do sign the agreements, they do not obey them. The legislation of these countries requires strict observance of bank and business secrecy and also quick, discreet and cheap financial services are provided. Countries known as financial or tax paradises are : Dubai – Jebel Ali Free Zone, Gibraltar, Hong Kong, Isle of Man, Lichtenstein, Macau, Mauritius, Monaco, Nauru, Nevis Island, Iceland –Norfolk Area , Panama, Samoa, San Marino, Isle of Sark, Seychelles, St. Kitts and Nevis, St. Vincent and Grenadine, Switzerland – canton Vaud and Zug, Turks and Caicos Islands, the USA – federal states Delaware and Wyoming, Uruguay, British Virgin Islands and Vanuatu
7. country known as offshore financial center (these countries define certain limitations in the process of direct activities registration of business entities in the country, provide high level of bank and business secrecy, liberal control over international trade business is performed, quick, discreet and cheap financial services and legal person registration are enabled. It is significant that these countries do no not have adopted relevant legislation in the area of prevention and detection of money laundering and terrorist financing. Countries known as offshore financial centers are: Andorra, Angola, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermudas, British Virgin Islands, Brunei Darussalam, Cape Verde, Cayman Islands, Cook Islands, Costa Rica, Delaware (USA), Dominica, Gibraltar, Grenada, Guernsey, Isle of Man, Jersey, Labuan (Malaysia), Lebanon, Lichtenstein, Macao, Madeira (Portugal), Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Nevada (USA), The Netherlands Antilles, Niue, Palau, Panama, Philippines , Samoa, Seychelles, St. Kitts and Nevis, St Lucia, St Vincent and Grenadines, Zug (Switzerland), Tonga, Turks and Caicos Islands, Uruguay, Vanuatu and Wyoming (USA).

Reporting entities should consider the following International organizations as competent for supervising the efficient measures implementation in the area of prevention of money laundering and terrorist financing and its harmonization with international standards:

1. European Bank for Reconstruction and Development
2. Committee on the Prevention of Money. Laundering and Terrorist Financing of the European Commission,
3. Financial Action Task Force on Money Laundering (FATF),
4. International Monetary Fund
5. World Bank
6. The Egmont Group is an international network of national Financial Intelligence Units specialized in the combating of money laundering and terorist financing
7. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL
8. International Organization of Securities Commissions (IOSCO)
9. The Committee of European Securities Regulators (CESR),
10. Committee of European Insurance and Occupational Pensions Supervisors(CEIOPS),
11. International Association of Insurance Supervisors (IAIS).

6.2.3. Business relations, products and transactions

Business relations that could represent high risk of money laundering and terrorist financing include:

1. business relations that include permanent and high amount assets payment from the costumer's accounts, or towards credit or financial institution in non- EU member states, or country which did not sign EU Pre-Accession Agreement , or business relations that include higher payments to the customer's account opened at credit or financial institution in non- EU member states, or country which did not sign EU Pre-Accession Agreement,
2. business relations that a foreign credit financial institution or other fiduciary institution performs, on behalf of the customer and as its representative, with registration office in non- EU member states, or country which did not sign EU Pre-Accession Agreement,
3. business relationships concluded without the simultaneous ***physical presence of customer, and due to that the conditions for simplified CDD are not fulfilled,***

Transactions that could represent high risk of money laundering and terrorist financing include:

1. payment from customer's account or payment to customer's account , which differ from the account that customer provided in the process of identification of the account through which customer regularly carried or has been carrying business activities (particularly in case of crossbred transactions)
2. transactions intended to be sent to a persons with the residence or registered office in country known as financial or tax paradise,
3. transactions intended to be sent to a persons with the residence or registered office in country known as off shore financial center,
4. transactions intended to be sent to non profit organizations with the registered office in: country known as off shore financial center, country known as financial or tax paradise or in non- EU member states, or country which did not sign EU Pre-Accession Agreement,

6.2.4. Previous experiences of the reporting entity with a customer

Customers that, regardless to the reporting entity's experience, present a high risk of money laundering and terrorist financing are as follows:

1. persons in relation to whom ,within past three years, the Administration for the Prevention of Money Laundering submitted request on temporary suspension of a suspicious transaction to the reporting entity,
2. persons in relation to whom, the Administration for the prevention of Money Laundering and terrorist Financing submitted request for ongoing monitoring of customer's financial activities to the reporting entity
3. Persons for which, within past three years, the reporting entity submitted data to the Administration for the Prevention of Money Laundering and terrorist financing, since, in relation to that person or transaction that this person executed, there are reasons for suspicion in money laundering and terrorist financing.

*6.3. Medium **(average)** risk of money laundering and terrorist financing*

Reporting entity classifies in the category of middle (average) risk the customers whose business relationship, product or transaction, based on the Guidelines criteria, can not be classified as high or low risk customers

6.4. Low risk of money laundering and terrorist financing

Reporting entity shall classify the following customers as customers with low risk of money laundering or terrorist financing:

1. customers from Article 4, paragraph 2 of the Law

    - companies for managing investment funds and branches of foreign companies for managing investment funds of other countries , companies for managing investment funds of member states that opened its branches in Montenegro or which are authorized for direct managing investment funds in Montenegro or third persons that are, in accordance with the Law that defines funds business activities, authorized by company for managing investment fund to perform certain business activities,
    - companies for managing pension funds and branches of foreign companies for managing pension funds and insurance companies;
    - companies authorized to deal in financial instruments and branches of foreign companies for dealing in financial instruments in Montenegro,
    - insurance companies, authorized for dealing with life insurance, branches of foreign insurance companies, from third countries, authorized for dealing with life assurance and insurance companies from the member states, that directly or through branches deal with life insurance in Montenegro, or other same institution fulfilling condition to possess registered office in the member state or third country

2. state body , local government body or other legal persons performing public competences
3. company whose financial instruments are accepted and traded at stock market or organized public market in one or more member states and in accordance with EU regulations or companies with registered office in the third country whose financial instruments are accepted and traded at stock market or organized public market in the member state or in the third country, under the condition that in the third country the requests for data publication, in accordance wit EU regulations, are in force.

CUSTOMER DUE DILIGENCE

1. Regular customer due diligence

Customer due diligence is the key preventive element in the system of detecting money laundering and terrorist financing. The purpose of customer due diligence measures is to credibly establish and confirm the true identity of the customer. Customer due diligence includes: establishing and analyzing the identity of a customer, establishing the beneficial owner of a customer when the customer is a legal person and the data on the purpose and intended nature of a business relationship or transaction and other data, in accordance with the provisions of the articles 7, 15, 16, 17, 20 of the Law.

A reporting entity shall establish and verify customer's identity on the basis of reliable, independent and objective sources (by checking the appropriate ID document).

It is forbidden to establish a business relationship or carry out a transaction in cases when it is not possible to identify the customer, or when the reporting entity ***has reasonable*** grounds to suspect the authenticity or credibility of the data, or the documents used by the customer for proving his/her identity, or when the customer is not ready or does not show readiness to cooperate with the reporting entity in establishing the authentic and complete data required by the reporting entity when it applies customer due diligence procedure. In such cases the reporting entity may not establish a business relationship, or it shall terminate the existing relationship or transaction and notify the Administration for the Prevention of Money Laundering and Terrorist Financing on the termination.

The reporting entity may shorten the customer due diligence procedure solely in those cases when there are reasonable grounds to suspect that a customer or transaction are related to money laundering or terrorist financing.

The Law proceeds from the basic assumption that certain customers, business relationships, products or transactions pose higher and others pose lower risks of money laundering or terrorist financing. Therefore for certain cases the Law prescribes especially strict customer due diligence procedures, while for certain cases it prescribes simplified customer verification measures.

2. Customer due diligence obligation

The reporting entity shall carry out customer due diligence in the following cases:

1. when establishing a business relationship with a customer (a business relationship is any business or contractual relationship established or concluded by a customer at a reporting entity and it is related to carrying out the professional activities of the reporting entity, for example, investment contract, stock broker contract, financial instruments management contract, customer's access to the rules of investment fund management, etc.),

2. when carrying out any transaction in the amount of € 15,000 and more, whether the transaction is carried out in a single operation or in several operations which appear to be linked. Under the 'transactions that are logically interlinked' we consider the following:
- two or more successive, separated transactions, amounting to more than € 15,000, executed by a certain customer on behalf of the same third person with the same purpose,
- two or more transactions amounting to more than € 15,000, executed by several persons with family or business links, on behalf of the same third person with the same purpose,

3. when there is suspicion about the accuracy or veracity of the previously obtained data on the customer or the beneficial owner of the customer,

4. in all cases when there are reasons to suspect that a transaction or a customer are related to money laundering or terrorist financing, regardless of the amount of the transaction.

2. Enhanced customer due diligence

When a certain customer, business relationship, product or transaction are considered as highly risky for money laundering or terrorist financing, reporting entities shall apply enhanced customer due diligence measures. As highly risky for money laundering or terrorist financing the Law defines the following: establishing a correspondent relationship with a bank or other similar credit institution that has a registered office in a third country, business relationships established with a politically exposed person and cases where the customer is not present when the establishing and verifying customer identity are made within the application of customer due diligence measures.

2.1. Enhanced customer due diligence for politically exposed persons

According to the provisions of the Law politically exposed persons pose high risk customers. Therefore a reporting entity shall apply enhanced due diligence measures in all cases when a customer is a person defined by the criteria of the Law and the Guidelines as a politically exposed person, before establishing a business relationship or executing a transaction.

Enhanced customer due diligence includes the application of additional measures, such as:

1. collecting data on the source of the funds and property that are or will be the subject of the business relationship, or transaction,
2. mandatory obtaining of a written consent of a superior responsible person before establishing a business relationship with such customer,
3. very careful monitoring of transactions and other business activities carried out by a politically exposed person at the reporting entity, after establishing the business relationship.

A reporting entity obtains information on whether a specific person is a politically exposed person or not on the basis of a signed written statement fulfilled by a customer before establishing a business relationship or executing a transaction (Questionnaire for identifying politically exposed persons). The written statement has to be made in the mother language and in English.

The written statement has to include the following data:

QUESTIONNAIRE FOR IDENTIFYING A POLITICALLY EXPOSED PERSON

In accordance with the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the LPMLTF, Official Gazette of Montenegro, No. 14/07), ____________ (reporting entity) must establish whether a customer is a politically exposed person when entering into a business relationship or executing transactions (Article 9 Paragraph 1 Item 2) with the customer .

A ***politically exposed person*** *is any natural person who works or has worked in the last year in a high-profile public position, including that person's immediate family members and co-workers.*

Immediate family members of a politically exposed person *are spouses or cohabiting partners, parents, brothers and sisters, as well as children and their spouses or cohabiting partners.*

Immediate co-workers of a politically exposed person *are all persons who have joint income from property, an active business relationship or any other form of close business contact.*

Pursuant to the requirements of the LPMLTF, we are kindly requesting that you answer the following questions.

1. Are you:

1.	a head of state?	YES	NO
2.	the head of a government?	YES	NO
3.	a minister or deputy or assistant thereof?	YES	NO
4.	Head of state administrative body or local administrative body, or his /her deputy or assistant and other official?	YES	NO
5.	an elected representative of a legislative body (MPs and other person appointed or elected by the Parliament)	YES	NO
6.	a holder of the highest judicial and constitutional court functions (judges, prosecutors, and their deputies)	YES	NO
7.	a member of a court of auditors or supreme auditing institutions and central bank governing board?	YES	NO
8.	an ambassador?	YES	NO
9.	A consul? (diplomatic agents)?	YES	NO
10.	a high-ranking officer in the armed forces?	YES	NO
11.	a member of the management or supervisory board of a company under majority state ownership?	YES	NO

2. Are you:

1.	An immediate family member of the persons defined in point 1? • Spouse of cohabiting partner • Parent • Brother or sister • Child born in a marital or extramarital relationship and his or her spouse or cohabiting partner	 YES YES YES YES	 NO NO NO NO
2.	An immediate co-worker of the persons defined in point 1 • Do you have joint income from property or an active business relationship with the persons defined above? • Do you have any other form of close business contact with the persons defined above?	 YES YES	 NO NO

3. Have you:

In the last 12 months worked in any of the positions set out in point 1?	YES	NO
Are you an immediate family member or co-worker of a person who has worked in any of the positions, set out in point 1, in the last 12 months?	YES	NO

If you have answered YES to any of the above questions, you are considered a politically exposed foreign person according to the law. We therefore kindly request that you state the origin of funds and property that are or will be the subject of the business relationship or transaction:

I, the undersigned, hereby confirm that the above stated data are correct and true.

____

Name and surname of person completing the questionnaire

____

Customer's address Customer's data of birth

____

Place and date Signature of the customer

____

Name and surname of the bank employee

____

Place and date Signature of the bank employee

I hereby authorize the entering into a business relationship with a politically exposed person.	
______________________________________	
Name and surname of the responsible senior staff member	
Place and date	Signature of the responsible senior staff member

In case of suspecting the accuracy of the data obtained in the statement the reporting entity can additionally verify the information by checking the public and other data available to the reporting entity (the reporting entity judges to which extent it will consider the commercial lists, i.e politically exposed persons data bases, credible and relevant for enhanced customer due diligence). Also, the data can be checked at: competent state authority, consular agencies or embassies of foreign countries in Montenegro.

A reporting entity shall pay special attention to any risk of money laundering and/or terrorist financing that could result from technical developments (ex. Internet banking) and put in place policies and undertake measures for preventing the use of new techology developments for the purposes of money laundering or terrorist financing. The reporting entities' policies and procedures for the risk related to a business relationship or transaction with customers that are not phisically present, are also applied when doing business with customers through new technologies.

3. Simplified customer due diligence

A reporting entity shall apply simplified customer due diligence in the following cases: when there is insignificant risk of money laundering or terrorist financing, when the data on a customer which is a legal person or its beneficial owner are transaparent, or publicly available. This means that a reporting entity in a certain case establishes and verifies the identity of a customer, but the procedure is simpler than the enhanced customer due diligence procedure.

A reporting entity will not establish a business relationship or execute a transaction before he/she establishes all the facts needed for customer risk assessment.

Simplified customer due diligence is not allowed when there is suspicion that a customer or transaction are related to money laundering or terrorist financing, or when the customer is, according to the risk assessment, categorized as a high risk customer.

4. Customer due diligence conducted by third parties

When establishing a business relationship, a reporting entity can, as a term prescribed by the Law, entrust a third person with customer due diligence procedure, previously verifying has the third person conducting customer due diligence procedure met all the requirements prescribed by the Law and bylaws.

A reporting entity verifies the fulfillment of the requirements by the third person in one of the following ways:

1. checking public or other available data bases,
2. checking the documents and business documentation provided to the reporting entity by the third person, or
3. obtaining a written statement from the third person by which the third person guarantees to the reporting entity that he/she has met the requirements.

If the third person, instead of the reporting entity, has conducted enhanced customer due diligence the third person is responsible for meeting the requirements from the Law, including reporting transactions obligation and the obligation of keeping data and documentation.

Even though the third person has carried out enhanced customer due diligence, instead of the reporting entity, the reporting entity is still responsible for the implementation of enhanced customer due diligence.

IMPLEMENTING THE MEASURES OF DETECTING AND PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING IN BUSINESS UNITS AND COMPANIES IN WHICH A CUSTOMER IS A MAJORITY SHAREHOLDER OR HAS A MAJORITY VOTING RIGHT, AND WHICH HAVE A REGISTERED OFFICE IN A THIRD COUNTRY

A reporting entity establishes a system of conducting unique policy of detecting and preventing money laundering and terrorist financing. For such purposes a reporting entity especially pays attention to implement the detecting and preventing money laundering and terrorist financing measures prescribed by the Law in relation to customer due diligence, suspicious transactions reporting, record keeping, internal audit, nominating an agent, keeping data and other important circumstances related to detecting and preventing money laundering or terrorist financing to the same, or similar extent in the business units and companies where the reporting entity is a majority shareholder or has a majority voting right, and which have a registered office in a third country.

If the implementation of detecting and preventing money laundering and terrorist financing in business units and companies where the reporting entity is a majority shareholder, or has a majority voting right is entirely contrary to the legislation of the third country where the business unit or company have a registered office, the reporting entity shall notify the Administration for the Prevention of Money Laundering and Terrorist Financing and take the appropriate measures for eliminating the risk of money laundering or terrorist financing, such as:

1. putting in place additional internal procedures for preventing, or diminishing the possibility of abuse for the purpose of money laundering or terrorist financing,
2. carrying out additional internal control over the reporting entity's business operations in all the key areas that are most vulnerable to money laundering and terrorist financing,
3. establishing internal risk assessment mechanisms for certain customers, business relationships, products and transactions,
4. implementing strict policy of classifying customers according to the degree of risk related to them and consistent implementation of the measures accepted on the basis of that policy,
5. additional training of the employees.

The Administration shall:

- ensure that all business units and companies where the reporting entity is a majority shareholder or has a majority voting right, and which have a registered office in a third country and their employees get introduced to the policy of detecting and preventing money laundering and terrorist financing,

- ensure, through the director of the business units and companies where the reporting entity is a majority shareholder or has a majority voting right, the internal procedures of detecting and preventing money laundering and terrorist financing, to be substantially integrated into their business processes,

- conducting ongoing monitoring of the appropriate and effective implementation of detecting and preventing money laundering and terrorist financing measures in the business units and companies where the reporting entity is a majority shareholder or has a majority voting right, and which have a registered office in a third country.

MONITORING OF CUSTOMER BUSINESS ACTIVITIES

I. **<u>The purpose of customer business activities monitoring</u>**

Regular monitoring of the customer business activities is the key for efficiency determination of proscribed measures implementation in the area of money laundering and terrorism financing detection and prevention. The purpose of customer business activities monitoring is to determine the legitimacy of the customer business and to verify the compliance of the customer business activities with provided nature and purpose of business relation which the customer concluded with compliance officer, or with customer's regular scope of work. Monitoring of customer business activities is divided into four different segments of customer's business with compliance officer as follows:

1. Monitoring and verification of customer's business compliance with provided nature and purpose of business relationship;
2. Monitoring and verification of the customer's resources origin compliance with the supposed resources origin which the customer stated when setting up business relationship with compliance officer;
3. Monitoring and verifying compliance of customer's business activities with the customer's usual scope of work;

4. Monitoring and updating of collected documents and data about the customer.

II. Measures of client's business activities monitoring

1. In order to monitor and verify the compliance of customer's business activities with the supposed nature and purpose of business relation which the customer concluded with reporting entity, the following measures are used:

    a. Data analysis on purchase and/or selling of financial instruments or other transactions for specific time period with the intention to determine whether, in relation to specific financial instruments purchase or selling or any other transaction, there exist possible circumstances for suspicion on money laundering and/or terrorism financing. Decision on suspicion is based on suspicion criteria determined by the list of indicators for recognizing customers and transactions with which there exist reasons for suspicion on money laundering, and/or list of indicators for recognizing clients and transactions with the view on reasons for suspicion on terrorism financing,

    b. Drafting new customer risk assessment and/or updating previous customer risk level.

2. The following measures are used for monitoring and verification of customer business activities compliance with customer's usual scope of business activities:

    a. Monitoring of financial instruments purchase and selling value, and/or other transactions above the specific limit – it is the decision of the reporting entity what would be the specific limit for specific customer above which the business activity of the customer would be monitored. The same is applied for every customer individually bearing in mind in particular the risk based category of customer (for efficient application of this measure the reporting entity may establish adequate information support),

    b. Analysis of specific purchase or selling of financial instrument, and/or other transaction with the view of suspicion on money laundering and terrorism financing when the number of selling or purchase of financial instruments exceeds certain amount. Analysis of suspicion of financial instruments purchase or selling and/or other transactions is based on suspicion criteria determined in the list of indicators for recognizing suspicious customers and transactions and/or list of indicators for recognizing customers and transactions with the grounds for suspicion on terrorism financing.

3. For monitoring and updating of collected documents and data about the customer:

    a. yearly customer analysis (simplified and deep and usual),

    b. yearly customer analysis (simplified and deep and usual), when there exist a doubt on authenticity of previously received data about the customer or about the real owner of the customer (if the customer is an legal entity),

    c. verification of customer data or of customer's legal representative in the court registry or any other public registry,

d. verification of received data within the premise of the customer or it's legal representative or assignee,

e. verification of list of persons, countries and other entities subject to application of UN Security Council measures or EU.

III. The scope of customer's business activities monitoring

The scope and intensity of customer's business activities monitoring depends on risk based approach level of specific customer, and/or categorization of the customer into specific risk category. Adequate scope of monitoring dedicated to business activities of specific customer understands following:

1. In the case when dealing with highly risk customer – determined monitoring measures of customer's business activities leveled as highly risk the reporting entity applies at least once a year. When dealing with highly risk customer the reporting entity regularly, at least once a year, conducts measures of repeated yearly customer analysis (simplified and deep and usual), if certain requirements, determined by the Law, have been met.

2. In the case of medium (average) risk customer – the reporting entity applies determined measures of monitoring customer's business activities at least once in three years. In the case of medium (average) risk customer the reporting entity, regularly, at least once a year, applies measures of repeated yearly customer analysis (simplified and deep and usual), if certain requirements, determined by the Law, have been met.

3. In the case of law risk customer the reporting entity regularly, at least once a year, applies measures of repeated yearly customer analysis, if certain requirements, determined by the Law, have been met.

Customer's business activities' monitoring is not required, if the customer did not carry out business activity (purchase and selling of financial instrument or other type of transaction) after concluding business relation. In this specific case the reporting entity would apply measures of monitoring business activities of the customer, after conducting the first following purchase or selling of financial instrument, and/or performing the following transaction.

In accordance with the policy of money laundering and terrorism financing risk based approach the reporting entity, in internal document, is in position to decide for more frequent monitoring of business activities of specific customer, than determined in the Guidelines and is also in position to establish additional measures to assist monitoring of customer's business activities and to determine the legitimacy of customer's business activities.

DATA DELIVERY

1.Notification on cash transactions

In case when specific customer carries out a cash transaction with the reporting entity, amounting to €15 000 and above, the reporting entity is liable to, in accordance with the Law, immediately after the transaction has been carried out, and/or in time frame of three working days after the transaction has been carried out, deliver data on this specific transaction to Administration for the Prevention of

Money Laundering and Terrorism Financing, by fulfilling the form provided in the Rule Book on the Manner of Reporting Cash Transactions Exceeding the Value of €15 000 and Above and Suspicious Transactions to the APMLFT (Official Gazette MN no.79. dated: 23, December 2008.).

Cash transaction is every transaction involving reporting entity accepting cash from the customer (coins and bank notes), and/or delivers cash to the customer amounting to €15 000 and above, regardless the value, that the reporting entity receives from the customer and/or delivers to the customer.

2. Notification on suspicious transactions

2.1. What is suspicious transaction?

The provisions of the Law determine that every transaction may be treated as suspicious if being by its nature, scope, complexity, value and links unusual, and/or without clearly visible economic or legal ground, and/or are not in accordance or in disproportion with usual and/or foreseen business of the customer and other circumstances in relation to status and/or other characteristics of the customer. Specific transactions of the customer and specific business relations as well may be treated as suspicious. The suspicious grade of certain customer, transaction or business relation is based on suspicion criteria determined in the List of Indicators for Recognizing Suspicious Clients and Transactions when there grounds for suspicion on money laundering, and/or in the List of Indicators for Recognizing Suspicious Clients and Transactions when there grounds for suspicion on terrorism financing. Indicators are basic guidelines to employees/compliance officers when recognizing suspicious circumstances in relation to specific customer, transaction carried out by the customer and/or business relation having concluded, therefore all employees with the reporting entity need to be familiar with Indicators in order to be able to use them in their work. When deciding whether the transaction is suspicious the compliance officer needs to provide any professional assistance to other employees.

Employees with reporting entity determining that there are reasonable grounds for suspicion on money laundering and/or terrorism financing need to notify the compliance officer for money laundering prevention or his/her deputy about this founding. The reporting entity needs to organize the procedure of suspicious transaction reporting between all organizational units and compliance officer, in accordance with the following instructions:

1. precisely determine the manner of data delivering (telephone, fax, secure electronic manner etc.),
2. determine the type of data being delivered (data about customer, reason for suspicion on money laundering etc.),
3. determine the manner of cooperation between organizational units with compliance officers,
4. determine the manner of treating customer when the APMLFT is temporarily blocking transactions,
5. determine precise role of compliance officer when reporting suspicious transaction,

6. prohibit data discovery about the situation that data, information or documents is or would be reported to the APMLFT,
7. determine measures related to continuation of business relation with customer (temporary ceasing of business relation, ceasing of business relation, performing measures of deep customer analysis and detailed monitoring of future business activities of the customer etc.).

Notification on suspicious transaction needs to be delivered to APMLFT before carrying out of business transaction was performed (telephone, fax or some other appropriate manner). The notification needs to contain specific time frame within the transaction, reported to APMLFT, is supposed to be performed. In the case of temporary notification, compliance officer may deliver the information on suspicious transaction to the APMLFT in electronic manner (over secure web page of the APMLFT, fax) or over telephone, but it also needs to be delivered in written form, the latest on the following working day.

PROFESSIONAL IMPROVEMENT

The compliance officers department responsible for human resources, in cooperation with compliance officer needs to create the program of professional preparation and improvement in the field of prevention and detection of money laundering and terrorism financing, for each calendar year, the latest till the end of the first quarter of business year. The program needs to contain:

- ✓ Content and scope of educational program,
- ✓ The goal of educational program,
- ✓ The manner or accomplishing educational program (teaching, workshops, practices etc.),
- ✓ Group of employees the program is dedicated at,
- ✓ Duration of educational program.

APPLICATION

These Guidelines are enforced on the day of signing and would be applied from 25, September 2009.

Number:

Podgorica, 14, September 2009.

In accordance with the article 112 a paragraph 5 of the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of the Republic of Montenegro ", No. 14/07 and 14/12), The Ministry of Finance adopted

RULEBOOK ON CONTENT AND TYPE OF PAYER'S DATA ACCOMPANYING ELECTRONIC FUNDS TRANSFER

Article 1

This Rule book defines the content and type of data which the reporting entity, providing payment operations or money transfer services (hereinafter: service provider), collects on the payer or enters into a form /message accompanying electronic funds transfer, other activities of service provider and exceptions from collecting data on payer when executing electronic funds transfer that represents insignificant risk for money laundering and terrorist financing.

Article 2

This Rulebook shall be applied on electronic funds transfers executed within the contry or internationally.

Article 3

The terms used in this Rulebook have the following meaning:

1) “ **a payer**” means a natural or legal person that has account opened with a service provider and allows transfer of funds from that account, and/or, when there is no account, natural or legal person who places an order for a transfer of payment order for funds transfer;

2) “**a payee**“ means a natural or legal person who is beneficial recipient of the transferred funds ;

3) “**transfer of funds**” means any transaction carried out electronically on behalf of a payer through a payment service provider, with a view to making funds available to payee at a payment service provider, irrespective whether the payer or the payee are the same person;

4) “**unique identifier**” means a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used to effect the transfer of funds;

5) “**batch file transfer**” means several individual transfer of funds which are bundled together for transmission.

CONTENT AND TYPE OF DATA OF THE

THE PAYER

Article 4

The payment service provider shall, during the process of providing payment operations or services of transferring funds, collect the following:

1) the name of a legal person or name and surname of the natural person that is a payer;

2) data on the head office of a legal person or address of residence of a natural person that is a payer;

3) account number .

If the payment service provider is not able to collect data from paragraph item 2 of this Article then the following data shall be entered into the form or message accompanying electronic funds transfer:

- date and place of birth of the natural person -a payer,

- identification number of a payer that is a costumer,

- unique identifier of apayer, as follows: registration number of legal person or registration/single identification number of natural person that performs a registered business activity or registration /single identification number of natural person that does not perform a registered business activity.

Where the payer does not have an account number, the payment service provider of the payer shall substitute it by unique identifier which allows the transaction to be traced back to the payer .

During the process of batch file transfers from a single payer, provision from paragraph 1 of this Article does not apply to the individual transfers bundled together therein, provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier.

The payment service provider shall put in place procedures for verification whether data on payer from paragraphs 1 and 4 of this Article are complete.

Other activities of the payment service provider

of the payer

Article 5

The payment service provider of the payer shall, before transferring the funds , establish and verify payer's identity through insight into payer's personal documentation issued by the competent state authority.

In case of transfers of funds from an account, verification may be deemed to have taken place if :

1) A payer's identity has been verified in connection with the opening of the account ;
2) in relation to a payer , that has already established a business relationship (old client) with the payment service provider, a subsequently verification has been carried out and data collected in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing.

In the case of transfer of funds not made from an account, the payment service provider of the payer shall verify the information on the payer only where the amount exceeds € 1 000 unless the transaction is carried out in several operations that appear to be linked together exceed € 1 000.

The payment service provider of the payer shall establish and verify payer's identity in case when there are reasons for suspicion (regardless to the amount and type of transaction) in money laundering or terrorist financing.

OTHER ACTIVITIES OF THE PAYMENT SERVICE PROVIDER

OF THE PAYEE

Article 6

The payment service provider of the payee shall detect whether all data on payer from Article 4 paragraph 1 of this Rulebook have been completed into a form or message accompanying electronic funds transfers.

The payment service provider of the payee shall refuse transfer of funds that does not contain the data on payer from Article 4 paragraph 1 of this Rulebook or shall require from the payer's service provider to complete payer's data within 3 (three days) since the date of money transfer order reception.

If the payment service provider of the payer files to complete required information within the prescribed deadline , the service provider of the payee shall refuse to carry out transfer of funds or terminate business relationship with that payment service provider.

The payment service provider of the payee shall report the competent state authority, without delay, when they evaluate that due to the lack of accurate or complete data on the payer there is a suspicion in money laundering or terrorist financing.

Exception from collecting payer's data in the process of electronic funds transfer

Article 7

The payment service provider shall not, in the process of electronic funds transfer, collect data on the payer in cases that represent low risk for money laundering and terrorist financing, as follows:

1) the use of credit and debit cards ,when:

a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services ,

b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies such transfer of funds;

2) in the process of providing services related to electronic funds transfer, when :

a) the total amount of executed payments on electronic data carrier, that may not be recharged, in the amount of up to € 150 ;

b) the total amount of executed payments on electronic data carrier, that may be recharged , within a calendar year, in the amount of up to € 2 500 , except if an electronic funds holder cashes, within the same calendar year, the amount of € 1 000 or more;

3) the use of mobile phone, other digital or informational technology devices, when the electronic funds transfer is carried out in advance and in the amount of up to € 150;

4) the use of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions:

a) a recipient and provider of payment system operations or money transfers services concluded a contract that permits payment for the provision of goods and services;

b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies such transfer of funds;

c) a payment service provider is a reporting entity from Article 4 Paragraph 2 of the Law on the Prevention of Money Laundering and Terrorist Financing;

5) a payer withdraws funds from it's personal account;

6) the payment service provider of the payee is able by means of a unique reference number to trace back, through the payee, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods and services;

7) the electronic checks are used ;

8) tax fees, fines or other duties are paid;

9) payer and payee are service providers and when they act on their behalf and for their account.

Article 8

This Rulebook shall come into effect eight days upon publishing in the "Official Gazette of Montenegro.

No: 02-11760

Podgorica, 27th November 2012.

Minister,

MiloradKatnić, PhD

In accordance with the article 8, paragraph 3 of the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Republic of Montenegro ", No. 14/07), The Ministry of Finance adopted

RULEBOOK ON DEVELOPING RISK ANALYSIS GUIDELINES WITH A VIEW TO PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

(Official Gazette of Montenegro, No. 20, from 17th March 2009)

Article 1

The rulebook defines closer criteria for developing risk analysis guidelines with a view of preventing of money laundering and terrorist financing of the supervising bodies listed in article 86 of the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the Law).

Article 2

The supervisory bodies listed in article 86 of the Law, due to the size and structure of the reporting entities, a scope and type of a client’s business activities, design the guidelines on risk analysis, based on which the reporting entity creates an internal act on risk analysis.

The content of internal procedures from paragraph 1 of this article is defined by the rulebook, as follows:

a) manner of establishing client’s acceptability;

b) risk asessment of groups and clients;

c) the manner of establishing the risk of product and services, with the view of the prevention of money laundering and terrorist financing;

d) manner of client’s identification;

e) client’s accounts and transactions supervision;

f) managing risks to which the reporting entities are exposed, in the area of the prevention of money laundering and terrorist financing;

h) training programs for employees.

Article 3

The risk factors based on which the level of risk of a client, group of client, business relationship, transaction or product is defined, are established by the supervisory bodies guidelines establish and particularly in following cases:

a) if the country of origin of a customer or beneficiary owner of a customer is on the FATF list of non cooperative countries, on the list of countries designated as ,,off-shore" zones or the list of countries which the supervisory body consider a risky based on its own assessment ;

b) if a customer or beneficiary owner of a customer is a person from a country against which were taken measures in accordance with the Resolutions of the UN Security Council ;

c) if a customer is a person from the List created in accordance with the Resolutions of the UN Security Council;

d) if a source of client's assets is unknown or unclear or assets whose source customer can not prove;

e) if there is a suspicion that customer acts by directions of third person;

f) if transaction route is unusual, particularly due to its basis, amount and manner of execution, purpose etc.;

g) if there are indications that customer performs suspicious;

h) if customer is PEP;

i) if client's accounts are connected with accounts of risky clients;

j) particularity of activities performed by customer .

Article 4

With the guidelines, the supervisory body directs reporting entity to define the level of client's risk, depending on the risk factors and also to the possibility of rejecting to conclude a contract with a customer for which the existence of a certain risk is established.

Article 5

With the guidelines , the supervisory body establishes, the procedure for monitoring transactions and business activities, performed by PEP, particularly taking into consideration the intention and purpose of transaction intention; as well as synchronization with its usual business activities

Article 6

With the guidelines, the supervisory body establishes the procedure for putting a person on the list of PEPs, for the purpose of defining the implementation of enhanced due diligence ,in accordance with the Law, and also defining the procedure for terminating the obligation of defining a person as PEPs.

Article 7

The Rule book shall come into force on the 8th day after it is published in the "Official Gazette Montenegro" ".

Number : 02-1544/2

Podgorica,11th March 2009

Ministry of Finance

Minister of Finance

Igor Lukšić Ph.D

.

In accordance with the article 46 of the on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of the Republic of Montenegro ", No. 14/07), The Ministry of Finance adopted

Rulebook on Indicators for recognizing suspicious customers and transactions

Article 1

The list of indicators for recognizing suspicious customers and transactions is closely defined by this Rulebook.

Article 2

The list of indicators for recognizing suspicious customers and transactions is printed together with this rulebook and it makes the integral part of it, as follows:

- List of Indicators for banks,

- List of Indicators for capital market,

- List of Indicators for the Customs Administration,

- List of Indicators for the Department of Public Revenues,

- List of Indicators for leasing companies,

- List of Indicators for auditors,

- List of Indicators for accountants,

- List of Indicators for lawyers and

- General indicators.

Article 3

This Rule book shall come into force on the 8th day after it is published in the "Official Gazette of the Republic of Montenegro" ".

No : 02-

Podgorica, 7th October 2009

Minister of Finance

dr Igor Lukšić

LISTOF INDICATORS FOR BANKS

CASH TRANSACTIONS

1. Depositing or converting into another currency large amounts of small denomination bills into large denomination bills especially if it is outside of the normal course of business of the customer.

2. Frequent payments or numerous bank notes that are battered or damaged.

3. Single payment of a large sum of money on an account of an natural person that is automatically withdrawn from the account.

4. Multiple deposits of small amounts on an account of an individual which are transferred to one account

5. Paying taxes with large amounts of cash..

6. Repeated (consecutive) conversions of large amounts of money into foreign currency.

7. Purchasing financial instruments (securities, insurance policies) in large amounts for cash.

8. Customer conducts cash transactions which are slightly below the legally determined maximum in order to avoid the reporting requirement.

9. Customer conducts transactions which are unusual for him. .

10. Transaction involves non-profit or humanitarian organizations without an obvious economic purpose, or where there is no logical relation between the purpose of the organization and other entities involved in the transaction.

UNUSUAL CHANGES ON THE ACCOUNTS

11. Opening accounts for which the signature authority is given to persons that have signature authority in several companies, especially if the companies are related

12. Opening accounts with the signature authority given to the persons that are neither family nor business related.

13. Opening accounts of legal entities on which deposits are made that are not in accordance with the scope of business of the customer

14. Transactions that are not economically justified.

15. Transactions related to payment operations in the country and abroad that are outside normal activities of the customer with regard to the goods, amounts, business partners, scope of turnover, etc.

16. Frequent advance payments

17. Providing illogical information on the transaction to bank officials.

18. Frequent ordering of traveller's checks, frequent issuing of letters of credit for large sums of money.

19. Short term inflows of a large sum of money on an account of the customer that has been inactive for a long time or payment on an account in an off-shore region

20. Multiply transactions carried out by several different persons to one account and without the clear purpose.

21. Flow of large sums of money from one account to another within a closed group of people

22. Attempt to open an account under a false name.

23. Accounts on which several small sums of money are deposited and there is one time withdrawal of a large sum.

24. Transactions involving several accounts, some of which become inactive for a long time.

25. Depositing a higher amount of cash as deposit for the purpose of obtaining credit, and afterwards an unexpected request form a customer to pay of the credit before the deadline

26. Customer deposits considerable amounts on an account and gives an order to a bank for the amounts to be transferred on the accounts of a great number of persons, especially in cases when there is no rational explanation or economic justification for such transactions

27. Frequent transfers to huge and rounded amounts.

28. Frequent transactions on the basis of advance payments or advance returns that are substantiated by a customer with the non- execution of commercial contracts.

29. Transfers of huge amounts in foreign countries from the account of a customer when the account balance originates from numerous cash deposits on different accounts of customers at one or more banks.

30. Small enterprise operating on only one location performs transactions of depositing or withdrawing funds in more branches of the same bank, which could be evaluated as impractical for that enterprise.

31. Considerable increase of the amount, or frequency of cash deposits or withdrawals from the account of an enterprise whose activity is providing professional and consulting services, especially when the deposited funds are immediately transferred on other accounts.

32. Transactions between private and business account of an enterprise, which do not indicate to a clear economic justification.

33. Transactions including withdrawal of funds soon after the funds have been deposited at reporting entity (only through an account), when this rapid withdrawal of funds is not justified in the business activity of a customer.

34. Unexpected/ sudden paying off a debt without a convincing explanation.

35. Loans granted by off-shore companies.

36. Unexplained electronic transfers of funds by a customer.

37. Accounts are used for receiving or paying of huge amounts, but they do not show so called normal activities related to the operating, such as, for example, payment of salaries, paying bills etc.

38. Transactions with a country that is considered as non-cooperative by Financial Action Task Force (FATF) or business relationships with customers whose permanent residence is in such countries.

39. Issuing payable guarantees by a third party unknown to the financial institution, which do not have a clear relationship with a customer or a good reason for offering such guarantees.

40. Transfers of huge amounts of money with instructions to pay of the funds to the beneficiary in cash.

41. A great number of different individuals paying in deposits on the same account number.

42. Depositing or payment of the higher amounts of the effective money (in Euro currency or other foreign currency) which significantly differ from the customer's usual transactions because they are not in accordance with incomes or customer's status, particularly if the transactions are not typical for the business activities of a customer.

43. Considerable increase of the amount, or frequency of cash deposits or withdrawals from the account of an enterprise whose activity is providing professional and consulting services, especially when the deposited funds are immediately transferred on other accounts

44. Trade or conversion of numerous traveller check's or securities for cash, especially if those transactions are not typical for a customer.

45. Frequent transactions based on the or return of advance which customer explains with non completed contracts.

46. Customer carries out transactions that include several intermediaries or accounts, especially if the customers who are carrying out those transactions are citizens of countries that do not apply regulations from the prevention of money laundering area or where very rigid laws on bank and business data secrecy are in force.

47. Transactions that are recognized as suspicious by employees with the bank, in accordance with their experience and knowledge.

48. Safe deposit box is only used by a person defined as an authorized person in the leasing contract and this person requires cancelling of the safe deposit box leasing contract.

49. Frequent remittance, domestic and foreign, in smaller amounts and ongoing- connected transactions, with the purpose of concealing the real amount of assets in transaction.

50. There are no evidence on transactions (data on sender), or provided evidence for transaction does not correspond to the swift message and other data for payment (contract, invoice, preliminary calculation, , annexes to a contract etc..

51. Politically exposed persons are carrying out transactions with countries which are is recognized as non cooperative by Financial Action Task Force (FATF), or establishing business relationships with clients whose place of residence is in these countries.

BEHAVIOUR OF CUSTOMERS AND EMPLOYEES

52. Customers open accounts or conduct transactions in the branch offices which are not economically or geographically justified

53. Customers conduct transactions through several accounts in several branch offices without the real economic or other reason.

54. Customers are nervous. They avoid answering questions related to the transactions. They assume a defensive posture. They are reluctant to provide identification. They provide false documents or data.

55. Transactions with large amounts of money conducted by public officials, clerks or employees or political exposed persons that are not in accordance with their income or position.

56. Customer asks for assistance to complete the documents while opening an account or he can not provide the necessary information.

57. Customer does not know or is unable or unwilling to provide information concerning the nature of the business or about the owners of the firm.

58. Documents do not show clearly the identity of owners and/or authorized persons to represent the firm.

59. Representatives of a business that is registered in territories of so called high risk countries or off-shore regions want to open an account.

60. Founders of the company are identified as suspicious by law enforcement or other sources.

61. There are valid reasons to believe that the submitted documents to open an account are forged or their authenticity can not be verified. .

62. Customer insists that a transaction is conducted promptly.

63. Customer offers statements that the money is clean and that it is not laundered without being questioned in this regard.

64. Customer refuses to show personal documents

65. Customer asks questions about certain facts, which point to his desire to avoid the reporting requirement.

66. Customer shows only copies of his personal documents.

67. Customer attempts to prove his identity using some other documents that are not usual personal documents..

68. The customer's documentation does not contain usual data such as phone number and address etc

69. The customer's personal documents are new and recently issued.

70. Customer has never been employed, and owns considerable funds on the accounts.

71. Customer holds open accounts in few branches of the same bank, deposits cash on each of them, and the sum of payments is a considerable one.

72. Customer often deposits funds for which they states that they originate from asset sale, while the existence of the asset is questioned.

73. Authorised persons for disposing of the funds on the account of an enterprise refuse to provide complete data on business of the enterprise.

74. Customer makes cash deposits on the account of their enterprise with the purpose of paying for "founder's loan" or "increase of founder's deposit".

75. Customer withdraws high sums of money from the account on which significant funds have been transferred on the basis of a credit granted from a country that does not implement the regulations from the prevention of money laundering area.

76. Customer transfers funds on the account in a country their enterprise has not had business relationship or receives remittances from business entities they had no connections and previous transfers

77. Orderer or the user/beneficiary of the remittance is the citizen of the country that does not apply regulations from the prevention of money laundering area, or which is on the consolidated list of the Sanctions Committee on the basis of UN Security Council Resolution 1267.

78. Customer carries out transactions with persons or companies registered in the countries known as narco-countries and through whose territory narcotics are distributed, or where very rigid laws on bank and business data secrecy are in force.

79. Customer – a legal person, submits a loan application, despite the fact that the economic and financial standing indicators do not imply the customer's need for a loan. The funds from the loan are afterwards transferred on the accounts in an off-shore bank, or in the favour of a third party, or are used without clear purpose.

80. When carrying out a transaction, a customer is supervised by a third person.

81. Customer frequently deposits or withdraws funds in the amounts that are somewhat lower than the threshold required for identifying and reporting.

82. Customer requires the business relationship to be terminated and to establish a new relationship with a bank in his own name, or in the name of a family member, with no documented traces left.

83. Customer frequently (in a short period of time) via cash dispensers withdraws cash in the amounts that are under the threshold required for identifying and reporting.

84. Customer carries out transactions in high amounts and through an account that has been inactive for a long period of time and possibly gives order for closing an account.

85. Customer frequently deposing assets, claiming that it derives from property sale while the existence of this property is disputable..

86. Customer has unusually good knowledge of legal provisions related to the prevention of money laundering and terrorist financing and reporting suspicious transactions, very "gabby" in relation with topics referring to money laundering and activities of terrorist financing, rapidly confirms that the assets at their disposal are "clean" and not laundered.

87. Politically exposed persons frequently depositing cash (in high amount), and the origin of money is not known or can not be established.

88. Natural person issues order to a bank to transfer assets to a third person without evidences on the purpose and intention of this transfer.

89. Customer opens account as natural person or they is an authorized person of a legal person but provides personal documentation issued in countries where dual documentation is still valid (states which do not exist but documents they have issued are still valid) and now he appears as non resident.

ELECTRONIC FUNDS TRANSFER

1. Customer transfers large amounts of money abroad with cash payment order to the foreign entity.

2. Customer receives large amounts of money, from foreign locations, that contains cash payment orders.

3. The amount of electronically transferred assets is out of usual business transactions of that customer.

4. Customer carries out fund transfer towards counties known for drugs production and export.

5. Customer carries out transactions within countries known for high level of bank and business secrecy, except when there is about countries that have accepted international standards on prevention of money laundering.

6. Customer carries out electronic fund transfer in/from free or off shore zone, even if this activity is not usual for customer's business activities.

7. Customer carries out fund transfers (in/from) and as a purpose for transaction states different derivative financial instruments (options, futures…)

LIST OF INDICATORS FOR CAPITAL MARKET

INDICATORS OF SUSPICIOUS TRANSACTIONS AT THE STOCK EXCHANGE BUSINESS

WHILE OPENING AN ACCOUNT

1. When a customer expresses unusual request for the privacy protection, especially with regard to the data related to his identity, type of industry, assets or business.

2. When a customer refuses or avoids showing the origin of funds for each transaction with the value exceeding 15.000 Euros or when there are grounds for suspicion that the funds were gained from illegal sources.

3. When an employee estimates that a customer broke a transaction into several separate transactions in order to avoid identification.

4. When a customer pulls from giving a payment order in order to avoid identification after he has been told in accordance with the law provisions that his identity should be checked.

5. When a customer is not interested in the commission, other expenses and the risks to the transaction.

6. When a customer conducts a transaction as an authorized person and he does not want to identify the entity in the name of which he conducts the transaction, especially if the entity resides and has the main office out of the Republic of Montenegro territory.

7. When a customer cannot explain the nature of his business industry.

8. When a customer has several accounts under the same name, or several sub accounts under different names for no particular reason.

9. When a customer is from or has an account in the country, which has been identified as a risk country, because it does not apply the standards in the area of the detection and the prevention of money laundering.

10. When a customer has been convicted for the criminal offenses involving the payment operations, the economic activities and discharging official duties.

WITH REGARD TO CONDUCTING THE TRANSACTION

1. The transaction a customer wants to conduct is not in accordance with his financial status or the course of business.

2. Customer shows interest in purchasing securities for large amounts without special analysis or broker's or investment manager's advice, and such a transaction does not have a clear financial purpose.

3. The transaction a customer wants to conduct is not of a kind that he would be expected to conduct, because the transaction has unclear purpose and is conducted under unusual circumstances.

4. Customer purchases securities from numerous accounts in the banks
where he previously deposited cash, especially if the funds were deposited in amounts which are slightly under the reporting threshold.

5. Customer conducts transfers of monetary funds or securities from one account to other account, none of which is connected to the customer.

6. Customer's account shows sudden inflow of monetary funds, especially ifthe customer's account has previously been inactive, or deposits are not in accordance with his financial status.

7. Customer's account shows inflow of monetary funds from the accounts in the countries which are risky because they do not apply standards in the area of the detection and the prevention of money laundering.

8. Customer's account shows major inflow of monetary funds while the securities account does not undergo any changes.

9. Customer attempts to create an image of real trade in securities, but instead he conducts fictitious or simulated trade in securities.

10. The proposed transaction is financed by the international wire transfer of money, especially from the countries without an efficient anti-money laundering system.

11. Announced block trade in shares at price slower than the market ones, when buyers are unknown or newly formed companies, and particularly the companies registered on offshore territories.

12. Customer invests in prime and very promising shares, without expressing an interest in the results, or suddenly and without purpose sells the shares.

13. Customer often changes brokerage houses in an effort to conceal the scope of their business and the financial standing.

14. Trades and transactions carried on through a brokerage-dealer house that has previously been punished by the Securities Commission for irregular or undue carrying on business.

15. Trade in securities with a planned loss, when a customer frequently purchases securities and soon after sells them below cost.

16. Trade in shares that have been the subject of collateral on the basis of granted loans to the share owners.

17. Customer has poor reputation; they is known for illegal activities from the past or connections with persons related to illegal activities.

INDICATORS OF SUSPICIOUS TRANSACTIONS FOR CUSTOMS ADMINISTRATION

IMPORTER/EXPORTER/GOODS

1. The business has previously committed Customs violation.

2. The business was founded recently and conducted substantial import/export operations over a short period of time.

3. The business uses services of a suspicious shipping or transport company.

4. The business is known to have financial problems.

5. The business is not specialized for trade but only occasionally conducts trading.

6. The business that is specialized in importing or exporting products from certain countries changes the source of procurement or destination of his products.

7. The business chooses to change location of the Customs examination.

8. Goods are imported from a country known as the source or transit country for narcotics.

9. The business is not registered in the Customs register.

10. Goods are imported or exported in an usual or indirect manner.

11. The value of goods are similar to or lower that the transport costs?

12. The number of the seal does not agree with the number written in the customs documentation.

13. The seals are either impossible to identify or they are perfectly clear.

TRAVELLER / VEHICLE

1. There is a failure to properly declare currency or goods to Customs authorities in accordance with the law.

2. The appearance of the traveller is not in accordance with the purpose of the stated travel.

3. If travelling by public conveyance there is a one way ticket.

4. Traveller is using a leased vehicle.

5. Driver is extremely cooperative or offers information without being asked.

6. The traveller’s passport has recently been issued.

7. The traveller always uses the same flight or schedule.

8. The traveller gives a vague or incomplete explanation of the purpose of the travel and the date of return?

9. The travel destination is known for being a source location for narcotics or other illegal activities.

10. There any indication of modification remodelling or changes to the vehicle that may signal secret compartments.

INDICATORS OF SUSPICIOUS TRANSACTIONS FOR THE TAX ADMINISTRATION

CASH CONTRARY TO REALIZATION

1. It is used in accounting for large enterprises while selling goods (services). Transaction is usually conducted, turnover is reported even if no payment was made at all. The same pattern is used for business expenditures. Activities with legal appearance through which cash could be sent to the business account are for example: food market business, restaurants and hotels, bars, night clubs, etc. For example, it also happens that individual payments of daily earnings are conducted even when the industry is not performed.

KEEPING RECORDS ON SUPPLIES

2. Accounting on cash is usually combined with supplies. Keeping records on supplies belongs to the system based on realization. Each abnormal increase or drop of figures related to the supplies should be examined.

BALANCE SHEET (ASSETS, FUNDS, LIABILITIES AND CAPITAL)

3. Balance sheet represents the reflection of the value of the capital that is engaged in certain business, loans, as well as data as to who the creditors are, retained profit that represents business pre-history of the company, assets engaged in that business, etc. It should be determined who participates in the ownership and loans. There is always suspicion in case the balance sheet is not in accordance with the tax returns.

METHODS OF LIVING COSTS AND THE METHOD ON NET VALUE AND DEPOSITS IN THE BANKS

4. How much money does the taxpayer spend, where did he earn the money and what does he do for living? If he cannot prove that the assets were paid from the business revenues, then there are other sources of funds. If the total bank deposits exceed the reported turnover and the taxpayer cannot prove where the money came from, the reason to conduct examination appears immediately. In general, whenever the source of funds cannot be proved the examination should be conducted.

CASH

5. Turnover gained in cash has tendency to be used for the new investments, or for personal needs, and the next step would be to send the money back to a firm from which it can be used without raising suspicion, i.e. that the source of money can be explained easily.

RECEIVABLES

6. Balance due, especially a large one, should be examined. This refers particularly to the buyers that are not related to certain business. This usually reveals some private activities that have been conducted through that business.

LIABILITIES TO CREDITORS AND SUPPLIERS

7. Loan given by a shareholder to a firm is shown as payable loan. It is always suspicious when capitalized firms, which have inappropriate status of basic funds according to the balance sheet, convert loans into share capital.

EXAMINING TURNOVER ON THE ACCOUNT

8. Was cash recorded in the turnover and was cash deposited in the banks together with the checks? If not, check the account in the banks due to potential unusual transactions, check the goods that was taken for personal use and whether those amounts were included in the total turnover.

BAD DEBT

9. Examine major and unusual items in the accounts (write-off) and check whether they were previously reported as revenues. In case of writing off from the account of a shareholder, taxpayer or foreigner that is subject to examination, examination should be obligatory.

TRAVEL EXPENSES AND ENTERTAINMENT EXPENSES

10. Are they business oriented or in favour of a shareholder or an employee? Are expenses for purchasing luxurious commodities related to business needs or in favour of the owner?

TRANSACTIONS WITH CONNECTED PERSONS

11. Compulsory examination, especially with large firms that have their own accessory companies located in foreign countries. Also, if the funds are obliged to be transferred to other persons, it is particularly important to examine firms whose the owners of which are both directors or clerks, because there are transactions between two parties (owner and firm) and it should be examined whether they are treated in accordance with «arms length transactions« i.e., under the reasonable conditions as if the parties involved in the transaction are not connected at all.

INDUSTRY MARGINS

12. Use of substantially lower or substantially higher margin than normal for the industry.

HIGH RISK LEGAL ACTIVITIES (RELATED TO THE BANKS – CONTRACTS ON FORFEITING, FACTORING, ETC.) AND THE FINANCIAL DERIVATIVES (FUTURES, OPTIONS AND SIMILAR CONTRACTS)

13. High Risk activities are included in the list because the bank with claims enters into the risky situation while collecting debt from the third person (person liable to perform the obligation assigned) – forfeiting, or the firm in case of factoring. Payment of claims does not depend on the bank or the firm, but on an uncertain event that was not known when the contract was signed. They are used mostly while delivering equipment (export) or constructing a building, so called "turn key" operations.

INDICATORS LIST FOR LEASING COMPANIES

1. Customer submits request for approving financial leasing and given data are incomplete or incorrect with obvious intent to conceal the basic information related to identity of customer or its business activity

2. Transactions for which directors or owners of legal persons , or persons on whose behalf the transaction was carried out, never appears in person not even to sign the contract on financial leasing but instead of them this is done by other persons possessing a special (ad hoc) authorization. All this is activities are performed with excuse that can not be checked (illness, unspecific obligations etc.) or give authorization to the third persons in order to avoid direct contact with employees with the leasing companies.

3. A request for financial leasing which seems unjustifiable due to the purpose of equipment or in relation to the business activity of a customer (for example: obvious disproportion between the size of investment and type of business of leasing receiver or in case when the equipment that is purchased by the contract on leasing is not appropriate to customer's business activity or to business activity which the customer plans to perform).

4. Distributor of the leased equipment performs partial delivery

In order to avoid the amount of transaction that is subject to report that must be delivered to APMLTF . In case when distributor, in cooperation with the receiver of leased equipment, delivers equipment through few leasing companies, in the aim of removing the risk it is important to establish the following: that the delivered equipment is completed or that delivered goods is supplement of the previously imported equipment which the receiver already uses (for example: spare parts for current maintenance).

5. Equipment leasing Business when the equipment is offered for price that significantly differs from the real market price.

6. Distributor of the leased equipment neither is the manufacturer nor it is known as seller of goods or equipment that is the subject of leasing.

7. Leasing business of second hand equipment that is not connected with the regular business activity of leasing equipment distributor and distributor is not involved in selling this type of equipment (neither new nor second hand equipment)

8. Leasing business for which the third party provides guarantees (assurance, mortgage, deposit etc. sl.) and when the connection between leasing user and the person offering guarantees is not clear as well as the reasons why the guarantee is offered to the leasing user.

9. Leasing business in which there is a provision on repurchasing leased equipment by distributor and it is offered by distributor spontaneously and under non-market conditions, and specially when distributor of leased equipment is not familiar to the leasing company.

10. Receiver or distributor of leased equipment unwillingly provides information on itself, its business activities or business relations with other leasing companies, especially when concealment of these information disables access to better conditions for concluding leasing business.

11. Customer with no justifiable reason communicates with leasing companies or its subsidiaries that are away from the company's register office.

12. Customer, with no real reason, performs payment form another subsidiary /the account different than the account defined in the original contract.

13. Customer submits request for approving leasing on the basis of guarantees issued or for which asset cover is provided by bank of suspicious solvency, bank from off shore country. Bank from a country through which drug trafficking is caring out or bank from a country where regulations on the prevention of money laundering and terrorist financing are not applied .

14. Customer offers, with no justifiable reasons, offers participation in leasing business and it is significantly higher than the amount that is usual at the leasing market.

15. Customers that are carrying out leasing business with cash payments or checks rather than transactions through the bank account

16. Customer pays its debt by a leasing contract with assets transferred form abroad and from accounts opened in banks situated in countries where the standards on the PML/TF are not implemented or from countries where the strict regulations on bank and business data secrecy and confidentiality are in force.

17. Customer deposits high amounts of cash as participation for getting leasing and afterwards unexpectedly pays off the rest of its debt before the payment deadline.

18. Customer signs the contract on financial leasing accompanied by a person that obviously supervises customer's behaviour or insists that the business should be done quickly.

19. Customer provides only copies of documents that are necessary for customer's personal identification or documents issued abroad and its authenticity can not be easily confirmed due to justifiable reasons.

20. Customer possess unusually good knowledge on regulations related to PML/TF and reporting suspicious transactions, customer is very talkative in relations to the topics on money laundering and financing terrorist activities and confirms quickly that their assets are "clean" and that they are not "laundered" .

INDICATORS LIST FOR AUDITORS AND ACCOUNTANTS

1. A customer is not familiar with their business and it can be concluded that the customer does not perform their business at all or performs it in a very limited range.
2. An auditor has never been enabled to check the business premises or the production facilities of a customer and it can be concluded that the company is fictitious.
3. Complicated organisational structure of the corporation which, in relation to its business activity, is not efficient and thus, it is not economically justifiable.
4. A legal person is established with no particular or justifiable business reason.
5. An orderer pays in advance for the business that has not been contracted yet, and it is less than likely that it will be realized.
6. High, unclear oscillations in incomes or incomes that are unusually high compared to the business expenditures.
7. Customer, contrary to their business practice, requires from an auditor to perform, in their name and for their account, a transaction for a customer
8. Unusual transactions, most often with related persons or persons that vary from the usual customers (for example: payments to natural persons).
9. There is no evidence on transactions (information, clarifications), or the evidence is not satisfactory.
10. Booking the transactions on the basis of unauthentic and incomplete documentation
11. Transactions involving legal persons where it is difficult to establish the identity of beneficiary owner.
12. Cash based business mainly appears at the legal person that conducts business activity for which cash payment is unusual type of realization of business transaction.
13. Payments for undefined activities or payments that vary from usual payments.
14. Enormous delay in opening account of legal person (account of legal person is opened much later after the establishment of the legal person)
15. A legal person is founded without any economic reason.
16. Frequent trips abroad that are, regarding the business activities of the legal person, unnecessary, or to be more exact, unusual.
17. A legal person possesses several recorded individual transactions that are, in comparison to other transactions, unusually high.
18. Executing cash transactions below the threshold for which an identification obligation is prescribed.
19. Cash business is usually performed below the threshold for which an obligation of reporting to the Administration is prescribed.
20. Concluding contracts on life insurance, with one shot premium, and early termination of contract without justifiable reason.
21. Opening numerous accounts without clear economic or legal justifiability and performing business activities via these accounts which, contrary to the regulations, are not presented in balances.
22. Conducting business activities with entities from the countries through whose territory narcotics are distributed, or from countries that do not apply AML/CFT regulations.
23. A customer performs recapitalization of the legal entity without economically justifiable reason.
24. A customer, without established reason, does not open a business account even one year after the registration into the Central Register of Commercial Court and it is known that this legal entity performs business activities.
25. A customer, without economical or legal justification, opens or has numerous accounts, or performs business activities through those accounts that are not, contrary to regulations, presented at the balance.
26. A customer does not possess records on permanent or contracted employees which is unusual for their business activity.
27. A customer is not sure where their business documentation is stored.
28. A customer often and with no founded reason, changes person(s) who do for them the accounting activities.
29. A customer, contrary to the business practice, requires from an accountant to perform, in their name and for their account, a transaction for the customer.
30. Termination of the contract on cooperation caused by the requirements for additional explanation of realization (or announced realisation) of certain transactions, without any founded reason.
31. High, unclear oscillations in incomes or incomes that are unusually high compared to the business expenditures.
32. Insufficiently explained short term income, that is in the amount 10 times higher than average monthly realisation in the previous year, for the same business activity, while there is no an increase in the scope of business activities.

33. Debt and obligation write offs that reach 10% of customer's assets.
34. Customer's business activities with entities from countries through whose territory narcotics are distributed, or from countries that do not apply AML/CFT regulations.
35. Customer's business activities with entities from countries that are known as "tax haven" (for example: payment for consulting services or payments for examining entities that do not conduct or are forbidden to conduct trade or production activities in the state where they are registered)
36. Inflows made from foreign accounts or outflows to foreign accounts from countries where the customer does not have any business partners.
37. Frequent, illogic payments to the daughter company or in other way related companies, or payments to natural persons.
38. Executing cash transactions below the threshold for which an identification obligation is prescribed.
39. Cash business is usually performed below the threshold for which an obligation of reporting to the Administration is prescribed.
40. Early cash repayments of credits or loans.
41. Providing loans to shareholders or employees, contrary to regulations.
42. Payments for undefined services.
43. A customer concludes contracts on life insurance, with one shot premium, and then, with no founded reason, terminates the contract prematurely.
44. There is no clear evidence on transactions or transactions are executed without a clear purpose.
45. Increase of equity for companies without additional registration of the change in the Central Register of the Commercial Court.
46. A customer, user of booking services, performs business activities that include significant number of cash transactions or amounts in cash.
47. A customer, user of booking services, uses complex structure without obvious business or any other reason, especially when the beneficiary owner of the company cannot be established.
48. A customer, user of booking services, has their registered offices in high risk countries, or performs business activities through or in high risk countries.
49. A customer states or confesses that they are involved in illegal activities.

50. A customer does not want the mail to be sent to their address in the country.

51. A customer is surveilled or monitored.

52. A customer unexpectedly expresses great interest in supervision and the policy of conducting supervision.

53. A customer is unknown and opposes to a direct contact.

54. A customer's private or business phone number is off or non-existent.

55. A customer is involved in activities that are not typical for their business.

56. A customer, without a specific reason, insists on quick carrying out of business or transaction.

57. A customer has recently established several business relationships with various financial institutions.

58. A customer tries to establish good and close relationships with the employees.

59. A customer uses various names or nicknames and a series of similar, but different addresses.

60. A customer uses other forms of postal addresses instead of the street address, which is unusual for that place or area.

61. A customer offers money, gifts or other unusual benefits as a favour done in return for carrying out obviously unusual or suspicious business.

62. A customer is under investigation for a criminal act of money laundering or terrorist financing.

63. A customer wants to convince the employee not to fill some of the documents needed for performing an activity or executing a transaction.

64. Customer's acting in relation to the reporting request indicates their wish to avoid fulfilling this obligation.

65. A customer is familiar with the rules on suspicious transactions reporting.

66. A customer seems to be very well acquainted with the cases related to money laundering and terrorist financing.

67. A customer starts, of their own initiative, to conclude that the funds are 'clean' and that they are not 'laundered'.

68. A customer provides suspicious or unclear information.

69. A customer submits inappropriate documents that are falsified, altered or irregular.

70. A customer is opposed to submitting ID documents.

71. A customer submits only the copies of ID documents.

72. A customer attempts to identify themselves with documents other than ID documents.

73. A customer submits the documents for the company too late.

74. All ID documents are issued abroad, i.e. their authenticity is difficult to check.

75. All the submitted ID documents are new, i.e. they have been issued recently.

76. When executing cash transactions, a customer brings high amounts of uncounted money.

77. The business is inconsistent with the customer's financial standing, i.e. with their usual business.

78. A business relationship or transaction are inconsistent with the usual manner of doing business, i.e. they have no economic value for the customer.

79. A business relationship or transaction are unnecessarily complicated.

80. The activities of a customer are not complied with the expectations related to the conducting affairs.

81. A business relationship or transaction involve non-profit or charity organizations, with no economic reason.

82. Customers and other parties involved in the business have no obvious or meaningful connections with Montenegro.

83. A customer uses payments tool issued in another country, although they do not either do business in that country or have permanent or temporary residence in that country.

84. Loans warrantied by banks in tax havens.

85. Given or taken loans from the companies in tax havens.

86. The business of a customer largely differs from the usual doing business in the profession.

87. A customer's living standard is beyond their possibilities.

88. A customer receives payments from unknown sources.

89. A customer enters non-existing or already collected debts in the accounting statements.

90. A customer has no employees which is unusual for conducting their affairs.

91. A customer is directly doing business at a loss, even though their existence is not endangered, so there are no reasons for doing business at a loss.

92. Checking the original documents reveals the mistakes in customer's carrying out business which cannot be seen from the business records.

93. A customer pays out (states) great amounts of money to their subordinates or in other way supervised companies whose manner of doing business differs from the usual one.

94. A customer has formidable property (vessels, luxury cars, residential apartments and residences) that is not covered by the usual scope of the business activity of a company or profession.

95. Foreigners issue bills for provided services of the company or organization with registered offices in countries where there is no appropriate AML legislation and that are known as tax havens, or that have a banking system that allows great secrecy of customers.

LIST OF INDICATORS FOR LAWYERS AND NOTRIES
GENERAL DATA ON CUSTOMER, ITS DOCUMENTATION AND INTENTIONS

1. Customer avoids the meeting and identification in person, breaches the business relationship with a lawyer and notary when they becomes informed on identification obligation.
2. Customer breaches business relationship by authorization (since they is authorized representative) because of the request for additional explanations or additional documentation, without obvious reasons.
3. Customer's phone is turned off or it is established that customer's number does not exist at all.
4. Customer uses fictitious name or address.
5. Customer possesses unusually good knowledge on regulations related to reporting suspicious transactions, and confirms quickly that their assets are "clean"
6. Customer unwillingly provides information on itself, its business activities or business relations with other persons (legal or natural), especially when concealment of these information disables access to better conditions for concluding specific contracts.
7. Customer provides only copies of documents that are necessary for customer's personal identification or documents issued abroad and its authenticity can not be easily confirmed due to justifiable reasons.
8. Customer offers much more money for the service that is provided to him/her than it is usual for that kind of business.
9. Customer requires advice on conducting specific legal business that is connected with criminal act.
10. Customer is a citizen of country through whose territory narcotics are distributed, or its registered office, or address, is in a country that does not apply regulations from the prevention of money laundering and terrorist financing area.
11. Customer comes to a lawyer and notary with high amount of cash, gold, precious stones or securities which they tries to deposite or deliver for performing a certain transaction or legal arrangement, in a manner that is unusual for regular financial business, or with obvious attempt to avoid financial institutions.
12. Business activity of a customer is very different from the ordinary business in theirs profession.

13. Customer requires advice from a lawyer and notary for unusual transactions or services in order to conceal the illicit origin of the funds.
14. Customer requires advice from a lawyer and notary in unusual working hours (early in the morning, late at night, outside working hours) or requires rapid execution without justified reason.
15. Customer frequently changes lawyer and notary in short period of time with no economically or legally justifiable interest.
16. Customer avoids to request service from the notary on whose official territory they lives or whose regular client they is, and requests service from another notary, though the requested service could be performed, with no difficulties, by the notary on whose official territory customer lives or whose regular client the customer is, and neither notary nor client have adequate explanation for such action.
17. Customer requires from lawyer and notary establishment of different companies, in short period of time, with no economically or legally justifiable reasons.
18. Notary and lawyer receive money from the client for performing payment to the third person although there is no justified reason to do so.
19. Customer, with no reasonable explanation, seeks to establish a company that would perform activity which is completely different from the customer's profession.
20. Customer buys real estates in the name of its relatives, friends and business associates.
21. Customer, frequently, in short periods of time, buys for cash, large amounts of stocks, bonds and other securities and invests cash in stock exchanges and funds, which is not in accordance with the usual behaviour of the customer.
22. Sale of the founding share of a legal person, founded in Montenegro, to the company that was registered by the same founders in the off shore area.

REAL ESTATE TRADE

1. Customer sold a real estate within a relatively short period even if in the process of sale it is obvious that this sale will be a business loss for customer.
2. Customer, in a short period, conducts numerous purchases without any economically or legally justifiable reasons.
3. Customer requires conducting trade contracts in high amounts (where the customer appears as buyer) and after realization of the first part of contracted business transaction aborts trade, specifically requires breach of the contract even if it is known that the customer possess enough financial assets for realization of the trade contract. By this act, customer consciously losses certain financial assets with no economically or legally justifiable reasons.
4. The pre-contract requires from lawyer and notary stating disproportionately higher prices than market prices.

DISPOSING CUSTOMER’S MONEY – SECURITIES OR OTHER PROPERTY. DISPOSING CUSTOMER’S BANK ACCOUNT, SAVINGS OR SHARE DEALING ACCOUNT

1. In the process of planning transaction, customer plans to make deposits at numerous accounts, (with the same bank but different subsidiaries or different banks), and then the total amount of payments, that is a significant sum, to transfer in countries that do not apply regulations from the prevention of money laundering and terrorist financing area .
2. Transactions with country that is designated by Financial Action Task Force (FATF) as non-cooperative or business relationships are established with entities whose place of residence is in the mentioned countries.
3. Frequent unusual transactions, often with persons that differ from regular customers.
4. Economically or legally unjustified customer’s business activities are performed with entities from countries that are known for production of narcotics or countries known as “tax paradises” (for example: payment for consulting services or payments for examining entities that do not conduct trade or production activities in the state where they are registered).
5. Customer, contrary to business practice, requires from lawyer and notary to perform, on their name and account, a transaction for a customer.
6. There are no clear evidences on transactions or transactions are executed without a clear purpose.

LIST OF INDICATORS FOR RECOGNITION OF SUSPICIOUS TRANSACTIONS FOR THE REPORTING ENTITIES IN REAL ESTATE TRADE AND CONSTRUCTION INDUSTRY

1. Customer pays a real estate in cash, in securities issued by a commercial bank or bearer cheques.
2. Customer buys a real estate in the name of relatives, friends, lawyers, shell companies and legitimate companies without reasonable explanation.
3. Real estate transfer is performed from one natural or legal person to the other person without reasonable explanation for that kind of transfer.
4. Customer buys real estate sight unseen (without seeing or checking it) or shows no particular interest in the characteristics of the real estate.
5. Contracting parties do not act on their own behalf and try to conceal the identity of real buyer or seller.
6. Customer wants to build a luxurious house in a peripheral, non-urbanized location.
7. Customer buyers and sells several real estates, in very short period of time, without reasonable explanation.
8. Customer requires that smaller amount out of the total price is stated in real estate purchase contract, and the rest of the amount to be paid in cash "under the table".
9. Several legal persons are included in a transaction although there is no connection between the transaction and business activity of legal persons or when the legal persons do not perform any business activity.
10. The buyer is not particularly interested in gathering better offers or achieving better paying conditions.
11. Purchase of real estates without certified contracts, based on internal agreements of two interested sides.
12. Buying and selling of real estates is performed on the same day or in short periods of time, with significant deviation from the market price.
13. Purchase of real estate is disproportionate to the customer's purchasing power.
14. Customers show great interest in performing sales transaction although there is no special reason.
15. The buyer shows extreme interest in certain real estate and location, and does not show interest in the price of that real estate (buys it at any price).
16. Transaction where the customer requests partial payment with short periods of time between the payments.

GENERAL INDICATORS

1. Customer brings high amount of cash and intend to execute a transaction.
2. Customer's business transactions are not in accordance with customer's known income or property.
3. Customer provides unclear explanation on its source of incomes or cash which they uses in business transactions.
4. Customer claims or states that the origin of incomes or cash is illegal
5. There are data that customer is allegedly involved in for illegal activities.
6. Customer requires paying in installments in order to avoid cash payment in the amounts which are slightly under the reporting threshold.
7. Customer requires that the report on cash transaction should not be composed or rejects to execute transaction after receiving information that there is reporting obligation.
8. Transaction that customer executes is not in accordance with theirs usual business practice.
9. Customer intends to buy property or conduct business on behalf of another person for example: acquaintance or cousin (besides its spouse).
10. Customer does not want that their name is recorded in any document that could connect him/her in relation with the certain business transaction.
11. Customer provides inadequate explanation why does they, in the last moment, changes names of persons that are used in relation with the transaction.
12. Customer negotiates on performing business by market price or price higher than required but demands that lower price should be provided in the documents, and they is paying price difference underhand
13. Customer pays advance in a high amount of cash, while the rest of it is financed from an unusual source or offshore bank.
14. Customer buys property, especially real estates, blindly (without seeing or checking it).
15. Customer buys property or invests in real-estate business in a short term period and acts as very interested in location, status or projected expenses for repairing the property.
16. Customer performs real-estate business (buying, selling, replacing) in cash and for the benefit of himself/herself, members of its family and third persons, in the amounts exceeding 150.000 €.
17. Customer would like to know more about unusual ways of paying.

18. Customer does not want to identify itself in case of real-estate trade in cash or identifies itself with counterfeited data or documents.
19. Customer that is known from the public life, buys real estates in high amounts and the value of the bought property differ from their income status.
20. Customer that purchases real estates is a young person and it is obvious that this customer disposes luxurious status symbols (expensive automobiles, motorcycles, vehicles, watches etc.).
21. Customers that are residents or non residents purchase real-estates for domestic legal person even if it is obvious that the purpose of real-estate trade is purchasing real-estate for non resident natural person.
22. Customer natural or legal person asks or executes transactions on realestate for natural or legal persons , residents or non residents, that are from off shore destinations or for off shore companies and also from countries known for narcotics distribution and production narcotics or countries that do not apply regulations from the prevention of money laundering and terrorist financing area.
23. Payments of high amount insurance premiums.
24. The insurance user requires cash payment for money form insurance or return of insurance premium in case that there is a high amount of money.
25. High insurance amounts for number of insurance policies, that are concluded in short time period, are paid in cash.
26. It is suspected that insurance policies are concluded on fictitious names, names of other persons or fictitious addresses.
27. One person owns numerous insurance policies issued at different insurance companies, especially if insurance contracts were concluded in a short time period.
28. Insurance policy owner makes changes at insurance contract and requires insurance policy with higher premium or to change monthly policy payments to annual policy payments or insurance at fixed premium, and it is not in accordance with its income status.
29. Cancelling insurance policy soon after concluding insurance policy contract soon after concluding insurance policy contract, especially when there is large amount premium.
30. Customer demands compensation from insurance, money that is demanded on the basis of compensation in case of cancellation of policy or overpaid amount of insurance premium to be paid off to a third party or transferred to the account of natural or legal person on the territory of the state where are applied high standards in the area of money laundering and in which are prescribed strict regulations on confidentiality and secrecy of bank and business data.
31. Customer accepts unfavourable terms of insurance contract, with regard to his health condition and age.
32. Companies that are owners of insurance policies pay on behalf of their employees unusually large insurance premiums or cancel policies in very short time period from the date of concluding insurance contract
33. Companies purchase insurance policies for their employees, and number of employees is lower than number of purchased policies: polices are issued even for persons that are not employed in company.
34. Insurance contract is concluded by person who carried out illegal activities in past or insurance contract is concluded by person that in some manner can be connected with these activities.
35. Contractor insurance or the insured insists on transaction secrecy, i.e. not to report the amount of the insurance premium or the amount of the insurance to the APMLTF despite the fact that it is a statutory obligation of the insurer. A customer attempts, by plead or bribe, to convince the employees in the insurance company to represent their interests which is against the law.

In accordance with the article 46 of the on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of the Republic of Montenegro ", No. 14/07 and 14/12), The Ministry of Finance adopted

Rulebook on Indicators for recognizing suspicious customers and transactions

(Official Gazette Montenegro, No. 26/12 of 24.05.2012)

Article 1

The list of indicators for recognizing suspicious customers and transactions is closely defined by this Rulebook.

Article 2

The list of indicators for recognizing suspicious customers and transactions is printed together with this rulebook and it makes the integral part of it, as follows:

- List of Indicators for banks,
- List of Indicators for capital market,
- List of Indicators for the Customs Administration,
- List of Indicators for the Department of Public Revenues,
- List of Indicators for leasing companies,
- List of Indicators for auditors,
- List of Indicators for accountants,
- List of Indicators for lawyers and
- General indicators.

Article 3

The Rulebook on Indicators for recognizing suspicious clients and transactions (Official Gazette of MNE, No. 69/09) shall cease to have effect on the day when this Rulebook comes into effect.

Article 4

This Rule book shall come into effect on the 8th day after its publication in the "Official Gazette of the Republic of Montenegro" ".

No : 02-5240

Podgorica, 9th May 2012

Minister of Finance

dr Milorad Katnic

Annex

LIST OF INDICATORS FOR RECOGNIZING SUSPICIOUS TRANSACTIONS AND CLIENTS

LIST OF INDICATORS FOR BANKS

CASH TRANSACTIONS

1. Depositing or converting into other currency large amounts of small denomination bills into large denomination bills especially if it is outside of the normal course of business of the customer.
2. Frequent payments or numerous bank notes that are battered or damaged.
3. Single payment of a large sum of money on an account of a natural person that is automatically withdrawn from the account.
4. Multiple deposits of small amounts on an account of an individual which are transferred to one account.
5. Paying taxes with large amounts of cash.
6. Repeated (consecutive) conversions of large amounts of money into foreign currency.
7. Purchasing financial instruments (securities, insurance policies) in large amounts for cash.
8. Customer conducts cash transactions which are slightly below the legally determined maximum in order to avoid the reporting requirement.
9. Customer conducts transactions which are unusual for him.
10. Transaction involves non-profit or humanitarian organizations without an obvious economic purpose, or where there is no logical relation between the purpose of the organization and other entities involved in the transaction.

UNUSUAL CHANGES ON THE ACCOUNTS

1. Opening accounts for which the signature authority is given to persons that have signature authority in several companies, especially if the companies are related.

2. Opening accounts with the signature authority given to the persons that are neither family nor business related.
3. Opening accounts of legal entities on which deposits are made that are not in accordance with the scope of business of the customer.
4. Transactions that are not economically justified.
5. Transactions related to payment operations in the country and abroad which are outside normal activities of the customer with regard to the goods, amounts, business partners, scope of turnover, etc.
6. Frequent advance payments.
7. Providing illogical information on the transaction to bank officials.
8. Frequent ordering of traveller's checks, frequent issuing of letters of credit for large sums of money.
9. Short term inflows of a large sum of money on an account of the customer that has been inactive for a long time or payment on account in an off-shore region.
10. Multiple transactions carried out by several different persons to one account and without clear purpose.
11. Flow of large sums of money from one account to another within a closed group of people.
12. Attempt to open an account under a false name.
13. Accounts on which several small sums of money are deposited and there is one time withdrawal of a large sum.
14. Transactions involving several accounts, some of which become inactive for a long time.
15. Depositing a higher amount of cash as deposit for the purpose of obtaining credit, and afterwards an unexpected request form a customer to pay of the credit before the deadline.
16. Customer deposits considerable amounts on an account and gives an order to a bank for the amounts to be transferred on the accounts of a great number of persons, especially in cases when there is no rational explanation or economic justification for such transactions.
17. Frequent transfers to huge and rounded amounts.
18. Frequent transactions on the basis of advance payments or advance returns that are substantiated by a customer with the non- execution of commercial contracts.
19. Transfers of huge amounts in foreign countries from the account of a customer when the account balance originates from numerous cash deposits on different accounts of customers at one or more banks.
20. Small enterprise operating on only one location performs transactions of depositing or withdrawing funds in more branches of the same bank, which could be evaluated as impractical for that enterprise.
21. Considerable increase of the amount, or frequency of cash deposits or withdrawals from the account of an enterprise whose activity is providing professional and consulting services, especially when the deposited funds are immediately transferred on other accounts.
22. Transactions between private and business account of an enterprise, which do not indicate to a clear economic justification.
23. Transactions including withdrawal of funds soon after the funds have been deposited at reporting entity (only through an account), when this rapid withdrawal of funds is not justified in the business activity of a customer.
24. Unexpected/ sudden paying off a debt without a convincing explanation.
25. Loans granted by off-shore companies.
26. Unexplained electronic transfers of funds by a customer.
27. Accounts are used for receiving or paying of huge amounts, but they do not show so called normal activities related to the operating, such as, for example, payment of salaries, paying bills etc.

28. Transactions with a country that is considered as non-cooperative by Financial Action Task Force (FATF) or business relationships with customers whose permanent residence is in such countries.
29. Issuing payable guarantees by a third party unknown to the financial institution, which do not have a clear relationship with a customer or a good reason for offering such guarantees.
30. Transfers of huge amounts of money with instructions to pay of the funds to the beneficiary in cash.
31. A great number of different individuals paying in deposits on the same account number.
32. Depositing or payment of the higher amounts of the effective money (in Euro currency or other foreign currency) which significantly differ from the customer's usual transactions because they are not in accordance with incomes or customer's status, particularly if the transactions are not typical for the business activities of a customer.
33. Considerable increase of the amount, or frequency of cash deposits or withdrawals from the account of an enterprise whose activity is providing professional and consulting services, especially when the deposited funds are immediately transferred on other accounts.
34. Trade or conversion of numerous traveller check's or securities for cash, especially if those transactions are not typical for a customer.
35. Frequent transactions based on the or return of advance which customer explains with non completed contracts.
36. Customer carries out transactions that include several intermediaries or accounts, especially if the customers who are carrying out those transactions are citizens of countries that do not apply regulations from the prevention of money laundering area or where very rigid laws on bank and business data secrecy are in force.
37. Transactions that are recognized as suspicious by employees with the bank, in accordance with their experience and knowledge.
38. Safe deposit box is only used by a person defined as an authorized person in the leasing contract and this person requires cancelling of the safe deposit box leasing contract.
39. Frequent remittance, domestic and foreign, in smaller amounts and ongoing- connected transactions, with the purpose of concealing the real amount of assets in transaction.
40. There are no evidence on transactions (data on sender), or provided evidence for transaction does not correspond to the swift message and other data for payment (contract, invoice, preliminary calculation, , annexes to a contract etc.
41. Politically exposed persons are carrying out transactions with countries which are is recognized as non cooperative by Financial Action Task Force (FATF), or establishing business relationships with clients whose place of residence is in these countries.

BEHAVIOUR OF CUSTOMERS AND EMPLOYEES

1. Customers open accounts or conduct transactions in the branch offices which are not economically or geographically justified.
2. Customers conduct transactions through several accounts in several branch offices without the real economic or other reason.
3. Customers are nervous. They avoid answering questions related to the transactions. They assume a defensive posture. They are reluctant to provide identification. They provide false documents or data.
4. Transactions in large amounts of money conducted by public officials, clerks or employees or political exposed persons that are not in accordance with their income or position.
5. Customer asks for assistance to complete the documents while opening an account or he cannot provide the necessary information.

6. Customer does not know or is unable or unwilling to provide information concerning the nature of the business or about the owners of the firm.
7. Documents do not show clearly the identity of owners and/or authorized persons to represent the firm.
8. Representatives of a business that is registered in territories of so called high risk countries or off-shore regions want to open an account.
9. Founders of the company are identified as suspicious by law enforcement or other sources.
10. There are valid reasons to believe that the submitted documents to open an account are forged or their authenticity cannot be verified.
11. Customer insists that a transaction is conducted promptly.
12. Customer offers statements that the money is clean and that it is not laundered without being questioned about that.
13. Customer refuses to show personal documents.
14. Customer asks questions about certain facts, which points to his desire to avoid the reporting requirement.
15. Customer shows only copies of his personal documents.
16. Customer attempts to prove his identity using some other documents that are not usual personal documents.
17. The customer's documentation does not contain usual data such as phone number and address etc.
18. The customer's personal documents are new and recently issued.
19. Customer has never been employed, and owns considerable funds on the accounts.
20. Customer holds open accounts in few branches of the same bank, deposits cash on each of them, and the sum of payments is a considerable one.
21. Customer often deposits funds for which they states that they originate from asset sale, while the existence of the asset is questioned.
22. Authorised persons for disposing of the funds on the account of an enterprise refuse to provide complete data on business of the enterprise.
23. Customer makes cash deposits on the account of their enterprise with the purpose of paying for "founder's loan" or "increase of founder's deposit".
24. Customer withdraws high sums of money from the account on which significant funds have been transferred on the basis of a credit granted from a country that does not implement the regulations from the prevention of money laundering area.
25. Customer transfers funds on the account in a country their enterprise has not had business relationship or receives remittances from business entities they had no connections and previous transfers.
26. Orderer or the user/beneficiary of the remittance is the citizen of the country that does not apply regulations from the prevention of money laundering area, or which is on the consolidated list of the Sanctions Committee on the basis of UN Security Council Resolution 1267.
27. Customer carries out transactions with persons or companies registered in the countries known as narco-countries and through whose territory narcotics are distributed, or where very rigid laws on bank and business data secrecy are in force.
28. Customer – a legal person, submits a loan application, despite the fact that the economic and financial standing indicators do not imply the customer's need for a loan. The funds from the loan are afterwards transferred on the accounts in an off-shore bank, or in the favour of a third party, or are used without clear purpose.
29. When carrying out a transaction, a customer is supervised by a third person.
30. Customer frequently deposits or withdraws funds in the amounts that are somewhat lower than the threshold required for identifying and reporting.

31. Customer requires the business relationship to be terminated and to establish a new relationship with a bank in his own name, or in the name of a family member, with no documented traces left.
32. Customer frequently (in a short period of time) via cash dispensers withdraws cash in the amounts that are under the threshold required for identifying and reporting.
33. Customer carries out transactions in high amounts and through an account that has been inactive for a long period of time and possibly gives order for closing an account.
34. Customer frequently deposing assets, claiming that it derives from property sale while the existence of this property is disputable.
35. Customer has unusually good knowledge of legal provisions related to the prevention of money laundering and terrorist financing and reporting suspicious transactions, very "gabby" in relation with topics referring to money laundering and activities of terrorist financing, rapidly confirms that the assets at their disposal are "clean" and not laundered.
36. Politically exposed persons frequently depositing cash (in high amount) and the origin of money is not known or cannot be established.
37. Natural person issues order to a bank to transfer assets to a third person without evidences on the purpose and intention of this transfer.
38. Customer opens account as natural person or he is an authorized person of a legal person but provides personal documentation issued in countries where dual documentation is still valid (states which do not exist but documents they have issued are still valid) and now he appears as non-resident.
39. Mortgaging real estate of high value which serves as guarantee for granting loans to another person, with no clear economic justification.
40. Granting loans to a domestic legal person when the founder of both legal persons is the same.
41. A foreign investor formally pays money onto the account of the domestic legal person on the basis of nominal share and significantly increases the nominal capital so that he returns the funds back into the main company abroad on different basis.

ELECTRONIC FUNDS TRANSFER

1. Customer transfers large amounts of money abroad with cash payment order to the foreign entity.
2. Customer receives large amounts of money, from foreign locations, that contains cash payment orders.
3. The amount of electronically transferred assets is out of usual business transactions of that customer.
4. Customer carries out fund transfer towards counties known for drugs production and export.
5. Customer carries out transactions within countries known for high level of bank and business secrecy, except when there is about countries that have accepted international standards on prevention of money laundering.
6. Customer carries out electronic fund transfer in/from free or off shore zone, even if this activity is not usual for customer's business activities.
7. Customer carries out fund transfers (in/from) and as a purpose for transaction states different derivative financial instruments (options, futures…)

LIST OF INDICATORS FOR CAPITAL MARKET

INDICATORS OF SUSPICIOUS TRANSACTIONS AT THE STOCK EXCHANGE BUSINESS

WHEN OPENING AN ACCOUNT

1. When a customer expresses unusual request for the privacy protection, especially with regard to the data related to his identity, type of industry, assets or business.
2. When a customer refuses or avoids showing the origin of funds for each transaction with the value exceeding 15.000 Euros or when there are grounds for suspicion that the funds were gained from illegal sources.
3. When an employee estimates that a customer broke a transaction into several separate transactions in order to avoid identification.
4. When a customer pulls from giving a payment order in order to avoid identification after he has been told in accordance with the law provisions that his identity should be checked.
5. When a customer is not interested in the commission, other expenses and the risks to the transaction.
6. When a customer conducts a transaction as an authorized person and he does not want to identify the entity in the name of which he conducts the transaction, especially if the entity resides and has the main office out of the Republic of Montenegro territory.
7. When a customer cannot explain the nature of his business industry.
8. When a customer has several accounts under the same name, or several sub accounts under different names for no particular reason.
9. When a customer is from or has an account in the country, which has been identified as a risk country, because it does not apply the standards in the area of the detection and the prevention of money laundering.
10. When a customer has been convicted before for criminal offenses against payment operations, economic activities and official duty.

WHEN CONDUCTING TRANSACTIONS

1. The transaction a customer wants to conduct is not in accordance with his financial status or the course of business.
2. Customer shows interest in purchasing securities for large amounts without special analysis or broker's or investment manager's advice, and such a transaction does not have a clear financial purpose.
3. The transaction a customer wants to conduct is not of a kind that he would be expected to conduct, because the transaction has unclear purpose and is conducted under unusual circumstances.
4. Customer purchases securities from numerous accounts in the banks where he previously deposited cash, especially if the funds were deposited in amounts which are slightly under the reporting threshold.
5. Customer conducts transfers of monetary funds or securities from one account to other account, none of which is connected to the customer.
6. Customer's account shows sudden inflow of monetary funds, especially if the customer's account has previously been inactive, or deposits are not in accordance with his financial status.
7. Customer's account shows inflow of monetary funds from the accounts in the countries which are risky because they do not apply standards in the area of the detection and the prevention of money laundering.
8. Customer's account shows major inflow of monetary funds while the securities account does not undergo any changes.
9. Customer attempts to create an image of real trade in securities, but instead he conducts fictitious or simulated trade in securities.
10. The proposed transaction is financed by the international wire transfer of money, especially from the countries without an efficient anti-money laundering system.
11. Announced block trade in shares at price slower than the market ones, when buyers are unknown or newly formed companies, and particularly the companies registered on offshore territories.
12. Customer invests in prime and very promising shares, without expressing an interest in the results, or suddenly and without purpose sells the shares.

13. Customer often changes brokerage houses in an effort to conceal the scope of their business and the financial standing.
14. Trades and transactions carried on through a brokerage-dealer house that has previously been punished by the Securities Commission for irregular or undue carrying on business.
15. Trade in securities with a planned loss, when a customer frequently purchases securities and soon after sells them below cost.
16. Trade in shares that have been the subject of collateral on the basis of granted loans to the share owners.
17. Customer has poor reputation; they is known for illegal activities from the past or connections with persons related to illegal activities.

LIST OF INDICATORS FOR CUSTOMS ADMINISTRATION

IMPORTER/EXPORTER/GOODS

1. The Customs Administration has previously initiated misdemeanour procedure against the company.
2. The company has been founded recently and has conducted substantial import/export operations over a short period of time.
3. The company uses services of a suspicious shipping or transport company.
4. The company is known to have financial problems.
5. The company is not specialized for trade but only occasionally conducts trading.
6. The company that is specialized in importing or exporting products from certain countries changes the source of procurement or destination of his products.
7. The company chooses to change location of the customs examination.
8. Goods are imported from a country known as the source or transit country for narcotics.
9. The company is not registered in the Customs register.
10. Goods are imported or exported in a usual or indirect manner.
11. The value of goods is similar to/ lower than the transport costs.
12. The number of the seal does not match with the number written in the customs documentation.
13. The seals are either impossible to identify or they are perfectly clear.

TRAVELLER / VEHICLE

1. There is a failure to properly declare currency or goods to Customs authorities in accordance with the law.
2. The appearance of the traveller is not in accordance with the stated purpose of travel.
3. Traveller travels by public transport with a one way ticket.
4. Traveller is using a leased vehicle.
5. Driver is extremely cooperative or offers information without being asked.
6. The traveller’s passport has been issued recently.
7. Traveller always uses the same flight or schedule.
8. Traveller gives a vague or incomplete explanation of the purpose of the travel and the date of return.
9. The travel destination is known for being a source location for narcotics or other illegal activities.
10. There are signs of modification remodelling or changes to the vehicle that may signal secret compartments.

LIST OF INDICATORS FOR THE TAX ADMINISTRATION

CASH CONTRARY TO REALIZATION

1. It is used in accounting for large enterprises while selling goods (services). Transaction is usually conducted; turnover is reported even if no payment was made at all. The same pattern is used for

business expenditures. Activities with legal appearance through which cash could be sent to the business account are for example: food market business, restaurants and hotels, bars, night clubs, etc. For example, it also happens that individual payments of daily earnings are conducted even when the industry is not performed.

KEEPING RECORDS ON SUPPLIES

2. Accounting on cash is usually combined with supplies. Keeping records on supplies belongs to the system based on realization. Each abnormal increase or drop of figures related to the supplies should be examined.

BALANCE SHEET (ASSETS, FUNDS, LIABILITIES AND CAPITAL)

3. Balance sheet represents the reflection of the value of the capital that is engaged in certain business, loans, as well as data as to who the creditors are, retained profit that represents business pre-history of the company, assets engaged in that business, etc. It should be determined who participates in the ownership and loans. There is always suspicion in case the balance sheet is not in accordance with the tax returns.

METHODS OF LIVING COSTS AND THE METHOD ON NET VALUE AND DEPOSITS IN THE BANKS

4. How much money does the taxpayer spend, where did he earn the money and what does he do for living? If he cannot prove that the assets were paid from the business revenues, then there are other sources of funds. If the total bank deposits exceed the reported turnover and the taxpayer cannot prove where the money came from, the reason to conduct examination appears immediately. In general, whenever the source of funds cannot be proved the examination should be conducted.

CASH

5. Turnover gained in cash has tendency to be used for the new investments, or for personal needs, and the next step would be to send the money back to a firm from which it can be used without raising suspicion, i.e. that the source of money can be explained easily.

RECEIVABLES

6. Balance due, especially a large one, should be examined. This refers particularly to the buyers that are not related to certain business. This usually reveals some private activities that have been conducted through that business.

LIABILITIES TO CREDITORS AND SUPPLIERS

7. Loan given by a shareholder to a firm is shown as payable loan. It is always suspicious when capitalized firms, which have inappropriate status of basic funds according to the balance sheet, convert loans into share capital.

CHECKING THE TURNOVER ON THE ACCOUNT

8. Was cash recorded in the turnover and was cash deposited in the banks together with the checks? If not, check the account in the banks due to potential unusual transactions, check the goods that was taken for personal use and whether those amounts were included in the total turnover.

BAD DEBT

9. Examine major and unusual items in the accounts (write-off) and check whether they were previously reported as revenues. In case of writing off from the account of a shareholder, taxpayer or foreigner that is subject to examination, examination should be obligatory.

TRAVEL AND ENTERTAINMENT EXPENSES

10. Are they business oriented or in favour of a shareholder or an employee? Are expenses for purchasing luxurious commodities related to business needs or in favour of the owner?

TRANSACTIONS WITH CONNECTED PERSONS

11. Compulsory examination, especially with large firms that have their own accessory companies located in foreign countries. Also, if the funds are obliged to be transferred to other persons, it is particularly important to examine firms whose the owners of which are both directors or clerks, because there are transactions between two parties (owner and firm) and it should be examined whether they are treated in accordance with «arms length transactions« i.e., under the reasonable conditions as if the parties involved in the transaction are not connected at all.

INDUSTRY MARGINS

12. Use of substantially lower or substantially higher margin than normal for the industry.

HIGH RISK LEGAL ACTIVITIES (RELATED TO THE BANKS – CONTRACTS ON FORFEITING, FACTORING, ETC.) AND THE FINANCIAL DERIVATIVES (FUTURES, OPTIONS AND SIMILAR CONTRACTS)

1. High Risk activities are included in the list because the bank with claims enters into the risky situation while collecting debt from the third person (person liable to perform the obligation assigned) – forfeiting, or the firm in case of factoring. Payment of claims does not depend on the bank or the firm, but on an uncertain event that was not known when the contract was signed. They are used mostly when delivering equipment (export) or constructing a building, so called "turnkey" system.

INDICATORS LIST FOR LEASING COMPANIES

1. Customer submits request for approving financial leasing and given data are incomplete or incorrect with obvious intent to conceal the basic information related to identity of customer or its business activity.
2. Transactions for which directors or owners of legal persons , or persons on whose behalf the transaction was carried out, never appears in person not even to sign the contract on financial leasing but instead of them this is done by other persons possessing a special (ad hoc) authorization. All this is activities are performed with excuse that cannot be checked (illness, unspecific obligations etc.) or give authorization to the third persons in order to avoid direct contact with employees with the leasing companies.
3. A request for financial leasing which seems unjustifiable due to the purpose of equipment or in relation to the business activity of a customer (for example: obvious disproportion between the size of investment and type of business of leasing receiver or in case when the equipment that is purchased

by the contract on leasing is not appropriate to customer's business activity or to business activity which the customer plans to perform).

4. Distributor of the leased equipment performs partial delivery in order to avoid the amount of transaction that is subject to report that must be delivered to APMLTF. In case when distributor, in cooperation with the receiver of leased equipment, delivers equipment through few leasing companies, in the aim of removing the risk it is important to establish the following: that the delivered equipment is completed or that delivered goods is supplement of the previously imported equipment which the receiver already uses (for example: spare parts for current maintenance).
5. Equipment leasing Business when the equipment is offered for price that significantly differs from the real market price.
6. Distributor of the leased equipment neither is the manufacturer nor it is known as seller of goods or equipment that is the subject of leasing.
7. Leasing business of second hand equipment that is not connected with the regular business activity of leasing equipment distributor and distributor is not involved in selling this type of equipment (neither new nor second hand equipment).
8. Leasing business for which the third party provides guarantees (assurance, mortgage, deposit etc. sl.) and when the connection between leasing user and the person offering guarantees is not clear as well as the reasons why the guarantee is offered to the leasing user.
9. Leasing business in which there is a provision on repurchasing leased equipment by distributor and it is offered by distributor spontaneously and under non-market conditions, and specially when distributor of leased equipment is not familiar to the leasing company.
10. Receiver or distributor of leased equipment unwillingly provides information on itself, its business activities or business relations with other leasing companies, especially when concealment of these information disables access to better conditions for concluding leasing business.
11. Customer with no justifiable reason communicates with leasing companies or its subsidiaries that are away from the company's register office.
12. Customer, with no real reason, performs payment form another subsidiary/the account different than the account defined in the original contract.
13. Customer submits request for approving leasing on the basis of guarantees issued or for which asset cover is provided by bank of suspicious solvency, bank from off shore country. Bank from a country through which drug trafficking is caring out or bank from a country where regulations on the prevention of money laundering and terrorist financing are not applied.
14. Customer offers, with no justifiable reasons, offers participation in leasing business and it is significantly higher than the amount that is usual at the leasing market.
15. Customers that are carrying out leasing business with cash payments or checks rather than transactions through the bank account.
16. Customer pays its debt by a leasing contract with assets transferred from abroad and from accounts opened in banks situated in countries where the standards on the PML/TF are not implemented or from countries where the strict regulations on bank and business data secrecy and confidentiality are in force.
17. Customer deposits high amounts of cash as participation for getting leasing and afterwards unexpectedly pays off the rest of its debt before the payment deadline.
18. Customer signs the contract on financial leasing accompanied by a person that obviously supervises customer's behaviour or insists that the business should be done quickly.
19. Customer provides only copies of documents that are necessary for customer's personal identification or documents issued abroad and its authenticity cannot be easily confirmed due to justifiable reasons.
20. Customer possess unusually good knowledge on regulations related to PML/TF and reporting suspicious transactions, customer is very talkative in relations to the topics on money laundering and financing terrorist activities and confirms quickly that their assets are "clean" and that they are not "laundered" .

INDICATORS LIST FOR AUDITORS AND ACCOUNTANTS

1. A customer is not familiar with their business and it can be concluded that the customer does not perform their business at all or performs it in a very limited range.

2. An auditor has never been enabled to check the business premises or the production facilities of a customer and it can be concluded that the company is fictitious.
3. Complicated organisational structure of the corporation which, in relation to its business activity, is not efficient and thus, it is not economically justifiable.
4. A legal person is established with no particular or justifiable business reason.
5. An orderer pays in advance for the business that has not been contracted yet, and it is less than likely that it will be realized.
6. High, unclear oscillations in incomes or incomes that are unusually high compared to the business expenditures.
7. Customer, contrary to their business practice, requires from an auditor to perform, in their name and for their account, a transaction for a customer.
8. Unusual transactions, most often with related persons or persons that vary from the usual customers (for example: payments to natural persons).
9. There is no evidence on transactions (information, clarifications), or the evidence is not satisfactory.
10. Booking the transactions on the basis of unauthentic and incomplete documentation.
11. Transactions involving legal persons where it is difficult to establish the identity of beneficiary owner.
12. Cash based business mainly appears at the legal person that conducts business activity for which cash payment is unusual type of realization of business transaction.
13. Payments for undefined activities or payments that vary from usual payments.
14. Enormous delay in opening account of legal person (account of legal person is opened much later after the establishment of the legal person).
15. A legal person is founded without any economic reason.
16. Frequent trips abroad that are, regarding the business activities of the legal person, unnecessary, or to be more exact, unusual.
17. A legal person possesses several recorded individual transactions that are, in comparison to other transactions, unusually high.
18. Executing cash transactions below the threshold for which an identification obligation is prescribed.
19. Cash business is usually performed below the threshold for which an obligation of reporting to the Administration is prescribed.
20. Concluding contracts on life insurance, with one shot premium, and early termination of contract without justifiable reason.
21. Opening numerous accounts without clear economic or legal justifiability and performing business activities via these accounts which, contrary to the regulations, are not presented in balances.
22. Conducting business activities with entities from the countries through whose territory narcotics are distributed, or from countries that do not apply AML/CFT regulations.
23. A customer performs recapitalization of the legal entity without economically justifiable reason.
24. A customer, without established reason, does not open a business account even one year after the registration into the Central Register of Commercial Court and it is known that this legal entity performs business activities.
25. A customer, without economical or legal justification, opens or has numerous accounts, or performs business activities through those accounts that are not, contrary to regulations, presented at the balance.
26. A customer does not possess records on permanent or contracted employees which is unusual for their business activity.
27. A customer is not sure where their business documentation is stored.
28. A customer often and with no founded reason, changes person(s) who do for them the accounting activities.
29. A customer, contrary to the business practice, requires from an accountant to perform, in their name and for their account, a transaction for the customer.
30. Termination of the contract on cooperation caused by the requirements for additional explanation of realization (or announced realisation) of certain transactions, without any founded reason.
31. High, unclear oscillations in incomes or incomes that are unusually high compared to the business expenditures.
32. Insufficiently explained short term income, that is in the amount 10 times higher than average monthly realisation in the previous year, for the same business activity, while there is no an increase in the scope of business activities.
33. Debt and obligation write offs that reach 10% of customer's assets.

34. Customer's business activities with entities from countries through whose territory narcotics are distributed, or from countries that do not apply AML/CFT regulations.
35. Customer's business activities with entities from countries that are known as "tax haven" (for example: payment for consulting services or payments for examining entities that do not conduct or are forbidden to conduct trade or production activities in the state where they are registered).
36. Inflows made from foreign accounts or outflows to foreign accounts from countries where the customer does not have any business partners.
37. Frequent, illogic payments to the daughter company or in other way related companies, or payments to natural persons.
38. Executing cash transactions below the threshold for which an identification obligation is prescribed.
39. Cash business is usually performed below the threshold for which an obligation of reporting to the Administration is prescribed.
40. Early cash repayments of credits or loans.
41. Providing loans to shareholders or employees, contrary to regulations.
42. Payments for undefined services.
43. A customer concludes contracts on life insurance, with one shot premium, and then, with no founded reason, terminates the contract prematurely.
44. There is no clear evidence on transactions or transactions are executed without a clear purpose.
45. Increase of equity for companies without additional registration of the change in the Central Register of the Commercial Court.
46. A customer, user of booking services, performs business activities that include significant number of cash transactions or amounts in cash.
47. A customer, user of booking services, uses complex structure without obvious business or any other reason, especially when the beneficiary owner of the company cannot be established.
48. A customer, user of booking services, has their registered offices in high risk countries, or performs business activities through or in high risk countries.
49. A customer states or confesses that they are involved in illegal activities.
50. A customer does not want the mail to be sent to their address in the country.
51. A customer is surveilled or monitored.
52. A customer unexpectedly expresses great interest in supervision and the policy of conducting supervision.
53. A customer is unknown and opposes to a direct contact.
54. A customer's private or business phone number is off or non-existent.
55. A customer is involved in activities that are not typical for their business.
56. A customer, without a specific reason, insists on quick carrying out of business or transaction.
57. A customer has recently established several business relationships with various financial institutions.
58. A customer tries to establish good and close relationships with the employees.
59. A customer uses various names or nicknames and a series of similar, but different addresses.
60. A customer uses other forms of postal addresses instead of the street address, which is unusual for that place or area.
61. A customer offers money, gifts or other unusual benefits as a favour done in return for carrying out obviously unusual or suspicious business.
62. A customer is under investigation for a criminal act of money laundering or terrorist financing.
63. A customer wants to convince the employee not to fill some of the documents needed for performing an activity or executing a transaction.
64. Customer's acting in relation to the reporting request indicates their wish to avoid fulfilling this obligation.
65. A customer is familiar with the rules on suspicious transactions reporting.
66. A customer seems to be very well acquainted with the cases related to money laundering and terrorist financing.
67. A customer starts, of their own initiative, to conclude that the funds are 'clean' and that they are not 'laundered'.
68. A customer provides suspicious or unclear information.
69. A customer submits inappropriate documents that are falsified, altered or irregular.
70. A customer is opposed to submitting ID documents.
71. A customer submits only the copies of ID documents.
72. A customer attempts to identify themselves with documents other than ID documents.
73. A customer submits the documents for the company too late.

74. All ID documents are issued abroad, i.e. their authenticity is difficult to check.
75. All the submitted ID documents are new, i.e. they have been issued recently.
76. When executing cash transactions, a customer brings high amounts of uncounted money.
77. The business is inconsistent with the customer's financial standing, i.e. with their usual business.
78. A business relationship or transaction is inconsistent with the usual manner of doing business, i.e. they have no economic value for the customer.
79. A business relationship or transaction is unnecessarily complicated.
80. The activities of a customer are not complied with the expectations related to the conducting affairs.
81. A business relationship or transaction involve non-profit or charity organizations, with no economic reason.
82. Customers and other parties involved in the business have no obvious or meaningful connections with Montenegro.
83. A customer uses payments tool issued in another country, although they do not either do business in that country or have permanent or temporary residence in that country.
84. Loans warrantied by banks in tax havens.
85. Given or taken loans from the companies in tax havens.
86. The business of a customer largely differs from the usual doing business in the profession.
87. A customer's living standard is beyond their possibilities.
88. A customer receives payments from unknown sources.
89. A customer enters non-existing or already collected debts in the accounting statements.
90. A customer has no employees which is unusual for conducting their affairs.
91. A customer is directly doing business at a loss, even though their existence is not endangered, so there are no reasons for doing business at a loss.
92. Checking the original documents reveals the mistakes in customer's carrying out business which cannot be seen from the business records.
93. A customer pays out (states) great amounts of money to their subordinates or in other way supervised companies whose manner of doing business differs from the usual one.
94. A customer has formidable property (vessels, luxury cars, residential apartments and residences) that is not covered by the usual scope of the business activity of a company or profession.
95. Foreigners issue bills for provided services of the company or organization with registered offices in countries where there is no appropriate AML legislation and that are known as tax havens, or that have a banking system that allows great secrecy of customers.

LIST OF INDICATORS FOR LAWYERS AND NOTRIES

GENERAL DATA ON CUSTOMER, ITS DOCUMENTATION AND INTENTIONS

1. Customer avoids the meeting and identification in person, breaches the business relationship with a lawyer and notary when they becomes informed on identification obligation.
2. Customer breaches business relationship by authorization (since they is authorized representative) because of the request for additional explanations or additional documentation, without obvious reasons.
3. Customer's phone is turned off or it is established that customer's number does not exist at all.
4. Customer uses fictitious name or address.
5. Customer possesses unusually good knowledge on regulations related to reporting suspicious transactions, and confirms quickly that their assets are "clean".
6. Customer unwillingly provides information on itself, its business activities or business relations with other persons (legal or natural), especially when concealment of these information disables access to better conditions for concluding specific contracts.
7. Customer provides only copies of documents that are necessary for customer's personal identification or documents issued abroad and its authenticity cannot be easily confirmed due to justifiable reasons.

8. Customer offers much more money for the service that is provided to him/her than it is usual for that kind of business.
9. Customer requires advice on conducting specific legal business that is connected with criminal act.
10. Customer is a citizen of country through whose territory narcotics are distributed, or its registered office, or address, is in a country that does not apply regulations from the prevention of money laundering and terrorist financing area.
11. Customer comes to a lawyer and notary with high amount of cash, gold, precious stones or securities which they tries to deposit or deliver for performing a certain transaction or legal arrangement, in a manner that is unusual for regular financial business, or with obvious attempt to avoid financial institutions.
12. Business activity of a customer is very different from the ordinary business in theirs profession.
13. Customer requires advice from a lawyer and notary for unusual transactions or services in order to conceal the illicit origin of the funds.
14. Customer requires advice from a lawyer and notary in unusual working hours (early in the morning, late at night, outside working hours) or requires rapid execution without justified reason.
15. Customer frequently changes lawyer and notary in short period of time with no economically or legally justifiable interest.
16. Customer avoids to request service from the notary on whose official territory they lives or whose regular client they is, and requests service from another notary, though the requested service could be performed, with no difficulties, by the notary on whose official territory customer lives or whose regular client the customer is, and neither notary nor client have adequate explanation for such action.
17. Customer requires from lawyer and notary establishment of different companies, in short period of time, with no economically or legally justifiable reasons.
18. Notary and lawyer receive money from the client for performing payment to the third person although there is no justified reason to do so.
19. Customer, with no reasonable explanation, seeks to establish a company that would perform activity which is completely different from the customer's profession.
20. Customer buys real estates in the name of its relatives, friends and business associates.
21. Customer, frequently, in short periods of time, buys for cash, large amounts of stocks, bonds and other securities and invests cash in stock exchanges and funds, which is not in accordance with the usual behaviour of the customer.
22. Sale of the founding share of a legal person, founded in Montenegro, to the company that was registered by the same founders in the off shore area.

REAL ESTATE TRADE

1. Customer sold a real estate within a relatively short period even if in the process of sale it is obvious that this sale will be a business loss for customer.
2. Customer, in a short period, conducts numerous purchases without any economically or legally justifiable reasons.
3. Customer requires conducting trade contracts in high amounts (where the customer appears as buyer) and after realization of the first part of contracted business transaction aborts trade, specifically requires breach of the contract even if it is known that the customer possess enough financial assets for realization of the trade contract. By this act customer consciously losses certain financial assets with no economically or legally justifiable reasons.
4. The pre-contract requires from lawyer and notary stating disproportionately higher prices than market prices.

DISPOSAL OF CUSTOMER’S MONEY – SECURITIES OR OTHER PROPERTY, DISPOSAL OF CUSTOMER’S BANK ACCOUNT, SAVINGS OR SHARE DEALING ACCOUNT

1. In the process of planning transaction, customer plans to make deposits at numerous accounts, (with the same bank but different subsidiaries or different banks), and then the total amount of payments, that is a significant sum, to transfer in countries that do not apply regulations from the prevention of money laundering and terrorist financing area.

2. Transactions with country that is designated by Financial Action Task Force (FATF) as non-cooperative or business relationships are established with entities whose place of residence is in the mentioned countries.
3. Frequent unusual transactions, often with persons that differ from regular customers.
4. Economically or legally unjustified customer's business activities are performed with entities from countries that are known for production of narcotics or countries known as "tax paradises" (for example: payment for consulting services or payments for examining entities that do not conduct trade or production activities in the state where they are registered).
5. Customer, contrary to business practice, requires from lawyer and notary to perform, on their name and account, a transaction for a customer.
6. There are no clear evidences on transactions or transactions are executed without a clear purpose.

LIST OF INDICATORS FOR RECOGNIZING SUSPICIOUS TRANSACTIONS FOR THE REPORTING ENTITIES IN REAL ESTATE TRADE AND CONSTRUCTION INDUSTRY

1. Customer pays a real estate in cash, in securities issued by a commercial bank or bearer cheques.
2. Customer buys a real estate in the name of relatives, friends, lawyers, shell companies and legitimate companies without reasonable explanation.
3. Real estate transfer is performed from one natural or legal person to the other person without reasonable explanation for that kind of transfer.
4. Customer buys real estate sight unseen (without seeing or checking it) or shows no particular interest in the characteristics of the real estate.
5. Contracting parties do not act on their own behalf and try to conceal the identity of real buyer or seller.
6. Customer wants to build a luxurious house in a peripheral, non-urbanized location.
7. Customer buyers and sells several real estates, in very short period of time, without reasonable explanation.
8. Customer requires that smaller amount out of the total price is stated in real estate purchase contract, and the rest of the amount to be paid in cash "under the table".
9. Several legal persons are included in a transaction although there is no connection between the transaction and business activity of legal persons or when the legal persons do not perform any business activity.
10. The buyer is not particularly interested in gathering better offers or achieving better paying conditions.
11. Purchase of real estates without certified contracts, based on internal agreements of two interested sides.
12. Buying and selling of real estates is performed on the same day or in short periods of time, with significant deviation from the market price.
13. Purchase of real estate is disproportionate to the customer's purchasing power.
14. Customers show great interest in performing sales transaction although there is no special reason.
15. The buyer shows extreme interest in certain real estate and location, and does not show interest in the price of that real estate (buys it at any price).
16. Transaction where the customer requests partial payment with short periods of time between the payments.

GENERAL INDICATORS

1. Customer brings high amount of cash and intend to execute a transaction.
2. Customer's business transactions are not in accordance with customer's known income or property.
3. Customer provides unclear explanation on its source of incomes or cash which they use in business transactions.
4. Customer claims or states that the origin of incomes or cash is illegal.
5. There are data that customer is allegedly involved in for illegal activities.
6. Customer requires paying in installments in order to avoid cash payment in the amounts which are slightly under the reporting threshold.
7. Customer requires that the report on cash transaction should not be composed or rejects to execute transaction after receiving information that there is reporting obligation.

8. Transaction that customer executes is not in accordance with theirs usual business practice.
9. Customer intends to buy property or conduct business on behalf of another person for example: acquaintance or cousin (besides its spouse).
10. Customer does not want that their name is recorded in any document that could connect him/her in relation with the certain business transaction.
11. Customer provides inadequate explanation why does they, in the last moment, changes names of persons that are used in relation with the transaction.
12. Customer negotiates on performing business by market price or price higher than required but demands that lower price should be provided in the documents, and they is paying price difference underhand.
13. Customer pays advance in a high amount of cash, while the rest of it is financed from an unusual source or offshore bank.
14. Customer buys property, especially real estates, blindly (without seeing or checking it).
15. Customer buys property or invests in real-estate business in a short term period and acts as very interested in location, status or projected expenses for repairing the property.
16. Customer performs real-estate business (buying, selling, replacing) in cash and for the benefit of himself/herself, members of its family and third persons, in the amounts exceeding 150.000 €.
17. Customer would like to know more about unusual ways of paying.
18. Customer does not want to identify itself in case of real-estate trade in cash or identifies itself with counterfeited data or documents.
19. Customer that is known from the public life, buys real estates in high amounts and the value of the bought property differ from their income status.
20. Customer that purchases real estates is a young person and it is obvious that this customer disposes luxurious status symbols (expensive automobiles, motorcycles, vehicles, watches etc.).
21. Customers that are residents or non residents purchase real-estates for domestic legal person even if it is obvious that the purpose of real-estate trade is purchasing real-estate for non -resident natural person.
22. Customer natural or legal person asks or executes transactions on real estate for natural or legal persons, residents or non residents, that are from off shore destinations or for off shore companies and also from countries known for narcotics distribution and production narcotics or countries that do not apply regulations from the prevention of money laundering and terrorist financing area.
23. Payments of high amount insurance premiums.
24. The insurance user requires cash payment for money form insurance or return of insurance premium in case that there is a high amount of money.
25. High insurance amounts for number of insurance policies, that are concluded in short time period, are paid in cash.
26. It is suspected that insurance policies are concluded on fictitious names, names of other persons or fictitious addresses.
27. One person owns numerous insurance policies issued at different insurance companies, especially if insurance contracts were concluded in a short time period.
28. Insurance policy owner makes changes at insurance contract and requires insurance policy with higher premium or to change monthly policy payments to annual policy payments or insurance at fixed premium, and it is not in accordance with its income status.
29. Cancelling insurance policy soon after concluding insurance policy contract soon after concluding insurance policy contract, especially when there is large amount premium.
30. Customer demands compensation from insurance, money that is demanded on the basis of compensation in case of cancellation of policy or overpaid amount of insurance premium to be paid off to a third party or transferred to the account of natural or legal person on the territory of the state where are applied high standards in the area of money laundering and in which are prescribed strict regulations on confidentiality and secrecy of bank and business data.
31. Customer accepts unfavourable terms of insurance contract, with regard to his health condition and age.
32. Companies that are owners of insurance policies pay on behalf of their employees unusually large insurance premiums or cancel policies in very short time period from the date of concluding insurance contract.
33. Companies purchase insurance policies for their employees, and number of employees is lower than number of purchased policies: polices are issued even for persons that are not employed in company.

34. Insurance contract is concluded by person who carried out illegal activities in past or insurance contract is concluded by person that in some manner can be connected with these activities.
35. Contractor insurance or the insured insists on transaction secrecy, i.e. not to report the amount of the insurance premium or the amount of the insurance to the APMLTF despite the fact that it is a statutory obligation of the insurer. A customer attempts, by plead or bribe, to convince the employees in the insurance company to represent their interests which is against the law.

Pursuant to the Article 37 Paragraph 2 of the Law on State Administration («Official Gazette of the Republic of Montenegro» No.38/03, 22/08 and 42/11), at the proposal of the Director of the Administration for Prevention of Money Laundering and Terrorist Financing, the Government of Montenegro, on the session on _________, established

R U L E B O O K

ON INTERNAL ORGANIZATION AND SYSTEMATIZATION OF THE

ADMINISTRATION FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Article 1

This Rulebook regulates internal organization and systematization of the Administration for Prevention of Money Laundering and Terrorist Financing (hereinafter referred to as the Administration), within the established competence of the Administration and sets out organizational units and their scope, workplaces and employment of trainees.

I ORGANIZATIONAL UNITS AND THEIR SCOPE

Article 2

Organizational units, within which execution of tasks is performed in the competencies of the Administration, are:

1. **SECTOR FOR ANALYTICAL AFFAIRS AND REPORTING ENTITIES CONTROL**

   1.1. ANALYTICS DEPARTMENT

   1.2. SUSPICIOUS TRANSACTIONS DEPARTMENT

   1.3. REPORTING ENTITIES CONTROL DEPARTMENT

2. **SECTOR FOR NATIONAL AND INTERNATIONAL COOPERATION**

3. **SECTOR FOR PREVENTION, INTEGRATION AND INFORMATION**

4. **UNIT FOR GENERAL AFFAIRS, FINANCE AND INFORMATION TECHNOLOGIES**

   4.1. GENERAL AFFAIRS AND FINANCE OFFICE
   4.2. INFORMATION TECHNOLOGIES OFFICE

Article 3

1. **<u>IN THE SECTOR FOR SECTOR FOR ANALYTICAL AFFAIRS AND REPORTING ENTITIES CONTROL</u>** tasks performed are related to: reception, record keeping and import of data submitted by the reporting entities; analysis and processing of data received on daily bases as well as analysis and processing of data on transactions and persons submitted by the reporting entities, for which there is reasonable grounds for suspicion of money laundering or terrorist financing; acting upon the requests of competent state authorities in accordance to the Law on prevention of Money Laundering and Terrorist Financing as well as submission of notifications on established reasonable grounds regarding persons and transactions on own initiatives; preparation of professional basis for the drafting of list of indicators for recognition of suspicious transactions and clients, participation in trainings for employees at reporting entities; preparation of guidelines for drafting risk analysis; direct supervision and taking administrative measures and actions; preparing and submitting request for initiation of misdemeanour procedure against the reporting entity and compliance officers at the reporting entity; inspection trainings, keeping records on inspection controls; preparing information, reports and analysis on performed controls, monitoring the implementation of regulations within its jurisdiction, and performing other tasks within its competence.

1.1. **IN THE ANALYTICS DEPARTMENT** tasks that are performed are related to: analysing and processing data submitted by the reporting entities, opening cases related to transactions and persons for whom there is reason to suspect that they committed money laundering or terrorist financing; opening cases upon the requests of competent state authorities; making requests for the data submission by the reporting entities, state authorities as well as foreign financial intelligence units; making reports-notifications based on carried out analysis of gathered data, information and documentation within the case; submitting proposal on forwarding reports-notifications to the competent state authorities for further action; forwarding reports-notifications to the competent state authorities; implementation of continuous monitoring of the persons' accounts for whom there is enough reason to take this measure, implementation of procedure for temporary suspension of transaction; participation in preparation of the basis for innovation of the list of indicators for recognition of suspicious transactions; cooperation with the reporting entities' compliance officers and participation in the trainings for employees at the reporting entities; analysis of the situation from the area of money laundering and terrorist financing; preparation of guidelines for drafting risk analysis; processing statistical data on the work of the Department; and other tasks within the scope of Department.

1.2. **IN THE SUSPICIOUS TRANSACTIONS DEPARTMENT** tasks that are performed are related to: analysis and data processing on transactions for which there is reason to suspect that money laundering or terrorist financing has been committed; opening cases related to received reports on suspicious transactions/suspicious activities or persons; opening cases upon the requests of competent state authorities; gathering all available data relevant for the analysis and processing; making reports-notifications related to a case; forwarding reports-notifications to the competent state authorities; implementation of continuous monitoring of the persons' accounts for whom there is enough reason to take this measure, implementation of procedure

for temporary suspension of transaction; participation in preparation of the list of indicators for recognition of suspicious transactions; preparation of feedback on reported suspicious transactions; processing of statistical data on transactions; preparation of guidelines for drafting risk analysis and other tasks prescribed by the regulations.

1.3. **IN THE REPORTING ENTITIES CONTROL DEPARTMENT** tasks of direct supervision that are performed are related to: gathering of additional data from the reporting entities, based on which, the action of reporting entities in the implementation of the Law is determined, other regulations and general acts; taking administrative measures and actions; preparing and submitting requests for initiation of misdemeanor procedures against reporting entities and compliance officers at reporting entities; inspection trainings, keeping records on inspection controls; preparing information, reports and analysis on performed controls, processing of documentation material from this area; integration of the data obtained by other supervisory authorities on measures taken regarding reporting entities and record keeping on that measures and other tasks prescribed by the regulations.

Article 4

2. **IN THE SECTOR FOR NATIONAL AND INTERNATIONAL COOPERATION** tasks that are performed are related to: establishing international cooperation with authorized authorities of other countries and international organizations; preparation of Memorandums of Understanding with other authorities and foreign financial intelligence services, data exchange with international authorities and organizations regarding prevention of money laundering and terrorist financing; submission of data to other competent authorities and requesting data from mentioned authorities regarding transactions or persons for whom there is reason to suspect that they committed money laundering or terrorist financing; participation in the preparation of the trainings for reporting entities' compliance officers; initiate amendments to the regulations related to or in connection with prevention and detection of money laundering and terrorist financing; preparation of analysis, materials and proposals for the implementation of the recommendations of international organizations and the preparation of materials in order to fulfil obligations arising from a membership in the MONEYVAl, Egmont group and other relevant international organizations; translation of regulations and other documents; participation in preparation of drafts, and proposals of regulations which are adopted on the basis of the Law on Prevention of Money Laundering and Terrorist Financing; participation in the making of the list of countries that apply the standards in the field of prevention of money laundering and terrorist financing and other tasks prescribed by the regulations.

Article 5

3. <u>IN THE SECTOR FOR PREVENTION, INTEGRATION AND INFORMATION</u> tasks that are performed are related to*:* preparation and participation in the implementation of training for compliance officers for the prevention of money laundering and terrorist financing at the reporting entities and employees that have direct contact with the client; monitoring and analysis of reports on work of the compliance officers; monitoring and analysis of published reports of international organizations, monitoring and analysis of the degree of harmonization with EU regulations in the AML/CFT area; preparation of reports within the competence of the Administration in relation to implementation of national strategic documents (Programs, Strategies and Action Plans); participation in the preparation of the proposals and reports on the implementation of measures within the competence of the Administration in the process of European and Euro-Atlantic Integration; preparation of periodic reports on the work of the Administration; regular reporting and informing the public about the work of the Administration; drafting proposals for submission of misdemeanour charges based on the submission of records of other supervisory authorities; supervision and analysis of implementation of program for professional development and training by the reporting entities.

Article 6

4. <u>IN THE UNIT FOR GENERAL AFFAIRS, FINANCE AND INFORMATION TECHNOLOGIES</u> tasks that are performed are related to: drafting general acts of the APMLTF, preparing individual acts on individual acts on executing the labour rights; personal record keeping; entering data in Central Personnel Registry; drafting documents for accounting salary, allowances and other incomes of the employees; financial, accounting and material management, preparation and processing of accounting documents; drafting and implementing integrity plan; free *access to information of public importance;* implementation of rules and regulation of procedures regarding mobbing; drafting financial plan and estimating the funds for the work of authorities and monitoring their execution; public procurement; receiving, distributing, registering and sending documents; archiving cases; as well as tasks related to: planning, development and maintenance of databases, planning, development and maintenance of applications, planning, development and maintenance of hardware, import of data, protection and storage of database, IT staff training and other tasks prescribed by the regulations, copying and photocopying tasks, delivering documents, driver's tasks.

4.1. <u>IN THE GENERAL AFFAIRS AND FINANCE OFFICE</u> tasks that are performed are related to: personnel, general-legal, organizational and other business issues, preparation of draft and proposal for the Rulebook on internal organization and systematization of the Administration; free *access to information of public importance*; preparation of the decisions on employment of civil servants and public emoployees and decisions on *rights and obligations* of civil servants and public employees based on ther working activities; public procurement procedures in accordance with the Law on Public Procurement; planning and executing the budget of the Administration; establishing and keeping records on implementation of financial transactions with the Treasury and treasury reports; processing

and record keeping of supporting documentation for all transactions recorded in the general register of the Treasury; monitoring the dynamics of inflow and expenditure of funds; verifying, synthesizing and consolidating financial data; keeping records and processing documentation for payment of salaries and other incomes; processing of documentation for an order for payment of all types of payments and other duties in accordance with the regulations; procurement of equipment, office and other materials and the implementation of public procurement procedures for the Administration; organizing repair of the equipment and other activities within the scope of the Administration; archive jobs (receiving mail, registering acts, keeping a register, distributing documents via internal delivery books, handling of seals and stamps) tasks of the courier - driver (delivering mail, maintaining and repairing cars, car registration) and other tasks in accordance with the regulations.

4.2. **IN THE INFORMATION TECHNOLOGIES OFFICE** tasks that are performed are related to: import of all types of data received by the reporting entities and other competent authorities; planning, development and maintenance of the database; planning, development, testing and maintenance of software; planning, development and maintenance of network infrastructure; safely storing all relevant data and ensuring the security of information system; creating different statistical reports, archiving documentation of the IT office; IT trainings for employees and other tasks prescribed by the regulations.

II SYSTEMATIZATION OF WORKPLACES

Article 7

For the execution of tasks, within the scope of the Administration, 38 workplaces for civil servants and public employees are established:

Number	Name of the workplace and conditions for performing work in a particular profession	Number of employees	Job description

1.	**The Director** - Higher education in *the scope of 240* credits of Montenegrin credit transfer system (MCTS), VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 3 years of working experience in management, or other relevant jobs that require autonomy in their work, passed professional exam	1	Manages the work of the Administration for the Prevention of Money Laundering and Terrorist Financing.
1. SECTOR FOR ANALYTICAL AFFAIRS AND REPORTING ENTITIES CONTROL			
2.	**Assistant to the Director** For the Sector For Analytical Affairs And Reporting Entities Control - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 3 years of working experience in management, or other relevant jobs that require autonomy in their work, passed professional exam	1	Performs tasks related to: steering the work of the Department and of employees in the Sector for Analytical Affairs And Reporting Entities Control, coordinating and organizing the work of the employees in the Sector and performs other tasks by Director's orders.
1.1. ANALYTICS DEPARTMENT			
3.		1	Coordinates, manages, controls the work of the employees in the Department and performs

	Head of the Department - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics or Law School, at least 3 years of working experience in management, passed professional exam, knowledge of English language – level B1, Computer literacy (word, excel, power point)		the most complex tasks within the scope of the Department. Organizes the execution of tasks related to: analysis and processing data on cash transactions as well as acting upon the requests of other state authorities. Proposes procedures and criteria for the performance of tasks within the competence of the Department. Approves the opening of the cases where reasonable grounds for the money laundering or other criminal offence is determined and proposes sending acts related to those cases. Participates in organizing trainings for the employees and compliance officers at the reporting entities. Participates in the drafting and innovation of list of indicators. Provides suggestions for the improvement of the working process in the Department. Participates in the preparation of the analysis of the situation from the area of money laundering and terrorist financing. Provides suggestions for establishing guidelines for drafting risk analysis. Prepares opinion on upgrading system for prevention of money laundering and drafts strategic analysis and plans. Drafts statistical reports and keeps records. Performs other tasks upon the Superior's orders.
4.	**Independent Adviser I** **- Analyst** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School, at least 5 years of working experience, passed professional exam and Computer literacy (word, excel, power point)	1	Performs tasks related to proccesing, analysis, record keeping and additional data received by the reporting entities in relation to the cases opened upon the request of competent state authorities as well as upon the initiative of the Administration. Receives, performs data entry and searches of data and reports through the database. Performs analysis of received data upon the established procedures and criteria. Makes reports on performed analysis and forwards them to the competent state authorities for further action. Gives initiative for opening analysis if, based on the obtained data, evaluates that it is needed. Provides suggestions for forwarding data and information for which there is strong enough suspicion for undertaking further steps. Comunicates with the reporting entities regarding submitted reports. Archives and keeps gathered data and information. Participates in the preparation of the list of

			indicators for recognition of suspicious transactions and clients. Participates in the preparation of the opinion on upgrading system for prevention of money laundering and participates in the drafting of strategic analysis and plans. Participates in organizing trainings for the employees and compliance officers at the reporting entities. Performs other tasks upon the Superior's orders.
5-6.	**Independent Adviser III** **Analyst** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 1 year of working experience, passed professional exam and Computer literacy (word, excel, power point)	2	Performs tasks related to proccesing, analysis, record keeping and additional data received by the reporting entities in relation to the cases opened upon the request of competent state authorities as well as upon the initiative of the Administration. Receives, performs data entry and searches of data and reports through the database. Performs analysis of received data upon the established procedures and criteria. Makes reports on performed analysis and forwards them to the competent state authorities for further action. Gives initiative for opening analysis if, based on the obtained data, evaluates that it is needed. Provides suggestions for forwarding data and information for which there is strong enough suspicion for undertaking further steps. Comunicates with the reporting entities regarding submitted reports. Archives and keeps gathered data and information. Participates in the preparation of the list of indicators for recognition of suspicious transactions and clients. Performs other tasks upon the Superior's orders.

7.	**Adviser I** **Analyst** **For other reporting entities** - Higher education in *the scope of 180* credits of MCTS (VI qualification level of education), School of Economics, Law School or Social Science School, at least 3 year of working experience, passed professional exam and Computer literacy (word, excel, power point)	1	Performs analytical work regarding primary processing, analysis and record keeping of the data received by the other reporting entities and collection of additional data. Performs entering of the received data into the database and analysis them. Makes reports on performed analysis and forwards it to the competent authorities(upon the assessment and approval of superiors). Archives and keeps received data. Performs other tasks upon the Superior's orders.
	1.2. SUSPICIOUS TRANSACTION DEPARTMENT		
8.	**Head of the department** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics or Law School, at least 3 years of working experience in management, passed professional exam, knowledge of English language – level B1, Computer literacy (word, excel, power point)	1	Coordinates, manages, controls the work of the employees in the Department and performs the most complex tasks within the scope of the Department. Organizes the execution of tasks related to: analysis and processing data on received suspicious transactions as well as acting upon the requests of other state authorities. Proposes sending acts related to those cases. Participates in organizing of trainings for employees and compliance officers at reporting entities. Participates in the preparation and innovation of the list of indicators. Proposes procedures and criteria for the execution of tasks within the Department's competence and develops policies, procedures and practices for

			identifying suspicious transactions. Provides suggestions for the improvement of the working process in the Department. Prepares the analysis of the situation from the area of money laundering and terrorist financing. Provides suggestions for establishing guidelines for drafting risk analysis. Drafts statistical reports and keeps records. Performs other tasks upon the Superior's orders.
9-10.	**Independent Adviser I** **Analyst** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 5 years of working experience, passed professional exam and Computer literacy (word, excel, power point)	2	Performs tasks related to proccesing, analysis, record keeping and additional data received by the reporting entities in relation to the cases opened upon the request of competent state authorities, upon the initiative of the reporting entities as well as upon the initiative of the Administration. Performs data entry and searches of data and reports through the database. Performs analysis of received data upon the established procedures and criteria, makes reports on performed analysis. Provides suggestions for: forwarding data and information for which there is strong enough suspicion for undertaking further steps or for feedback information in the absence of sufficient grounds for processing. Proposes a measure of temporary blockage of funds. Comunicates with the reporting entities regarding submitted reports. Archives and keeps gathered data and information. Participates in the preparation of the list of indicators for recognition of suspicious transactions and clients. Prepares opinion on upgrading system for prevention of money laundering and participates in the drafting of strategic analysis and plans. Participates in organizing trainings for the employees and compliance officers at the reporting entities. Performs other tasks upon the Superior's orders.

11-12.	**Independent Adviser III** **Analyst** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 1 year of working experience, passed professional exam and Computer literacy (word, excel, power point)	2	Performs tasks related to proccesing, analysis, record keeping and additional data received by the reporting entities in relation to the cases opened upon the request of competent state authorities, upon the initiative of the reporting entities as well as upon the initiative of the Administration. Performs data entry and searches of data and reports through the database. Performs analysis of received data upon the established procedures and criteria, makes reports on performed analysis. Provides suggestions for: forwarding data and information for which there is strong enough suspicion for undertaking further steps or for feedback information in the absence of sufficient grounds for processing. Comunicates with the reporting entities regarding submitted reports. Archives and keeps gathered data and information. Participates in the preparation of the list of indicators for recognition of suspicious transactions and clients. Participates in organizing trainings for the employees and compliance officers at the reporting entities. Performs other tasks upon the Superior's orders.
	1.3. REPORTING ENTITIES CONTROL DEPARTMENT		

13.	**Chief inspector** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 5 years of working experience at inspection works, passed professional exam and Computer literacy (word, excel, power point)	1	Coordinates the work of the employees in the Department and performs the most complex tasks within the scope of the Department related to: performance of direct supervision and control of the reporting entities and taking administrative measures and actions, processing and analysing additional data from the reporting entities based on which, the action of reporting entities in the implementation of the Law is determined, submitting requests for initiation of misdemeanor procedures, sumission of information and reports and data record keeping. Performs inspection trainings, processes the documentation material from this area, taken by the reporting entity; participates in planning of the supervision. Participates in organizing trainings for the employees and compliance officers at the reporting entities. Participates in preparation of list of indicators. Performs other tasks upon the Superior's orders

14-16.	**Inspector I** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 5 years of working experience, passed professional exam and Computer literacy (word, excel, power point)	3	Performs tasks related to: direct supervision and taking administrative measures and actions; gathering of additional data from the reporting entities based on which, the action of reporting entities in the implementation of the Law, other regulations and general acts are determined, submitting requests for initiation of misdemeanor procedures against the reporting entitites and compliance officers at the reporting entities, keeping records on performed inspections and measures taken; preparation of information, reports and analysis on performed controls and other tasks upon the Superior's orders.
17.	**Inspector II** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 3 years of working experience, passed professional exam and Computer literacy (word, excel, power point)	1	Performs tasks related to: direct supervision and taking administrative measures and actions; gathering of additional data from the reporting entities based on which, the action of reporting entities in the implementation of the Law, other regulations and general acts are determined, submitting requests for initiation of misdemeanor procedures against the reporting entitites and compliance officers at the reporting entities, keeping records on performed inspections and measures taken; reports performed controls and statistics reports in relation to inspection supervision as well as other tasks upon the Superior's orders.
2. SECTOR FOR NATIONAL AND INTERNATIONAL COOPERATION			
18.		1	Performs tasks related to: steering the work of the Sector and of employees in the Sector for

	Assistant to the Director - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 3 years of working experience in management, or other relevant jobs that require autonomy in their work, passed professional exam, knowledge of English language – level B2		National and International Cooperation, coordinating the work of the employees in the Sector and performs other tasks by Director's orders.
19.	**Independent Adviser I** **Adviser for national and international cooperation** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 5 years of working experience, passed professional exam, knowledge of English language – level C2 and Computer literacy (word, excel, power point)	1	Performs tasks related to: data exchange with competent state authorities, othorities of other states and international organizations, establishing cooperation with competent state authoritie, foreign FIUs and international organizations; preparing data delivery requests for mentioned authorities and correspondence with the competent authorities of other countries; participation in preparation of proposals to amend the regulations which are adopted based on the Law on Prevention of Money Laundering and Terrorist Financing. Recording and keeping received data and other tasks upon the upon the Superior's orders.

20.	**Independent Adviser I for prevention of terrorist financing** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, Law School or Social Science School, at least 5 years of working experience, knowledge of English language – level C2 and Computer literacy (word, excel, power point)	1	Performs tasks related to: establishing cooperation with foreign FIUs and international organizations in relation to prevention of terrorist financing (TF), provides suggestions on cases related to TF which should be forwarded to Analitytics Department, participation in preparation of proposals to amend the regulations which are adopted based on the Law on Prevention of Money Laundering and Terrorist Financing; participates in creating and implementing measures from the action plans concerning the prevention of TF; proposes TF typology based on the practise and makes reports containing measures to improve the current situation, follows the recommendations and guidelines in the area of TF; creates web site related to the area of terrorist financing and updates data. Performs other tasks upon the upon the Superior's orders.
21.	**Independent Adviser III** **Translater for English language** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, Social Science School – english language, at least 1 year of working experience, passed	1	Performs tasks related to: translation of relevant EU regulations with which it is necessary to harmonize national legislation in the area of prevention of money laundering and terrorist financing, translating reports of relevant international organizations and translating other acts for the needs of the Administration and other tasks upon the upon the Superior's orders.

	professional exam and Computer literacy (word, excel, power point)		
<u>3.SECTOR FOR PREVENTION, INTEGRATION AND INFORMATION</u>			
22.	**Assistant to the Director** - Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School at least 3 years of working experience in management, or other relevant jobs that require autonomy in their work, passed professional exam, knowledge of English language – level B1	1	Performs tasks related to: steering the work of the Sector and of employees in the Sector for Prevention, Integration and Information, coordinating the work of the employees in the Sector and performs other tasks by Director's orders.
23.	**Independent Adviser I** **-** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of	1	Performs tasks related to: preparation and participation in the implementation of training for compliance officers; drafting proposals for submission of misdemeanour charges based on the submission of records by other supervisory authorities;

	Economics, Law School or Social Science School, at least 5 years of working experience, passed professional exam, knowledge of English language – level B2 and Computer literacy (word, excel, power point)		analysis of international standards and monitoring the degree of harmonization of international regulations in the AML/CFT area with the regulations (EU, EGMONT, FATF) from the AML/CFT area; participates in the implementation of projects financed by the EU funds or other international organizations and performs other tasks by Superior's orders.
24.	**Independent Adviser I for prevention** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 5 years of working experience, passed professional exam, knowledge of English language – level C1 and Computer literacy (word, excel, power point)	1	Performs tasks related to: Performs tasks related to: participation in the preparation and organization of trainings of compliance officers of reporting entities and emplyees that have direct contact with the client, drafting proposals for submission of misdemeanour charges based on the submission of records by other supervisory authorities; monitoring and analysis of the degree of harmonization of the Law on Prevention of Money Laundering and Terrorist Financing and regulations adopted pursuant this law with relevant EU regulations in the area of prevention of money laundering and terrorist financing, monitoring and analysis of international organizations' published reports regarding the prevention of money laundering and terrorist financing and performs other tasks upon Superior's orders.
25.	**Independent Adviser III for integration** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, Law School or Social Science School, at least 1 year of working experience, passed	1	Performs tasks related to: preparation of reports on the fulfilment of obligations under the competence of the Administration in the process of European and Euro-Atlantic Integration; reports in relation to implementation of national strategic documents (Strategies and Action Plans); monitoring published statements related to the activities of the Administration, preparing texts and statements in order to inform the public on the work of the Administration, deciding on requests for free access to information and other tasks upon the Superior's orders.

	professional exam, knowledge of English language – level B1 and Computer literacy (word, excel, power point)		
***4.* UNIT FOR GENERAL AFFAIRS, FINANCE AND INFORMATION TECHNOLOGIES**			
26.	**Head of the Unit** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, Law School, at least 3 years of working experience in management, passed professional exam and Computer literacy (word, excel, power point)	1	Coordinates the work of the employees and performs the most complex tasks related to: drafting general acts of the APMLTF, preparing individual acts related the exercise of labour rights, the preparation of materials in order to report the Government of Montenegro on the work of the Administration in accordance to the Law, preparing summary statistics reports on the work of the Administration and keeping unique records on money laundering and terrorist financing, providing technical and other working conditions for all employees in the Administration, in cooperation with the Independent Adviser for IT performs activities related to the planning of information system and hardware - software structure, project management and coordinating activities in the IT area and other tasks upon the Director's orders
4.1. GENERAL AFFAIRS AND FINANCE OFFICE			

27.	**Independent Adviser I for finance, accounting and public procurement** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of Economics, at least 5 years of working experience, passed professional exam and Computer literacy (word, excel)	1	Performs tasks: verifying the accuracy and validity of requests for paying with the state's money, processing requests for budgetary expenditures and payments relating to the APMLTF; preparation of financial plan – budget and report on the execution of the financial plan, preparing quarterly and semi-annual reports, as well as balance sheet of the Administration's budget, adjustment of accounting and the actual condition of the assets and liabilities, preparation of documents for payment of salaries, withdrawals and cash payments; tasks of the officer for the public procurement, storage and archiving of accounting records and documentation related to public procurement and other tasks upon the Superior's orders.
28.	**Independent Adviser III** **For personnel issues** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, Law School, at least 1 year of working experience, passed professional exam and Computer literacy (word)	1	Performs tasks related to: preparation and submission of periodic reports on the work of the Administration, preparation of general acts of the Administration; personal record keeping, enters data in the Central Personnel Registry, preparation of individual acts on impelentation of labour rights. Participates in preparation of the Law and bylaws regarding prevention of money laundering and terrorist financing. Performs tasks related to: integrity plan, implementation of measures in order to prevent and possibly report mobbing, keeping records of gifts, cooperation with non-governmental sector and other tasks upon the Superior's orders.

29.	**Administrative Assistant** **Record keeper** - Secundary education in *the scope of 240* credits of MCTS, IV qualification level of education, at least 1 year of working experience, passed professional exam and Computer literacy (word, internet)	1	Perform tasks of the record keeper related to receiving mail, stamping received mail, registering acts, keeping registar, distributing documents via internal delivery books, sending mail, deregistering acts; storing of archived cases, keeping archive books; handling and keeping seals and stamps, copying and delivering material and other tasks upon the Superior's orders.

30.	**Independent Administrative Assistant** **Secretary** - Secundary education in *the scope of 240* credits of MCTS, IV qualification level of education, at least 3 year of working experience, passed professional exam and Computer literacy (word, internet)	1	Performs tasks releted to technical preparation (complets, delivers, stors and keeps) of materials for the purpose of holding meetings attended by the Director; mediation in conducting telephone conversations and reception of visitors at Director's office; keeping planner of obligations and conducting Director's meetings; typing tasks for the Director as well as other tasks upon the Superior's orders.
31.	**Independent Administrative Assistant** **Archivist** - Secundary education in *the scope of 240* credits of MCTS, IV qualification level of education, at least 3 year of working experience, passed professional exam and Computer literacy (word, internet)	1	Perform tasks of the archivist related to archiving cases; storing of archived cases, keeping registration book, arranging archive material, technical preparation of reports and required attachments within the Unit, keeps records, takes care of the consumption and obtaining the necessary administrative and other material as well as other tasks upon the Superior's orders.
32.	**Senior Public employee** **Driver** Secundary education in *the scope of 240* credits of MCTS, IV qualification level of	1	Performs tasks of driving and taking care of the maintenance of official vehicles and performs other tasks upon the Superior's orders.

	education, at least 1 year of working experience, passed professional exam and and driving license (category B)		
33.	**Senior Public employee** **Courier-deliverer** Secundary education in *the scope of 240* credits of MCTS, IV qualification level of education, at least 1 year of working experience, passed professional exam and and driving license (category B)	1	Performs tasks related to: delivery of mail and other documents. Performs other tasks tasks upon the Superior's orders.
4.3. INFORMATION TECHNOLOGIES OFFICE			

34.	**Independent Adviser I for IT** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of natural science and mathematics or School of electrical engeenering, at least 5 years of working experience, passed professional exam, knowlegde of English language – level B1	1	Performs tasks related to: planning of information system and hardware-software structure, managing projects, gathering and coordinating the implementation of the users' requirements. Gives professional opinion on the upgrading information system, participates in creation and drafting of statistical reports and performs other tasks upon the Superior's orders.
35.	**Independent Adviser III** **Programmer** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of natural science and mathematics or School of electrical engeenering, at least 1 year of working experience, passed professional exam	1	Performs tasks related to: development of information system of the Administration, creation of database, creation of aplication for database management, training of other employees od the Administration, participates in the creation of statistical reports and performs other tasks upon the Superior's orders.

36.	**Independent Adviser III** **System administrator** Higher education in *the scope of 240* credits of MCTS, VII 1 qualification level of education, School of natural science and mathematics or School of electrical engeenering, at least 1 year of working experience, passed professional exam	1	Performs tasks related to: control of the functioning of the equipment and maintenance of the equipment in the network, maintenance of database, import of data, maintenance and control of the functioning of software on the computers and performs other tasks upon the Superior's orders.
37-38.	**Administrative Assistant** **Operator** - Secundary education in *the scope of 240* credits of MCTS, IV qualification level of education, at least 1 year of working experience, passed professional exam and Computer literacy (word, excel)	2	Performs tasks related to: import of data received in paper form by the reporting entities and other competent authorities, monitoring receipt and import in the database of electronic letters and regular reports by the reporting entities, performing primary analysis of certain data, conduct relevant statistics, archiving documents of the IT office, testing and listing errors of the software solutions as well as other tasks upon the Superior's orders.

Article 8

In the Administration for Prevention of Money Laundering and Terrorist Financing, for the purpose of training, one or more trainees with higher or secondary professional education can be employed.

III TRANSITIONAL AND FINAL PROVISIONS

Article 9

Arrangement of employees of the Administration for Prevention of Money Laundering and Terrorist Financing, pursuant to this Rulebook, shall be carried out within 30 days from the date of entry into force of this Rulebook.

Article 10

With the entry into force of this of this Rulebook, the Rulebook on internal organization and systematization of the Administration for Prevention of Money Laundering and Terrorist Financing No. 0601-455/8-10 from 17/02/2011 and 0601-455/11-12 from 23.03.2012 ceases to be valid.

Article 11

This Rulebook shall enter into force on the eighth day of the date of publication on the notice board of the Administration for Prevention of Money Laundering and Terrorist Financing, after its adoption by the Government of Montenegro.

Number: 0601-171/5-13 **DIRECTOR**

Podgorica, 28/06/2013 **Vesko Lekić**

E X P L A N A T I O N

The Administration for Prevention of Money Laundering (hereinafter referred to as the Administration) was formed by the Decree of the Government of the Republic of Montenegro on 15/12/2003 (Official Gazette of the Republic of Montenegro No. 67/03).

The Administration for Prevention of Money Laundering and Terrorist Financing was founded with the Decree on the organization and working method of the state administration (Official Gazette of Montenegro No. 5/12), as an independent authority of the Administration and performs tasks as stipulated by the Law on Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro No. 14/07 from 21.12.2007, No. 04/08 from 17.01.2008 and 14/12 from 07.03.2012), which are related to gathering, analysing and delivering to the competent authorities, data, information and documentation necessary for detection of money laundering and terrorist financing, creating standards and methodologies for establishing and developing policy, procedures and practices for recognising suspicious transactions; developing special programs for prevention of money laundering and terrorist financing, with procedures and programs of inspection and training employees for recognizing suspicious transactions; verification of transactions and persons in relation to for which there is suspicion in money laundering or terrorist financing; temporarily suspension of transactions, initiating amendments and changes of regulations referring to or related prevention and detection of money laundering and financing terrorism; establishing international cooperation with authorized representatives of other countries and international organizations; participation in the drafting and consolidating the list of indicators for recognizing of suspicious transactions; participation in training of employees and authorized representatives of the competent state authorities, drafting risk analysis guidelines; publishing statistical data in the area of prevention and detection of money laundering and terrorist financing; supervision over the implementation of the Law on PMLTF within defined competences of APMLTF; as well as other activities that are within APMLTF authority.

The new Law on civil servants and state employees (OGM no. 66/12 from 31 December 2012) prescribed the necessity of making changes and amending the current Rulebook on internal organisation and systematisation of the APMLTF. In accordance with the mentioned, this rulebook on internal organisation and systematization shall define conditions for work positions of civil servants and administrative assistants within APMLTF.

The suggested Rulebook is harmonized with the new Law on civil servants and state employees (OGM No. 39/11 from 4 August 2011, 50/11 from 21 October 2011, 66/12 from 31 December 2012).

The suggested changes of the Rulebook on internal organisation and systematisation of the APMLTF are drafted based on new working requirements that resulted from increasing scope of work requirements and APMLTF competences.

The new Rulebook prescribes founding of three Sectors, within which tasks are performed from the core business of the authority, as well as one Unit, as an organizational unit for performing work within Administration's competences. Within the Sector for Analytical Affairs and Reporting Entities Control, Departments are established where the individual functions of the authority are carried out.

Change that is proposed is switching Reporting Entities Control Department from the National and International Cooperation and Supervision Sector into a new Sector for Analytical Affairs and Reporting Entities Control, instead of IT Department that is switched from this new Sector into Unit for General Affairs, Finance and Information Technologies. Thus, the former Department for National and International Cooperation is transformed into Sector for National and International Cooperation.

In the Sector for Analytical Affairs and Reporting Entities Control there are Analytics Department, Suspicious Transactions Department and Reporting Entities Department. In this way it is intended to provide higher correlation between the complementary tasks, as well as faster and closer cooperation, exchange and binding data and information between the Departments that work on similar i.e. related tasks.

It was mentioned that IT Department (information technologies) is eliminated as a separate Department and with the proposed solution the working positions are transferred in the special Office within Unit for General Affairs, Finance and Information Technologies in order for tasks of administrative - technical nature to be grouped and linked into a single unit.

In this manner, the functional grouping of tasks was ensured in order to achieve cost-effective and efficient performance of duties or implement the functions of the Administration. The aim is to link tasks by type, complexity, nature and mutual connenction.

With the proposed Rulebook, the internal organizational structure of the Administration for the Prevention of Money Laundering and Terrorist Financing is changed, but the existing number of the work positions is kept.

In accordance with titles, special conditions in accordance with the legislation were determined with the Rulebook.

Probation work, as a special condition, is provided for the work for which it is estimated that this condition is necessary, considering the nature and type of work and specific training or skills that civil servant or public employee should have, and which should to be determined in the probation work.

It is provided that one or more trainees with higher or secondary professional education can be employed for training in the Administration.

Provided systematization is in function of implementing basic principles and obligations of the authority and provides primarily lawful and proper work, effectiveness and cost-effectiveness of acting, public and transparent work; effective control and responsibility for the work and acting; simple work procedures, and optimal use of human, financial, material, technical and other authority's resources. Mentioned systematization enables coverage of all types of work to be performed in the Administration for Money Lanudering and Terrorist Financing according to the Law.

On the basis of Article 33 paragraph 5 of the Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro, no. 14/07), the Ministry of Finance has adopted

RULEBOOK

ON THE MANNER OF REPORTING CASH TRANSACTIONS EXCEEDING €15,000 Or MORE AND SUSPICIOUS TRANSACTIONS

TO THE ADMINISTRATION FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

I GENERAL PROVISIONS

Article 1

(1) The reporting entities from Article 4 paragraph 2 of the Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro, no. 14/07, hereinafter: the Law) shall deliver to the Administration for the Prevention of Money Laundering and Terrorist Financing (hereinafter: the Administration) data on any cash transaction in the amount of €15.000 or more and on any suspicious transaction regardless of the amount and type.

(2) Lawyers, law offices and law partnership companies, notaries, stock exchanges and clearing and depository houses shall deliver to the Administration data on any suspicious transaction regardless of the amount and type.

(3) The administration body responsible for customs affairs shall provide data to the Administration on any transport across the state border of money, checks, bearer securities, precious metals and precious stones whose value or amount is €10.000 or more, as well as on any transport or attempt of transport of money, checks, bearer securities, precious metals and precious stones whose value or amount is less than €10.000 when there are reasons for suspicion of money laundering or terrorist financing related to that person.

(4) Report from paragraph 1 of this Article shall contain data on any executed cash transaction in the amount of €15.000 or more and any suspicious transaction regardless of the amount and type.

(5) Report on a suspicious transaction shall be delivered prior to the execution of the transaction, i.e. when a customer gives to a reporting entity an order for carrying out a transaction.

(6) Data from paragraphs 1, 2 and 3 of this Article shall be forwarded using the Reporting Forms printed together with the present Rulebook and shall become attachment thereto. The Forms are as follows:

Reporting Form 01 for BANKS;

Reporting Form 02 for STOCK EXCHANGES;

Reporting Form 03 for BROKERS & FUNDS;

Reporting Form 04 for CENTRAL DEPOSITARY AGENCY (CDA);

Reporting Form 05 for MERCHANTS AND INTERMEDIARIES;

Reporting Form 06 for CUSTOMS;

Reporting Form 07 for INSURANCE COMPANIES and

Reporting Form 08 for OTHER REPORTING ENTITIES.

II THE MANNER OF REPORTING

Article 2

Data from Article 1 paragraph 1 of this Rulebook shall be forwarded in the following manner:

1) by registered mail;

2) by personal delivery or courier;

3) by CD ROM and

4) by secure electronic mail in a format previously prescribed and approved by the Administration.

III ELECTRONIC REPORTING

Article 3

(1) For delivering data via secure electronic mail a reporting entity shall fill in a User Account Form in order to meet the conditions for reporting under the user account of the compliance officer and his/her deputy and deliver it to the Administration together with the request/application.

(2) On the basis of the request from paragraph 1 of this Article the Administration shall open and assign user orders to the compliance officer and his/her deputy.

Article 4

(1) The compliance officer and his/her deputy shall upon the call from the Administration take the user order personally signing the statement of taking the user order.

(2) The compliance officer and his/her deputy shall keep the data from the user order in strict secrecy.

(3) The compliance officer and his/her deputy shall apply and obey the provisions from the statement of taking the user order.

Article 5

(1) In case a compliance officer or his/her deputy is replaced, reporting entity shall immediately inform the Administration on that replacement and undertake activities and measures in order to prevent sending data to the Administration under his/her identification, that is ask for revocation of the user order.

(2) In case the confidentiality of user order data has been disrupted a reporting entity, or a compliance officer or his/her deputy shall inform the Administrattion immediately, ask for revocation of the user order and opening of a new user order.

IV TRANSITIONAL AND CLOSING PROVISIONS

Article 6

The Rulebook on the manner of reporting transactions exceeding €15,000 and suspicious transactions to the Administration for the Prevention of Money Laundering (''Official Gazette of the Republic of Montenegro'', no.55/05) shall cease to be applicable on the day of entering into force of this Rulebook.

Article 7

This Rulebook shall enter into force on the eighth day after the day of its publishing in the ''Official Gazette of the Republic of Montenegro''.

No:

Podgorica, 16th December 2008

MINISTER OF FINANCE

dr Igor Lukšić

GUIDELINES
ON BANK RISK ANALYSIS AIMED AT PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

Podgorica, 25.02.2010

Pursuant to Article 17 paragraph 1 of the Central Bank of Montenegro Law (OGM 52/00, 53/00, 47/01, 04/05), and with the meaning of Article 8 paragraph 3 of the Law on Prevention of Money Laundering and Terrorism Financing (OGM 14/07, 04/08) and Article 2 paragraph 1 of the Rulebook on the development of guidelines on risk analysis with a view to preventing money laundering and terrorism financing (OGM 20/09), the Council of the Central Bank of Montenegro, on its session held on 25. February 2010, issued

GUIDELINES
ON BANK RISK ANALYSIS AIMED AT PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

1. These guidelines shall determine in detail the criteria for issuing internal act of banks and branches of foreign banks (hereinafter referred to as: banks) on risk analysis aimed at preventing money laundering and terrorism financing.

2. Risk of money laundering and terrorism financing

The risk of money laundering and terrorism financing, with the meaning of Article 5 point 5 of the Law on the Prevention of Money Laundering and Terrorism Financing (hereinafter: the Law), is a risk that a client would use the financial system for money laundering or terrorism financing, i.e. that the business relationship, transaction or a product would be directly or indirectly used for money laundering or terrorism financing.

Money laundering, with the meaning of Article 2 of the Law, is considered especially:

1) exchange or other transfer of money or other property which originates form a crime;
2) obtaining, possession or use of money or other property which originates from a crime;
3) concealing a nature, place of deposit, movement, disposal, ownership or rights regarding money or other property which is the consequence of a crime.

Terrorism financing, with the meaning of Article 3 of the Law, is considered especially:

1) providing or gathering, or an attempt to provide or gather money or other property, directly or indirectly, with a goal or with a consciousness that it would be completely or partially used for implementation of a terrorist act or used by terrorist or a terrorist organization;
2) instigation or assistance in providing or gathering assets or property from item 1 of this Article.

3. Risk analysis of money laundering and terrorism financing

With the meaning of Article 8 paragraph 1 of the Law, a bank is obliged to create a risk based approach in order to determine the estimation of risk of a group of clients or a client, business relationship, transaction or a product, in order to prevent usage of its services or products for purpose of money laundering or terrorism financing.

In that sense, the bank is obliged to adopt an **internal act on risk based approach** and to apply the risk based approach.

3.1 Identification of the client

Before establishing the business relationship with its client, the bank is obliged to identify the client. With the meaning of Article 7 of the Law, the identification of the client is the procedure which includes:

1) establishing the identity of a client, or if the identification is previously done, to verify the identity based on reliable, independent and objective sources;

2) gathering information about the client, i.e. if the information are gathered, verifying gathered information based on reliable, independent and objective sources.

3.1.1 Identification and verification of a natural person or an entrepreneur

A bank shall, pursuant to Article 14 of the Law, establish and verify the identify of a client who is a natural person, i.e. its legal representative, entrepreneur, or natural person which performs the activities, by verifying the personal identification document of a client, while the client is present, and gathers the following data:

Client data – natural person	
Client data – natural person	• name; • address of temporary and permanent residence, • date and place of birth • tax file number (hereinafter TFN) of a natural person, i.e. its representative; • number, type and title of a state body which issued the document; • name, address of temporary and permanent residence, date and place of birth of the natural person, who has the access to the safe; • purpose and assumed nature of the business relationship, including the information on activities, i.e. the status of a client (employed, unemployed, student, retired, farmer, etc.); • data of establishing the business relationship, i.e. date and time when that person had access to the safe;
Client data – entrepreneur	• name; • address of temporary and permanent residence; • date and place of birth of the entrepreneur or a natural person who performs the activity, who establishes a business relationship or performs a transaction, i.e. a private person on their behalf the business relationship or transaction is performed, type and title of a state body which issued the document; • company, address and, if given, ID number of the entrepreneur or a natural person which performs the activity;
Data on transaction	• date and time of transaction; • the amount and currency of the transaction; • the purpose of the transaction and name and address of temporary and permanent residence, i.e. company and residence of a person for whom the transaction is intended for; • the manner how the transaction was made;

	• data on the source of the property and assets, which were or will be the subject of a business relationship or a transaction;
Data related to the person representing the client (legal representative or authorised person)	• name and family name, address of temporary and permanent residence, date and year of birth, TFN and number of a personal document and title of the state body which issued the personal document.

The identity of a client who is a natural person can be also established based on qualified electronic confirmation of a client, issued by a service provider of certification in accordance with the regulations on electronic signature and electronic business.

3.1.2 Establishing and verifying the identity of a client – legal person

With the meaning of Article 15 of the Law, the bank shall establish and verify the identity of a client who is a legal person, i.e. its legal representative, or authorised representative by inspecting the original or a certified copy of a personal document (that cannot be older than three months) from the Central Register of the Commercial Court (hereinafter: CRCC) or other suitable public register, which on behalf of the legal person is submitted by the legal representative.

The bank may also establish and verify the identity of the legal person and gather information referred to in Article 71 paragraph 1 of the Law by verifying the information with the CRCC or other suitable public register. With its regards, the bank shall state the date, time and name of the person who verified the information on the statement from the register. The statement from the register shall be filed in accordance with the provisions of the Law.

If the data required by the Law (Article 71 paragraphs 2, 7, 9, 10, 11, 12, 13 and 14) cannot be determined by inspecting the original or certified copies of personal documents, the missing data shall be gathered directly from the representative or the authorised person.

If the bank, during establishing and verifying the identity of a legal person, is suspicious about the validity of given data or validity of documents and other business documentation used for obtaining data, the bank is obliged to receive a written statement from the representative or authorised person before establishing the business relationship or the transaction.

If the client is a foreign legal person performing activities in Montenegro through a business office, the bank shall determine and verify the identity of a foreign legal person and its business office.

The information that the bank collects about a client who is a legal person, are given in the following table:

Client data – legal person	
Client data	• company; • address; • registered office and ID number of a legal person who establishes the business relationship or performs a transaction, i.e. legal person on whose behalf the business relationship is established or transaction is performed
Data related to establishing a business relationship	• date of establishing a business relationship or access to the safe; • the purpose and the assumed nature of the business relationship, including the information on client's activity.
Data related to performed transaction	• date and time of transaction; • the amount and the currency of the transaction; • the purpose of the transaction and name and temporary and permanent residence, i.e. company and residence of a person for whom the transaction is intended for; • the manner how the transaction was made; • data on the source of the property and assets.
Data related to the person represented by the client (legal representative or authorised person)	• name; • temporary and permanent residence; • date and place of birth and TFN of the representative or authorised person who, on behalf of another legal person or other person of a civil law concludes the business relationship or performs a transaction; • number and type of a personal document; • title of the state body that issued the personal document.
Data related to the beneficiary owner	• name; • temporary and permanent residence; • date and place of birth of the real client owner of the legal person, i.e. in the case of Article 19 paragraph 3 item 2 of the Law, data about the category of a person in whose interest is founding and activity of the legal person or similar legal subject of a foreign law.

When performing the transaction based on the established business relationship amounting to EUR 15,000 or more, the bank is obliged to confirm the identity of the natural person who performs the transaction on behalf of the legal person, for example to establish and confirm the identity of the legal representative or authorised person directly inspecting their private documents, during their presence.

If the transaction is performed by an authorised person, that person has to submit a verified written authorisation issued by the legal representative. The bank shall file the written authorisation issued by the legal representative or a client's authorised person.

If both the legal representative and authorised person are absent during the transaction (for example transactions through e-banking), the procedures that the bank requests during the use of a qualified digital certificate and a password to confirm the identity of the legal representative or authorised person during the process of transaction shall be applied.

3.1.3 Establishing the beneficiary owner of the legal person

As a part of establishing and confirming a client who is a legal person, the bank is obliged, besides the identification, to confirm the beneficiary owner of that legal person. With the purpose of gathering information, the bank shall implement the measures and operations to a person which is the beneficiary owner.

When it comes to the high-risk client, the bank must confirm the given data, if they were not received from the reliable and independent source (for example if the only source of data during establishing the identity of a client was a written statement of the legal representative, in that case the bank has to verify the data to the extent when it gains understanding about the ownership of the legal person and its control structure, in order to identify all beneficiary owners of the client.

The beneficiary owner of a company, i.e. a legal person in a sense of Article 19 of the Law is: (1) a natural person who, directly or indirectly, is the owner of more than 25% of the business share, the right to vote or other rights, based on which that person participates in management i.e. capital with more than 25% of share or has a prevailing influence in asset management of that company and

(2) a natural person who indirectly provides or is providing assets to the company and based on that has the right to significantly influence the decision making of the management bodies of the company during decision making on the financing and business.

According to the abovementioned definition, the beneficiary owner is a natural person which participates (directly or indirectly) in the management of a legal person, based on more than 25% of ownership share. During identification of the beneficiary owner, it is necessary to check the ownership share of a certain natural person in a legal person, as well as the ownership share of the legal person which is under control of that natural person.

The bank may receive information on ownership based on the original or a certified copy from the court register or other official register submitted by the legal representative or authorised person on behalf of the legal person. In addition, the bank may apply provisions of the Law which enable that the data regarding the beneficiary owner can be verified directly in the court register or other public register, or through other available sources.

If all the required data referring to the beneficiary owner (for example the date and place of birth) cannot be obtained from a court register or other official register, the bank may obtain the missing data from the legal representative or its authorised person.

A foreign owner is considered to be a company, legal person, as well as institution or other person of a foreign law, which is directly or indirectly the owner of at least EUR 500,000 of the business share of the stocks, i.e. share in the capital.

The beneficiary owner of the institution or another person of a foreign law (trust, fund or similar) who accepts, manages or shares property assets for certain purpose, with the meaning of this Law is considered to be:

(1) a natural person who, directly or indirectly, disposes with more than 25% of the property of the legal person or a similar subject of foreign law, (2) a natural person who is appointed or definable as the owner of more than 25% of income from the managed assets.

The bank has to verify the structure of the ownership for the clients – legal persons and gather all necessary data related to the beneficiary owner, in accordance with the Law.

If the legal person has the registered office in Montenegro, the bank is recommended to perform direct verification in the court register or other public register, in order to gather or confirm data referring to the beneficiary owner of that legal person.

If one of beneficiary owners is a foreign legal person, the bank is recommended to gather data related to the beneficiary owner of that legal person based on the original or a certified copy from the foreign register (that cannot be older than three months) or from the business documents submitted by the legal representative or the authorised person on behalf of the client. Since the bank has no information regarding the validity of documents from another country, it is recommended that the legal representative of the client or authorised person deliver an electronic statement from the public register from another country.

If, due to objective reasons, the legal representative is unable to present required documentations which clearly show the data related to the owner, those data shall be provided from the written statement delivered by the legal representative or its authorised person. In addition, the bank will also request a written statement from the legal representative in case of doubt in validity of submitted data.

If the legal representative shows unwillingness to cooperate with the bank in providing necessary data and for that reason the beneficiary ownership cannot be determined, the bank should not establish a business relationship. If the business relationship is established, in situation when a client avoids submitting all data required by the law, it is advised to the bank to use it as the indicator for revealing a suspicious activity of a client related to money laundering and terrorism financing.

If the bank, in addition to undertaken measures, is unable to receive data related to the beneficiary owner (besides the detailed analysis of the ownership structure), due to the complexity of the structure itself, in such cases the bank is allowed to establish (or continue) such business relationship, providing that the bank gathers written statement of the legal representatives or the authorised

person and classifies such client as a high-risk client, which needs enhanced due diligence of business activities. It should be mentioned that this is applied in exceptional cases, and is not usual practice.

In the case of following the procedure of establishing a legal person's beneficiary owner referred to above, the bank is obliged to prove to the authorised supervisory body that it has implemented in appropriate manner the procedure to establish the beneficiary owner, and it is the complex ownership case which justifies the bank's conduct. At the same time, the bank is advised to evaluate the complex ownership structure as a possible reason to report suspicious transactions.

Besides, banks should request from their clients written information on each change of beneficiary owners.

The internal acts of banks should define the procedure for determining the beneficiary owner, taking into account the provisions of the Law referred to above.

3.2 The manner of establishing the client's acceptability

By the means of the internal act, the bank is obliged to determine the conditions for the assessing the acceptability of a client on the basis of gathered and verified data and information on the client before establishing the business relation. This is the procedure that includes the identification of a client and the beneficiary owner, and if the client is a legal person, gathering information on the purpose and the nature of the business relation or transaction and other information with the meaning of Article 11 paragraph 1 of the Law.

Beside the abovementioned procedure, Article 11 paragraph 2 of the Law prescribes that a bank may exceptionally perform stipulated due diligence measures during the establishment of the business relation with the client, if it is necessary for the purpose of establishing the business relation and if there is insignificant risk of money laundering or terrorism financing.

When it identifies, i.e. gathers and verifies all data on a client stipulated by the Law, the bank establishes the business relation with the client.

By the means of the internal act, the bank shall also define reasons to reject entering into business relationship with the client, and especially if:

- the state of origin of the client or the client's beneficiary owner is on the list of non-cooperative countries, issued by the Financial Action Task Force (FATF), on the list of countries stated as "off-shore" zones or the list of countries considered by the supervisory body as countries exposed to risk;
- the client or client's beneficiary owner is a person from the country against which measures of the UN Security Council Resolutions have been undertaken;
- the client is a person form the List composed according to the UN Security Council Resolutions.

3.3. Risk assessment of individual client, group of clients and business relationship

The bank performs the risk assessment of an individual client or a group of clients on the basis of risk analysis approach. Before the creation of a client's risk assessment, the bank is obliged, in addition to the identification, the bank is obliged to conduct client due diligence the identification, within the meaning of Article 9 of the Law, and especially in the following **cases**: (1) when entering into business relationship with a client, (2) in the case of one or more related transactions amounting to EUR 15 000 or more, (3) when there is doubt into the accuracy and the authenticity of gathered data on a client's identification, (4) when there is a suspicion of money laundering or terrorism financing regarding a client or a transaction.

As a rule, the bank performs customer due diligence before establishing the business relationship or before performing the transaction and only exceptionally when establishing business relation, if there is insignificant risk of money laundering or terrorism financing.

In the case when the bank has established the business relation to the client and the client performs one or more related transactions amounting to EUR 15 000 or more, the bank shall collect only additional data (e.g. the purpose of transaction, data on source of assets, data on receiver of assets, and the like).

The measures the bank is obliged to perform in the customer due diligence procedure include:

- identification of a client or the beneficiary owner, if a client is a legal person;
- gathering and verification of data on client, i.e. the beneficiary owner, or if a client is a legal person gathering data on the purpose and the nature of the business relationship or transaction and
- after establishing the business relation, the bank shall regularly monitor business activities of the client and it shall verify the compliance of these activities with the nature of business relationship and the usual scope and the type of client' operations.

The table below shows the cases in which the bank is obliged to perform standard client due diligence, as well as the measures to be overtaken in order to perform client due diligence:

Cases in which the bank is obliged to perform standard client due diligence				
Measures to be overtaken by the bank in order to perform	(1) when establishing business relation	(2) when performing one or more connected transactions amounting to EUR 15.000 and above	(3) when there is doubt into the accuracy and the authenticity of gathered data on a client's identification	(4) when there is a suspicion of money laundering or terrorism financing regarding a client or a transaction
(a) identification of a client	Yes	Yes	Yes	Yes
(b) determining beneficiary owner	Yes	-	Yes (additional data)	Yes (additional data)

	(c) collecting required data	Yes	Yes	Yes	Yes
	(d) identification of a client when accessing the safe	Yes	-	Yes	Yes (when there is a suspicion of ML and TF regarding a client)
	(e) collection of additional data for the client which is a PEP	Yes	Yes	Yes	Yes

Since the bank may neither perform business relationship nor perform transactions if all measures prescribed within the standard client due diligence have not been performed, a client's business activities shall continue to be monitored as long as the business relationship lasts.

Besides the standard client due diligence, the bank shall dispose with special forms of client verification prescribed by the Law, including the: enhanced client verification and simplified client verification (described in Chapter 3.3.1).

After performing the verification of the client, the bank shall, on the basis of the risk factors, classify the client into a certain category of money laundering and terrorism financing risk. Taking into account the fact that the risk analysis of money laundering and terrorism financing requires proper information on the client and its operations, it is recommended that the classification of the client by risk categories is performed by the organizational unit which knows the client the best together with the compliance officer for the purpose of detecting and prevention of money laundering and terrorism financing.

Immediately after establishing business relationship, the bank shall determine the so-called initial risk profile of a client and it shall classify the client into the appropriate risk category.

Besides the classification of new clients and determining their risk profiles, the bank is obliged to also classify the existing clients.

During the duration of the business relationship with the client and monitoring its business activities, the bank is obliged to update all data and to classify the client into the appropriate category. This means, for example, if a bank determines that the some client's operations are significantly distracting his regular operations, the bank has to perform additional analysis of a client's operations, in order to determine the reasons for such distracting. On the basis of the additional analysis, compliance officer has to estimate the client's risk profile and if necessary, to reclassify it.

Banks are also recommended to establish procedures for regular update regarding the assessment of the risk profile of a client to which there are no significant violations of the normal operations. This may be done during the regular updating of documents and the data on the client.

By the means of the internal act, the bank shall determine the dynamics of risk assessment of clients depending on the client itself and its operations.

If a client, on the basis of risk factors, may be classified into different risk categories referring to money laundering and terrorism financing, the client shall be assigned only one risk profile presenting the highest risk.

3.3.1 Special types of client verification

The Article 24 of the Law stipulates the following special types of client verification:

- Enhanced client verification and
- Simplified client verification.

The bank is obliged, along with identification of a client, to undertake additional measures for client verification during:

- concluding an open account relationship with a bank or other similar credit institution, with a headquarters outside the EU or outside the countries from the List;
- concluding a business relationship or performing transactions from Article 9 paragraph 1 item 2 of this Law with a client, who is a politically exposed person as defined in Article 29 of this Law;
- verification of a client who is not present during identification and verification of the identity.

The bank is obliged to apply the measure or measures of enhanced client verification referred to in Article 26 (open account banking relationship with a credit organizations of a third country), Article 27 (politically exposed persons) and Article 28 (identifying a client in absence) of the Law, in the cases when it estimates that, due to the nature of the business relationship, form and manner of performing business transactions, business profile of a client, or other circumstances related to the client, there is or may occur a risk of money laundering or terrorism financing.

3.3.1.1 Enhanced client verification

a) Open accounts and banking relationships with banks from third countries

Relationship of an open account relation is a contract relationship between domestic and foreign credit organization, created by opening a bank account of a foreign credit organization with the domestic credit organization (for example, opening of loro account).

Article 26 of the Law prescribes that open account relationship with a bank with headquarters in third country presents an increased risk and therefore requires that bank performs additional verification and due diligence of the client, which is illustrated in table below:

Open account relationship with a bank with headquarters in a third country				
Case stipulated by the law ↓	1) Authorisation of compliance officer in the bank ↓	2) Receiving additional documentation and data ↓	3) Additional verification and client due diligence of business ↓	4) Additional measures ↓
Open account relationship with banks from third countries	Yes	Yes (data defined by Article 26 of the Law)	Yes	Upon bank's assessment

Bank employees in charge of concluding contracts on open accounts relationships with the bank or similar financial organization with headquarters in a country outside of EU or a country not listed at the list of countries who do not comply with standards in area of prevention of money laundering and terrorism financing, are obliged, before concluding the contract, to undertake the procedure of enhanced verification of the client and to provide written agreement of the complying officer in the bank.

The bank gathers the required data from public or other available records, i.e. by verifying the personal and business documents, delivered by the bank or other similar credit organization with the registered office outside of EU and outside countries on the list.

Data the bank is required to provide in the case of concluding an open account relationship with a bank from a country outside of EU or outside countries from the list include:

- date of issuance and duration of validity of licence for performing banking services, title and the registered office of the relevant state body that issued the licence;
- description of implemented internal procedures, related to exposure and prevention of money laundering and terrorism financing, and especially procedures of client verification, verification of the real owners, reporting data on suspicions transactions and clients to the relevant bodies, record keeping, internal control and other measures which the bank, or other similar credit organization, performed with regards to prevention and revealing of money laundering and terrorism financing;
- description of a system setting in area of revealing and prevention of money laundering and terrorism financing, applied in third country, where the bank or other similar credit organization has headquarters and is registered;

- written statement that the bank or other similar credit organization in country where it has headquarters, i.e. where it is registered is under legal supervision and that, in accordance with the laws of that country, it is obliged to apply adequate regulations in the area of revealing and prevention of money laundering and terrorism financing;
- written statement that the bank, or another similar credit organization, is not doing business as a “shell-bank”;
- written statement that the bank or another similar credit organization has no established relations and is not establishing business relationships and does not perform transactions with ”shell-banks”.

In the cases that the bank has concluded an open account relationship with a bank outside the EU or outside of the List of countries, before the Law came into force, the bank is obliged to request and gather all required data and information regarding the bank. If the bank does not receive all the requested data, it is recommended that the bank should discontinue such open account banking relationship.

b) Client as politically exposed person

1. The procedure to include persons on the list of politically exposed persons

Pursuant to Article 27 of the Law, a politically exposed person is a natural person which acts or has acted during previous year on a high public position in the state, including members of immediate family and close associates.

In order to determine politically exposed persons and members of immediate family and close associates with the meaning of the Law, the bank can act in one of the following ways:

- the client fills out the form (enclosed to these guidelines and representing its integral part, the form PEP);
- gathering information from public sources;
- gathering information based on accessing database including lists of politically exposed persons (*World Check PEP List*, inquiry through internet, etc.).

The procedure of establishing close associates of politically exposed persons is applied if the bank estimates that, based on documented facts, such relationship exists.

The bank is obliged to identify clients pursuant to the Law, and at the same time, in one of the manners described in paragraph **2** of this section, to determine whether a client is the politically exposed person.

Upon determining that the client is a politically exposed person, a bank employee is obliged to perform enhanced client verification (Article 25 of the Law) which includes additional measures in the cases of:

- concluding business relationship or performing transactions referred to in Article 9 paragraph 1 item 2 (performing one or more transactions amounting to EUR 15,000 or more);
- assessing that, due to nature of the business relationship and manner of performing the transaction, the business profile of a client, i.e. other circumstances related to the client, there is or there might be a risk of money laundering or terrorism financing.

In addition, as a part of enhanced client verification – politically exposed person, pursuant to the Law, a bank employee is obliged to:

- provide written consent of complying officer from the bank, before establishing business relationship with a client.
- provide data on source of property and assets which are the subject of a business relationship, i.e. transaction, from personal and other documents submitted by the client, and if it is not possible to acquire needed data from submitted documents, the data are provided directly from client's written statement;
- carefully follow transactions and other business activities performed at the bank by politically exposed person after establishing business relationship, especially bearing in mind the purpose and intention of transaction as well as the compliance with its usual business.

Additional measures implemented in procedure of a client extended verification				
Case prescribed by law ↓	1) Authorisation of the compliance officer in the bank ↓	2) Receiving additional documentation and data ↓	3) Additional verification and client due diligence of business ↓	4) Additional measures ↓
Politically exposed person	Yes	Data defined by Article 26 of the Law	Yes	Upon bank's assessmen t

The bank is obliged to establish a list of politically exposed persons, which will in an adequate manner be available to bank employees with direct contact with clients.

2. Procedure of cessation of obligation to treat a person as politically exposed person

The bank is obliged to establish the procedure of cessation of treating a client as politically exposed person with an internal act. That implies bank's obligation that after one year of cessation of acting as a politically exposed person on a prominent position within a county, that person, as well as members

of their immediate family and associates, should be excluded from the list of politically exposed person.

After establishing a business relationship with a politically exposed person, members of their immediate family and associates in accordance with the Law, the bank is obliged to keep special records about such persons and transactions.

The bank is obliged to update their list of politically exposed persons on regular basses, in order to implement the procedure of extended verification of a client pursuant to the Law and for those clients who at the time of starting a business relationship were not publically exposed persons with the meaning of the Law.

c) Establishing client's identity in absence

With the meaning of Article 28 of the Law regarding identifying and verification of client's identity in absence, the bank is obliged within enhanced client verification, along with identification referred to in Article 7, to undertake one or more additional measures, such as:

- provide additional documents, data or information, based on which the client's identity is verified;
- verify provided documents or provide a certificate from a foreign financial organization which performs payment services that the first payment of the client was made on the debt of the account held by that organization.

Additional documents, data or information based on which the clients' identification is verified may be as follows:

- for residents a prove on residence issued by the relevant state body which keeps record on residence;
- personal references (for example if it is possible to receive references from another bank's client);
- previous references from the bank related to the client;
- data on source of assets and property which are or will be the subject of a business relationship;
- certificate on employment of a public function performed by the client.

For natural persons, banks may additionally verify submitted documents in at least one of the following ways:

- confirming the date of birth by using official personal document (for example birth certificate, passport, or other public records);
- confirming the permanent address (for example by using an TFN, bank statement, or a letter issued by a public institution);
- contacting a client by phone, letter or electronic mail in order to confirm gathered information after the bank account was open (for example, non-operating phone line, returned letter of incorrect e-mail address should indicate that additional verification is needed).

For legal persons, banks may additionally verify submitted documents in at least one of the following ways:

- reviewing financial reports and other documents about business;
- reviewing public registers or other inquiries in order to establish that legal person is still in business, that is was not deleted from the register or is not in bankruptcy, or that it is not in process of ceasing the business, being deleted from the register or bankruptcy;
- independent verification of information, such as using public and private databases;
- contacting client via phone, mail or electronic mail.

3.3.1.2 Simplified verification of a client

As a part of a special verification of a client, a bank may during establishing business relationship or during performance of one or several connected transfers amounting to EUR 15,000 or more, apply simplified verification of clients with residence in EU or is on the list of countries issued by the Ministry of Finance of Montenegro.

With the meaning of Article 29 of the Law, low risk clients to whom the simplified client verification is implemented include:

- branch banks of foreign banks and other financial organizations, savings banks and savings-loan organizations, post offices, associations for management of investment funds and branch offices of foreign associations for management of investment funds, associations for management of retirement funds and branch offices of foreign associations for management of retirement funds, life insurance companies and branch offices of foreign life insurance companies which perform life insurance services, organizers of classic and special lottery games
- state body or body of local government and other legal persons performing public authority;
- company whose securities are included in trade on organized market in countries which are EU members or other countries which apply EU standards;
- clients referred to in Article 8 paragraph 4 of this Law, for which there is insignificant risk of money laundering and terrorism financing.

In case when the client has a insignificant risk of money laundering and terrorism financing, the bank shall, during simplified client verification, implement fewer measures for client due diligence. In accordance with that, bank is not obliged to verify the client, nor is it necessary to establish the beneficiary owner. The data the bank is obliged to gather in the procedure of simplified client verification are given in table below:

Simplified verification and client due diligence – data on client being a legal person	
Client data	• company, • legal person's registered office, i.e. on whose behalf and for whose account the business relationship is established.
Data on establishing business relationship	• date of establishing business relationship • purpose and nature of establishing business relationship
Data on performed transactions pursuant to Article 9 paragraph 1	• company and registered office of the legal person, on whose behalf and for whose account the transaction is made;

item 2 of the Law, i.e. on one or more connected transactions amounting to EUR 15,000 or more	• name of the representative or authorised person who on behalf of the legal person performs transaction; • date and time of transaction; • amount of transaction, currency and manner of transaction; • purpose of transaction and name and residence, i.e. company and residence of legal person for whom the transaction is intended for. We note that the bank gathers the abovementioned information by inspecting the original or certified copies of documents issued by the CRCC, delivered by the client, or by direct inquiry. If the listed data cannot be obtained, the missing data are taken from the original or certified copies of personal documents and other business documentation, submitted by the client or written statement of the representative or authorised person. Date of issuance of the documents must not be older than three months.
Data on a person representing the client (legal representative or authorised person).	Proscribed data for legal representative or authorised person, requested for those persons during regular verification of the client.

It should be noted that the performing of simplified client verification is allowed only for clients (legal persons) defined by Article 29 of the Law and who comply to its provisions, i.e. do not perform suspicious transactions, as well as that the bank cannot enlarge the number of clients to which the simplified client verification would be performed.
Besides the above mentioned legal requirements that the bank is obliged to perform during the simplified client verification procedure, the bank is recommended to:

- identify unusual and suspicious activities;
- deliver data and documents upon the request of authorised state body and
- implement certain measures regarding the specific case.

With its regards, it is recommended to the bank to also provide regular due diligence of business activities of those clients.
It is also recommended in such cases that the bank should create a risk profile of a client and follow activities on regular bases in accordance with the established risk profile of that client. Frequency and scope of bank's activities should be adjusted with the low level risk, bearing in mind client's category.

3.3.2 Risk factors determining the risk level of a client or group of clients and business relationship

Internationally accepted standards that serve as a basis of methodology for risk-based approach for prevention of money laundering and terrorism financing (e.g. FATF and Wolfsberg guidelines), include the following risk factors:

- **Client risk factor:** risk factors related to client's status or activities (for example state body, politically exposed person, client whose activities are related to cash transactions, non profit organizations, and the like)
- **Risk factors related to business relationship:** risk of business relationship, e.g. with a client whose country of origin does not follow standards in the prevention of money laundering and terrorism financing, politically exposed person and other business relationships which according to bank's estimation are of high risk.
- **Risk factors related to geographic region:** countries with inadequate systems for prevention of money laundering and terrorism financing, countries with high level of corruption or

criminal activities, countries against which were announced restrictive measures by international organizations;

Risk factors determining risk level of a certain client or groups of clients, business relationship and well as risk factors related to geographical region are illustrated in the following risk matrix. Albeit the factors presented in matrix, the bank may define additional factors related to specific nature of client's business activity.

<table>
<tr><th colspan="2">Client risk factor</th></tr>
<tr><td>K1</td><td><u>Insignificant risk</u>

The client to which the bank performs simplified verification in accordance with the Law, i.e. the client with headquarters in EU or belongs to the countries from the list established by the Ministry of Finance of Montenegro, is evaluated as a client with insignificant risk:
branch offices of foreign banks and other financial organizations, savings banks and savings-loan organizations, post offices, associations for management of investment funds and branch offices of foreign associations for management of investment funds, associations for management of retirement funds and branch offices of foreign associations for management of retirement funds, life insurance companies and branch offices of foreign life insurance companies which perform life insurance services, organizers of classic and special lottery games (obligors from Article 4 paragraph 2 items 1, 2, 3, 4, 5, 6, 8 and 9);
state body or a local government body and other legal persons performing public authority;
company which securities are included in trade on organized market in countries which are EU members or other countries which apply EU standards;
clients referred to in Article 8 paragraph 4 of the Law, for which there is slight risk for money laundering and terrorism financing.</td></tr>
<tr><td>K2</td><td><u>Low level risk</u>

The client is classified into this category based on verification directly after establishing business relationship and which satisfies all legally stipulated requests, a client to which the bank during due diligence procedure has not noticed violation of usual business activities, and to which the bank does not apply neither nor simplified verification in accordance with the Law.</td></tr>
<tr><td>K3</td><td><u>Middle level risk</u>

The client is classified into this category based on verification, due diligence and evaluation that the customer cannot be placed in category with insignificant risk, low risk or high risk level, and the bank has notices some deviations in regular business activities while performing due diligence.</td></tr>
<tr><td>K4</td><td><u>High risk</u></td></tr>
</table>

<table>
<tr><td></td><td>The bank performs extended verification in accordance with the Law towards that client, and a client where while performing due diligence of business activities the bank has noticed significant discrepancy from usual business activities, and especially:

• the client cannot prove the source of assets, or the source of assets is unknown or unclear;
• the client was not present during identification and verification of identity;
• there is a suspicion that the client acts upon instructions or order of a third person;
• there is unusual route of transaction, especially regarding the purpose, amount, mode of performance, purpose and similar;
• there are indications that client performs suspicious transactions;
• client is politically exposed person with the meaning of Article 2 of the Law, and bank performs extended verification referred to in Article 25 paragraph 1 item 2;
• the bank account of the client is connected with accounts of clients with higher risk;
• the client whose legal representative, authorised person or the real owner is a politically exposed person;
• the client is a foreign legal person who is forbidden to perform certain activities (for example trade, manufacturing or other activity) in country where it is registered or foreign legal person registered in a country where registration of off-shore companies is allowed;
• the client with complex legal layout or ownership structure where it is difficult to establish the real owner;
• client is a financial organization which does not request or is not obliged to receive authorisation from the relevant body to perform business activity or is not obliged to implement measures related to prevention of money laundering and terrorism financing in accordance with the legislation of the country of origin;
• client that bank has delivered reports on suspicions transaction to the relevant supervisory body within the last three years;
• the client for which the relevant supervisory body gave order about temporary cancelation of transaction or request for permanent due diligence;
• the client is a person listed on internal black list of the bank or the banking group.</td></tr>
<tr><td colspan="2"><u>High</u> risk factors in business relationship</td></tr>
<tr><td>BR</td><td>Business relationship with a client to which the bank implements enhanced verification measures pursuant to the Law include:

• business relationship with a bank from the third country;
• business relationship with politically exposed person.</td></tr>
<tr><td colspan="2"><u>High</u> risk factors related with geographic region[2]</td></tr>
<tr><td></td><td>High risk countries where client has residence i.e. permanent residence (natural persons) or headquarters for legal persons, includes the following countries :</td></tr>
<tr><td>G1</td><td>• countries with enforced sanctions, embargo or similar measures by United Nations;</td></tr>
</table>

G2	• countries for which the relevant international bodies or organizations have established a) the lack of adequate laws, regulations and other measures to prevent money laundering and terrorism financing; b) financing or supporting terrorism activities or that terrorist organizations are active in those countries; c) the significant level of corruption or other criminal activities;
G3	• countries which are not members of European Union or signatories of the Agreement on the European Economic Area nor they belong to the equivalent third countries;
G4	• which, according to the international organization FATF[3], belong to a non-cooperative countries or territories and in case of *off-shore* financial centre listed on the document prepared by the relevant body.

3.4 Risk factors related to products/transactions relate to: sensibility of the product or service regarding their misuse for purpose of money laundering or terrorism financing (for example electronic money transfer).

Risk factors related to products or transactions of high risk	
	Risk factors related to products or services of high risk are related to sensibility of the product or service regrinding their misuse for purpose of money laundering or terrorism financing, such as:
P/T 1	• international services of correspondent banks of third countries which include commercial payments;
P/T 2	• for persons who are not clients of the bank (for example if a person is using the service of a bank which acts as intermediary bank; • services which insure higher level of anonymity, such as electronic banking, international money transfer or similar. .
P/T 3	• cash transactions ; • occasional transactions which are not consistent with client's activities or with expected purpose of an account. .

3.5 Risk categories of clients

Classification of a client and groups of clients into certain risk category based on defined risk factors		
Category of risk	***Code of risk***	***Risk factor***
Insignificant risk	A	The bank classifies a client in category A if the bank applies simplified verification pursuant to the Law (K 1).
Low level risk	B	The bank classifies a client in category B, immediately after establishing a business relationship (to which a simplified verification pursuant to the Law is not applied, i.e. the client is not classified into category A) and a client to which while performing due diligence client's business activities the bank did not notice discrepancy from regular business activities (K2).
Middle level risk	C	The bank classifies a client in category C, where during due diligence the bank has noticed some discrepancies from regular business activities. (K3).
High level risk	D	The bank classifies a client in category D (K 4) : • the bank has noticed significant discrepancy from regular business activities; • to whom high risk factors are related with the geographic region (G1, G2, G3, G4); • client is related with high level risk factors regarding business relationships (BR); • client is related to high level risk factors regarding the product or service (P/T 1, P/T2 and P/T 3).

____

Note: With regards to the information on risk countries i.e. non-cooperative countries or territories which do not fulfil the key international standards related to money laundering or terrorism financing please refer to internet pages of relevant international bodies:
MONEYVAL:

www.coe.int/t/dghl/monitoring/moneyval and FATF: www.fatf-gafi.org

3.6 Monitoring client's accounts and transactions

A bank is obliged to continuously perform appropriate measures to detect unusual or suspicious activities based on the list of indicators for the identification of clients and transactions which reasonable grounds to suspect money laundering or terrorism financing. All clients must be included in this procedure, regardless of their risk profile.

A bank also has to establish appropriate procedures for due diligence of client's business activities, whereas the scope and implemented measures have to be consistent with the client's risk profile. The measures to be implemented by the bank to the client classified into appropriate risk category are given in the table below:

Measures to be taken by a bank with a view to monitoring clients classified into risk categories			
Risk category	***Code of risk category***	***Customer due diligence***	***Monitoring***
Insignificant risk	A	Simplified client due diligence	Annual
Low risk	B	Standard client due diligence	Semi-annual
Middle risk	C	Standard client due diligence, with additional necessary measures as assessed by the bank	Quarterly
High risk	D	Enhanced customer due diligence	Monthly

3.7 Risk management that the bank is exposed to in area of prevention of money laundering and terrorism financing

The bank is, pursuant to the Law, obliged to manage all risks it is exposed to in its activities, which includes risk management regarding money laundering and terrorism financing.

In this sense, the bank is obliged to establish a system for managing risk from money laundering and terrorism financing, which shall provide:

- identification of risks coming from the existing risks or those that may originate from new business products or bank activities;
- risk measurement by setting up mechanisms and procedures for accurate and due risk assessment;
- due diligence and risk analysis;
- control and minimising the risk.

The risk management system has to be appropriate to the size of the bank, complexity of offered products and services in its business activities.

The risk management system regarding money laundering and terrorism financing shall include at least:

- developed processes for risk management;
- clearly defined authorisation and responsibilities for risk management;
- efficient and reliable system of information technology;
- manner and dynamics of reporting and informing the Board of Directors and bank management on risk management.

For the purpose of adequate risk management in area of prevention of money laundering and terrorism financing, the bank is obliged to decrease exposure to risk which is outcome of new

technologies which enable anonymity (electronic or internet banking, electronic money, etc.), and in that sense the policies and procedures issued by the bank shall especially define:

- identification of a customer using electronic banking;
- validity of signed electronic document;
- reliable measures against forging documents and signatures on documents;
- systems which ensure and enable safe electronic banking;
- other conditions in accordance with positive regulations which regulate the above mentioned area of business activities.

Banks must have policies and procedures that shall require complete information on the purpose and the nature of the business relationship or regarding the transaction with absent clients and they are obliged to apply them while establishing the business relationship with the client or when performing the enhanced client verification.

For the purpose of secure identification of a client using electronic banking, the bank may use various methods of identifications, including PINs, passwords, smart cards, biometrics and qualified electronic certificates.

3.7.1. Measures for prevention of terrorism financing based on risk-based approach

Unlike money laundering, terrorism financing has different characteristics and therefore risk based approach regarding terrorism financing requires more complex set of factors for risk assessment as well as more complex methods in order to establish the existence of terrorism financing.

The nature of source of terrorism financing can be different depending on terrorist organizations, bearing in mind that assets used for financing terrorist activities can result from both legal and illegal sources. When the sources of financing terrorist activities are resulting from criminal activities, the approach based on risk assessment of money laundering is applicable to terrorism financing as well. Bearing in mind that the transactions referring to terrorism financing are usually implemented in small amounts, those transactions, regarding their amount through application of risk-based approach on money laundering, are considered as low risk transactions, and therefore it is complicated to identify terrorism financing.

In the cases when sources of financing terrorist activities result from legal sources, it is even more difficult to identify that legally acquired assets are used for terrorist purposes. With its regards, some activities for preparation of terrorist activities can be unhidden, such as the procurement of necessary material or payment of certain services.

The problems of identifying terrorism financing are complex, therefore various institutions and state bodies are dealing with the problem, while the obligation of the bank particularly regarding the reporting to the Administration for Prevention of Money Laundering and Terrorism Financing about suspicious transactions which could be related to terrorism financing. With its regards, it is very important that the banks supervise cash transactions and transactions with countries for which relevant international organizations or bodies have determined to finance or assist terrorist activities.

3.8 Professional training and improvement of bank employees

The important element of the efficient system for prevention of money laundering and terrorism financing is adequate and timely training and development of professional skills of employees performing tasks of identifying and preventing money laundering and terrorism financing.

Professional training of employees referring to prevention of money laundering and terrorism financing measures must include good knowledge of regulatory requests and internal politics and procedures adopted by the bank in order to successfully manage risks in this area.

All employees, whose tasks are anyhow related to the implementation of measures related to prevention of money laundering and terrorism financing, have to be included in the professional training program.

Training needs have to be adjusted to the special needs of employees according to individual lines of work, i.e. according to the specific tasks they perform. In that sense, the techniques in identifying and prevention of money laundering has to be presented to employees working as bank tellers and to employees working in other sectors involved in the programme of identifying and prevention of money laundering and terrorism financing.

Special attention should be paid on newly hired employees, who need to be informed about the basic measures undertaken in the bank regarding identification and prevention of money laundering and terrorism financing.

In addition, it is very important to educate compliance officers and their deputies in order to enable them to recognise new forms, techniques and trends related to money laundering and terrorism financing. It implies their information and update to legal and regulatory changes in order to adjust internal acts with new regulations timely.

The management of the bank has to be informed with the risk that the bank may face due to lack of compliance with regulations in the money laundering and terrorism financing area, as well as due to inadequate training of employees who are, as part of their duties, obliged to implement measures on the prevention of money laundering and terrorism financing.

The bank has to keep adequate records on completed education, especially with regards to persons included in education, date of seminars, courses, workshops, etc.

Professional training and improvement of bank employees related to prevention of money laundering and terrorism financing has a goal to raise awareness of the employees about the importance of timely undertaken measures for prevention of money laundering and terrorism financing.

4. Banks shall harmonize their internal acts to these Guidelines as well as perform other activities necessary for applying these Guidelines within 60 days of their publishing.

5. These Guidelines shall come into force on the day following their publishing at the website of the Central Bank of Montenegro.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

No.:0101- 258/2-8 President of the Council

Podgorica, 25.02.2010 Ljubiša Krgović

FORM FOR IDENTIFICATION OF A POLITICALLY EXPOSED PERSON
Form: PEP

With the meaning of Article 27 of the Law on Prevention of Money Laundering and Terrorism Financing (hereinafter: the Law), OGM 14/07 and 4/08), a bank shall determine whether the client is a politically exposed person.

FORM FOR IDENTIFICATION OF A POLITICALLY EXPOSED PERSON

Politically exposed person, with the meaning of the Law, is a natural person that is acting or has been acting in the last year on a distinguished public position in a state, including his/her immediate family members and close associates.
Members of a politically exposed person's immediate family are a marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters.
A close associate of a politically exposed person is a natural person that has a common profit from the asset or established business relationship or other type of close business contacts.

Pursuant to the Law, please answer the following questions:

Table 1

Are you a natural person that is acting or has been acting in the last year on a distinguished public position in a state?

1.	president of a country, prime minister, minister, deputy or assistant minister, head of public administration body or local administration body or its deputy, other officials;	YES	NO
2.	elected member of Legislative body (members of parliament and all other persons appointed/elected by the parliament);	YES	NO
3.	carrier of the highest legal and constitutionally-court functions (judges, plaintiffs and their deputies);	YES	NO
4.	a member of the Audit courts, i.e. supreme Audit institutions and the Central Bank Councils;	YES	NO
5.	ambassador, consul or the general officer of the armed forces	YES	NO
6.	a member of management or supervisory body of an state owned enterprise	YES	NO

Table 2

Are you an immediate family member of a person referred to in table 1?

1.	marital or extra-marital partner;	YES	NO
2.	children born in a marital or extra-marital relationship and their marital or extra-marital partners;	YES	NO
3.	parents, brothers and sisters.	YES	NO

Table 3

Are you a close associate of a person referred to in table 1?		
1. do you have a common profit from the asset or established business relationship or other type of close business contacts;	YES	NO
2. are you in some other type of closer business contact with persons referred to in Table 1?	YES	NO

Table 4

Data which client submits to a bank after the expiry of 12 months from the day when his acting at the public function expires, pursuant to which the bank is not longer obliged to treat the client as an politically exposed person.		
1. Did the 12 months period from the day when your public function in the State expired?	YES	NO
2. Are you a family member or a close associate of a physical person's that acted at the public function referred to point 1 of this table?	YES	NO

If your answer to any of the questions above in Tables 1, 2 or 3 was YES, you are, pursuant to the Law on Prevention of Money Laundering and Terrorism Financing classified as a Politically exposed person. Therefore, please state the origin of assets or property which are, or shall be the subject of business relation or transaction**:**

____
____

____
____

____
____

In hereby confirm that the abovementioned data are true.

____
Client's name and surname

____
Client's address Client's date of birth

____
Place and date Client's signature

____
____

____
Name and surname of a bank's employee

____
Place and date

____
Signature of a bank's employee

I agree to establish business relations and/or perform transaction with a politically exposed person.

____
Name and surname of the responsible person in a bank

____
Place and date

____
Signature of the responsible person in a bank

Pursuant to Article 17 paragraph 1 point 2), and read in conjunction with Article 38 paragraph 2 of the Central Bank of Montenegro Law (OGRM 52/00, 53/00 and 47/01) and Article 35 paragraph 5 of the National Payment Systems Law (OGM 61/08), the Council of the Central Bank of Montenegro, at its session held on 20 March 2009, enacted

D E C I S I O N

ON MORE DETAILED CONDITIONS FOR PAYMENT SYSTEMS LICENSE ISSUING AND REVOKING AND GRANTING APPROVALS

(OGM 24/09 of 1 April 2009)

I. BASIC PROVISIONS

Article 1

This Decision shall govern the detailed conditions for payment systems license issuing and revoking and issuing of approvals of changes in the contract on payment systems or in rules of the payment system.

II. PAYMENT SYSTEMS LICENSE ISSUING

Article 2

The meeting of the authorised representatives of the Central Bank of Montenegro (hereinafter: the Central Bank) and representatives of the payment system operator shall be organised upon the request of the bank that intends to become the operator of the payment system (hereinafter: payment system operator) prior to the submission of license application.

The representatives of the payment system operator shall inform the representatives of the Central Bank at the meeting referred to in paragraph 1 above on the planned timeframes of the beginning of the work of the payment system, payment system participants, basics of the business strategy of the payment system, the manner of providing staffing and technical capacities for the performance of the payment system, and other issues relevant for payment system management.

The minutes shall be kept at the meeting referred to in paragraph 1 above, which shall be signed by the representative of the Central Bank and payment system operator respectively.

Article 3

Payment system operator shall provide that:

1) payment system has corresponding legal basis in all relevant jurisdictions;
2) payment system provides final settlement as at value date without delay, during the day and by the end of the day, at the latest;
3) payment system in which multilateral calculation is performed is able, as a minimum, to provide timely finalisation of daily settlement in case of inability to settle the largest individual calculated liabilities of the participants;
4) payment system has objective and publicly disclosed criteria for participating in the system, which enable fair and open access to the system; and
5) payment system management is efficient, responsible and transparent.

Article 4

Payment system operator shall submit the license application to the Central Bank in writing.

The following shall be attached to the license application under paragraph 1 above:

1) Authorisation for the person the Central Bank will cooperate with during the review procedure for license issuing for payment system operator;
2) Information on the payment system operator (name, registered office and the address of the payment system operator);
3) Documents showing that the payment system operator has technical, organizational and functional capacity for operational payment system management, as well as control mechanisms and security mechanisms for risk management;
4) Business plan of the payment system for the first three operation years;
5) Documents on persons with special powers and responsibilities in the payment system;
6) Data on the participants in the payment system;
7) Draft contract on payment system;
8) Draft payment system rules;
9) Statement of the authorised person of the payment system operator that the information submitted and documents delivered are up-to-date, complete and accurate;
10) Statement that the payment system operators will immediately inform the Central Bank on all changes occurred in data attached to the license application;
11) Evidence on the executed payment of fee charged for license issuing; and
12) Other documentation the operator deems is necessary for deciding upon request.

If specific original documents attached to the license application are in foreign language, they must be translated by the authorised translator and verified in accordance with the law.

Article 5

The payment system operator shall submit the following documents as evidence showing that the payment system operator has technical, organizational and functional capacity for operational payment system management, as well as control mechanisms and security mechanisms for risk management:

1) Evidence on legal basis for using business premise and equipment needed for performing activity as payment system operator;
2) Detail description of technological organisation and information system support, as well as description of technical standards applied in the payment system and description of measures for the provision of technical security in payment system operations;

3) Evidence on existence of the control mechanisms and security mechanisms for risk management;
4) Evidence that the information system that supports the payment system is designed and realised to provide high availability of the system in regular activities and contingencies;
5) Evidence that the payment system does not jeopardise the compatibility with the functioning of other payment systems, safety and stability of the financial system in Montenegro;
6) Proposal for the organisation and job position scheme that regulates organisational part of the bank that will perform activities of the payment system operator, by officers with qualifications and work experiences;
7) Data and documents on persons with special powers and responsibilities in the payment system (name and last name, uniform identification citizen's number, permanent address and evidence on qualifications and specialisations, including data on prior work engagements for the previous five years or shorter if the work engagement of these persons is shorter than five years), showing their expertise and competence for performing operations with special powers and responsibilities in the payment system.

Article 6

Business plan of the payment system for the first three years shall include but not be limited to:

1) Detail description of the activities to be performed by the payment system;
2) Strategy and plan of development and economic sustainability of the projected activities, including the assessment of sources of financing;
3) Risk analysis, risk management and risk minimising (guarantee fund, and the like);
4) Evidence that the plan is based on realistic economic indicators;
5) Description of organisational structure, including projected number of employees and establishing persons authorised for the communication with the Central Bank;
6) Description of internal controls including manner and means of efficient monitoring;
7) Programme of measures against money laundering.

Article 7

Draft Payment System Contract shall include but not be limited to:

1) Counterparties – payment system operator and participants, as well as other persons (agent for settlements, and the like);
2) Mutual rights and obligations of counterparties and other persons;
3) Payment system governance and management;
4) Procedure in case of amending the contract, contract termination and ceasing of payment system activities.

Article 8

During the review process of license application, the Central Bank may require additional information and evidence from the applicant.

The applicant shall inform the Central Bank immediately on all changes in data or documents submitted with the application which occur during the process of deciding upon application.

Article 9

The Central Bank shall pass a decision to deny the license issuing to the payment system if it evaluates that the payment system operator does not meet the conditions for payment system management specified in the National Payment System Law and this Decision.

III. LICENSE REVOCATION

Article 10

The Central Bank shall pass a decision on revoking the license issued to the payment system operator in cases specified in Article 37 of the Law.

The decision referred to in paragraph 1 above shall contain detail explanation of the reasons for license revocation.

IV. ISSUING OF APPROVALS FOR AMENDING THE PAYMENT SYSTEM CONTRACT OR PAYMENT SYSTEM RULES

Article 11

The licensed payment system operator shall submit in writing the request for obtaining approval for amending payment system contract or payment system rules.

The following documents shall be submitted with the request referred to in paragraph 1 above:

1) Draft of the document amending the payment system contract and/or draft of the document amending payment system rules;
2) Detail explanation of the reasons for amendments; and
3) Evidence of executed payment of fee for issuing approval.

During the review process of the submitted request for obtaining approval under paragraph 1 above, the Central Bank may require additional information.

In the procedure of passing a decision upon request for obtaining approval referred to in paragraph 1 above, the Central Bank shall, in particular, evaluate the impact of the requested amendments to the risk management in the payment system.

The Central Bank shall deny the request for obtaining approval referred to in paragraph 1 above, if it evaluates from the documents and other known facts that the requested amendments would cause disturbance in such payment system, jeopardise compatibility with the functioning of other payment systems, safety and stability of the financial system in Montenegro, or if such amendments violate the law and regulations of the Central Bank.

The Central Bank shall pass a decision on the request for obtaining the approval referred to in paragraph 1 above.

V. FINAL PROVISION

Article 12

This Decision shall enter into force on the eighth day following that of its publication in the Official Gazette of Montenegro.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

No. 0101-325/3-3

PRESIDENT OF THE COUNCIL

Podgorica, 20 March 2009

Ljubiša Krgović, m.p.

Pursuant to Article 17 paragraph 1 point 2) of the Law on the Central Bank of Montenegro (OGRM 52/00, 53/00 and 47/01) and Articles 26 and 27 of the Law on National Payment Operations (OGM 61/08), at its meeting held on 20 March 2009, the Council of the Central Bank of Montenegro passed the following

DECISION

on issuing and use of remote access payment instruments

and the manner and deadlines for reporting

(OGM 24/09 as of 1 April 2009)

I. GENERAL PROVISIONS

Article 1

This Decision shall regulate in more detail issuing and use of remote access payment instruments and the manner and deadlines for reporting to the Central Bank of Montenegro (hereinafter: the Central Bank) on the number and type of issued remote access payment instruments and other data concerning issuing and using remote access payment instruments.

Article 2

Specific terms and expressions used in this Decision shall have the following meanings:

1) **"remote access payment instruments"** are banking payment cards and electronic banking payment applications;

2) **“remote access payment instrument issuer”** is a bank and foreign bank branch which license or approval covers the issuing of remote access payment instruments;
3) **“remote access payment instrument acceptor”** is a person who signs the contract on accepting the payment via a remote access payment instrument with the issuer of the remote access payment instrument;
4) **“remote access payment instrument holder”** is a person who signs the contract on issuing and use of remote access payment instrument with the remote access payment instrument issuer;
5) **“Automated Teller Machine (ATM) terminal”** is automated device that allows the withdrawal of funds, payment of services, transfer of funds between accounts, review account balance and make other transfers using banking payment cards, as well as other activities not regarded as being transfers;
6) **“Point of Sale, Point of Service (POS) terminal”** is a device that allows the use of the banking payment cards for the purchase of goods and services or withdrawal of cash;
7) **“virtual POS terminal”** is logically defined POS that is used for transfers of funds to via accounts or for the payment of goods and services via the Internet, ATMs or digital phone, as well as via on-line use of banking cards.

Article 3

The issuer of remote access payment instrument is obliged to prepare, in writing, the general terms and conditions referring to the issuing and use of the remote access payment instruments that shall contain, as a minimum, the elements laid down in Article 25 of the Law on National Payment Operations (OGM 61/08).

The issuer of the remote access payment instrument shall publicly disclose general terms and conditions for the issuing and use of remote access payment instruments.

Article 4

Mutual rights and obligations of both the issuer and the holder of a remote access payment instrument shall be regulated in a contract on the issuing and use of the remote access payment instruments that shall contain the general requirements for the issuing and use of remote access payment instruments as its integral part.

Article 5

Mutual rights and obligations of both the issuer and the acceptor of remote access payment instrument shall be regulated in a written contract on accepting payments via remote access payment instruments that shall contain, as a minimum, the elements laid down in Article 24 of the Law on National Payment Operations (OGM 61/08).

Article 6

Remote access payment instrument acceptor may reject to accept payment via a remote access instrument, provided that it has been regulated in the contract signed with the issuer and in the following cases:

1) Expiration of validity of the remote access payment instrument;
2) Information on a lost or a stolen remote access payment instrument;
3) Mismatch of the signature on the remote access payment instrument with the signature on the transaction document or identification document;
4) Refusal of the holder to submit the document confirming his/her identity or if it has come to the knowledge of the acceptor that an unauthorised person uses the remote access payment instrument;
5) Inability to obtain the confirmation of transfer execution;
6) Concerns regarding an unoriginal or counterfeited remote access payment instrument or a lack of any of the prescribed security features on the remote access payment instrument;
7) Lack of signature of the holder on the remote access payment instrument if such a signature is required for the purpose of legal validity of the remote access payment instrument.

Article 7

A remote access payment instrument acceptor may require a remote access payment instrument holder to submit a personal document verifying his/her identity.

The remote access payment instrument acceptor may retain the remote access payment instrument provided that this has been specified in the contract signed with the holder, in the following cases:

1) expiration of validity of the remote access payment instrument;
2) information on lost or stolen remote access payment instrument;
3) mismatch between the signature on the remote access payment instrument and the signature on the transaction document or the identification document;
4) use of the remote access payment instrument by an unauthorised person;
5) receiving of order from the remote access payment instrument issuer to retain the specific remote access payment instrument.

The remote access payment instrument acceptor shall follow the procedures concerning security, in the manner specified in the contract signed with the issuer, and it shall not reveal any information on the number of the remote access payment instrument and personal information of the holder or any other information on the holder or remote access payment instrument to unauthorised persons, and it shall prevent irregular use, copying and takeover of data on the remote access payment instrument.

Article 8

The remote access payment instrument acceptor shall specify available remote access payment instruments on a visible place in its business premises.

Article 9

The remote access payment instrument issuer and acceptor shall review all complaints of the holder subject to his/her dispute with the acceptor under the procedure and within deadlines specified in the contract signed between the issuer and the acceptor.

II. BANKING PAYMENT CARDS

Article 10

Banking payment card (hereinafter: the banking card) is a type of remote access payment instrument where information is electronically stored and which is used many times for the purpose of holder identification, remote access to the bank account and/or preliminary set up of the credit limit agreed with the issuer, and for the purpose of the following transfer executions:

1) Cash withdrawal through ATMs;
2) Transfer of funds between accounts through ATMs;
3) Payment of services through ATMs;
4) Payment of goods and services and cash withdrawal through POS;
5) Payment of goods and services, and transfer of funds between account through virtual POS;
6) Checking of balance in the account; and
7) Execution of other activities that have not character of a transfer.

Banking card acceptor in the territory of Montenegro must sign a contract on accepting payment through the banking card with the bank issuer with a registered office in Montenegro.

Article 11

The banking card may be:

1) a debit card, which allows the holder to access funds up to the allowed amount in the bank account or up to the limit agreed between the issuer and the holder;
2) a credit card, which allows the holder to access funds up to the preliminary agreed amount between the holder and the issuer.

Article 12

The banking card shall be owned by the bank that has issued such a card.

The banking card shall be used by the holder.

Article 13

The banking card shall be issued based on the contract on issuing and use of the banking card, signed between the issuer and the holder, subject to the holder's opening of the account with the issuing bank for transfers to be executed by this card.

Prior to signing the contract under paragraph 1 above, the issuer shall notify the holder in writing on general terms and conditions of the issuing and use of banking cards, including the minimum of their content.

The contract on issuing and use of the banking card shall contain the following, as a rule:

1) description and manner of use of the banking card, as well as the description of functions and manner of use ATMs and POS terminals;
2) rights and obligations of the issuer and the holder, as well as consideration to be shown by the holder with a view to protecting the card from destruction, loss, theft, forgery or any other form of misuse;
3) personal identification number of card and obligation of the holder to keep it confidential;
4) deadline in which the account of the holder will be debited, as well as the value date;
5) timeframe in which certain transfers may be disputed by the holder and the description of conditions and procedures for the submission of complaints and provision of security;
6) limits for cash withdrawal from ATMs and payments through POS terminals, as well as deadlines and conditions for the use of a loan granted for payments using cards.

When a banking card is used abroad, the issuer shall also inform the holder in writing about the following:

1) amount of each fee to be paid for the transfer in a foreign currency;
2) the exchange rate for translation of the foreign currency used in the transfer, including the relevant exchange rate date.

General terms and conditions of the issuing and use of banking cards shall be an integral part of the contract on the issuing and use of the banking card.

Article 14

The banking card shall be issued under determined conditions and includes the following, but not limited to: full name of the issuer, number of card, expiry date of the card and identification number of card issuer.

The banking card shall be personalised by the issuer through recording relevant data on the holder on the banking card medium.

Article 15

The card issuer shall specify the personal identification number (hereinafter: the PIN) for each holder with respect to their cards and shall ensure that each PIN is kept confidential.

The PIN shall contain at least four digits and shall be used for the holder identification.

A card shall be used with the PIN specified for such a card if this represents the requirement for its use.

The PIN shall be used in transfers using banking cards by pressing the PIN of the holder on the keypad of an ATM or a POS terminal.

In the event the holder forget his/her PIN, the issuer shall issue a new card with a new PIN or specify the new PIN for the same card within 15 days following the receipt of information by the holder, unless otherwise agreed.

Article 16

Upon the receipt of the order from the holder, the issuer shall execute the corresponding transfer in accordance with the contract on issuing and use of the banking card.

The holder shall:

1) use the card only personally in accordance with the established terms and conditions concerning the issuing and use of the card and take care of it in an orderly and appropriate manner;
2) keep secret his/her PIN and take all necessary measures to keep PIN secret from third parties;
3) immediately inform the card issuer in cases when:
   - the card has been destroyed, stolen, forged or misused in any other way as well as in case when the PIN has been revealed to any third party;
   - transfer has been executed using the banking card without the holder's approval;
   - the holder has found an error or discrepancies in keeping his account by the issuer;
4) take care of coverage in the account that has been opened for that card, including the loan granted by the issuer.

The holder may submit the information referred to in paragraph 2 point 3) above by phone, fax or by giving a written statement to the card issuer. The issuer shall ensure the receipt of this information at any time during the period of 24 hours through previously published phone numbers, fax numbers and setting up the procedure of attesting the receipt of information, including the time of receipt.

Upon the receipt of information referred to in paragraph 2 point 3) of this Article, the issuer shall take necessary measures to prevent a further use of the banking card even in cases when the holder's handling the card has been the result of negligence.

Article 17

The issuer shall provide the possibility of performing transfer from all ATM or POS terminals that are financially serviced with it using any payment card in the territory of Montenegro.

ATM and POS terminals shall meet the security requirements determined by the card issuer in accordance with international standards.

Article 18

Interbank transfer authorisation using banking cards in the territory of Montenegro shall be performed by the card issuer after the receipt of messages sent by the bank which ATM or POS terminals have been used in the transfer (hereinafter: the bank acceptor).

Article 19

Interbank transfer authorisation performed online in the territory of Montenegro using banking cards issued abroad shall be performed by authorising messages directly sent to the card issuer by the bank acceptor in Montenegro.

Article 20

Transfers under Article 10 hereof in the territory of Montenegro shall be authorised (approved) or denied by the issuer authorisation system after verification if the transfer has been performed under the provisions of Article 22 herein.

Article 21

The issuer shall calculate the transfer executed by the banking cards.

Article 22

The holder may withdraw cash from an ATM terminal up to a maximum limit within 24 hours and may execute payments via a POS terminal up to a maximum limit for a specific period or one transfer.

The holder may, subject to provisions under paragraph 1 above, execute payments via banking cards up to the available amount in its account and/or up to a credit limit pre-agreed with the issuer.

Article 23

Upon the completion of transfer using the banking card, the issuer shall inform the holder in writing on the following in particular, but not limited to:

1) the type, date, hour and number of transfer so that it can be identified by the holder, and on terminal from which the transfer has been executed;
2) the amount of transfer that debited the holder's account, including the amount in foreign currency;
3) the amount of fees and commissions; and
4) the exchange rate applied for transfers in foreign currency.

The issuer shall provide the holder with the possibility to verify transfers executed by the banking card over the specific time period and the amount of funds in the holder's account.

Article 24

The issuer shall, upon the card expiry, return the card to the holder on the day specified in the contract, and in case of early termination of the contract, on the day of contract termination.

Article 25

Contract on issuing and use of the banking card may be signed, subject to the holder's account consent, with a person not being the contracting party to this agreement (hereinafter: the additional card holder). Provisions of Articles 10, 11, 14, 15, 16, 22 and 24 herein shall apply to the additional card holder.

The holder shall bear financial responsibility for the additional card holder.

Article 26

Banking card transfers in the territory of Montenegro shall be executed solely in euros.

Article 27

All transfers executed using banking cards through ATM and POS terminals shall be registered automatically in chronological order, based on the operating rules of the card issuer, following procedures and using technical means of external media (magnetic tape, magnetic disk, flexible magnetic disk, optical disk or other means), which ensure safekeeping and accurate reproduction of information and prevent any modifications whatsoever.

The card issuer shall keep registered information and all documents that refer to banking card transfers within deadlines specified by the law regulation the national payment transactions.

The issuer shall be responsible for proving proper execution of the banking card transfers and banking account records, as well as for proving that no technical or any other omissions have occurred during the execution of such transfers and record keeping.

Banking card payment system operator

Article 28

Banking card issuers – participants in the national payment system – may designate one bank to be the payment system operator of banking cards issued in Montenegro (hereinafter: the card system operator).

The bank – card system operator shall, for obtaining licence for banking card payment system, meet the conditions specified in the Law on the National Payment Operations and the decision prescribing detailed conditions for payment system licensing

Article 29

The card system operator shall:

1) maintain communication with the RTGS system;
2) set the payment system rules to be binding on all payment system participants serviced by it;
3) test and approve technical equipment and software of the payment system participants it services to ensure their compatibility with the authorisation systems and ability to prevent any unauthorised access;
4) be technically equipped to manage direct or indirect link of ATM and POS terminals in the territory of Montenegro with the system it services;
5) maintain communication between the payment system it services and analogue payment systems.

The card system operator shall allow the possibility of:

1) authorisation (approval) of transfers using banking cards;
2) activating banking cards;
3) personalising banking cards;
4) setting and changing PINs of the banking cards;
5) performing other services under its business activities.

Article 30

A contract concluded between card system operator and issuers participating in such system shall contain authorisation of the issuers to the card system operator to deliver the settlement order in the RTGS system of the Central Bank for executing interbank transfer resulting from transfers under Article 10 herein.

Article 31

Data on transfers through banking cards shall be transferred from the card issuer to the card system operator and vice versa in the format, manner and under the procedure set forth in the card system rules.

The card system operator shall calculate multilateral net positions between issuers – participants in such a system arising from banking card transfers issued in Montenegro.

The card system operator shall ensure the execution of interbank banking card transfers by issuing orders in the RTGS system in accordance with Daily Work Time Schedule of the RTGS system, under the procedure and in the manner to be specified by the Central Bank.

In the event of insufficient funds in the settlement account of the issuer in RTGS system for executing transfers arising from the use of the banking card, the card system operator shall deny authorisation of the transfer by the card of the issuer, subject to the notification from the Central Bank.

Agent for settlement of transfers executed by specific banking card in the territory of Montenegro

Article 32

Settlement of transfers executed by a specific banking card in the territory of Montenegro may be performed also by the agent for settlement of transfers executed using a specific banking card (hereinafter: the settlement agent).

The Central Bank or a commercial bank may perform the function of the settlement agent if they sign a separate contract with the respective international organisation that is the owner of the card license.

The settlement agent shall perform the settlement of interbank transfers between banks having their registered office in Montenegro which issue the specific card and become members of such a settlement system.

The settlement of interbank transfers between banks with the registered office in Montenegro which issue specific card shall be performed in accordance with the authorised instructions given by the international organisation that is owner of such card license for settlement and operating settlement procedures.

III. ELECTRONIC BANKING PAYMENT APPLICATIONS

Article 33

Electronic banking payment applications shall be a type of a remote access payment instrument (Internet payment applications, token, PDA devices, contact-free payments and the like) which serve for electronic transfers and other actions that do not have the character of a transfer, subject to a separate contract (hereinafter: the contract on providing electronic banking services).

Article 34

Pursuant to the contract on providing electronic banking services and using electronic banking payment application:

1) the bank – issuer provides electronic access to funds kept in the holder's accounts and performs actions ordered by the holder;
2) the holder instructs the bank to debit his account for the amounts of executed transfers and fees and commissions or to pay the amounts from the account specified by the bank.

Article 35

In addition to provisions specified in Article 4 herein, the contract on providing electronic banking services shall contain in particular:

1) rules for electronic identification of holder; and
2) rules to which the holder must adhere when executing transfers and using other services specified in the contract.

Article 36

1) A bank that provides services in accordance with the contract on providing electronic banking services shall:
2) ensure the safety of transfers executed by the holder paying due attention and using adequate technical means;
3) provide the holder with information on executed transfers and calculation, as well as paid fees and provisions within the specified deadlines and in the manner specified under the contract;
4) immediately inform the holder in case of denial or inability to execute an authorised transfer due to reasons beyond the bank's influence.

Article 37

The holder shall not disclose any information on activities specified in the contract on providing electronic banking services when such a disclosure could cause inefficiency of mechanisms that provide the safety of transfers.

The holder shall bear expenses of all transfers executed due to the failure to observe the provisions referred to in paragraph 1 above.

Article 38

Instructions of the holder influencing the execution of transfers by the bank may be revoked only before the execution of a transfer.

Article 39

The holder shall submit to the bank objections with respect to the information under Article 36 point 2) herein, in the manner and within deadlines specified in the contract.

The holder shall submit to the bank objections that refer to the following, in particular:

1) doubtful transfers included in the notification; and
2) errors or irregularities in calculations.

The holder shall immediately inform the bank if he has not received notification on transfers in the manner and within deadlines specified in the contract.

The bank shall immediately consider objections and notifications of the holder referred to in paragraphs 1, 2 and 3 above.

IV. REPORTING ON REMOTE ACCESS PAYMENT INSTRUMENTS

Article 40

Remote access payment instrument issuers shall submit to the Central Bank information on the number and type of remote access payment instruments that have been issued, as well as on the value of executed transactions and/or turnover accomplished with the remote access payment instruments.

Remote access payment instrument issuers shall submit to the Central Bank reports to contain the following information, in particular:

1) the number of acceptors that have signed the contracts on accepting payments by banking cards,
2) the number of signed contracts on issuing and use of banking cards;
3) the number of signed contracts on providing electronic banking services;
4) the number and value of transfers executed using banking cards and based on electronic payment applications;
5) the number of ATM and POS terminals owned, and those not owned but used for transfers, and the number and value of transfers executed through these terminals;

6) executed transfers and registered attempts to execute transfers violating the regulations (frauds, thefts and the like) or good business practices.

Remote access payment instrument issuers shall also provide, at the Central Bank's request, other information on issued remote access payment instruments or executed transfers.

Article 41

Remote access payment instrument issuers shall submit to the Central Bank reports referred to in Article 40 of this Decision on monthly basis, no later than within eight days following the respective reporting month.

Issuer shall submit reports referred to in paragraph 1 above electronically and, subject to the Central Bank request, in hard copy.

V. FINAL PROVISION

Article 42

This Decision shall enter into force on the eighth day following that of its publication on the Official Gazette of Montenegro.

THE CENTRAL BANK OF MONTENEGRO COUNCIL

Decision no. 0101-325/3-5

PRESIDENT OF THE COUNCIL

Podgorica, 20 March 2009

Ljubiša Krgović, m.p.

Pursuant to Article 17 paragraph 1 point 2) of the Central Bank of Montenegro Law (OGRM 52/00, 53/00 and 47/01) and Article 40 paragraph 3 of the National Payment Systems Law (OGM 61/08), the Council of the Central Bank of Montenegro, at its meeting held on 20 March 2009, passed the following

DECISION

on Payment Systems Oversight

OGM 24/09 as of 1 April 2009

I. BASIC PROVISIONS

Article 1

This decision shall govern the manner of carrying out the payment systems oversight.

Article 2

The Central Bank of Montenegro (hereinafter referred to as the Central Bank) shall promote and provide safety and efficiency of the payment systems through the payment systems oversight for the purpose of maintaining financial system stability.

The Central Bank shall conduct the payment systems oversight applying the following principles: transparency, implementation of international standards and principles, use of authorities and competences, implementation of consistency and cooperation with other authorities.

Article 3

The payment systems oversight shall encompass:

- compliance of payment system with the principles for payment system functioning determined under this decision (hereinafter referred to as the oversight of payment systems functioning);

- technical, organizational and functional capacity of payment system operator for operational management of the payment system;

- existence and functioning of the oversight mechanisms and mechanisms of safety and risk management;

- compatibility of the payment system and its impact on the safety of the national financial system;

- compliance of the payment system performance with the payment system rules; and

- other activities with respect to the payment system set forth in the law,

regulations of the Central Bank and other payment system rules.

II. OVERSIGHT OF PAYMENT SYSTEMS FUNCTIONING

Article 4

The Central Bank shall perform the oversight of the payment systems functioning through the assessment of the compliance of the operations of the payment system with the principles for the payment system functioning as determined in this decision.

Article 5

The principles for the payment system functioning shall be determined for the following:

1) Systemically important payment systems; and
2) Other payment systems.

Systemically important payment systems shall be the systems where the disruptions in the operations of the system or in the work of the participant of the payment system may cause serious disruptions in the financial system.

Other payment systems shall be the systems where disruptions in the operations of the system or in the work of the participant of the payment system may not cause serious disruptions in the financial system.

Article 6

Systemically important payment system shall be the system that meets at least one of the following conditions:

1) it is the only national payment system or core payment system through which the highest value of total payments is processed;
2) it processes largest individual payments;
3) it has been used for settlement of the transactions at the financial market (foreign currency market, securities market, and the like) or for the settlement of the payments of other payment systems.

Article 7

The principles for the payment systems functioning (hereinafter referred to as the Core Principles) shall be the following:

1) The system should have a well-founded legal basis under all relevant jurisdictions.

2) The system's rules and procedures should enable participants to have a clear understanding of the system impact on each of the financial risks they incur through participation in it.

3) The system should have clearly defined procedures for the management of credit risks and liquidity risks, which specify the respective responsibilities of the system operator and the participants and which provide appropriate incentives to manage and contain those risks.

4) The system should provide prompt final settlement on the day of value, preferably during the day and at a minimum at the end of the day.

5) A system in which multilateral netting takes place should, at a minimum, be capable of ensuring the timely completion of daily settlements in the event of an inability to settle by the participants with the largest single settlement obligation.

6) Assets used for settlement should preferably be a claim on the Central Bank; where other assets are used, they should carry little or no credit risk and little or no liquidity risk.

7) The system should ensure a high degree of security and operational reliability, and should have contingency arrangements for timely completion of daily processing.

8) The system should provide a means of making payments which is practical for its users and efficient for the economy.

9) The system should have objective and publicly disclosed criteria for participation, which permit fair and open access.

10) The system's governance arrangements should be effective, accountable and transparent.

Article 8

The operations of the systemically important payment systems should be complied with all Core Principles.

The operation of other payment systems should be complied with at least principles 1), 4), 5), 9) and 10) of the Core Principles.

Article 9

The Central Bank shall give the assessment of the level of the payment system compliance with the Core Principles based on the oversight of the payment system functioning conducted through the assessment of the payment system compliance with the Core Principles.

The Central Bank shall give the assessment of the compliance of the payment system with Core Principles using the following scale:

- Compliant: the system is fully compliant with the Core Principles;
- Largely compliant: the system is largely compliant with the principles 1), 4), 5), 9) and 10) of the Core Principles;
- Partly compliant: the system is not largely compliant with the principles 1), 4), 5), 9) and 10) of the Core Principles;
- Non-compliant: the system is not compliant with the Core Principles.

Article 10

Depending on the assessment of the compliance of the payment system with the Core Principles, the Central Bank shall undertake appropriate measures and activities to provide the compliance of the payment system with the Core Principles.

III. PAYMENT SYSTEMS OVERSIGHT

Article 11

The Central Bank shall perform the oversight of the payment systems which itself does not operate, through the following:

1) on-site inspection of the operations of the payment system; and

2) off-site, through permanent analysis of information, data and documents which the payment system operator submits to the Central Bank upon its request, as well as through monitoring of payment system transactions in the Central Bank Payment System for executing interbank payments.

Article 12

Payment system oversight may be:

1) partial, when one or several oversights referred to in Article 3 of this Decision and/or when the assessment of compliance of the payment system functioning is performed with one or more Core Principles; and
2) full, when all oversights under Article 3 of this Decision are performed, which serves for the assessment of compliance of the payment system functioning with all Core Principles.

Article 13

The payment systems oversight shall be performed by the employees of the Central Bank authorized for such operations.

Notwithstanding paragraph 1 above, the Central Bank may authorize other relevant institutions for carrying out the payment system oversight which itself operates, and it may authorize also persons not employed with the Central Bank for carrying out specific tasks during the payment system oversight.

Article 14

The Central Bank shall notify, as a rule, the payment system operator on the planned on-site inspection 10 working days prior to the inception of inspection.

Notwithstanding paragraph 1 above, if the reports and information held by the Central Bank disclose irregularities that may be significant for the safety and soundness of the financial system functioning, on-site inspection may be commenced even without prior notification.

Article 15

Payment system operator shall enable authorized examiners of the Central Bank a free insight in documentation and functioning of the information technology and computer database of the payment system and it shall provide, upon the request of the authorized examiners, copies of the specific documents in hard and/or electronic form.

Article 16

Report shall be made on the completed oversight.

The oversight report shall be confidential and shall not be disclosed either partly or wholly without approval of the Central Bank.

Article 17

Payment system operator may submit its objections to the oversight report to the Central

Bank within eight working days following the day of its receipt.

The Central Bank may directly check the payment system operator's remarks contained in its objections to the report and, in that case, the Central Bank shall make an addition to the report, and the payment system operator may submit its objections to this addition within three working days after the day of its receipt.

The Central Bank shall consider the received objections and notify the payment system operator of accepting or non-accepting those within eight days of the day of receiving objections to the oversight report or objections to its addition to the oversight report.

Article 18

If it is determined that the payment system operator violates the payment system rules or acts contrary to the regulations, the Central Bank shall take measures set forth in the law governing the national payment operations.

IV. FINAL PROVISION

Article 19

This decision shall enter into force on the eighth day following that of its publication in the Official Gazette of Montenegro.

COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

Decision no. 0101-325/3-4

PRESIDENT OF THE COUNCIL

Podgorica, 20 March 2009

Ljubiša Krgović, signed

6

Pursuant to Article 17 paragraph 1 point 2) of the Central Bank of Montenegro Law (OGRM 52/00, 53/00, 47/01) and Article 5 paragraph 3 of the National Payment System Law (OGM 61/08), at its session held on 23 and 24 February 2009, the Council of the Central Bank of Montenegro passed the following

DECISION

on the conditions and manner of performing certain activities involved in the transfer execution by the agent

(OGM 24/09 as of 1 April 2009)

Article 1

This decision regulates activities involved in the transfer of funds (hereinafter: the transfer) which an agent may perform and prescribes more detailed conditions and manner of performing such activities by an agent.

Article 2

A performing institution may entrust the agent to perform some of the activities involved in the transfer execution, for its account and on its behalf, involving the acceptance of the transfer orders and the remitting thereof to the performing institution for their execution and the acceptance and execution of cash payment and payout orders.

The agent shall perform the activities it has been delegated by presenting the place for the acceptance, remittance and execution of the orders under paragraph 1 above which the performing institution receives or remits and at which clients have immediate access to accepting, remitting or executing of such orders.

Article 3

An agent, within the meaning of this decision, may be a performing institution or another legal persons which:

- has been registered with the competent authority to perform the financial intermediary business;
- has adequate technical and technological infrastructure to ensure safe and efficient performance of activities it is entrusted with; and
- has professional staff capable of performing the activities it is entrusted with.

Article 4

An agent which is not a performing institution may not be a payment system participant.

A performing institution being the agent may not execute the transfers it has been entrusted with through the RTGS system.

Article 5

The agent shall enter into an agreement with the performing institution on the delegation of certain activities involved in the transfer execution.

The agreement under paragraph 1 above shall detail: activities involved in the transfer execution which the agent shall perform for the performing institution; rights, obligations, and responsibilities of the performing institution and the agent and the contract validity period.

Article 6

The performing institution shall inform the Central Bank of Montenegro on the concluded agreement and activities to be performed by the agent on its behalf, no later than within three days as of the agreement date.

Article 7

The performing institution shall be liable for all actions and any and all failures of the agent to perform the transfer execution activities it has been entrusted with.

Article 8

Should the examination of the performing institution establish that the performing institution is non-compliant with this decision or other regulations due to the failures made by the agent, the Central Bank of Montenegro shall order the performing institution to terminate the agreement with such an agent.

Article 9

The Decision on the on the Conditions and Method of Performing Domestic Payment Operations by the Authorized Agent (OGRM 78/04) shall be repealed on the day of entry into force of this decision.

Article 10

This decision shall enter into force on the eighth day following that of its publication in the Official Gazette of Montenegro.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

Decision no. 0101-325/2-24

THE PRESIDENT

Podgorica, 24 February 2009 ***Ljubiša Krgović, signed***

Pursuant to Article 17 paragraph 1 point 2 of the Law on Central Bank of Montenegro (“OG RoM”, Nos. 52/00, 53/00 and 47/01) and Article 11 paragraph 5 of the Law on National Payment Operations (“OG RoM”, No. 61/08), the Council of the Central Bank of Montenegro, on its session held on 23 and 24 February 2009, issued

DECISION

on the structure of the transfer execution account and the detailed conditions and manner of account opening and closing

(«OG MNE», No. 24/09 ,15/11)

I. BASIC PROVISIONS

Article 1

This Decision shall regulate the structure of transfer execution account (hereinafter: the account) and closer conditions and manner of opening and closing of the account with performing institutions.

Article 2

The “accounts”, in terms of this Decision, shall mean the accounts which performing institutions open for the execution of the national payment operations. The accounts shall register monetary inflows, outflows and balance.

II. STRUCTURE OF THE ACCOUNT

Article 3

The account shall be uniquely denoted by numerical character.

Numeric character of the account consists of the three following parts:

1) Fixed number of the performing institution (three numeric characters);
2) Account number (thirteen numeric characters); and
3) Control number (two numeric characters).

Written documents shall be allowed to have three-part numerical character prescribed by the paragraph 2 of this Article, separated by dashes, while leading zeros in the second part may be omitted.

Numeric character of the account is used only in electronic form, solely as the line of eighteen digits, prescribed by paragraph 2 of this Article.

Article 4

Fixed number of the performing institution is the unique identification number of the performing institution, which the Central Bank of Montenegro (hereinafter: the Central Bank) shall determine for each performing institution.

Article 5

Account number shall be determined by the performing institution.

Article 6

Control number shall be calculated for the line of sixteen digits (fixed number of the performing institution and the account number) according to the international standard ISO 7064, MODUL 97. Control number shall be obtained by multiplying the line of first sixteen digits with 100, dividing the obtained number by 97, and by subtracting the rest from 98. The obtained result, expressed by two digits, shall represent the control number. If there is no rest during the subtraction, control number shall be 98.

Article 7

Structure of the account, prescribed by provisions of Articles 3-6 of this Decision is compulsory in cases when the performing institution opens the accounts for execution of national payment operations for legal entities, natural persons who perform registered activity and natural persons who do not perform registered activity.

Performing institution may open the accounts which structure is different than the structure prescribed by provisions of Articles 3-6 of this Decision to natural persons who do not perform registered activity, but national payment operations cannot be performed via these accounts.

III. OPENING AND CLOSING OF THE ACCOUNT

Article 8

Being the performing institution, the Central Bank shall open and close the accounts of other performing institutions and bodies which are legaly obliged to have accounts with the Central Bank.

In addition to the account from paragraph 1 of this Decision, the Central Bank may open the accounts to the following bodies:

1) European Central Bank;
2) Central banks of other countries; and
3) Central Depository Agency – the account for the monetary balancing of the subprime market transactions (cash pool).

Article 9

Performing institution, except the Central Bank shall open and close:

1) The accounts of legal entities and natural persons who perform registered activity; and

2) The accounts of natural persons who do not perform registered activity.

Article 10

Performing institutions, bodies and entities from Articles 8 and 9 of this Decision shall be clients of the performing institution, within the meaning of this Decision.

Performing institutions shall open the accounts from Articles 8 and 9 of this Decision, according to the contract on the opening of the account, concluded with the client.

Contract on the opening of the account of the performing institution shall be concluded according to the written request for the opening of the account and the documents prescribed by this Decision.

Article 11

Request for the opening of the account shall contain the following data on the requester:

1) Name of the legal entity or natural person who performs registered activity, that is, name of the natural person who do not perform registered activity;
2) Place – head office, that is, place of residence, address and telephone number;
3) Activity – type of operations of legal entity or natural person who performs registered activity;
4) Registration number of legal entity or natural person who performs registered activity, that is identity code of the natural person who do not perform registered activity;
5) Stamp and signature of the person authorized for the representation of the legal entity or natural person who performs registered activity, that is, signature of the natural person who do not perform registered activity.

In addition to the request from paragraph 1 of this Article, legal entity or natural person who performs registered activity submits the following documents:

1) Confirmation on registration – registration in the Central Register of the Commercial Court, that is, acts on registration with other authority in charge, if it requires registration;

2) Founding act of the authority in charge, if it requires registration;

3) Abstract from the law, if it is established directly pursuant to the law;

4) Registration note on classification by activities of the statistics authority, if its classification is performed by the statistics authority;

5) Act on registration with tax authority which contains tax number of the requester, if such registration is prescribed;

6) Filled card of deposited signatures of persons authorized for signing the order for managing the account's assets, signed by the authorized person of the requester, verified by the stamp by which order for execution of transfers shall be verified;

7) Act on appointment of authorized person of the requester;

8) Verification of the signature of authorized person of the requester;

9) Evidence on the payment of the compensation, that is, the fee, if they are prescribed.

When a requester is the person whose account, according to regulations, is excluded from the enforced collection, in addition to the documents from paragraph 2 of this Article, it shall submit documents which certify that this account is excluded from the enforced collection.

Notwithstanding paragraph 2 of this Article, in addition to the request for opening of the account for payment of funds for establishing a new legal entity, only contract on establishing of that legal entity shall be submitted.

When a requester is a natural person who does not perform registered activity, in addition to the request he shall deposit his signature, and if other person is authorized to sign orders for managing the account assets, signature of that person shall be deposited as well.

In addition to the request and documents from paragraph 2 of this Article, performing institution will ask for other data, that is, other documents, if it is prescribed by the law or other regulation, and may also ask for additional documents which it considers necessary for deciding upon the request.

When, on the basis of submitted request and documents, performing institution determines that the conditions for opening of the accounts are fulfilled, it shall conclude the contract on opening of the account with the client.

Article 12

Card with deposited signatures of persons authorized for signing the orders for managing the account assets of the legal entity or natural person who performs registered activity, must contain the following data:

1) Account number;
2) Name of the requester;
3) Head office, address and telephone number of a client;
4) Name, identity code and address of a person authorized for signing the order;
5) Manner of signing (individual or collective);
6) Signature of the person authorized for signing;
7) Date;
8) Signature of the authorized person and stamp of the requester;
9) Signature of the authorized person and stamp of the performing institution; and
10) Other data requested by the performing institution which opens the account.

Article 13

Executed transfer shall be registered by performing institutions at the level of individual clients' accounts.

Performing institutions are obliged to register data promptly and on a daily basis and to provide correctness of recorded data.

Performing institution is obliged to keep the documents for the period of five years, and electronic data on executed transfers for the period of ten years, from the day of transfer execution.

Article 14

Performing institution shall close the client's accounts on the basis of his written request for closing of the account, and the assets from the closed accounts shall be transferred to the account specified in the request.

In addition to the data referred to in Article 11 paragraph 1 of this Decision, request for closing of the account shall especially contain: number of the account which closing is requested and number of

the account to which the assets are transferred, and in addition to the request, credit order shall be submitted.

Notwithstanding paragraph 1 of this Article, performing institution may close the accounts of its client without the request, if the client terminates to exist as legal entity pursuant to the law or other regulation.

In case of paragraph 3 of this Article, if the legal successor or other person in favour of whose account the transfer is executed is not prescribed by regulation or other legal act, performing institution shall transfer the assets which are not in use from closed accounts to opened account.

Article 15

Performing institution shall close all accounts of the client which is in the bankruptcy or liquidation proceedings, pursuant to the request of bankruptcy or liquidation administrator, and shall open the bankruptcy or liquidation account.

In addition to the request referred to in paragraph 1 of this Article, bankruptcy or liquidation administrator shall submit the following documents:

1) Request for the opening of the bankruptcy or liquidation account to which the following documents are enclosed:

- Notification of a decision on initiation of the bankruptcy or the liquidation proceeding;
- Registration note of the statistics authority on classification by activities of the client in bankruptcy or in liquidation, if the classification is done by the statistics authority;
- Act on registration of the client in bankruptcy or in liquidation with the tax authority, which contains tax number of the client in bankruptcy or in liquidation, if such registration is prescribed; and
- Filled card of deposited signatures of the persons authorized for signing the orders for managing the account assets of the client in bankruptcy or in liquidation, signed by authorized person, verified by the stamp with which orders for the transfer execution shall be verified;

2) Order for execution of transfer of assets from all accounts of the client in bankruptcy or liquidation which shall be closed, before the closing, to the open account of the client in bankruptcy or liquidation;
3) Request for closing of all accounts of the client against whom bankruptcy or liquidation proceeding initiated;
4) Evidence on payment of compensation or fee, if they are prescribed.

Article 16

Performing institution shall execute transfer from the accounts of the client which are closed to the open account of the client in bankruptcy or liquidation, which still may be active until closing of the accounts of the client against whom bankruptcy or liquidation proceeding initiated.

Article 17

If the bankruptcy proceeding terminates and the client against whom bankruptcy or liquidation proceeding initiated continues work, upon the request of the bankruptcy administrator or other authorized person, performing institution shall close accounts of the client against whom bankruptcy proceeding terminated, and shall open a new account.

In addition to the request from the paragraph 1 of this Article, the following documentation shall be submitted:

1) Request for the opening of the account with:

- Notification of a decision on termination of the bankruptcy proceeding against the client;
- Registration note of the statistics authority on classification by activities of the client against which the bankruptcy proceeding terminated, if the classification is done by the statistics authority;
- Act on registration of the client against which the bankruptcy proceeding terminated with the tax authority, which contains tax number of the client, if such registration is prescribed; and
- Filled card of deposited signatures of the persons authorized for signing the orders for managing the account assets of the client against which the bankruptcy proceeding terminated, signed by authorized person, verified by the stamp with which orders for the transfer execution shall be verified;

2) Order for execution of transfer of the assets from the closing account of the client against which the bankruptcy proceeding terminated before their closing, to the new account of the client;
3) Request for closing of the account of the client against which the bankruptcy proceeding terminated;
4) Evidence on the payment of compensation or fee, if they are prescribed.

Article 18

Performing institution shall execute transfer from the account of the client against which the bankruptcy proceeding terminated to a new account of that client, which cannot be active until closing of the client's account which he had during the bankruptcy proceedings.

Article 19

Performing institution shall close the accounts of the client whose status changed, pursuant to the request of that client or its legal successor, and shall execute transfer from the closed accounts to the account specified in the request.

In addition to the request from paragraph 1 of this Article, the client or his legal successor shall submit:

1) Request for opening of account of the client whose status changed, with:
- Notification of a decision on registration of the status change in the register of the authority in charge;
- Act on registration of the client created by the status change, if such registration is prescribed;
- Registration note of the statistics authority on classification by activities of the client whose status changed, if the classification is done by the statistics authority;

- Act on registration of the client who is the legal successor of the client with the status change with the tax authority, which contains tax number of the client, if such registration is prescribed; and
- Filled card of deposited signatures of persons authorized for signing the orders for managing the account assets of the client created by the status change, signed by authorized person, verified by the stamp with which orders for the transfer execution shall be verified;

2) Order for execution of transfer of the assets from all closing accounts of the client who, according to the status change, does not exist any more before their closing, to the new account of one or more clients created by the status changed, that is to the account of the incorporating client;
3) Request for closing of all accounts of the client who, according to the status change, does not exist any more, with the notification of the decision on deleting of the client who, according to the status change, is not legal subject any more, from the register of the authority in charge;
4) Evidence on payment of the compensation or fee, if they are prescribed.

Article 20

Decision on unique structure for identification and classification of the accounts for performing national payment operations ("OG RoM", No. 78/04) and Decision on opening, maintaining and closing of the accounts for performing national payment operations ("OG RoM", No. 78/04 and 06/05) shall cease to be valid as of the day this Decision comes into force .

Article 21

This Decision shall come into force on the eighth day following its publication in the “Official Gazette of Montenegro”.

COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

Decision No. 0101-325/2-19 **PRESIDENT**

Podgorica, 24 February2009 ***Ljubisa Krgovic***

Pursuant to the Article 8 paragraph 3 of the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro", no 14/07 and 4/08, hereinafter referred to as the Law) and the Article 2, paragraph 1 of the Rulebook on Developing the Guidelines for Risk Analysis for the Purpose of Preventing Money Laundering and Terrorist Financing ("Official Gazette of Montenegro", no 20/09), the Council of the Insurance Supervision Agency at its 61st session held on 7 March 2011, adopted

THE GUIDELINES

on the Risk Analysis of the Money Laundering and Terrorism Financing in the Insurance Companies

Article 1

These Guidelines shall determine in detail the content of business policy acts of insurance companies dealing with life insurance and branches of foreign insurance companies without legal entity status licensed to perform life insurance business in Montenegro (hereinafter referred as the Obligors), that the Obligors use in order to regulate management of money laundering and terrorism financing risk, related risk analysis, procedures with clients depending on the risk category the Obligor has classified it to, as well as other procedures in the area of preventing money laundering and terrorism financing, which are required for reducing this risk to the minimum.

Obligor's Duties

Article 2

The Obligor shall adopt an internal act on business policy which is to regulate the following activities:

- development of a risk analysis in relation to the money laundering and terrorism financing, with the purpose of defining areas of business which are, given the possibilities of money laundering or terrorism financing, more or less critical, i.e. of self-determining other risks in business operation,

- definition of measures and manner for their implementation for the purpose of preventing the risk of money laundering and terrorism financing,

- appointment of person authorized for implementation of measures aimed at preventing the risk of money laundering and terrorism financing and undisturbed performance of activities by this person,

- training program for employees, especially for authorized person, for the purpose of adequate fulfillment of activities prescribed by the Law and these Guidelines,

- collection of data in a manner prescribed by the Law and these Guidelines,

- reporting to the authorities in a manner prescribed by the Law,

- assessment of procedures on prevention of money laundering and terrorism financing implemented by the insurance brokers or agents that the Obligor cooperates with,

- treatment of client's data in the procedure of establishing identity, reviews of and monitoring the basis for establishing client's identity and risk factor,

- treatment of data on transactions performed under the business relationship with the client, especially of those that cause doubt whether they are appropriate for the type of business and in line with the client's risk and information on the respective client,

- keeping records in a manner prescribed by the Law.

The Obligor shall deliver the act set forth under the paragraph 1 of this Article to the Insurance Supervision Agency (hereinafter referred to as the Agency), together with the accompanying decision of the Board of Directors within 15 day upon its adoption.

Appointment of the Authorized Person

Article3

The Obligor shall upon the adoption of internal procedures from the Article 2 of these Guidelines, without any delay appoint a person (hereinafter referred to as the Authorized Person) for performance of work prescribed by the Law and these Guidelines.

The Obligor shall under the internal act from the Article 2 of these Guidelines appoint a person as the deputy of the authorized person, which is to deal with affairs from the paragraph 1 of this Article in the event the authorized person is prevented from duly performance of these affairs. The Authorized Person and its deputy shall be persons that meet requirements under the Article 36 of the Law.

Data on the Authorized Person and its deputy, as well as on replacement of such persons, shall be delivered to the Agency within 15 days upon adoption of the respective decision.

The Obligor shall provide persons from the paragraph 1 and 2 of this Article with regular training and professional development for affairs and tasks they perform, as well as with adequate offices and technical capacities for the work.

Internal audit shall quarterly assess qualifications of the Obligor for performance of activities aimed at prevention of money laundering and terrorism financing and those findings shall comprise a part of the quarterly report of the internal audit, which is to be adopted by the Board of Directors.

Identification, Review and Monitoring Measures

Article 4

Measures of identification, review and monitoring of clients, respectively of transactions performed during a business relationship with a client, shall be performed in a manner prescribed by the Law and these Guidelines and shall be performed especially in the following situations:

1) when establishing a business relationship with a client;
2) in the event of one or more related transactions having the value of 15.000€;
3) when there is a doubt concerning the accuracy or validity of obtained data on identification of a client;
4) when there are doubts that a transaction or a client is related to money laundering or terrorism financing.

When conducting identification, review and monitoring measures, the Obligor shall take into consideration the following criteria:

1. general criteria on the basis of which a client, a business relationship, a product or a transaction are classified as more or less risky for money laundering or terrorism financing,
2. criteria for assessing the client's risk, respectively of his/her key business activities in the sense of money laundering or terrorism financing, including the assessment of probabilities for its business to be misused for money laundering or terrorism financing,
3. criteria for managing the risk of money laundering and terrorism financing that the Obligor possesses.

Within the conduct of these criteria the Obligor shall comply with the following instructions:

1. the client shall be classified into the risk category on the basis of determined risk factors specified in the Article 5 of these Guidelines,

2. in the event that upon collection of required data, the Obligor assesses that there is a high risk of money laundering and terrorism financing, the Obligor may also classify a client, a transaction, a product or a business relationship into the high risk category, even though according to the factors from the Article 6 of these Guidelines they belong to the low risk category,
3. when determining the risk grade category, a client, a business relationship, a product or a transaction, which according to the factors from the Article 6 herein would be classified as a high risk, cannot be classified as a medium risk or a low risk,
4. in the event that a transaction is performed via an intermediary, the Obligor shall undertake measures prescribed by the Article 28 of the Law.

Risk Factors

Article 5

The Obligor shall consider the following cases as the risk factors for the purpose of determining the client's acceptability and establishing its risk grade profile:

a. home country of the client, home country of the majority owner or beneficiary owner of the client is listed as a country where FATF (Financial Action Task Force) recommendations are not sufficiently applied or is deemed as risky according to the assessment of local authorities,
b. home country of the person that conducts transactions with the client, regardless the position of such a country on the list referred to in the item a) of this paragraph,
c. a client, a majority owner or a beneficiary owner of the client, or persons that perform transactions with the client, are persons that the corrective measures have been instituted against in order to establish institutional peace and safety, all in accordance with the United Nations Security Council Resolutions,
d. unknown or unclear source of client's funds or funds whose source the client cannot prove,
e. cases that cause suspicion that the client is not acting on his own account or is acting upon orders or instructions of third parties,
f. unusual way of executing transactions, especially taking into consideration its ground, amount and manner of execution, purpose of account opening, as well as activities of client if the client performs economic activities,
g. cases that causes indices that the client performs suspicious transactions,
h. client is politically exposed person in the manner prescribed by the Law,
i. risk grade of other persons related to the client,
j. specificity of affairs performed by a client,
k. client's presence at the conclusion of business relationships,
l. problems with identification documents or other documentation.

In conjunction with the risk factors from the item 1 of this Article, the Obligor may use the internal act from the Article 2 in order to expand the list with other factors or to define it in more details or to clarify situations stated in the previous paragraph of this Article pursuant to own risk assessments on certain segments of its business.

Risk Categories

Article 6

The Obligor shall classify a client into one of the following categories:

a) high-risk grade;

b) average –risk grade;

c) low-risk grade.

The high-risk grade clients are deemed to be persons that fulfill:
- condition from the Article 5, paragraph 1, item a, b, c and h of these Guidelines or
- two or more conditions from the Article 5, paragraph 1, item d, e, f, g, i , j , k or l.

The average-risk grade clients are deemed to be clients that according to the provisions from the paragraph 2 of this Article cannot be classified as the high-risk grade clients and the Obligor shall undertake regular review and monitoring measures for them as prescribed by the Law.

Notwithstanding the previous paragraph of this Article, the Obligor may also deem the persons that have entered into the insurance contract via a representative as the average risk clients, subject to the fulfillment of the following conditions:

- that the insurance company has requested copies of the documents collected by the representative,

- that the first premium payment or the first installment of the premium was paid from the client's account to the representative's account.

Low risk clients are deemed to be:

- the state authorities, local self-government authorities and other persons entrusted with public authorizations,

- persons that according to the rules of the Ministry of Finance represent a low risk for money laundering and terrorism financing,

- companies whose securities are admitted to trading with EU Member Countries or other countries where EU standards apply on stock exchanges,

- persons from the Article 4, paragraph 1, item 1, 2, 4, 5, 6, 8, 9 of the Law with their registered office in EU or a country from the list determined by the Ministry of Finance.

In addition to conditions for classification into the risk grade categories from the paragraph 1 of this Article, the Obligor may in the internal act prescribe more strict conditions for classification of clients into the category of average or high risk grade.

Determination of Risk Grade Category

Article 7

The Obligor shall classify a client, a business relationship, a product or a transaction into a risk grade after performing the following procedures:
1. identification of identity or correspondence of a client with the data collected for preparation of a risk grade assessment,
2. assessment of delivered data in the sense of the risk grade criteria on money laundering and terrorism financing,
3. assessment of additional documents and their analysis if it was assessed that their delivery is required.

When determining the risk category, the Obligor shall also use the lists of indicators prescribed by the authorities for the purpose of recognizing suspicious clients and transactions, particularly paying attention to the following situations:

1. payment of insurance premiums in large amounts,

2. request of the insurance beneficiary for the insurance payment or return of insurance premium to be paid in cash in case of large amounts,

3. large insurance payments with more insurance policies concluded in a short period of time are paid in cash,

4. there is a suspicion that the insurance policies, which were concluded in a short period of time, are paid in cash,

5. there is a suspicion that the insurance policies were concluded under false names, under the names of other people or with false addresses,

6. one person is the holder of a large number of policies issued by different insurance companies, especially if the insurance contracts were concluded in a short period of time,

7. policy owner performs amendments to the insurance contract requesting the insurance policy with higher premium or demands to change monthly payment of premiums to the annual or lump sum payment, which is not in correspondence with its financial standing,

8. canceling the insurance policy shortly after the insurance contract is concluded, especially when the policies with large premiums are involved,

9. a client requests for compensations from insurance and payments demanded on the basis of compensation in the event of canceling the policy or overpaid insurance premiums to be paid to a third party or transferred to the account of a physical or legal entity from a country that does not apply strict standards on prevention of money laundering or where strict regulations on confidentiality and secrecy of banking and business data are in force,

10. client accepts unfavorable terms of the insurance contract regarding to his health condition or age,

11. companies that hold insurance policies on behalf of their employees pay unusually high insurance premiums or cancel policies in a very short time after the date of entering into the insurance contracts,

12. companies purchase life insurance policies for employees, but number of employees is lower than the number of purchased policies,

13. insurance contract is concluded by a person that was involved in illegal activities in the past or insurance contract is concluded by a person that in some manner can be associated with the aforementioned person,

14. insurer or insurance holder insists on transaction secrecy, i.e. not to report the amount of the insurance premium or the insurance sum to the Administration, despite the legal obligation of the insurer to do so,

15. a client attempts by a plead or a bribe to persuade employees of the insurance company to act in his/her interests contrary to the Law,

16. large or unusual indemnity claims or claims whose grounds cannot be determined with certainty,

17. duration of life insurance policy is shorter than three years.

Procedure from the paragraph 1 of this Article is conducted through a form that contains prescribed data which is to be filled in by the client, as well as through collection of other documents, originals or duly certified copies, and by the analysis of data collected in previously described manner which is to be performed by the Obligor's employee.

After conducting the procedure from the paragraph 1 of this Article, the client shall be classified into a certain risk category and the decision on possibilities to enter into business relationship shall be issued thereupon.

In the event that the client is assessed as a high risk client, the Obligor shall determine the client's acceptability and may refuse to enter into agreement with the client with whom the existence of any of the above mentioned risks have been determined.

The Obligor may also condition entering into a contract or extension of already concluded contract with fulfillment of specific additional conditions determined by the internal act of the Obligor.

The Obligor shall in its internal act prescribe conditions under which the authorized personnel are obliged to refuse entering into a business relationship or conduct of transaction with a client or cases that require written consent of the authorized person.

Monitoring Business Activities

Article 8

In the process of monitoring business relationship with a client, the Obligor shall reexamine grounds of the initial assessment of client's or business relationship risk and if needed shall determine a new risk assessment (subsequent determination of risk grade).

Monitoring from the paragraph 1 of this Article shall be performed:

- in case of average-risk clients – once a year or if the beneficiary is changed or after any amendments to the contract,

- in case of high-risk clients – at least once a year , but it is possible even more often depending on the assessment of the Obligor,

- in case of low-risk clients – examination whether the data used for classifying the client into this category have remained the same.

In subsequent determination of risk grade the Obligor shall especially take into consideration the following circumstances:

1. significant changes in circumstances that the assessment of client's or business relationship risk is based upon or change in circumstances that significantly affected classification of a certain party or a business relationship into a certain risk category,
2. reasons to doubt the authenticity of data that the assessment of client's or business relationship risk is based upon,

3. discrepancy between the data obtained in a repeated control and the initial data.

In case of existence of one or more circumstances from the previous paragraph of this Article the Obligor may classify the client into a higher risk category.

Exception from the Obligation to Review and Monitor the Client

Article 9

Exceptionally from the Article 4 of these Guidelines, the control of a client does not necessarily have to be performed when entering into a life insurance contract:

- if an individual installment of premium or multiple installments of insurance premium payable in one calendar year, in total do not exceed the amount of 1,000.00 €,
- if payment of a single premium does not exceed the amount of 2,500.00 € per year,
- with a low risk client according to these Guidelines.

Identification of Clients

Article 10

The Obligor shall establish identity of a client and collect data on the client and transaction (hereinafter referred to as the identification) in the manner prescribed by the Law before establishing a business relationship and exceptionally upon it, but not later than the moment when the insured could exercise its rights arising from the policy.

Documents that the data necessary for identification are determined upon shall not be older than three months.

In the event of serious doubts regarding the beneficiary's identity or in the event when a beneficiary could be assessed as a high risk client, the Obligor shall examine the identity by obtaining a duly certified client's written statement.

In case that despite the measures undertaken for identification of a client or the beneficiary owner of a client, which is a legal entity, the identification can not be determined with certainty, the Obligor may refuse to enter into such transaction.

Identity of Physical Entity and Transaction Data

Article 11

The Obligor shall verify identity of a client –physical entity by examining personal documents of a client issued by the relevant state authorities (identity card, travel document or another public document that the identity of a physical entity can undoubtedly be determined upon) in his presence and the following data shall be collected on such occasion:

- name and surname, date and place of birth, place of residence or place of temporary residence of such person,
- personal ID number and place of issuance, name of the authority issuing the identity document,
- unique citizen's civil registry number of physical entity that is opening an account or is performing a transaction, respectively on whose behalf an account is to be opened, a business relationship is to be established or a transaction is to be performed,

- name and surname, number of personal document, date and place of birth and place of issuance, as well as the unique citizen's civil registry number of the proxy if the business relationship is established in such a manner,
- type and purpose of the transaction,
- date that the business cooperation was established on,
- date and time the transaction was executed on,

In case of entering into a contract through an intermediary or a representative, the insurance company shall get in possession of documents that the intermediary/representative has collected and shall request for the first premium payment or the first premium installment to be paid through the client's account.

Identity of Legal Entity and Transaction Data

Article 12

The Obligor shall verify identity of a client – legal entity by examining the original or certified copy of document from the Commercial Court Central Registry (hereinafter referred to as the CCCR) or other adequate public registry, submitted by a representative on behalf of the legal entity and shall particularly define the following data:

1) name, address of the registered office and unique identification number of the legal entity establishing a business relationship or on whose behalf a business relationship is being established or a transaction is performed,

2) name of the person, place of residence or temporary place of residence, date and place of birth and unique identification civil registry number of the representative or authorized person, which is entering into a business relationship or performing a transaction on behalf of a legal entity or any other person entitled to civil rights, as well as the number and title of the authority issuing such personal document,

3) purpose and forecasted nature of business relationship, including information on the client's business activity,

4) date and time the transaction was executed on,

5) transaction sum and the transaction currency,

6) purpose of the transaction and name of the person, and place of residence or temporary place of residence or company and registered office of the person that the transaction is intended to,

7) manner of performing a transaction,

8) data on the source of assets and finances that were or are to be subject of a business relationship or a transaction,

9) existence of reasons that cause doubts regarding money laundering or terrorism financing.

In addition to data from the paragraph 1 of this Article the Obligor shall also in situations from the Article 4 paragraph 1 of these Guidelines obtain the following data on the beneficiary owner of the legal entity:

- name, residence address or temporary place of residence of the beneficiary owner,

- date and place of birth of the beneficiary owner of the legal entity,
- data on the category of person whose interest is the establishing and actions of legal entity or similar legal entity of foreign laws, in the case from the Article 19 paragraph 3 item 2 of the Law.

If the Obligor when establishing and verifying identity of a legal entity doubts the authenticity of obtained data or credibility of documents or other business documentation the data were obtained from, it shall also be obliged to procure a written statement from a representative or authorized person before establishing a business relationship or executing a transaction.

Representative's Identity

Article 13

If establishing a business relationship or undertaking a transaction by a representative or authorized person (proxy), the obligors shall verify identity of authorized person (representative, proxy) and the client on whose behalf and for whose account an account is to be opened or a transaction is to be executed and all of it solely on the basis of personal or other public documents, such as:

- a document issued in a prescribed form by a state authority within its competence or an institution and other legal entity having public authorizations entrusted by the Law, and
-a written authorization – power of attorney, certified by a notary, consulate, court or a state administration authority.

When establishing and verifying identity of a representative, the Obligor shall provide a written statement if doubting the authenticity of obtained data and especially in cases when:

- a written authorization (power of attorney) was given to a person who obviously is not closely related to the client (for example, family connections, business connections and similar) in order to execute transactions using the client's account;
- a client's financial status is known and the intended transaction does not correspond to his/her financial status;
-during business relationships with a client, some unusual transactions are noticed.
.

Politically Exposed Persons

Article 14

The Obligor shall establish an adequate procedure in order to ascertain whether a potential client or a beneficiary owner of the client is a politically exposed person under the meaning of the Article 27 of the Law.

The Obligor shall use the following sources in order to identify politically exposed persons:
a) a form that is to be filled in by the client,
b) information collected from public sources,
c) information obtained from accessing databases that include lists of politically exposed persons (*World Check PEP List*, Internet, etc.).

Procedure for identification of close associates of politically exposed persons shall apply if the relationship with the associate is publicly known or if the Obligor has reasons to believe that such relationship exists.

Before establishing a business relationship with a politically exposed person, person that is entering into a business relationship shall:

- obtain data on source of funds and assets that are subject to the business relationship or transaction from personal and other documents presented by the client and if prescribed data cannot be obtained from submitted documents the data shall be obtained directly by the client's written statement;
- obtain written consent of the direct supervisor before establishing business relationship with a client.

The consent from the paragraph 3 indent 2 shall be made in written form, printed or electronic, and it will not be necessary to obtain it for execution of each separate transaction on behalf and for the account of the client.

After establishing a business relationship with a politically exposed person, with members of his/her immediate family and with close associates, the Obligor shall keep special records on these persons and transactions which are to be undertaken on behalf and for the account of these persons.

Authorized person of the Obligor shall monitor with due care all business activities he/she performs with a politically exposed persons and if notices that circumstances related to usual business activities of the client have changed, he/she shall notify the authorized person on such transactions in the shortest possible time.

Obligors shall regularly update their lists of politically exposed persons and may expand them also to those clients that at the time when the business relationship was established had not been politically exposed persons within the meaning of the Law.

From the list of politically exposed persons the Obligor may delete only persons for whom at least one year has passed since the date when their term or the status that made them classified into this list had expired.

Obligors shall keep data on politically exposed persons in electronic form.

Record Keeping and Submission of Data

Article 15

Obligor or the Obligor's authorized person shall keep records and collect data and documents on all clients, other persons and transactions in relation to the activities undertaken pursuant to the Law and these Guidelines in written and electronic form and keep them at least ten years from the date of transaction execution or closing of business cooperation.

The Obligor shall promptly submit to the Administration the transaction data suspicious for money laundering and terrorism financing, which were collected in the process of establishing and monitoring business relationship with clients.

The Obligor shall provide the Insurance Supervisory Agency with access to all data, information and documentation collected in the process of establishing and monitoring business relationships with clients.

Data Protection

Article 16

The Obligor shall in its internal act define a procedure for protection of data in accordance with the Article 80 of the Law, as well as the obligation of all employees to treat all data they get in possession during their work in accordance with the Law.

Article 17

These Guidelines shall enter into force on the eight day upon their delivery to the Obligors.

FOR THE COUNCIL OF THE AGENCY

Veselin Popović

Pursuant to Article 30, paragraph 4 and Article 42 paragraph 6 of the Law on Insurance (Official Gazette of the Republic of Montenegro 78/06 and Official Gazette of Montenegro 45/12), the Ministry of Finance has adopted the

RULEBOOK

ON DETAILED REQUIREMENTS FOR LICENSING INSURANCE BUSINESS ACTIVITIES AND THE MANNER OF PROVING THE FULFILMENT OF SUCH REQUIREMENTS

Scope

Article 1

This Rulebook prescribes detailed requirements for licensing insurance business activities (hereinafter referred to as the license) and the manner of proving the fulfilment of such requirements.

Licensing Application for Insurance Companies

Article 2

Along with the documentation specified in Article 30 of the Law on Insurance (hereinafter referred to as the Law) the following shall be enclosed to the licensing application:

1) authorization for the person that the Insurance Supervision Agency (hereinafter referred to as the Agency) will cooperate with in the procedure of decision-making in respect of such application, which must include addresses and contact telephone and be signed by all founders and certified with the competent court, or by the seal of the founder-legal entity, unless the legal entity comes from the country where such manner of authentication is not common;
2) the decision on successfulness of the initial issue of shares not less than the value of equity referred to in Article 21 of the Law on Insurance, issued by the Securities Commission;
3) in case of a shareholder – a legal entity intending to acquire qualified holding:
   a) an extract from the register where the legal entity is registered, or ID or passport copy for a natural person having over 10% of capital or a voting right in such legal entity and data on the total nominal amount of shares and percentage of the share in the equity of the insurance company,

   b) completed questionnaires containing data on persons responsible for managing such an entity, including the data on their previous work experience;

   c) certificate of a competent authority that such entity and the persons managing such legal entity have not been unconditionally sentenced to imprisonment for the period exceeding three months for a crime against payment operations or a commercial crime, property crime or a criminal offence against call of duty;

4) in case of a natural person intending to acquire a qualified holding:
   a) a completed questionnaire containing data on such a person, including data on previous work experience of such a person;

   b) a bank account statement, a decision of a competent court regarding probate, or other

similar evidence of origin of the funds for purchase of shares;

c) ID card or passport copy;

d) certified copy of employment records file;

5) data on persons who are, according to Article 24 of the Law, related to qualified holders of shares as follows:

a) in case of a person related to qualified holders of shares to the level of a natural persons:

- in respect of capital – submitted is a certificate of the share in capital, an extract from the Central Depositary Agency (CDA) or relevant records regarding the number of owned shares, and other;
- in respect of management – submitted is the list of members of the Board of Directors, a decision on appointment of a member of the Board of Directors, and other;
- in other respects – submitted is other relevant evidence (contract of business association or other form of association, extract from adequate master citizens' registers, and other);

b) in case of market recognizable entities, relevant evidence of their listing on a stock exchange or rating, for entities included in the stock exchange listing or rated by internationally renowned rating agencies (Moody's, Standard and Poor's, Fitch);

c) in case of an entity that is a member of a group, submitted is the list of companies in the group, including their organisational structures and a description of the management system in the group;

6) list of persons proposed for members of the Board of Directors and the executive director, with the following evidence:

a) a completed questionnaire for the persons proposed for members of the Board of Directors or Executive Director, including data on their previous work experience;

b) ID card or passport copy;

c) a certified copy, or transcript of a university diploma in economics, law, organizational, or technical field,

d) a copy of employment records file, an extract from relevant records, an employment contract, a decision on assigning to relevant tasks,

e) a recommendation from a previous employer regarding demonstrated special expertise and skills in rational business judgement and decision-making, successful performance of managing activities and good business reputation;

7) data on the person to carry out the activities of an authorised actuary, as follows:

a) ID card or passport copy,

b) CV, including particularly the data on previous work engagement and experience, successful performance of activities relevant for the function of an authorised actuary of the company and the data if such person has already performed the function of an authorised actuary with

another legal entity and if so which, and if such person has been released from duty of an authorised actuary prior to the expiry of the term of office due to failure to act in line with the obligations of the function of an authorised actuary;

c) a certified statement of such a person that he/she has met the requirements stipulated in Article 48 of the Law;

d) a copy of the decision on acquiring the title of an authorised actuary.

A certificate by a competent authority regarding the data from penal records or relevant tax authority that is to be enclosed to the application referred to in paragraph 1 of this Article may not be older than six months.

Proposed insurance conditions, premium tariffs and other acts of business policy referred to in Article 39 of the Law, which make an integrated part of the documents that are submitted along with the application referred to in paragraph 1 of this Article, are submitted along with the authorised actuary's opinion, produced in line with the Rulebook regulating the contents of the opinion of an authorised actuary.

Work experience of the persons who are the members of management bodies (members of the Board of Directors and Executive Directors) is deemed to include work experience of at least three years in managing an insurance company or other business organisation which is by size and business activity comparable to an insurance company for which the license is sought, or such experience in managing other comparable tasks relevant for performance of managing activities in an insurance company.

The questionnaires referred to in paragraph 1 item 3 sub-item b, item 4 sub-item a and item 6 sub-item a of this Article are given in Schedule 1 and Schedule 2 that make an integrated part of this Rulebook.

Organisational, Human Resources and Technical Capabilities

Article 3

Along with the licensing application for insurance business activities, the following is enclosed as evidence of organisational and human resources capability:

1) act on internal organisation and systematisation of work places,
2) decision on business unit organisation,
3) Rulebook on internal audit performance,
4) other acts regulating internal functioning of the insurance company.

In terms of paragraph 1 of this Article, organisational capability is deemed to include establishment of such organization that facilitates successful performance of activities of the company in the scope and in the manner as stipulated by the Law, business plan and business policy acts of such company.

In terms of paragraph 1 of this Article, human resources capability is deemed to include the relevant qualification structure of employees with required work experience for each work place, as well as the planned schedule for staffing the systematized positions that needs to accompany the planned increase of the scope of operations and the expansion of the organizational network of the company in the fashion that enables continuous fulfilment of all legal obligations of the company.

To prove technical capability of the insurance company, in addition to the application referred to in paragraph 1 of this Article, enclosed are the deed of title, certified lease contracts, contracts on assignment of rights to use, leasing contracts and other, that evidence:

a) ownership or right to use in other respect the business premises for performance of insurance activities, which meet the requirements for performance of such activities as prescribed by the local self-government authority and facilitates adequate performance of activities in line with the business plan;

b) possession of computer and other equipment and software application support for performance of insurance activities that are in terms of the scope and technical specifications adequate to the number of employees and the planned scope of operations of the company and are compatible with the standard requirements for equipment and software applications used in the information system for the insurance sector.

Financial Position and Stability

Article 4

Financial position and stability of applicants – persons intending to acquire qualified holding will be assessed by the Agency based on the submitted reports, or consolidated financial statements including the authorised auditor’s opinion for the last three years, based on which the Agency establishes if its performance in the previous three years has been successful and stable, if it enables acquiring of the requested level of qualified holding in the insurance company, and if the manner of financing of the qualified holding threatens ordinary operations of the party intending to acquire the qualified holding.

Licensing Application for Branches of Foreign Insurance Companies

Article 5

The provisions of Article 2 paragraph 1 items 1, 6 and 7 and paragraphs 2 to 6 and Article 3 of this Rulebook shall be accordingly applied to the application of a foreign company for licensing of its branch.

Transitional and Final Provision

Article 6

As of the day this Rulebook enters into force, the Rulebook on Detailed Requirements for Licensing Insurance, Brokerage and Agency Activities, and Provision of Ancillary Insurance Services, and the Manner of Proving the Fulfilment of such Requirements (Official Gazette of the Republic of Montenegro 8/07) shall be rescinded.

Article 7

This Rulebook shall enter into force on the eighth day after its publication in the Official Gazette of Montenegro.

Number: 02-3131/1

Podgorica, 13 March 2013

Minister

Radoje Žugić, PhD, m.p.

MONTENEGRO

SECURITIES AND EXCHANGE COMMISSION
Number: 01/9-193/1-12
Podgorica, 9 February 2012

DRAFT

GUIDELINES

for risk analysis aimed at preventing money laundering and terrorist financing for capital market participants

Prepared by:

Azra Šehović

Marina Mugoša

MONTENEGRO

SECURITIES AND EXCHANGE COMMISSION

GUIDELINES

for risk analysis aimed at preventing money laundering and terrorist financing for capital market participants

February, 2012

Pursuant to Article 8, paragraph 3 of the Law on Prevention of Money Laundering and Terrorist Financing ("Official Gazette" Nos. 14/07 and 4/08) - (hereinafter referred to as: the Law) and Article 2, paragraph 1 of the Rulebook on drafting guidelines on risk analysis aimed at preventing money laundering and terrorist financing ("Official Gazette of MNE" no. 20/09), and exercising the powers under Article 86 of the Law, Securities and Exchange Commission (hereinafter: the Commission), at its 296th session of February 9, 2012 has adopted

GUIDELINES

for risk analysis aimed at preventing money laundering and terrorist financing for capital market participants

1. These Guidelines establish specific criteria for making internal documents on risk analysis aimed at preventing money laundering and terrorist financing at authorized participants in the capital market, management companies of investment and pension funds and investment funds, custodians and depository banks and other entities dealing in securities as their professional activity (hereinafter referred to as: capital market participants).

2. **The risk of money laundering and terrorist financing**

In the context of Article 2 of the Law, the following shall, in particular, be considered as money laundering:

1) conversion or other transfer of money or other property originating from criminal

activity;

2) acquisition, possession or use of money or other property proceeding from criminal

activity;

3) concealment of the true nature, origin, depositing location, movement, disposition,

ownership or rights concerning money or other property originating from criminal

activity.

In the context of Article 3 of the Law, the following shall, in particular, be considered as terrorist financing:

1) providing or collecting or an attempt of providing or collecting money or other property,

directly or indirectly, with the aim or in the knowledge that they are to be used, in full or

in part, in order to carry out a terrorist activity or used by a terrorist or terrorist

organization;

2) encouraging or assisting in providing or collecting the funds or property referred to in item 1 of this Article.

The risk of money laundering and terrorist financing, in the context of Article 5 item 5 of the Law shall mean the risk that a client will use the financial system for money laundering or terrorist financing, or that a business relationship, a transaction or a product will indirectly or directly be used for money laundering or terrorist financing.

3. Risk analysis aimed at preventing money laundering and terrorist financing

A capital market participant shall prepare and adopt an internal document on risk analysis aimed at preventing money laundering and terrorist financing, pursuant to Article 8 paragraph 1 of the Law.

A capital market participant is obliged, upon the adoption of internal documents on risk analysis aimed at preventing money laundering and terrorist financing, to appoint a person (hereinafter referred to as: authorized person) and his/her deputy in accordance with the Law, who will perform duties prescribed by the Law and these Guidelines.

The authorized person and his/her deputy must be persons who fulfill conditions referred to in Article 36 of the Law. Information on the authorized person and his/her deputy shall be submitted to the Commission latest within 15 days of adoption of the appropriate decision.

3.1. Identification of a client

A capital market participant is obliged to identify a client prior to establishing a business relationship in the context of Article 7 of the Law.

A person who receives the order on behalf and for the account of a capital market participant is obliged to carry out identification of the client (employed in the *''back office'').*

3.1.1. Identification of a natural person

A capital market participant is obliged to verify and identify the client's identity of a natural person by inspection of the client's identity document issued by the competent public authority (ID card, passport or other official document upon which the identity of a natural person may be undoubtedly verified), in the client's presence and in this respect shall obtain the following information:

- name and surname, date and place of birth, residence or place of residence, identity document number and place of issue, status and name of the authority which issued the identity document as well as a unique master citizenship number and tax identification number of the natural person who opens the account, establishes a business relationship or executes a transaction;
- name and surname, date and place of birth, residence, identity document number and place of issue, a unique master citizenship number of a legal representative who opens the account on behalf of another person, establishes a business relationship or executes a transaction;
- account opening date or establishing a business relationship;
- the nature and purpose of the transaction;
- date and time of transaction execution;
- the amount of the transaction
- type and manner of transaction execution.

A capital market participant may refuse the establishment of a business relationship with the client if the client's identity cannot be determined with sufficient certainty.

3.1.2. Identification of a legal person

A capital market participant is obliged to establish and verify the identity of the client / legal person, i.e. his/her legal representative by inspection of the original or certified copy of the

document from the Central Register of the Commercial Court (hereinafter: CRCC) or other

appropriate public register, submitted by an agent on behalf of a legal person, which may not be older than three months.

A capital market participant may establish and verify the identity of a legal person and obtain data from Article 71 item 1 of the Law by checking CRCC or other appropriate public register. On the register excerpt that has been checked, a capital market participant shall indicate date and time and the name of the person who inspected the document thereof. A capital market participant shall keep the excerpt from the register in accordance with the Law.

A capital market participant shall obtain data from Article 71 items 2, 7, 9, 10, 11, 12, 13 and 14 of the Law by inspection of the originals or certified copies of documents and other business documentation. If data cannot be determined by checking identifications and documentation, the missing data shall be obtained directly from an agent or authorized person through inspection of documents and business documentation which shall be submitted by a legal representative. If the missing data are not possible to determine in the prescribed manner for objective reasons, the employee shall establish the missing data based on a written statement obtained from the authorized person.

Should a capital market participant, during establishing and verifying the identity of a legal person, have doubts as to the accuracy of the obtained data or veracity of identification and other business documentation from which the data have been obtained, he/she is obliged, prior establishing of a business relationship or transaction execution, to obtain a written statement from a legal representative or an authorized person.

Capital market participants may refuse the establishment of a business relationship with a client or execution of a certain transaction if, despite taking measures referred to in this Article there are still serious doubts regarding the identity of the actual client.

Identification of the client- legal person shall encompass:

- company, registered office, address, legal person ID number, tax identification number (hereinafter referred to as: TIN) of a legal person opening the account, establishing a business relationship or exercising a transaction, i.e. on whose behalf the account is opened, a business relationship established or transaction executed;
- account opening date or establishing a business relationship;
- the nature and purpose of the transaction;
- date and time of transaction execution;
- the amount of the transaction;
- manner of transaction execution.

During identification, in the context of this Article, capital market participants shall take the following actions:

a) before establishing a business relationship or executing a transaction, establish and verify the identity of the client as well as the identity of the beneficial owner based on documents, data and information by means of which the identity can be reliably and indisputably established;

b) take measures that will enable verification and establishment of the ownership structure of the client and the actual control over the client in order to determine the identity of the beneficial owner of the client;

c) obtain and keep records and documentation upon which the identity and risk factor of the client is determined;

d) continuously monitor the business relationship with the client, including transactions during this relationship (do transaction correspond to the type of business and risk of the client as well as to the information about the client), and documentation on monitoring of business relationship;

e) if possible, and before establishing a business relationship with the client, determine reasons due to which the client terminates contractual relationships with other capital market participant;

f) in the course of transactions of the client who has been identified, and using technologies that do not involve direct contact, apply the procedures that allow previous verification of authenticity and accuracy of the transaction orders and the authenticity of their applicant.

3.1.3. Identification of a legal representative or authorized person

When establishing a business relationship or undertaking transaction by a legal representative or authorized person (proxy), capital market participants are required to carry out identification of the authorized person (agents, proxies) and the client on whose behalf and for whose account the account is opened or transaction is executed exclusively based on personal or other public documents, such as:

- Documents issued in a prescribed form by a public authority within its competences, i.e. by an institution or other legal person within public authorization entrusted by law, as well as written authorization - power of attorney, certified by a notary, consulate, court or public administration bodies.

If the obliged entity, when establishing and verifying identity of an agent, doubts the accuracy of the obtained data, especially in cases when:

- there is a written authorization (authorization) was granted to a person who obviously does not have very close ties (e.g. kinship, business, etc.) with the client to perform transactions using the client's account;
- the client's financial situation is already known and funds in the account of the client

or funds in connection with that account do not match its financial status;

- in the course of business relationship with the client, notices any unusual transactions, it is obliged to obtain his/her written statement.

A capital market participant may refuse the establishment of a business relationship with a client or execution of a certain transactions if, despite taking the above measures, there are still serious doubts about the identity of the actual client.

3.1.4. Identification of a beneficial owner of a legal person

A capital market participant is also obliged, during inspection and check of the client who is a legal person, to establish the beneficial owner of such legal person.

Beneficial owner of a business organization, i.e. legal person referred to in Article 19 of the Law shall be:

(1) a natural person who indirectly or directly owns more than 25% of the shares, voting rights and other rights, on the basis of which he/she participates in the management, or owns more than a 25% share of the capital or has a dominating influence in the assets management of the business organization, and
(2) a natural person that indirectly ensures or is ensuring funds to a business organization and on that basis has the right to influence significantly the decision making process of the business organization's management company when decisions regarding financing and business are made.

Also, a business organization, legal person, as well as an institution or other foreign legal person that is directly or indirectly a holder of at least €500,000 of shares, i.e. capital share.

As a beneficial owner of an institution or other foreign legal person (trust, fund and the like) that receives, manages or allocates assets for certain purposes, in the context of the Law, shall be

considered:

1) a natural person, that indirectly or directly controls more than 25% of a legal person's assets or of a similar foreign legal entity;

2) a natural person, determined or determinable as a beneficiary of more than 25% of the income from the managed property.

A capital market participant may obtain data on ownership based on the original or certified copy of the court register excerpt or other official registry filed by a legal representative or an authorized person on behalf of the legal person. In addition, a capital market participant may apply provisions of the Law that allow data linked to beneficial owner to be obtained by a direct verification in the court register or other public register, or through other available sources.

If all prescribed data related to a beneficial owner (e/g. date and place of birth) cannot be obtained from the court register or other official register, a capital market participant may obtain the missing data from a written statement submitted by a legal representative or his/her authorized person. A capital market participant will also require a written statement from a legal representative if there is a doubt about the authenticity of submitted data.

A capital market participant must establish ownership structure for clients that are legal persons and obtain all necessary information regarding the beneficial owner, in accordance with the Law.

A capital market participant may refuse to establish a business relationship with the client, if, regardless the submitted documents, there are still serious doubts about the identity of the client.

3.2. Client acceptance policy

Capital market participants are obliged to establish by their internal document risk factors act based on which the level of client's risk, business relationship, transaction, i.e. product or service is determined before establishing a business relationship.

3.2.1. Risk factors

A capital market participant is required to determine risk factors based on which the level of risk of the client, business relationships and transactions are determined, and at least four of them, such as: geographic risk, client's risk, transaction risk and services risk.

3.2.1.1. Geographic risk

Factors, based on which it is determined whether a certain country or geographic area carries a higher risk of money laundering and terrorist financing, include:

(a) countries which are subject to sanctions, embargoes or similar UN measures;
(b) countries which are identified by the Financial Action Task Force - FATF or other credible international organizations, as those that finance or provide support to terrorist activities, as well as those which have certain terrorist organizations operating in it;
(c) countries labeled by the FATF or other credible international organization, as countries that lack internationally recognized standard for prevention and detection of money laundering and terrorist financing;
(d) countries that are, based on the competent international organizations' assessment, labeled as countries with a high level of organized crime due to corruption, arms trafficking, human trafficking or human rights violations;
(e) countries that are, according to the assessment of international organizations (FATF, the Council of Europe, etc.), classified among non-cooperative countries or territories;
(f) countries that are off-shore regions.

3.2.1.2. Client risk

A capital market participant shall establish clients that present high risk, such as:

(a) clients whose funding source is unknown or unclear, i.e. which cannot be proved by the client;
(b) clients who are suspected of not acting on their own behalf, i.e. carrying out the instructions of a third party;
(c) clients who entrusted actions and measures of knowledge and monitoring of client's operations to a third party;

(d) clients that perform their business activity or execute transactions under unusual circumstances, especially taking into account its ground, the amount and manner of execution, purpose and similar or, which means the following:

- significant and unexpected geographical distance between location of the client and capital market participants, in which the client establishes a business relationship or executes a transaction;
- frequent and unexpected establishment, without economic justification, of similar business relationships with more participants in the capital market, such as opening of accounts with several capital market participants, entering into a number of agreements for mediation in a shorter period of time, etc;
- frequent transfers of funds from one fund to another;
- termination of membership immediately after the conclusion of a membership contract;
- request to transfer funds accumulated on the individual account of a fund member to a current account of a third person, or to an account in the country that does not apply strict AML standards
- insisting on the secrecy of a transaction and similar.

(e) clients where, owing to the structure, legal form or complex and ambiguous relationships, the nature of the relationship or transactions makes it difficult to identify the beneficial owners, such as off-shore legal persons with unclear ownership structure and not founded by the company from a country that adheres to standards for the prevention of money laundering and terrorist financing comparable to the standards stipulated by the Law;

(f) clients that do not apply standards in the field of prevention of money laundering and terrorist financing;

(g) clients (natural or legal persons) that are registered on the list of persons against whom United Nations or the Council of Europe measures are in force;

(h) clients residing or having a registered office in the entities that are not subject to international law, i.e. not internationally recognized as states (such entities provide the possibility of fictitious registration of legal person, enable issuance of fictitious identification documents and the like);

(i) clients represented by persons who do such activity (lawyers, accountants or other professional representatives), especially when a capital market participant has contact with the agents only;

(j) firms with disproportionately low number of employees compared to their scope of work performed, which do not have their infrastructure, business premises, etc;

(k) private investment funds;

(l) persons whose offer to establish a business relationship was rejected by another obligor, regardless of the manner in which the fact was learned of, i.e. disreputable persons;

(m) a client is a politically exposed person in the context of Article 72 of the Law;

(n) a client is a foreign legal person not performing or prohibited from engaging in trading, production or another activity in the state where it is registered (this is the case of a legal person having its registered office in the state known as an off-shore financial center, and for which certain restrictions apply regarding the performance of registered activity in the state);

(o) a client is a fiduciary or other similar organization of a foreign company with unknown or concealed owners or management;

(p) a client has a complex status structure or a complex ownership chain (complex ownership structure or a complex ownership chain hindering determination of client's real owner, and/or person that indirectly provides assets based on which it can exercise supervision and which can be directed, or in other ways significantly influence the directors' decision-making process considering finances and operations);

(q) a client which, in performing its activities should not, or which is not required to be licensed by a relevant supervisory authority for performance of its activities, and/or pursuant to the national legislation is not subjected to the measures that apply in the field of detecting and preventing money laundering and terrorist financing;

(r) a client is a non-profit organization (institution, company or other legal person, i.e. entity which does not perform economic activities) and meets one of the following conditions: has a registered office in a country known as an off-shore financial center, has a registered office in the state that is not a signatory to the Treaty on European Union; among its members or founders there is a natural or legal person who is a resident of any of states that have their registered office in the state that is not a signatory to the Treaty on European Union;

(s) a client is a foreign legal person established using bearer shares.

3.2.1.3. Transaction risk

The following transactions shall be considered as a transaction risk:

(a) transactions that substantially deviate from the standard way of executing the transaction;

(b) transactions with no economic justification;

(c) transactions conducted in a way avoiding standard and usual control methods;

(d) transactions involving several parties without an apparent economic purpose, several mutually connected transactions executed over a short period of time or in several

consecutive intervals, under the designated thresholds for transactions reported to the Administration;

(e) loans to legal persons and, in particular, loans from founders from a foreign country to a legal person in the country;

(f) Transactions where it is obvious that the client is trying to conceal the true cause and reason for the transaction;

(g) payment for services for which there is no market value or determinable price;

(h) transactions where the client refuses to provide documentation;

(i) transactions where the documentation does not match the manner of execution of the transaction;

(j) transactions where the source of funds is unclear or their relationship with the client's business operation cannot be determined;

(k) Announced block transactions in shares, especially when including newly-formed companies or companies registered in off-shore destinations that appear as buyers;

(l) Trading in shares on a regulated market, which were the subject of lien following the loans to share owners;

(m) Service payments to client's partners coming from the off-shore destinations and where the documentation clearly shows that the funds come from the countries in the region;

(n) Transactions intended for persons, i.e. entities against which there are measures in force introduced by the United Nations or the Council of Europe;

(o) Transactions which a client would execute for and on behalf of the person or entity against which there are measures in force introduced by the United Nations or the Council of Europe;

Some other transactions entailing high risk of money laundering and terrorism financing include:

- payment of funds from the client's account, i.e. payment of funds on the client's account other than the client's account stated when the client was identified, i.e. it usual business account (especially when involving international payments – transactions);
- transactions intended for persons domiciled or registered in a state known as an off-shore financial center;
- transactions intended for non-profit organizations having registered office in a country known as off-shore financial center.

3.2.1.4. Service risk

Service risks relates to the following risky services:

a) services that are new in the market, i.e. which were not previously offered in the financial sector and must be monitored separately in order to determine the actual risk level;
b) electronic placement of orders for trading in securities in the cases established by obligor's procedures;
c) provision of services to persons when there is no previously established business relationship within the meaning of the Law (those kinds of services for which the employee in a capital market participant, based on his/her experience estimated to carry a high risk level);
d) provision of services by opening of the so-called omnibus accounts the assets credited to which come from different sources, belong to several clients but are recorded to one account in the account-provider's name;
e) payment of funds to earmarked accounts, and it is not certain that the service will be conducted;
f) services entailing high ML/FT risk include all bearer negotiable instruments, but also negotiable instruments that are either in bearer form, made out to a fictitious payee, endorsed without restriction, or otherwise in such form that title thereto passes upon delivery and all other incomplete instruments signed, but with the payee's name omitted.

A capital market participant, besides the above mentioned risk factors, based on which the risk level of the client, business relationships and transactions are determined, may also determine other risk factors.

3.2.2. Risk categories

Capital market participants, depending on the above mentioned risk factors, classify clients into the appropriate risk categories, such as low risk, average risk and high risk clients.

Low-risk category includes:

- state authorities, local government bodies and other legal persons that exercise public functions;
- companies whose securities are admitted to trading in EU member states or other countries where EU standards are applied to stock exchanges;
- persons referred to in Article 4, paragraph 2, items 1, 2, 4, 5, 6, 8, 9 of the Law, or other appropriate organization having registered office in the EU or in the state from the list established by the Ministry of Finance;
- clients referred to in Article 8 paragraph 4 of the Law, having insignificant risk of money laundering and terrorist financing.

The average risk category includes clients that cannot be classified into low risk and high risk category, and in which a capital market participant, during monitoring of its operations, established deviation from its usual business activities.

High risk category of a client, business relationships and transactions includes the risks referred to in 3.2.1.1., 3.2.1.2, 3.2.1.3. and 3.2.1.4.

When a capital market participant faces situations that represent a high risk of money laundering or terrorist financing, it will take enhanced measures of inspection and monitoring as set out in Articles 26-28 of the Law, as well as the measures that follow:

- visiting the address provided by the client;
- requesting additional documents and information from the client;
- gathering information by the other client;
- checking the Internet;
- gathering information on funds' source;
- determination of client's activities by visiting its production and administrative capacities or by gathering information from its partners;
- other measures that a capital market participant deems necessary.

3.3. Assessment of client's risk

A capital market participant is obliged, in addition to client's identification, to take measures of inspection and monitoring of the client set out in Article 9 of the law, and especially:

a) to open a securities account or establish other forms of business cooperation with the client;
b) take into account any transaction or several interrelated transactions in the total amount of EUR 15.000 or more;
c) where there is a doubt about the accuracy or validity of obtained data on customer identification;
d) on each transaction, regardless the value of the transaction, there is a suspicion of money laundering or terrorist financing in connection with the transaction or the client.

Measures that a capital market participant is obliged to carry out in the procedure of inspection and the monitoring of the client are as follows:

• identification of the client and a beneficial owner, if the client is a legal person;

• obtaining verification of information about the client or beneficial owner, if the client is a legal person, obtaining information on the purpose and nature of the business relationship or transaction, and

• after establishing a business relationship, a capital market participant shall regularly monitor business activities of the client and verify the compliance of these activities with the nature of business relationship and the usual scope and the type of client's operations.

Simplified and enhanced customer due diligence

In addition to the identification and a customer due diligence, a capital market participant is required to conduct special forms of inspection of the client, such as: enhanced customer due diligence (politically exposed persons and establishing of the identity of the client in absentia) and simplified customer due diligence.

3.3.1.1. Enhanced due diligence

a) Client as a politically exposed person

In order to establish the politically exposed persons and members of their immediate families and close associates within the meaning of the Law, capital market participants may proceed in one of the following manners:

- by completing a written form by the client;
- by gathering information from public sources;
- by gathering information based on insight into databases that include lists of politically exposed persons *(World Check PEP List,* etc.).

The process of establishing close associates of politically exposed persons shall apply if a relationship with an associate is publicly known or if a capital market participant has reasons to believe that such relationship exists.

Before establishing a business relationship with politically exposed person, a capital market participant is required to:

- obtain information about the source of funds and assets that are subject of a business relationship. i.e. transaction, from personal and other documents submitted by the client, and if the required data cannot be obtained from the submitted documents, the same shall be obtained directly from the client's written statement;
- obtain the written consent of the person responsible, in accordance with the internal acts of a capital market participant, before establishing a business relationship with the client.

The consent of the responsible person referred to in paragraph 3, indent 2 shall be given in writing, in print or electronic form.

After establishment of a business relationship with politically exposed person, members of his/her immediate family and close associates in accordance with the Law, a capital market participant is obliged to keep separate records on these persons and transactions undertaken on behalf and for the account of these persons.

After obtaining the approval from the authorized person it is not required to obtain approval for execution of each separate transaction on behalf and for the account of the client, however a capital market participant is obliged to monitor with particular attention transactions and other business activities that are carried out in the organization by a politically exposed person, and, where applicable, inform the authorized person on these transactions in the shortest possible period of time. It is considered that the need referred to in paragraph 6 of this Article exists, if the transaction is not in accordance with the source of funds on client's account.

A capital market participant is required to regularly update its list of politically exposed persons as to conduct the process of enhanced customer due diligence in accordance with the Law and for those clients who, at the time of entering into a business relationship, have not been politically exposed persons within the meaning of the Law.

A capital market participant is obliged is obliged to keep data on politically exposed persons both in written and electronic form.

b) Establishing the identity of the client in absence

In establishing and verification of the client in absentia, and pursuant to Article 28 of the Law, a capital market participant is obliged, within enhanced customer due diligence, in addition to identification referred to in Article 7 to undertake one or more additional measures such as:

• to obtain additional documents, data or information, on the basis of which he/she verifies

customer identity;

• to verify submitted documents or obtain a certificate from a financial institution

performing payment operations, that the first customer's payment has been made on the

account opened with that relevant institution.

3.3.1.2. Simplified customer due diligence

A capital market participant, in the context of Article 29 of the Law, may conduct a simplified customer due diligence that is:

- state body or local governance body and other legal persons exercising public powers;
- organizations whose securities are included in the trade on the regulated market in the EU member states or in other states where the EU standards are applied on the stock

  exchanges;

- persons referred to in Article 4 paragraph 2 items 1, 2, 4, 5, 6, 8 and 9 of the Law or other appropriate institution that has a registered office in the EU or in a state from the list established by the Ministry of Finance;
- clients referred to in Article 8 paragraph 4 of the Law, for whom there is an insignificant risk of money laundering and terrorist financing.

3.4. Supervision over the accounts and transactions of the client

A capital market participant is required to continuously supervise the accounts and transactions of the client in order to prevent money laundering and terrorist financing. A capital market participant can effectively control and reduce the risk only if there is information on business operations of the client in order to identify transactions in accordance with the client's profile. In this sense, a capital market participant shall establish appropriate procedures for regular and careful monitoring of client's business activities, where the scope and applied measures shall be in accordance with the client's risk profile. A capital market participant should especially pay attention to all complex, unusual large transactions and all unusual types of activities that have no apparent economic or lawful purpose. The subject of intensive monitoring shall be the accounts and transactions associated

with clients who are classified into the high risk category for which a capital market participant defines key indicators, such as the origin of funds, type of activities, place of business and other.

A capital market participant shall perform supervision over the accounts and transactions at**:**

- low risk clients – not less than once a year;
- average risk clients – not less than twice a year;
- high risk clients – not less than quarterly.

3.5. Management of risks to which a capital market participant is exposed regarding anti-money laundering and terrorist financing

A capital market participant shall, in accordance with the Law, continually manage the risk of money laundering and terrorist financing, to which it is exposed in its operations, and which aims to identify those areas of business that are, considering the possibility of money laundering and terrorist financing, more or less critical, i.e. a capital market participant shall itself determine main risks in these areas and measures to address them.

The system for management of risk of money laundering and terrorist financing shall as a minimum include:

- developed processes for risk management;
- clearly defined authorities and responsibilities for risk management;
- efficient and reliable system of information technology;
- the method and dynamics of reporting and informing the management of a capital market participant on risk management.

System for management of risk of money laundering and terrorist financing shall provide:

- risk identification;
- risk assessment;
- monitoring and analyzing the risk;
- risk control;
- taking measures and minimizing the risks;
- reporting to supervisory authorities.

3.6. Professional education and training of capital market participant's employees

A capital market participant should provide regular training and education of employees, as well as newly employed who, directly or indirectly, perform activities of anti-money laundering and terrorist financing. Professional training of employees regarding prevention of money laundering and terrorist financing includes knowledge of regulations in this area, internal regulations and policies adopted by a capital market participant. A capital market participant should keep adequate records of staff training (courses, workshops, seminars).

3.7. Record keeping and submission of data

In order to enable accurate and timely submission of data to the Administration for the prevention of money laundering and terrorist financing in accordance with the Law, a capital market participant is required to keep records and safeguard documentation on all persons and transactions and shall keep data and documentation related to the opening of accounts, establishing business cooperation, as well as executing a transaction or a client, in written and electronic form and to safeguard the same for at least ten years following the date of execution of the transaction or termination of business cooperation.

The authorized person of the capital market participant daily makes and in written and electronic form keeps separate records on persons and transactions that exceed the amount of EUR 15,000.

Daily reviews of persons and transactions shall be submitted on a monthly basis to a responsible person of a capital market participant, up to the fifth day of the month for the previous month.

A capital market participant shall deliver without delay the data on transactions suspected to indicate money laundering or terrorist financing occurring in the course of its activities as well as on transactions that have already been completed to Administration for prevention of money laundering and terrorist financing.

3.8. Prohibition on disclosure of data and information

Data and information about the transactions which a capital market participant finds in the implementation of the Law and documentation relating to suspicious transactions and the accompanying documentation shall be considered confidential and kept separate from other data and documentation in accordance with the Law.

A request for granting a permit for access to restricted data shall be submitted to the authorized person of the capital market participant that is obliged to decide upon the request in the shortest possible period of time and in accordance with the conditions prescribed by the Law.

1. Capital market participants are obliged to prepare/comply their internal documents with these Guidelines and conduct other activities necessary for ensuring the application of these Guidelines within the period of 60 days following the date of their publication.

2. Instruction on risk analysis of money laundering, „know your client" procedures and other procedures for recognizing suspicious transactions of 11/28/2008 shall cease to be valid on the date of entry into force of these Guidelines.

3. These Guidelines shall come into force on the date following the date of their publication on the website of Montenegro Securities and Exchange Commission.

PRESIDENT OF SECURITIES AND EXCHANGE COMMISSION

Zoran Đikanović, P

MONTENEGRO

SECURITIES AND EXCHANGE COMMISSION

Number: 01/9-879/1-11

Podgorica, 29/04/2011

PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING INSPECTION GUIDE

April, 2011

I Introduction

Preventing money laundering and terrorist financing inspection guide (hereinafter referred to as: the Guide) provides instructions to employees in the Securities and Exchange Commission (hereinafter referred to as: the Commission) for conduction of inspection to prevent money laundering and terrorist financing (hereinafter referred to as: AML/TF) in capital market participants.

The Guide describes inspection principles, as well as standard methodology for planning, management, enforcement, recording and reporting on AML/TF inspection progress. It shall be applied exclusively during inspection related to money laundering and terrorist financing in accordance with the Law on Prevention of Money Laundering and Terrorist

Financing („Official Gazette of Montenegro“, Nos. 14/07 and 14/08) and Instruction

on risk analysis of money laundering, „know your client” procedures and other procedures for recognizing suspicious transactions. However, the Guide serves as the assistance for the examiners to bring conclusions on risk management regarding AML/TF issues in the capital market participant that is subject of inspection.

The Guide was prepared by the Securities and Exchange Commission with the assistance of EU member states' experts and within the framework of the Twinning project under the name *Strengthening* the *Regulatory and Supervisory Capacity* of *Financial Regulators* - IPA 2008 MONTENEGRO.

The Commission shall regularly make audit of this Guide and, if necessary, make changes and amendments within its content in case of changes in legal provisions, international standards development and best practices.

The Guide has been adopted at the Commission's 254th session held on April 29, 2011.

Description

Inspection of capital market participants is prescribed by the Law on Securities and by by-laws.

Requests for anti money laundering and terrorism financing are defined by the Law on Anti Money Laundering and Terrorist Financing ("Official Gazette of Montenegro", No. 14/07) – (hereinafter referred to as: the Law).

The Commission adopted Instruction on risk analysis of money laundering, „know your client” procedures and other procedures for recognizing suspicious transactions (hereinafter referred to as: the Instruction) on November 28, 2008.

The Instruction, among other things, regulates detailed requirements for adopting procedures of capital market participants regarding recognition of suspicious transactions at the capital market.

During inspection of compliance of capital market participants with regulations, examiners should refer to the Law and Instructions.

Money laundering

Article 2 of the Law prescribes that, within the meaning of this Law, the following, in particular, shall be considered as money laundering:

1) exchange or other transfer of money or other property derived from criminal activity;
2) acquisition, possession or use of money or other property derived from criminal activity;
3) concealing the nature, origin, place of deposit, movement, disposition, ownership or rights related to money or other property derived from criminal activity.

Money laundering is done in a way to conceal the sources, change form or moving the funds to a place where they are less likely to attract attention.

Money laundering process usually involves three stages, during which there may be numerous transactions that could attract the attention of capital market participants to money laundering:

a) Placement - physical disposal of cash proceeds derived from illegal activity;

b) Layering - separating illegal proceeds from their source by creating complex layers of financial transactions in order to disguise the audit trail and providing anonymity;

c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be normal business funds.

Terrorist Financing

In the context of this Law, Article 3, the following shall, in particular, be considered as terrorist financing:

1) providing or collecting or an attempt of providing or collecting money or other property, directly or indirectly, with the aim or in the knowledge that they are to be used, in full or in part, in order to carry out a terrorist activity or used by a terrorist or terrorist organization;
2) encouraging or assisting in providing or collecting the funds or property from the item 1 of this Article.

Terrorism is primarily intended with the purpose of intimidating a population or compelling a Government to abstain from performing certain proceedings by using threat of violence, damaging buildings, endangering lives, serious risks to health or safety of residents or interruption of key public services or infrastructure. As with other criminal organizations, terrorist organizations require financial support to achieve those goals. They develop sources of funding, resources for money laundering / hiding assets or their origin and ways of ensuring that funds can be used to obtain material and other logistical items needed to commit terrorist acts.

Sources of terrorist financing can originate from both legal (e.g. paid membership dues, donations, business operations, etc.) and illegal sources (e.g. from criminal activities such as kidnapping, extortion, fraud and drug trafficking, etc.). Terrorist financing involves amounts that are not always large, and the associated transactions may not necessarily be complex given that some sources of terrorist funds may be legitimate. However, the methods used by terrorist organizations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organizations to launder their funds. Even where the funds are derived from legitimate sources, terrorist organizations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organization and the funds.

Prevention of terrorist financing is prescribed by the Law and appropriate regulations on penalties, United Nations Security Council resolutions, European directives and notifications of the FATF.

Risk-based approach:

Risk-based approach is an important reference in the legal and regulatory framework. The Based on risk concept means that policies, measures and procedures provided by legal and regulatory framework must be based on the type and extent of risks faced by participants in the capital market: the higher the risk, financial institutions should make greater efforts to address these risks. Risk-based inspections help the Commission to use its resources more efficiently and ensure that the examiners implement most of the time examining areas that present the highest risk.

Risk-based approach:

(a) recognizes that the threat to capital market participants from money laundering and terrorist financing differs from clients, legal systems, products and distribution channels;

(b) enables participants in the capital market to apply different approaches to clients in a way that links the risk in certain areas;

(c) enables participants in the capital market to implement their own approach through procedures, systems, inspections and regulations in certain circumstances; and

(d) helps to design the system of cost elimination.

Systems and inspections will not detect and prevent any attempts of money laundering activities and terrorist financing. Risk-based approach puts emphasis on areas where is necessary and where the greatest impact exists. The Commission should achieve efficiency in the process of inspection through well-managed inspection.

II Inspection objectives

When inspection is carried out, AML/TF should make an assessment of capital market participants in relation to AML/TF in order to ensure compliance with legal provisions, determine whether a participant in the capital market pursues corrective action if deficiencies are identified and whether capital market participant constantly monitors transactions and activities of his/her clients. The Commission should use a risk-based approach depending on the size and complexity of operations of capital market participants. However, regardless of the size and complexity of the capital market participants, all inspections of AML/TF should be carefully planned, effectively managed and properly implemented in order to achieve their objectives.

Objectives of such inspection are as follows:

(a) ensuring adequacy of policies and procedures specified for AML/TF;

(b) determining whether AML/TF policies and procedures have been properly applied and implemented;

(c) determining whether the AML/TF policies and procedures are subject to regular verifications and determining the adequacy of such verifications; and

(d) determining compliance with obligations that capital market participants have based on relevant regulations related to AML and/or TF, by-laws and guidelines;

I Inspection approach

During carrying out of an inspection, the examiners should be able to compare theory with practice. As a first step, they need to determine what capital market participants defined in their policies, procedures, systems and inspections to combat money laundering and terrorist financing. Inspection should be based on fully documented evidence available in the premises of capital market participants, which can be supplemented by oral explanations of authorized persons. As a second step, the examiners should be in a position to test all aspects of policies, procedures, systems and inspections, based on random or targeted sample. When the inspection reveals significant deficiencies in the sample, examiners should expand testing in order to determine whether the deficiencies identified in capital market participants are of systemic nature.

Examiners should be aware that the Commission has the obligation to report to the Administration for Prevention of Money Laundering on all cases where a doubt on money laundering and terrorist financing exists if those cases have not been reported by the institution that is subject to inspection.

Planning and inspection

An important condition for successful performance of the inspection is the process of planning and inspection. For the purposes of planning and inspection, the following stages should be implemented:

- Main inspection plan
- Pre-inspection
- Field work
- Post-inspection
- Supervision and monitoring

Main inspection plan

Main inspection plan (hereinafter referred to as: MIP) The main inspection plan is the basis for work associated with the stage of planning and inspection and covers planned activities for the whole year. This step is not usually applied to target inspections. MIP is prepared with the participation of sector managers and examiners. MIP should be prepared 1-2 months before the end of each year. When making MIP, additional factors should be taken into account, such as:

- **Requirements related to Human Resources -** The number of examiners in the team depends on the number of capital market participants that should be monitored during the next calendar year. Each inspection team should consist of at least two examiners who will ensure the application of the "four eyes principle".

- **Availability of Human Resources** – Information about plans for absence of employees within the inspection department over the next calendar year should be got. Inspections should be arranged in such a way as to allow employees' entitlement to annual leave. For example: reduced number of direct (on-site) supervision during the summer months should be planned.

- **Optimization of Human Resources -** Confirm that Inspection Department has sufficient human resources to fulfill the inspection plan during the calendar year. If the number of human resources is reduced and additional staff cannot be provided, it is necessary to alter significantly the list of inspections in order to make a priority list for capital market participants. Those with the lowest priority should be placed on the bottom of the list.

- **The main review of MIP –** Determine which examiner will run the particular inspection. Appoint members of the inspection team. Prepare a reserve list in case of team member's absence.

- **Approval of MIP –** Present Commissioners a draft for review and approval according to Commission's approval procedures.

Technical Resources

The issue of technical resources is also important for meeting objectives of the inspection. Technical resources should be considered on the basis of need 'per team' rather than 'per person' and specify the equipment for the team only during the inspection period. As a minimum, each team should have at its disposal:

- Laptop PC – Each team must have at least one in order to make professional remarks regarding inspection,
- Portable printer – when necessary;
- Communication – mobile phone for communication with colleagues from the Commission;
- Other special requests – Chief examiners must inform the Head of the Sector on specific tools or equipment necessary for special inspection, with explanations of their needs.

Pre-inspection

During the pre-inspection stage, the following should be done:

- Re-confirm the requirements for human and technical resources;
- Ensure that necessary resources exist;
- Define whether the inspection has the status of regular or extraordinary inspection;
- If it is a regular inspection, prepare and submit to a capital market participant that is subject to inspection the decision on the inspection;
- Prepare necessary documents for identification and accreditation that will be used by examiners during the inspection;
- Review previous inspection's reports and other historical documents;
- Verify with sources of information the most recent issues that are worthy of attention but which are not covered by the historical documents.

Information review in the pre-inspection stage

Samples of items that examiners must examine at its registered office include:

- File on a capital market participant;
- Correspondence;
- Unsolved issues from previous inspections;
- Documentation on inspection activities and measures to be implemented;
- Regular information obtained from the Commission regarding Report on suspicious transactions;
- Information obtained from the Administration for the Prevention of Money Laundering and Terrorist Financing regarding reporting;
- Changes in business operations;
- Changes in inspections;
- Minutes of the meeting of the Board of Directors, if any;
- Audit reports;
- Responses and corrective measures of inspections and audits;
- Newspaper articles, including Internet sources;
- Revised reports, management letter, if any;
- Training Procedures related to AML/TF.

Immediate inspection

Basic inspection and administrative functions to be performed:

- Weekly (usually on Monday morning), the Director should hold progress review meetings with the main examiner.
- In case of any significant negative effects, it should be responded promptly.

During the immediate inspection, the team should use Procedures for carrying out the inspection [included in Annex]

Post-inspection

- Review documents related to inspection, working documents, comments of the inspection, inspection and the minutes (if completed);
- If the minutes are not completed and given to the capital market participant before leaving of the inspection team, arrange the meeting with representatives of the capital market participants in order to submit the minutes within [1-2] weeks;
- Ensure that the Minutes on inspection are completed on time;
- Review/discuss the Minutes on inspection with the Head of the Department in the Commission;
- Deliver the Minutes to a capital market participant;

- Ensure proper reference and completion of documentation on the inspection in the file of capital market participant;
- 'Close' the file on inspection documentation.

Supervision and Monitoring

- Review the inspection reports and detailed comments on inspection in order to supervise the monitoring.
- If certain implementation measures are included, specify the type of measure and date (if known).
- Out of the comments of capital market participants to inspection comments, pay attention to dates that are given for corrective measures. Emphasize the last mentioned dates.
- Send a letter to a capital market participant, consulting that its corrective actions are taken into account and that they should inform the Commission when and which deficiencies will be resolved.
- When information from capital market participants are obtained, update corrective actions taken.
- Review the records of capital market participants in order to verify whether all corrective actions have been completed, or whether the final corrective actions have been implemented.
- If a capital market participant claims that all measures have been taken, send a letter requesting a formal confirmation of this fact.
- If only corrective action with the last date has been taken and other items have not been taken yet, send a letter requesting details of the undertaken activities.
- If a capital market participant responds by claiming that all deficiencies are removed - it should be entered in the record of a capital market participant.
- If a capital market participant responds that some of identified deficiencies which have not been removed yet have a new deadline - it should be envisaged for the next inspection.
- Repeat the process until all claims of capital market participants are fulfilled
- If a capital market participant fails to respond or to provide ambiguous answers, all the remaining items should be marked and make a note as to bring it within the next regular inspection.

Written notes on the results of the above mentioned steps should be regularly kept, as well as in the files of the capital market participants for the next inspection.

CREATING A SCOPE OF INSPECTION

Timely, effective and risk-based control is essential for effective regulatory oversight function. The risk-based control ensures that the Commission often controls those capital market participants that represent the highest risk of possible misuse of AML/ TF, while those that present less risk should be monitored less frequently. All controls should be based on risk, which means that the examiners have to spend more time looking for areas with high risk, and less time for low risk areas. The risk may be based on the nature of business operations of the capital market participants, quality of management and employees or its internal procedures, as well as on adequacy of management and capabilities of persons authorized to identify, manage and monitor risks and to take timely measures to correct identified problems

Creating a scope of an inspection is an integral part of risk-based inspection process that helps examiners to indicate high-risk areas to be controlled and to determine appropriate procedures for these inspections. Creating a scope of an inspection is the planning inspection process that links risk profile of a capital market participant with the required inspection programs in order to enable target evaluation of capital market participants' business operations regarding AML/TF and make appropriate assessments and conclusions. It allows the examiner to understand the current risk profile of a capital market participant based on a review and analysis of the previous inspection minutes, earlier information on management and evaluation of changes in operations, number of employees or external circumstances.

Based on the conclusions prepared by the Commission's examiner, the team leader determines appropriate areas for inspection, the scope of direct inspection and inspection procedures to be used. Scope of inspection may be changed based on findings during the process of making a scope of inspection that should follow.

I. Inspection management

Effective management of inspection ensures that inspection team members meet inspection objectives and to work effectively. The level and sophistication of methods and procedures of inspection management vary, depending on the size and complexity of business operation.

Team leader's responsibilities

The team leader is a person who is most responsible for inspection management. Responsibilities of a team leader include:

- **Planning, organization and conduct of inspection**: The team leader is responsible for creating the scope of inspection, determining inspection objectives, exchange of information on inspection objectives with the inspection team and ensuring that the team meets objectives of the inspection.
- **Tasks and monitoring of tasks fulfillment**: The team leader must determine what expertise is required to perform certain aspects of inspection and assign tasks accordingly. He/she is responsible for achieving maximum efficiency from the performance of a coordinated review of security and stability that are consistent with the scope of inspection. Depending on the scope of inspection, the team leader may delegate the competences of management to certain examiners for efficiency and in order to improve the administrative skills and management skills for examiners.
- **Assignment of priorities to inspection tasks** and determination of optimal use of extensive reviews through the inspection program. Maximization of efficiency by assigning the

examiner a task to perform or coordinate activities in order to avoid duplication of efforts where feasible.

- **Informing inspection team members on the assignments of all team members,** including their participation in the segments of inspection which will include extensive verifications throughout the inspection program. Examiners should be provided with the necessary information and resources in order to perform the tasks efficiently.
- **Explanation of risk assessment and justification for making the scope** appropriate for each examiner's assignment.
- **Conversation about the impact of information obtained and discovered during an inspection** on the risk profile of a capital market participant, possible changes within the scope, possibilities for implementation of a comprehensive review within the inspection program and opportunities to meet deadlines for fulfilling the tasks during inspection. Adapt tasks on the basis of these considerations.
- **Monitoring inspection progress** in order to achieve objectives of the inspection timely and identify needs for adjusting the scope, number of employees and the end date. The team leader should inform the Head of the Department if the changes in scope have been made or if there are other events that may affect the schedule or completion date.
- **Preparation of minutes of the inspection:** entry of inspection conclusions, change of comments and completion of the minutes. Preparation and storage of working papers. Proper record keeping of the necessary inspection data.
- **Serves as the main link of communication:** The team leader is the contact person from the Commission with whom the authorized person in the capital market participants should discuss on key issues related to inspection. Employees in the capital market participants and other employees of the Commission must know how to exchange information and when to exchange information. During inspection, it is important that only one person in charge from the Commission provides answers to important questions. The team leader should coordinate this in case questions arise.
- When other competent authorities (supervision authorities) participate in the inspection, close cooperation with these bodies should be kept.
- At the beginning of inspection, the team leader should talk to Executive Director or to a designated representative of the capital market participants on certain administrative aspects of the inspection, which include:
    - Timeframe for obtaining required information.
    - Availability of examiners to respond to questions asked by employees who prepare required information.
    - Names of key contact persons.
    - Premises
    - Working hours.
    - Use of the equipment.
    - Expected duration of the inspection.
    - Any planned interruption (which should be reduced to a minimum).
    - Names of assistant examiners.
- The team leader should arrange (regular) meetings with the Executive Director to discuss the progress of inspection and refer issues of concern. Inspection should be carried out effectively in order to reduce to a minimum unnecessary disturbance of the capital market participants' work. Discuss any unsolved issues indicated by the management regarding inspection progress to the Commission's examiner.
- The team leader should arrange a final inspection meeting with the management of the capital market participant, in order to discuss about conclusions of carried inspection, overall conclusions and recommendations of the inspection.

II. Inspection

On the basis of risk assessment, the examiners determine appropriate inspection programs and procedures to be used. They can use a combination of procedures when carrying out the inspection. They should carry out a detailed survey of areas of higher risk for AML/TF and deal actively with all urgent and important issues which have been highlighted during scope creation process and inspection conduct. For example, if risk factors require the examiner to go beyond standard procedures of inspection and to extend the scope of the inspection or any other area for which the more detailed inspection is necessary.

Conducting meetings with the management

After the beginning of direct inspection, it is recommended to conduct an initial meeting at the premises of a capital market participant. Participants in this initial meeting should be employees who will be involved in inspection - the Executive Director and other staff responsible for AML/ TF, preferably. At this stage, a general discussion with the participants is held. Additional discussions will be held during inspection process (if necessary).

The discussion process is used to confirm, amend or supplement a preliminary evaluation of the risk profile of a capital market participant, changes in risk profile, management's response to these changes and management's records on changes monitoring. The discussions should cover the influence on the following items' operations:

- Strategic development of business operations and implementation;
- Changes in organizational structure and line responsibility;
- Scope and efficiency of the employees training program;
- Changes in operations that can affect current carrying out of compliance activities;
- Activities taken on remedying deficiencies identified during previous inspections or audits;
- Status of the management in the implementation of the official written compliance policy;
- Change of existing products or development of new ones;
- Significant audit findings and management’s response to those findings;
- Management’s commitment to formal adopted procedures or standard practices or their abandonment.

The discussion process should be adapted to address questions about specific circumstances for each capital market participant, especially as response to findings of the analysis prior the inspection. This process will help the examiners to adjust the scope of inspection and to determine to what extent they will examine certain operations, as well as implementation of relevant requirements of laws and regulations related to AML/TF.

Capital market participant should be informed on the purpose of inspection, as well as on the fact that he/she should provide answers to specific questions. A capital market participant should provide physical arrangements for appropriate work processes, as well as an access to necessary equipment. The main contact person in a capital market participant should be approved both on behalf of capital market participants and the Commission's Inspection Team.

During the inspection a few interviews should be done. Each interview should be documented in the file of a capital market participant. The knowledge and skills level of major employees in a financial institution in the field of AML/ TF as well as for customer due diligence, record keeping and reporting requirements.

Decision-making process within a capital market participant

An important part of the inspection process is evaluation of decision-making process within a capital market participant.

Support and solutions of the management of a capital market participant, as well as its involvement in the development and inspection of framework and risk inspections represent main conditions for adequacy of inspection framework. This involvement is also explained by the fact that management makes strategic decisions, gives directives, adopts decisions, is actively informed or orders information that should be obtained, and takes initiatives related to aspects of integrity and corporate governance freed of corruption. For example: The adoption of decisions approving the criteria for approval of clients, for unacceptable risks and for termination of relationships with clients without conducting customer due diligence (CDD).

Quality of management

The following aspects are of importance for the evaluation of management quality:

1. Management teams should have *sufficient knowledge and experience* in prevention of risk and influence of inspection measures for these risks diminishing. Due to lack of knowledge and experience, any adequate management or control of corporate activities cannot exist;
2. The so-called "risk appetites" (interest in risky operations): readiness of management to undertake risks and their conduct regarding risk inspections must contribute to the following:
- active participation of management of capital market participants, in analyses and vision of risk and their readiness for undertaking adequate inspection measures, for example, related to human resources and IT for planning monitoring system within the framework of CDD.
- management neither approves clients or products nor provides services for whose existence a capital market participant has no information or has not met them yet;
- development of those products or services must be preliminary made sufficiently without any risk to the integrity;
- management evaluates and urgently adjusts a manner of policy enforcement, as well as planned procedures and measures.

Functional structure

The functional structure regulates place of given position in the process, as well as relationship of the position in relation to other positions within the structure. Functional structure is appropriate when positions for all necessary steps are approved - for example, to combat fraud, registration of incidents or processes for CDD. Important steps in the approval process include, for example, providing empowers for client approval based on the "four eyes principle" and approval of high-risk clients by the management.

Development of risk-based approach in the process of customer due diligence

The type and completeness of procedures within the CDD depend on the type and degree of risk. The type and degree of risk are closely linked to specific features of the client, products and service offered by a capital market participant, as well as with the combination client-product. The greater the risk, a capital market participant should put more efforts in order to reduce such risks. The capital market participant is expected to divide users into risk groups based on difference in the type and extent of risk. These risks range from low to high. This division must be based on objective and visible indicators of risk. The risk-based approach predicts that the approval procedures and customer identification, as well as monitoring of products and transactions are particularly based on risk groups in which clients are assigned. Identical risks must be addressed using the same inspection of CDD.

During inspection of the adequacy of CDD procedure, examiners from the Commission should establish whether a capital market participant has clearly specified:

- Positions, tasks, competences (authorizations), reporting hierarchy;
- Competences for planning, enforcement and performance of internal inspections of compliance with CDD;
- independent inspection and assessment of planning adequacy and operations of CDD.

Relationships with clients

Customer due diligence policy client may define a higher theoretical level of requirements for special elections regarding approval, identification and monitoring of the clients. For example: clients, that a capital market participant unambiguously does not want to approve (unacceptable risk), the activities of the client for which a capital market participant does not want to be connected, transactions to and from persons where a capital market participant does not want to participate (for example, high risk states and territories), transactions in which a capital market participant does not want to participate according to the Law of undesirable regimes and their support companies and associated regulatory framework (a list of UN and EU sanctions).

Regarding CDD, capital market participants are expected to have defined policy (as well, as measures and procedures) regarding:

(a) Approval of the clients, taking into consideration the following aspects for each separate case:

- Justification of risk indicators for classification of clients into categories, depending on the risk;
- Approval criteria (aspects that should be taken into account when approving the client)
- Authorization for adoption of decisions related to the approval;

- Necessary information and documentation (for inspection and monitoring) of the client regarding the approval;

- Criteria for unacceptable risk, criteria for a client's exit policy, authorizations and competences in decision-making;

- Clear defining of competences related to CDD

(b) Identification and verification of the client:

- Regulations related to client identification;

- Defining of the client, risk analyses of parties involved in transactions;

Category/type of information for inspection and monitoring of the client: Law on Prevention of Money Laundering and Terrorist Financing and the Instruction.

Category/type of documentation for inspection and monitoring of the client are defined by the Law on Prevention of Money Laundering and Terrorist Financing and the Instruction.

- Archiving, storage of clients 'data, re-assessment of a client's risk category;

- Problems in identification/verification;

(c) monitoring of products and transactions:

- Guidelines and assistance for detection of irregular, unusual and suspicious transactions;

- Frequency and completeness of verification, depending on risks;

- Indicators of high risk products, regular products, /previous/ behavior of the client, special characteristic of products and type of transaction;

- on-site inspection/verifications

- clear defining of managers' responsibility regarding regulations related to AML/TF in relation to unusual transactions and activities connected with compliance for identification, analyses and processing of unusual and suspicious transactions.

(d) Management of risk, compliance and training:

- Position, tasks and competences related to function of employees working on monitoring of the compliance;

Assessment of nature and degree of risk analyses

1. Determining whether a capital market participant, during the analysis of risk for the purpose of strategic planning, risk classification in the client and acceptance of individual user), as a minimum, has taken into consideration:
   (a) Client characteristics (nature, description of condition, related accounts, ownership organization, structure of the capital, inspections and organizational structure , country of origin, business activities, source and destination of funds);
   (b) Combination of special clients using special products;

(c) Experience the institution has with different types of clients, products and services;
(d) Products' characteristics (vulnerability of improper conduct, distribution);
(e) Purpose for which the client intends to use product or services;
(f) Changes in characteristics of client's operations.

2. Determining whether a capital market participant particularly acknowledged and analyzed the risk of risk financing through foundations, charities and societies.
3. Determining whether a capital market participant particularly recognized and analyzed the risk of money laundering by clients and by small and medium enterprises (special attention should be paid to: the potential stores, off-shore companies, funds for specific purposes, business activities with a high risk of money laundering such as non-registered holder's shares).
4. Determining whether a capital market participant particularly recognized and analyzed (risk of) legal entities with non-registered holder's shares.
5. Determining that a capital market participant knows the identity of end user of each client and that it analyzed the risks associated with the end user (particular attention should be paid to: complex organizational structures, trusts, funds for special purposes).
6. Determining that a capital market participant for each client, analyzed the risks associated with the source of funds and the source and destination of funds.
7. Determining whether, when analyzing risk of the client's country of origin, a capital market participant takes into account as a minimum:
    - High-risk countries from specific regions in the world, that are, according to FATF, involved in specific forms of serious crime;
    - countries where corruption is widespread, according to Transparency International;
    - states that have been introduced an arms embargo, financial sanctions and trade sanctions;
    - tax avoiding and off-shore centers;
8. Determining that a capital market participant enables use of existing methods and trends of money laundering and terrorist financing in its risk analysis, when assessing the vulnerability of its activities, products or services to be used for illegal purposes.
9. Determining whether a capital market participant takes into consideration, as a minimum, risk of distribution of products to *customers on a non-personal basis*.

Evaluate whether the analysis method represents complete and sufficiently deep analysis.

Evaluation of risk classification systematism within clients

Risk classification within clients

<u>Note:</u> During assessment of control measures, a regulator must take into consideration that capital market participants tend to underestimate risks that occur in clients/ products. This can be encouraged by the desire to reduce effort of clients' testing.

1. Define whether a capital market participant has made systematics of risk classification at clients and criteria used in written form (audit records), for example during policies or acceptance procedures of the user.
2. Define whether the classification risk method includes adequate, objective and verifiable indicators.
3. Define whether those indicators encompass at least one risk indicator and consequences related to clients and products.

4. Define the method which a capital market participant uses for realization of insight into the clients' database risk profile.
5. Define the adequacy of criteria that are within the base of different risk categories.
6. Define the fact to which extent nature and number of risk categories correspond to nature, size and complexity of clients, activities, products and services.
7. Define whether all clients of a capital market participant are classified according to a risk category.
8. In relation to already classified clients, define whether identifiers for risk classification were applied in an appropriate manner, also based on risk analyses and data in the file (acceptance) of the client.
9. Define that systematics related to risk classification is properly applied to a client's database.

Analyses of parties involved in transactions that may represent a risk to a capital market participant

10. Define whether the procedure of acceptance and identification of the client includes guidelines and means which, as a minimum, contains:
    - that the identity of parties involved in transactions with the client is known to a capital market participant;
    - that a capital market participant makes risk analyses based on objective and verifiable indicators, in order to evaluate whether the involved party represents high risk. Indicators include risk indicators and opinions linked to characteristics of the client and products;
    - that considerations, data and documents used are documented, for example, in the clients' files or in transactions data.
11. Rating of adequacy of systematics and indicators used by capital market participants in order to determine whether the involved party represents risk.
12. Evaluations, regarding certain products and services offered by a capital market participant and regarding transactions in those products and services, whether:
    - the identity of involved parties are known and documented;
    - risks existing at these parties are completely and closely analyzed;
    - a risk analysis is made in a proper manner.

Evaluation of setting and functioning of procedures for regular updating of clients' data and review of client's risk profile

1. Define that a capital market participant formulated policy and procedures on frequency and manner based on which:
    - data on clients are regularly updated;
    - a client's risk profile is regularly checked.
2. Evaluate whether policies and procedures sufficiently enable circumstances that specify changes in risk profile which require re-assessment. Define whether a capital market participant takes into consideration mentioned circumstances:
    - of changes in services offered to clients;
    - of changes in clients' behavior patterns;
3. Evaluate adequacy:
    - of manners in which data on clients are regularly updated;

- of a manner in which a client's risk profile is re-assessed (including type of additional information and collected data, verification method).

4. Define that updating of client's data and frequency and scope of verification were made in accordance with risk linked to the client.
5. Define that data on high risk clients are updated and that their risk profile is reviewed at least *once a year.*
6. Define that policy and procedures of verification are regularly submitted to all segments of operations and that they are adequately conducted.
7. Define that regular re-assessment leads or has led to an adequate monitoring.

Monitoring of client's account and transactions

Monitoring of client's account and transactions provides (and maintains) insight into nature of the client, business operations and their financial status. This insight allows for capital market participants to identify high risk situations, for example, in case:

- of transactions that differ from client's profile or envisaged aim of the account;
- of unusual or suspicious transactions, transaction forms or activities on the account, use of certain (combination) of services and products of capital market participants.

Evaluation of appearance and operations of monitoring client's account and transactions

General

1. Evaluate the adequacy of the system for monitoring accounts and transactions of the client. Take into consideration the following aspects:
   (a) a degree up to which the monitoring of client's transactions has been made and realized (computerized monitoring vs. manual monitoring);
   (b) a degree up to which the monitoring method adequately corresponds to a risk size and size of client's database.
2. Define whether the monitoring procedures use specific definition of non-standard, unusual and suspicious transactions. Evaluate the adequacy of internal guidelines for non-standard, unusual and suspicious transactions and reporting on these transactions to officers in charge for monitoring compliance with AML/TF, and then to the Administration for the Prevention of Money Laundering.
3. Define that monitoring of accounts and transactions per client is performed on a consolidated basis, including accounts and transactions of foreign organizations. Determine whether the *consolidated position* of the client is up to date and reliable.

Automatic monitoring system

4. Evaluate progress made in the design and implementation of monitoring systems and the adequacy of the organization of project management.
5. Evaluate the adequacy of functionality of automated monitoring system using, for example, a comparison with functional design. Define the scope, depth and frequency of monitoring.
6. Evaluate the adequacy of organization and compatibility of IT systems with other clients and transactions systems.

SInternal manual monitoring in linear organization

7. In cases where the customer accounts and transactions are manually monitored, assess effectiveness of enforced activities of inspection. Define:
   - (a) Effective and real 'scope of inspection';
   - (b) Expertise and education of persons (as the account manager is) who perform inspection activities;
   - (c) adequacy of means of control;
   - (d) adequate, reliable reports as the ground for carrying out inspection activities;
   - (e) adequate reporting on findings arising from activities;
   - (f) adequate reports and explanations of conclusions derived from the findings;
   - (g) adequate structure of reporting on findings and conclusions.

Define that procedures ensure that transactions for which there is a possibility to be related to money laundering or terrorist financing have been reported to the Administration for the Prevention of Money Laundering correctly, completely and at the right time. Define that these procedures are adequately implemented.

AML/TF compliance officer

A capital market participant should appoint at least one person as a compliance officer responsible for the area of AML/TF. Appointment of a compliance officer shall require the prior approval of the Executive Director. Accordingly, examiners should ensure that the roles and competences of a compliance officer responsible for the area of AML/TF are clearly defined and to determine that:

- the role has been set to a management level in the organization;
- the role and competences are clearly defined and documented;
- the person who performs this job has an adequate experience and has been trained in appropriate manner for AML/TF procedures;
- the officer is allowed to have complete access to all records related to identification, account and transactions of the client;
- there are adequate reporting lines to the Board and the management, when needed: and
- reporting of suspicious transactions to Administration for Prevention of Money Laundering does not require approval or consent of any person.

Examiners from the Commission should determine whether the officer in charge for compliance in the field of AML/TF has made a regular check and tested the completeness of documentation for opening of a client's account, the adequacy of inspection and verification of the client and whether the data on transaction can be obtained in a reasonably short period of time. Examiners should also determine whether the results of verification and inspections made by employees during the monitoring of the activities of high-risk accounts/unusual transactions are regularly submitted to the officer in charge for compliance in the field of AML/TF.

Record keeping

Examiners from the Commission should check a sample of the account in order to determine whether the records are kept in an adequate manner when opening an account.

The review of record keeping policy should be done. Examiners should define:

- that a capital market participant keeps all records on information of clients, including records of accounts and details of transactions involving the transfer of funds for at least 10 years (without prejudice to other laws and regulations) following the date of the transaction regardless of whether the client has terminated business relationship with the bank after transaction was done;
- that a capital market participant keeps personally identification data obtained through the process of customer due diligence for at least 10 years (without prejudice to other laws and regulations) after termination of the business relationship.

Instruments by which records are kept should be examined and it should be evaluated whether they are readily available in case of the competent authority's request.

Define whether the manner in which records are kept provides effective audit records on clients' transactions.

Examiners from the Commission shell determine whether a capital market participant respected defined policies.

Examiners from the Commission shell determine whether the officer in charge for compliance in the field of AML/TF keeps a register of internal reports on suspicious transactions and to review the register in order to determine:

- whether employees properly report on suspicious cases;
- whether immediate activities have been taken and recorded. Evaluate the average time required for reporting to the Administration for the Prevention of Money Laundering;
- in cases where the report was not submitted to the Administration for the Prevention of Money Laundering, check whether the reasons why it was not done were stated. Examiners should decide whether the decision is justified. If internal guidelines have been given or it was found that assistance is needed, or whether a certain case should be reported to the Administration for the Prevention of Money Laundering, check if they are appropriate and whether they were properly applied.

Choose a sample of cases reported to Administration for Prevention of Anti Money Laundering and Terrorist Financing and establish whether procedures defined for reporting by market participant were applied and whether that information are complete and appropriate.

If a clean record is kept in the file (or, if there seems to be unusually low level of internal reports), determine why employees have not made any report and ensure that both management and employees are aware of their obligation to report suspicious cases and to know well what is considered as a suspicious case.

Harmonization

Verify compliance, programs and scope in order to determine whether the independent testing is extensive, precise and adequate. Verification of compliance should encompass:

- total integrity and efficiency of harmonization program with AML/TF including policies, procedures and processes;
- adequacy of policies and procedures for opening of the account and "Know your client" (KYC) as well as whether they are harmonized with internal requirements;
- requirements for keeping records on AML/TF;
- recognition and reporting of suspicious transactions;
- respecting of policies and procedures for AML/TF by employees in companies licensed for operations on capital market;
- appropriate testing of transactions, with special emphasize on high risk operations (products, services, and geographic locations);
- adequacy of training, including scope, material accuracy, training schedule and attendance monitoring; and
- integrity and accuracy of management information systems (MIS) used in harmonization programs with AML/TF.

Determine the extent to which testing should be done regarding adequacy of the work done in relation to the compliance function and its competence and independence. In case that the work being done by a person in charge of the compliance function is adequate and its function is highly professional and independent, it may be necessary for the examiners to carry out only minimal verification. Otherwise, they will have to conduct a thorough check to ensure compliance with policies and procedures.

Education and training of employees

Get the training program in a capital market participant in order to determine whether the management has given the appropriate importance to current education, training and compliance and whether employees have access to appropriate and current training program for AML/TF:

- for all employees;
- for newly employed;
- for all appropriate employees who, directly or indirectly, work with clients and/or their transactions;
- for employees competent for compliance function;
- regular training renewing for all employees.

Review the training material and evaluate its clarity, scope, relevance and accuracy. Identify the scope of the training and whether it took into account the specific risks of individual business lines. Evaluate whether the training material is in a form that employees can easily use and that can always be easily available to appropriate staff for invitation and change.

Define that the training has been done by officer in charge for compliance with AML/TF or other person with appropriate knowledge or, where applicable, the person outside of the company.

Ensure that a capital market participant keeps records on attendance during training sessions and makes regular schedule of sessions to be updated.

If necessary, conduct interviews with employees in a capital market participant in order to evaluate their knowledge of policy for AML/TF and legal requirements.

IV <u>Inspection report</u>

Primary objective of an inspection report is to describe situation in a capital market participant, submit analysis of preventive systems emphasizing the advantages and disadvantages. Any non-compliance with the law, by-laws or internal regulations should be stated. Appropriate recommendations and measures are also a mandatory element of the report.

The report must be mandatory for both the Executive Director and employees.

Taking into account that the management of a capital market participant does not have enough time to get acquainted with the voluminous documents, the report should be made as a multiple levels report. It should begin with a summary which should quickly and easily present conclusions to the management. Details follow later and they are sent to employees for solving.

Report gives a picture of a capital market participant, its activities and business operations. It should include both positive and negative facts, and to give positive comments on those areas in which the capital market participant has reached the expected standard and to identify those areas in which errors, failures, breaches have been observed, etc.

The final report should be submitted to the management of a capital market participant few days after inspection was completed. Ideally, the record should be done during the field work and it should be 90% completed at the end of inspection. However, if there are questions that should be included in the report that require consultation with other departments and staff within the Commission, it may take a few more days.

Good practice is presented by presenting the report to the management of a capital market participant at a meeting held at the premises of the capital market participant within no more than one/two weeks after completion of the inspection.

Pursuant to Article 8 paragraph 3 of the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 14/07) and Article 2 of the Rulebook on drafting guidelines on risk analysis aimed at preventing money laundering and terrorism financing (OGM 20/09), the Games of Chance Administration hereby defines

GUIDELINES ON RISK ANALYSIS AIMED AT PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

LEGAL BASIS

- The Law on the Prevention of Money Laundering and Terrorist Financing (OGM 14/07);
- Rules of procedure of the authorised person, the manner of conducting the internal control procedure, data keeping and security, the manner of records keeping, and professional training of employees (OGM 80/08);
- Rulebook on the submitting of information on cash transactions to the amount and exceeding 15,000 € and suspicious transactions to the Administration for the Prevention of Money Laundering and Terrorism Financing (OGM 79/08);
- Rulebook on drafting guidelines on risk analysis aimed at preventing money laundering and terrorism financing (OGM 20/09).

These guidelines stipulate more detailed risk factors to be used to identify the risk degree of individual clients, a group of clients, a business relationship, transactions and/or products for which the obligor prepares an internal act on risk analysis.

Pursuant to Article 86 paragraph 1 point 5 of the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter `the Law`), the Games of Chance Administration supervises the implementation of the Law and enabling regulations, in line with the law providing for inspection control of obligors under Article 4 paragraph 1 point 9 and/or operators of the usual and special games of chance.

MAIN PRINCIPLES OF THE FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING

1. Identification and verification of a client's identity

Before the establishment of any business relationship or executing any business transaction, obligors shall obtain the required information on a client, i.e. determine his/her identity.

Client identification procedure shall include:

1) the establishing of the client's identity and/or if the identity has already been established, verify the identity based on reliable, independent and objective sources;
2) the collection of information on the client and/or if the information has already been acquired, verify the collected data based on reliable, independent and objective sources.

When a client is a natural person, the obligor shall determine and verify his/her identity by checking his/her identification document in the client's presence and thus obtain information under Article 71 point 4 of the Law. If the provided identification document renders it impossible to determine the prescribed information, the lacking information shall be obtained from another identification document that the client submits.

If during the establishing and verifying of the client's identity the obligor raises any doubt regarding the authenticity or reliability of the identification and other business documents from which the information has been obtained, the obligor shall request a written statement from the client.

In case the client's identity is impossible to establish or verify, the obligor may not enter into a business relationship or execute a business transaction, i.e. he must discontinue all the existing business relationships with such a client.

2. Implementation of the law and standards

In the performing of their registered activity, the obligor shall act in line with the enacted laws and enabling regulations prescribing the detection and prevention of money laundering and terrorism financing and ensure that the prescribed measures are incorporated in their acting at all levels, thus providing for the full compliance of their business with the Law.

The Montenegrin legislation governing the prevention of money laundering and terrorism financing is harmonized with the following relevant legislation:

1. Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering;
2. Directive 2001/97/EC of the European Parliament amending Directive 91/308/EEC;

3. Directive 2005/60/EC of the European Parliament and the Council of 26 October 205 on prevention of the use of the financial system for the purpose of money laundering and terrorist financing**;**
4. FATF Recommendations (40+8+1);
5. UN Convention against Corruption.

Through the MONEYVAL Committee, the Council of Europe also accepts the aforesaid documents as references in its Evaluations.

3. Cooperation with the Administration for the Prevention of Money Laundering and Terrorist Financing

The Law prescribes full cooperation of the obligors and the supervisory authorities. The obligation of cooperation between the obligors and the supervisory authorities is extremely important when the requested data, information, and documents on a client or a transaction give rise to the suspicion of money laundering or terrorist financing. The cooperation is also essential in case of reporting any behaviour or circumstances that are or could be connected with money laundering or terrorist financing and which represent a threat to the security, stability and reputation of the Montenegrin financial system. This is why the developing of internal procedures must in no way, whether directly or indirectly, restrict the cooperation between the obligors and the Administration for the Prevention of Money Laundering and Terrorist Financing or in any other way have effect on the efficiency of such cooperation.

4. Adoption of an internal act

The obligors shall accept a common policy of risk management in money laundering and terrorism financing, this involving the adoption of internal procedures regarding, in particular: client verification, risk analysis, and detecting clients and transactions that give rise to the suspicion of money laundering or terrorism financing.

It is particularly important that all employees are familiar with such procedures, to behave in accordance with them, and use them in their work.

The content of the Internal act to be developed by the obligor:

a) the manner of establishing client acceptability;

b) the assessment of group and client risks;
c) the manner of establishing the risk of products and services from the aspect of the prevention of money laundering and terrorism financing;
d) the manner of client identification;
e) the supervision of clients` accounts and transactions;
f) risk management to which the obligors are exposed in the context of money laundering and terrorism financing;
g) employee training program.

5. Professional training

The obligor shall provide for regular professional training and advancement of all employees directly or indirectly involved in the prevention or detection of money laundering or terrorism financing.

RISK ASSESSMENT

1. Purpose of risk analysis

Pursuant to the Law, the risk of money laundering or terrorist financing represents the risk that a customer will use the financial system for money laundering or terrorist financing, or that a business relationship, a transaction or a product will be indirectly or directly used for money laundering or terrorist financing. In order to prevent too large exposure to money laundering and terrorist financing, the Law requires the obligor to make an assessment regarding the level of exposure of a certain client, a business relationship, a product or a transaction to the risk of money laundering or terrorist financing. Drafting the risk analysis is the necessary prerequisite for the implementation of the prescribed measures for customer analysis. The classification of a client, a business relationship, a product or a transaction under one of the risk categories shall depend on the form of customer verification that the obligor must perform in line with the Law (enhanced customer verification, simplified customer verification, and the standard customer verification).

2. Risk management policy and risk analysis

The obligor and/or its management (management team) may, if proved to be necessary for a more efficient enforcement of provisions of the Law and the Guidelines, accept an adequate risk management policy regarding money laundering and terrorism financing before drafting the risk

analysis. The aim of accepting such a policy is primarily to identify those business areas of the obligor that are, considering the possibility of misuse for the purpose of money laundering or terrorism financing, more or less critical, which means that the obligor should identify the main risks in this area and determine the actions to deal with them. In developing the starting points for accepting the risk management policy on money laundering and terrorism financing, the obligor shall take into account the following criteria to closely define in their policy the following:

6. purpose and aim of managing the risks of money laundering and terrorist financing and their relation with the business objective and strategy of the obligor,
7. areas and business processes of the obligor which are exposed to the risk of money laundering and terrorist financing,
8. risks of money laundering and terrorist financing in all key business areas of the obligor,
9. measures for dealing with the risk of money laundering and terrorism financing,
10. role and responsibilities of the obligor's management (management team) in the introduction and accepting of risk management policy on money laundering and terrorist financing.

3. Drafting risk analysis

Risk analysis is the procedure in which the obligor defines:

- the assessment of probability that their business may be misused for money laundering or terrorist financing,
- the criteria for the classification of a customer, a business relationship, a product or a transaction as less or more risky regarding money laundering or terrorist financing,
- the establishing of consequences and measures for efficient managing of such risks.

In drafting the risk analysis, the obligor shall take the following criteria into account:

4. the obligor develops risk categories in line with the risk criteria, thus classifying a customer, a business relationship, a product or a transaction under one of the risk categories,
5. in determining the risk categories, the obligor may, in line with its risk management policy, classify a customer, a business relationship, a product or a transaction as a high-risk regarding money laundering and terrorist financing and perform enhanced customer verification,
6. in determining the risk category for a customer, a business relationship, a product or a transaction marked as high-risk under the Law and the Guideline, the obligor must not classify them as medium (average) risk or minor risk.

4. Developing risk assessment

4.1. Initial risk identification

In line with the risk analysis, the obligor must prepare risk assessment of every individual customer, business relationship, product or transaction and before entering into the business relationship or executing the business transaction they must:

5. establish the identity of the client with the collected required information on the client, the business relationship, the product or the transaction and other information that the obligor should obtain for risk assessment,
6. evaluate the obtained information in the context of risk criteria for money laundering and terrorist financing (risk identification),
7. establish risk assessment of a client, a business relationship, a product or a transaction which must be based on the preceding risk analysis wherein the client, business relationship, product or transaction have been classified under one of the risk categories,
8. carry out customer analysis (enhanced customer verification, simplified customer verification and regular customer verification).

4.2. Subsequent risk identification

As a part of regular follow-up of the customer's business relationship, the obligor re-examines the initial assessment of risk or the business relationship assigned to the customer and, if proved to be necessary, assigns a new risk assessment (subsequently identifies the risk). The obligor shall re-examine the grounds for the initial risk assessment of a customer or a business relationship in the following cases:

1. if there has been a material change in the circumstance under which the client or the business relationship had been originally assessed, thus calling for classifying such a client or business relationship under a different risk category,
2. if the obligor suspects the accuracy of information which have been used as the basis for risk assessment of a certain client or business relationship.

9. Criteria for establishing customer risk category

In the risk assessment of a customer, a business relationship, a product or a transaction, the obligor must take the following criteria into account:

1. type and business profile of the client,

2. geographical origin of the client,
3. nature of a business relationship, a product or a transaction, and
4. the obligor's history with the client.

In addition to the criteria listed above, the obligor may also follow other criteria in the assessment of risk of a client, a business relationship, a product or a transaction, such as:

1. the source of funds which are the subject of the business relationship or transaction in case of a client specified as a politically exposed person under the criteria laid down in the Law,
2. the client's knowledge of a product and his experience and/or knowledge in that field,
3. other information showing that a client, a business relationship, a product or a transaction could bear higher risk.

6. Client risk categories

As for the risk categories, clients, business relationships, products and transactions can be classified under 4 main risk categories, these being:

1. extremely high risk, which renders doing business with such a client prohibited,
2. high risk,
3. medium (average) risk, and
4. minor risk.

6.1. Prohibition of doing business with a client

Clients with which doing business is prohibited due to the immediate and high risk of money laundering and terrorist financing are:

1. clients listed as persons subject to the United Nations Security Council or the European Union measures – relevant measures are: financial sanctions covering the freezing of assets in an account and/or the prohibition of disposal of property (economic sources), military embargo prohibiting trade in weapons with such a party, and the like,
2. clients residing or having their registered office in entities which are not subject to international law, meaning that they have not been internationally recognized as states (such entities allow fictive registration of a legal person, issuing of fictive identification documents, and the like).

6.2. High risk of money laundering or terrorist financing

6.2.1. Type, business profile and structure of a client

Clients representing high risk of money laundering or terrorist financing are the following:

1) Client is a politically exposed person, that is, a person that is acting or has been acting in the last year on a distinguished public position in a state, including his/her immediate family members and close associates:
2) presidents of states, prime ministers, ministers and their deputies or assistants, heads of administration authority and municipal authorities, as well as their deputies or assistants and other officials;
3) elected representatives of legislative authorities;
4) holders of the highest juridical and constitutionally judicial office;
5) members of the State Auditors Institution or supreme audit institutions and central banks councils;
6) consuls, ambassadors and high officers of armed forces;
7) members of managing and supervisory bodies of enterprises with the majority state ownership.

Marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters shall be deemed immediate family members of a politically exposed person.

A natural person that has a common profit from the asset or established business relationship or other type of close business contacts shall be deemed a close assistant of a politically exposed person.

6.2.2. Geographical origin of a client

Clients bearing a high risk of money laundering and terrorism financing shall be deemed those permanently or legally residing and/or having their registered office in:

1. a non-EU member state or a country not being a signatory to the EU Association agreement,

2. a country which has been assessed by the international authorities to be well-known in the production or well-organised and developed drug trafficking (countries in the Middle and Far East which are known for heroin production: Turkey, Afghanistan, Pakistan and countries of the golden triangle (Myanmar, Laos, Thailand), countries in the South America known for cocaine production: Peru, Columbia and the neighbouring countries, countries of the Middle and Far East, and Latin America known for the production of Indian hemp: Turkey, Lebanon, Afghanistan, Pakistan, Morocco, Tunis, Nigeria and the neighbouring states, and Mexico),
3. a country which has been assessed by the international authorities to be well-known for a high level of organised crime involving corruption, trade in weapons, human trafficking or the violation of human rights,
4. a country assessed by the international organisation Financial Action Task Force (FATF) as non-cooperative state or territory (these are states and/or territories which, according to FATF, do not have in place adequate legislation governing the prevention or detection of money laundering or terrorist financing, there is no financial supervision by the state or it is inadequate, in which the establishment or operations of financial institutions is allowed without a licence or an approval from the national authorities, a country which encourages the opening of anonymous accounts and/or allows other anonymous financial instruments, a country which has improper system of recognizing and reporting suspicious transactions, in which the legislation does not recognize the obligation of determining the beneficial owner, international cooperation is inefficient or nonexistent).
5. a country which is subject to the UN or EU measures which include, in particular, total or partial discontinuation of economic relations, railway, maritime, air, postal, telegraphic, radio and other communication links, the suspension of diplomatic relations, military embargo, road embargo, and the like,
6. a country known as financial and/or tax haven (such countries allow complete or partial tax exemptions and/or rate of taxation is much lower than in other countries. They usually do not have double taxation agreements or even if they do have them such agreements are not adhered to, their legislation allows it, request strict adherence to the banking and professional secret, and fast, discreet and cheap financial services are provided. Countries generally known as being tax havens are: Dubai – Jebel Ali Free Zone, Gibraltar, Hong Kong, the Isle of Man, Lichtenstein, Macau, Mauritius, Monaco, Nauru, Nevis Islands – area Norfolk, Panama, Samoa, San Marino, Sark, Seychelles, St. Kitts and Nevis, St. Vincent and Grenadines, Switzerland – cantons Vaud and Zug, Turks and Caicos islands, the United States of America – federal states Delaware and Wyoming, Uruguay, Virgin Islands and Vanuatu),
7. a country which is generally known as an off-shore financial centre (such countries impose limitations on immediate performance of registered activities of registered business in the country, ensure a high degree of banking and professional secret, there is a liberal supervision of foreign trade, and fast, discreet and cheap financial services are provided, and registration of legal persons. These countries do not have proper legislation governing the detection and prevention of money laundering and terrorist financing. Countries in the world known as off-shore financial centres are: Andorra, Angola, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermudas, British Virgin islands, Brunei Darussalam, Cape Verde, Caiman islands, Cook islands, Costa Rica, Delaware (USA), Dominica, Gibraltar, Grenada, Guernsey, the Isle of Man, Jersey, Labuan (Malaysia), Lebanon, Lichtenstein, Macao, Madeira (Portugal), Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Nevada (SAD), the Netherlands Antilles, Niue, Palau, Panama, Philippines, Samoa, Seychelles, St. Christopher and Nevis, St. Lucia, St. Vincent and Grenadines, Zug (Switzerland), Tonga, Turks and Caicos islands, Uruguay, Vanuatu and Wyoming (SAD).

The international organisations authorized for the monitoring of efficiency of implementation of measures regarding the prevention of money laundering and terrorist financing in line with international standards, the obligors should respect the authority of the following international organisations:

12. European Bank for Reconstruction and Development,
13. EC Committee on the Prevention of Money Laundering and Terrorist Financing,
14. Financial Action Task Force (FATF),
15. International Monetary Fund,
16. World Bank,
17. International association of financial supervisory authorities dealing with detection and prevention of money laundering and terrorist financing – Financial Intelligence Units (Egmont Group),
18. Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL),
19. International Organisation of Securities Commissions(IOSCO),
20. Independent Committee of European Securities Regulators (CESR),
21. Committee of European Insurance and Occupational Pensions (CEIOPS),
22. International Association of Insurance Supervisors (IAIS).

6.2.3. Business relationships, products and transactions

Business relationships that could bear a high risk of money laundering and terrorist financing are the following:

4. business relationship involving ongoing or large payments from a client's account and/or to a credit or a financial institution in a non-EU member state and/or country which is not signatory to the EU Accession Agreement, and/or business relationship involving larger payments to a client's account open with a credit or a financial institution in a non-EU member state or a country which is not a signatory to the EU Accession Agreement.

6.2.4.The obligor's history with a client

Clients deemed by the obligor based on the prior experience to bear a high risk of money laundering and terrorist financing are the following:

1. persons for which the Administration for the Prevention of Money Laundering and Terrorist Financing has submitted requests to the obligor in the last three year for a temporary suspension of execution of suspicious transactions,

2. persons for which the Administration for the Prevention of Money Laundering and Terrorist Financing has submitted requests to the obligor for an ongoing monitoring of the client's financial operations,
3. persons for which the obligor has delivered information in the last three years to the Administration for the Prevention of Money Laundering and Terrorist Financing since such persons or transactions they have performed gave rise to suspicion of money laundering or terrorist financing.

6.3. Medium (average) risk of money laundering and terrorist financing

The obligor shall classify under the medium (average) risk category those clients, business relationships, products or transactions which cannot be classified under high or minor risk category in accordance with the criteria laid down in the Guidelines.

6.4. Minor risk of money laundering and terrorist financing

For clients bearing minor risk of money laundering or terrorist financing, the obligor shall adhere to the following:

ANALYSIS (VERIFICATION) OF CUSTOMER

1. Regular analysis (verification) of the customer

Customer analysis represents a key preventive element in the system of detecting money laundering and terrorist financing. The customer analysis is aimed at determining and verifying, in a reliable way, the actual identity of a customer. It shall cover the following: determining and verifying the customer's identity and other data in accordance with the provisions of Article 7 of the Law.

The obligor shall determine and verify customer's identity based on reliable, independent and objective sources (review of appropriate identification document).

It is prohibited to establish a business relationship or execute transactions when the customer's identity cannot be determined, or when the obligor has reasonable doubt regarding the truthfulness or credibility of data and/or documentation confirming the customer's identity, and in situation

when the customer is not ready or does not express readiness to cooperate with the obligor in determining accurate and complete data required as part of the customer's analysis. In such a case, the obligor shall not establish business relationship, and shall terminate the existing business relationship or transaction and notify the Administration for the Prevention of Money Laundering and Terrorist Financing thereon.

The obligor may shorten the procedure of customer's analysis exceptionally in cases when and provided there are no reasons to suspect in money laundering or terrorist financing in case of the customer or transaction in question.

The Law starts from the basic assumption that some customers, business relationships, products or transactions represent higher risks and other represent lower risks of misuse for the purposes of money laundering or terrorist financing. For that reason, the Law, for specific cases, requires particularly strict procedures for identifying and verifying customer, while in other cases it allows simplified measures for customer verification.

2. Obligation to perform customer analysis (verification)

An obligor shall undertake the analysis (verification) of customer in the following cases:

3. when establishing a business relationship with a customer (business relationship is any business or other contractual relationship that a client establishes or concludes with obligor and it is connected with the performance of obligor' activity);
4. in any transaction of €15 000 or more, regardless of whether it is one or several transactions which are obviously interconnected. Logically interconnected transactions shall be the following:
- two or more consecutive, but separated transactions amounting altogether to more than € 15 000;
- two or more transactions, amounting together to more than € 15 000, executed by several persons which are connected by family or business relationship, in favour of a third party for the same purpose:
5. when there is a suspicion about the accuracy or veracity of the obtained customer identification data, and
6. when there are reasonable grounds for suspicion of money laundering or terrorist financing with respect to the transaction of customer, regardless of the amount of transaction.

3. Enhanced customer analysis (verification)

Obligors shall apply measures of enhanced customer verification in the cases when a customer, business relationship, product or transaction is classified as highly risky from the aspect of money

laundering or terrorist financing. The Law particularly defines business relationships established with politically exposed persons as highly risky from the aspect of money laundering or terrorist financing.

3.1. Enhanced analysis (verification) of politically exposed persons

Pursuant to the provisions of the Law, politically exposed persons represent highly risky customers; therefore the obligor shall carry out an enhanced analysis in all cases when such person acts as a client who is, pursuant to the criteria from the Law and the Guidelines, defined as politically exposed person before establishing the business relationship or executing the transaction.

Enhanced customer analysis (verification) shall cover the implementation of the following additional measures:

4. gathering of data on sources of funds and assets that are or will be the subject of business relationship and/or transaction,
5. obtaining a written consent of the superior responsible person before establishing business relationship with a customer,
6. scrutinising transactions and other business activities carried out with the obligor by a politically exposed person, after establishing business relationship.

The obligor obtains the information on whether a specific person is politically exposed person from the signed written statement filled in by the customer before establishing business relationship or executing the transaction (Questionnaire for the identification of the politically exposed persons). Written statement shall be made in local and English language.

The written statement shall include the following information:

QUESTIONNAIRE FOR IDENTIFICATION OF POLITICALLY EXPOSED PERSONS

Pursuant to the Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter referred to as LPMLTF, OGM 14/07),____________(obligor), when establishing business relationship or executing transactions (referred to in Article 9 paragraph 1 point 2) with a customer, shall determine if a client is politically exposed person.

Politically exposed person, in the meaning of this Law, shall be any natural person that is holding or has held in the last year a distinguished public position in a state, including his/her immediate family members and close associate.

Immediate family members of the politically exposed person shall be marital or extra-marital partner and children born in a marital or extra-marital relationship and their marital or extra-marital partners, parents, brothers and sisters.

Close associate of the politically exposed person shall be any natural person that has a common profit from the asset or established business relationship or other type of close business contacts.

Pursuant to LPMLTF, please answer the following questions.

1. Are you:

1.	President of the State?	YES	NO
2.	Prime Minister?	YES	NO
3.	Minister or his/her deputy or assistant?	YES	NO
4.	Head of government body and local self government body, and his/her deputies and/or assistants and other officials?	YES	NO
5.	Selected representative of legislative bodies? (members of the Parliament and all persons appointed/elected by the Parliament)	YES	NO
6.	Holder of the highest judicial and constitutionally judicial functions? (judges, prosecutors and their deputies)	YES	NO
7.	Member of accounting courts, and/or supreme auditing institutions and Central Bank's Council?	YES	NO
8.	Ambassador?	YES	NO
8.	Consul? (diplomatic representatives)	YES	NO
9.	High officer of the Army?	YES	NO
10.	Member of managerial or supervisory body of a majority state owned company?	YES	NO

2. Are you:

1.	Immediate family member of persons listed in Table 1 above?		
	• Marital or extra-marital partner • Parent • Brother or sister • A child born in a marital or extra-marital relationship and their marital or extra-marital partner	YES YES YES YES	NO NO NO NO
2.	• Close associate of persons listed in Table 1 – Do you have common profit from the assets or established business relationship with the above-mentioned persons? • Are you in any other type of close business contact with the above-mentioned persons?	YES YES	NO NO

3. Have you:

been covering any of the positions mentioned in Table 1 for the last 12 months?	YES	NO
been immediate family member of close associate of persons covering any public position referred to in Table 1 for the last 12 months?	YES	NO

If you have answered YES any of the above-mentioned questions, you are politically exposed person pursuant to the Law. You are kindly asked to mention the origin of funds or assets that are or will be the subject of the business relationship or transaction:

____

____

I, the under-signed, hereby confirm that the data above is true and accurate.

Name of the person filling out the questionnaire

Customer's address

Customer's date of birth

Place and date

Customer's signature

Name of the Bank's employee

Place and date

Signature of Bank's employee

I hereby agree to establish business relationship with the politically exposed person.

Name of responsible employee

Place and date

Signature of the responsible employee

In case of any suspicion concerning the veracity of data obtained from the statement, the obligor may additionally verify the data by reviewing public and other information available to the obligor (the obligor shall determine how much and to what extent he will consider commercial listings i.e. databases of politically exposed persons reliable and relevant for the enhanced customer analysis). The obligor may verify such data with competent authorities, consular representatives or embassies of foreign states in Montenegro.

The obligor shall pay special attention to every money laundering and/or terrorist financing risk which might arise from new technologies (e.g. Internet banking) and establish policies and undertake measures for the prevention of use new technologies for the purpose of money laundering and terrorist financing. Policies and procedures of obligors addressing the risk arising from business relationship or transactions with customers that are not physically present shall also be applied in business activities with customers carried out by using new technologies.

7. Simplified customer verification

The obligor shall conduct simplified customer verification when the risk of money laundering or terrorist financing is insignificant. It means that the obligor in a specific case determines and verifies customer's identity, but the procedure is simpler than with enhanced customer verification.

The obligor shall not establish business relationship or execute transaction before he determines all the facts needed for the risk assessment of the customer.

Simplified verification of the customer shall not be allowed when there is suspicion of money laundering or terrorist financing with respect to customer or transaction, i.e. if a client is classified as highly risky customer pursuant to risk assessment.

8. Analysis of customer by third party

When establishing business relationship, the obligor may entrust customer's analysis, as a condition prescribed by the Law, to a third party, but it has to make sure in advance if the third party that shall conduct customer's verification fulfils all conditions prescribed by the Law and enabling regulations.

The obligor shall verify the fulfilment of the conditions related to the third party in one of the following manners:

4. review public or other available documents,
5. review documents and business documentation submitted to the obligor by the third party, or
6. obtain from the third party written statement guaranteeing to the obligor the fulfilment of the required conditions.

If the third party has conducted enhanced customer analysis instead of the obligor, the third party shall be responsible for the fulfilment of the obligations under the Law, including the obligation of reporting the transaction, and keeping data and documentation.

Although a third party has conducted enhanced customer analysis instead of obligor, the obligor shall be still liable for the implementation of the enhanced analysis measures.

IMPLEMENTATION OF MEASURES FOR DETECTING AND PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING IN BUSINESS UNITS AND COMPANIES IN WHICH THE OBLIGOR HAS MAJORITY SHARE OR VOTING RIGHTS AND WHICH HAVE THEIR REGISTERED OFFICE IN A THIRD COUNTRY

The obligor shall establish the system of maintaining a uniform policy of detecting and preventing money laundering and terrorist financing. In that respect, it shall ensure that the measures for detecting and preventing money laundering and terrorist financing prescribed by the Law with respect to the analysis of the customer's verification, reporting on suspicious transactions, keeping records, internal audit, appointing authorised persons, keeping data and other important information regarding detection and prevention of money laundering or terrorist financing are also being conducted, to an equal and/or similar extent, in business units and companies in which the obligor has majority share or voting rights and which have a registered office in a third country.

When the implementation of standards for detecting and preventing money laundering and terrorist financing in business units and companies where the obligor has majority share or voting rights explicitly violates the laws of the third country in which such business unit or company has registered office, the obligor shall notify the Administration for the Prevention of Money Laundering

and Terrorist Financing thereon and undertake appropriate measures to remove risks of money laundering or terrorist financing, such as:

6. establish additional internal procedures to prevent and/or reduce the possibility of misuse for the purpose of money laundering or terrorist financing,
7. conduct additional internal controls of the obligor's business in all key areas that are mostly exposed to risk of money laundering and terrorist financing,
8. establish internal mechanisms for risk assessment of specific customers, business relationships, products and transactions,
9. carrying out strict policy of customer classification according to risk and consistently carry out measures accepted on the basis of such policy,
10. perform additional training of employees.

The management of the obligor shall:

- ensure that all business units and companies in which the obligor has majority share or voting rights and which have a registered office in a third country, and their employees, are made familiar with the policy of detecting and preventing money laundering and terrorist financing;
- ensure that the directors of business units and companies where the obligor has majority share or voting rights include in business processes, to a greater extent, internal activities of detecting and preventing money laundering and terrorist financing;
- perform permanent oversight of appropriate and efficient implementation of measures of detecting and preventing money laundering and terrorist financing in business units and companies in which the obligor has majority share or voting rights and which have their registered office in a third country.

Business units and companies in which the obligor has majority share or voting rights and which have registered office in a third country shall at least once a year inform parent obligor on accepted measures for detecting and preventing money laundering, particularly on customer analysis (enhanced, simplified and regular verifications), risk assessment, identification and reporting on suspicious transactions, safeguard and keeping data and documentation, and keeping records of customers, business relationship and transactions.

MONITORING BUSINESS ACTIVITIES OF CUSTOMERS

1. Purpose of monitoring customer business activities

Regular monitoring of business activities of customer represents a key point for determining the effectiveness of implementing measures prescribed for detecting and preventing money laundering and terrorist financing. The purpose of monitoring customer's business activity shall be to establish legality of operations of the customer and verification of compliance of the customer's business with anticipated nature and purpose of business relationship, which the customer has established with the obligor, i.e. its usual scope of affairs. Monitoring of business activities of the customer shall be divided in four parts of customer's business with the obligor:

1. monitoring and verifying the compliance of customer's business with anticipated nature and purpose of business relationship,
2. monitoring and verifying the compliance of customer sources with anticipated sources of funds the customer mentioned when establishing business relationship with the obligor,
3. monitoring and verifying the compliance of customer's business with usual scope of his affairs,
4. monitoring and regular updating of documents and data obtained on a customer.

2. In monitoring and updating documents and data obtained on a customer, the following shall be performed:

a. Annual customer analysis (simplified, enhanced and regular),
b. Annual customer analysis (simplified, enhanced and regular), when there is a suspicion on veracity of the previously obtained data on customer,
c. Verification of customer data,
d. Verification of data obtained directly from customer,
e. Verification of listings of persons, states and other entities that are subject to measures of the United Nations Security Council or the European Union.

3. The scope of monitoring customer business activity

The scope and intensity of monitoring customer's business depend on the risk assessment of the particular customer, i.e. on its classification in a specific risk category. Monitoring of customer's business shall include the following:

1. in case of customers involving high risk – the prescribed measures of monitoring customer's business classified as highly risky shall be conducted at least once a year. In case of customers involving high risk, the obligor shall conduct, regularly and at least once a year, measures of repeated annual customer analysis (simplified, enhanced and regular), if the conditions prescribed by the Law have been met;
2. in case of customers involving medium (average) risk – the prescribed measures for monitoring customer's business classified as medium (average) risk shall be conducted at least every three years. In case of customers involving medium (average) risk, the obligor shall conduct, regularly and at least once a year, measures of repeated annual customer

analysis (simplified, enhanced and regular), if the conditions prescribed by the Law have been met.

3. in case of customers involving low risk, the obligor shall conduct, regularly and at least once a year, measures of repeated annual customer's analysis, if the conditions prescribed by the Law have been met.

The obligor may, in its internal rules and procedures and in accordance with its risk management policy for money laundering and terrorist financing, opt for more frequent monitoring of business activity of a specific type of customers than it is provided in the Guidelines and establish additional measures for monitoring customer's business and checking the legality of customer's operations.

DATA SUBMISSION

1. Informing on cash transactions

If a customer executes cash transaction with the obligor in the amount of € 15 000 or more, the obligor shall, pursuant to the provisions of the Law, submit to the Administration for the Prevention of Money Laundering and Terrorist Financing information on such transaction, immediately after, and not later than three working days since the day of execution of the transaction, in the form attached to the Rulebook on the manner of data submission on cash transactions of € 15 000 and more and suspicious transactions (OGM 79/08).

Cash transaction shall be any transaction where the obligor receives cash from the customer (notes and coins), i.e. where the obligor delivers to the customer cash of € 15 000 or more, regardless of the currency received from or delivered to the customer.

2. Informing on suspicious transactions

2.1. What is a suspicious transaction?

Pursuant to the provisions of the Law, suspicious transactions shall be all transactions that are unusual by their nature, volume, complexity, value or connectivity, i.e. that do not have clearly visible economic or legal basis or that are not in accordance or are disproportional to usual and/or expected business of the customer, as well as other circumstances that are connected with the

status or other features of the customer. Specific transactions as well as business relationships of the customer can be treated as suspicious. The assessment of suspicion of a specific customer, transaction or business relationship is based on criteria determined in the List of indicators for identifying suspicious customers and transactions for money laundering and list of indicators for identifying customers and transactions suspicious for terrorist financing. This list of indicators represents the basis for employees/authorised persons in identifying suspicious circumstances connected with a customer, transaction executed by a customer or business relationship established by a customer; therefore, obligor's employees must be familiar with the indicators so that they could use them in their work. Authorised person shall provide all professional assistance to employees in the assessment of suspicious transaction.

When the employees of the obligor determine that there are reasons for suspicion in money laundering or terrorist financing, they shall immediately inform the person authorised for the prevention of money laundering or his deputy. The obligor shall organise the procedure of reporting suspicious transactions among all organisational units and the authorised person pursuant to the following instructions:

1. determine in more details the manner of submitting data (by phone, fax, secure electronic way, etc.),
2. determine type of information to be submitted (information on customers, reasons for suspicion in money laundering, etc.),
3. determine the manner of cooperation of organisational units with the authorised person,
4. determine actions taken towards the customer in case of temporary blockade of transaction by the Administration for the Prevention of Money Laundering and Terrorist Financing,
5. establish the role of authorised person of the obligor in reporting suspicious transaction,
6. prohibit revealing of information that the data, information or documentation is or will be reported to the Administration for the Prevention of Money Laundering and Terrorist Financing,
7. determine measures regarding further relationship with the customer (temporary suspension of operations, termination of business relationship, performance of enhanced customer analysis and detailed monitoring of future business activities of the customer, etc.).

Report on suspicious transaction must be submitted to the Administration for the Prevention of Money Laundering and Terrorist Financing before the realisation of the business transaction (by phone, fax or in other appropriate manner). The report must indicate the time limit by which the transaction on which the Administration for the Prevention of Money Laundering and Terrorist Financing is informed should be executed. In case of premature reporting, the obligor may submit information on the suspicious transaction to the Administration for the Prevention of Money Laundering and Terrorist Financing electronically (through secure web page of the Administration for the Prevention of Money Laundering and Terrorist Financing), by fax or phone, but it must be also submitted in writing on the following working day at the latest.

PROFESSIONAL TRAINING

The human resources department of the obligor, in cooperation with the authorised person, shall prepare a programme of annual professional training in the area of prevention and detection of money laundering and terrorist financing for each calendar year not later than by the end of the first quarter of the business year. The programme should specify:

1. the scope and content of the training programme,
2. the objective of the training programme,
3. manner of realisation of the training programme (lectures, workshops, exercises, etc.),
4. the number of employees to be covered by the training programme,
5. duration of the training programme.

IMPLEMENTATION

These Guidelines shall enter into force on the day of their adoption, and they shall apply as of 1 January 2010.

No: 02/01-1351/1

Podgorica, 25 December 2009

DIRECTOR

Aleksandar Moštrokol, M.S.

In accordance with Article 86 paragraph 12 of the Law on Business Organizations (OG RMNE No. 6/02 and OG MNE No. 17/07, 80/08 and 36/11) the Ministry of Finance has issued

INSTRUCTION

FOR THE WORK OF THE CENTRAL REGISTRY OF BUSINESS ENTITIES AND FORMS FOR REGISTRATION

Subject

Article 1

This Instruction shall regulate the work of the Central Registry of Business Entities (hereinafter: CRBE) and forms for registration of entities dealing with business activity.

Submitting a registration application

Article 2

The registration procedure is initiated by submitting a registration application to the CRBE, directly or via mail.

The registration application is accompanied by the original, certified transcript or certified copy of documents necessary for registration in accordance with the Law on Business Organizations.

The name of the organization containing Arabic and Roman numerals does not have to be in Montenegrin.

Together with the registration application one shall submit a proof of paid fee for registration in CRBE.

The documents submitted electronically are considered as signed by the authorized person in accordance with the regulations defining electronic signature.

The registration application is submitted using the forms PS-01 (registration – business entities), PS – 01a (registration – entrepreneur), PS- 01b (registration – the foreign company branch), PS – 01c (registration – investment fund), PS – 01d (registration of a part of the entity), PS – 02 (change of data – business entity), PS – 02a (change of data – entrepreneur), PS – 02b (change of data – the foreign company branch), PS – 02c (change of data – investment fund), PS – 02d (change of data – a part of the entity), PS – 03 (initiating liquidation), PS – 03a (cease of registration - entrepreneur), PS – 03b (cease of registration – the foreign company branch), PS – 03d (cease of registration– a part of the entity), PS – 03e (cease of registration of business entity), which are an integral part of this Instruction.

Registration

Article 3

CRBE issues a confirmation on submitted registration application.

The confirmation from paragraph 1 of this Article contains: the sign of CRBE, the number under which the registration application is recorded, the time of submitting the registration application, the subject of the registration, the list of received documents and information on the amount of paid registration fee.

Upon receiving the registration application, the CRBE checks the fulfillment of conditions for registration.

Each subject registered in the CRBE gets registration number.

Each additional change of data in the CRBE contains the same number under which the business organization was registered for the first time.

The amendment of registration data or registration of liquidation decision, besides the registration number, also contains a special number issued by CRBE.

During the registration procedure, CRBE can correct technical errors, and this is recorded in special records in CRBE.

If the correction is made after the registration procedure is completed, CRBE notes the date of making the correction, creates an explanation and delivers notification on the made correction to the person authorized to receive documents in limited liability companies, stock companies, foreign company branches, or to the general partner of limited partnership, partner in the partnership or entrepreneur.

Reservation of a name

Article 4

The reservation of name for stock company, limited liability company and limited partnership, as well as the transfer of reservation to another person is done using the form PS-00 (reservation of a name) which is an integral part of this Instruction.

If the CRBE determines that the name for which a form has been submitted is not reserved or entered in the CRBE, it shall reserve that name for exclusive use of the applicant for the period of 120 days which cannot be restored.

The owner of the reserved name can transfer the reservation to another person by sending a notification to the CRBE which contains the name and address of the person to which the transfer is made.

Entry of the registered name

Article 5

A stock company, limited liability company, limited partnership or foreign company branch can submit a request for entering the name to the CRBE if:

- a registered stock company, limited liability company, limited partnership or foreign company branch give a written approval that a requestor can use their name and deliver to the CRBE a decision on the change of the existing name, or
- the requestor delivered to the CRBE a certified copy of a final court decision entitling him the right to be registered under the name he requests, or
- a stock company, limited liability company or limited partnership, as well as a foreign company branch, has merged with another stock company, limited liability company, limited partnership or foreign company branch, or
- a stock company, limited liability company, limited partnership or foreign company branch has overtaken more than ¾ of property, including the name of another stock company, limited liability company, limited partnership or foreign company branch.

Entry of the name of a company branch

Article 6

If a company registered for performing business activity in Montenegro performs the activity through its branch, the name of the company branch is entered in the CRBE by submitting an

application and delivering the decision of the competent authority of the company on organizing a branch of the company.

The name of the branch of the company contains the full name of the company.

The registration of the name of the branch of the company is performed only for administrative purposes, i.e. for notifying the beneficiaries of the CRBE on the recorded branches of individual subject of the entry.

Entry of the name of other forms of performing economic activities

Article 7

The other forms of performing economic activities, whose establishment is defined by special regulations, are entered in the CRBE.

Determining the registration number

Article 8

A registration number is defined in the following manner:

Identification 1 mark				ordinal number 1		Number of change			

Records keeping

Article 9

Stipulated records of the registration numbers are kept in the CRBE in electronic form, and it contains the following identification marks:

1) for entrepreneurs - identification mark 1;
2) for partnerships – identification mark 2;
3) for limited partnerships - identification mark 3;
4) for stock companies - identification mark 4;
5) for limited liability company - identification mark 5;

6) for a foreign company branch - identification mark 6;
7) for a non-governmental organization - identification mark 7;
8) for an institution - identification mark 8;
9) for cooperatives - identification mark 9;
10) for other forms of performing economic activity - identification mark 10;
11) for investment funds - identification mark 11;

Each form of performing economic activity, a non-governmental organization, institution and cooperative, registered in CRBE, is assigned a main number from the stipulated records of registration numbers, and the identification number is written before the registration one.

Collection of documents

Article 10

CRBE keeps a collection of documents of the register and other supporting books and records.

The supporting books and records are regularly updated and their computer processing is carried out through application of unique standards.

The collection of documents of the register contains the documents upon which the registration of a certain subject or entry of any change of data on the subject is made, as well as evidence and documents issued by competent authorities within certain procedures and all other evidence and documents whose filing in the collection of documents is provided for by law.

The collection of documents is kept for each type of performing economic activity, non-governmental organization, institution and cooperative and it is marked with the registration number of that type.

The collection of documents can be recorded and kept on microfilms.

The documents submitted for registration in CRBE are taken out from the file after issuing the decision on registration and put into the collection of documents.

If the registration is denied, the documents are not taken out from the file.

The documents that are taken out are put in a wrapper where the registration number of that type of organizing and the name of the subject are written.

When taking out the documents they are catalogued.

Electronic records

Article 11

CRBE copies computer data from the documents submitted for registration (backup copies) twice a day.

One copy is kept in the CRBE and the other one is on a daily basis delivered for filing to the state authority competent for information.

The electronic copy (backup copy) is kept for at least 10 days.

The data from the CRBE database are available on the CRBE website.

Termination of applying

Article 12

The validity of Instruction on work of the Central Registry and registration forms (OG RMNE, No. 25/02, 43/03 and 6/05 and OG MNE, No. 43/08, 19/10 and 24/11) shall cease on the day of coming into effect of this Instruction.

Coming into effect

Article 13

This Instruction shall come into effect on the eighth day since the day of its publishing in the Official Gazette of Montenegro.

Number: 01-3900

Podgorica, 5 April 2012

Montenegro

MINISTRY OF INTERIOR AND PUBLIC ADMINISTRATION

STRATEGY

FOR PREVENTION AND SUPPRESSION OF TERRORISM, MONEY LAUNDERING AND TERRORIST FINANCING

Podgorica, September 2010

C o n t e n t s

SUMMARY

ABBREVIATIONS

1. INTRODUCTION 5

2. METHODOLOGY 6

3. TERRORISM.. 6

3.1. The basic characteristics of terrorism.. 6

3.2. Legal and institutional framework for prevention and suppression of terrorism...................................7

3.2.1. National legal framework..7

3.2.2. International legal framework...9

3.2.3. Institutional framework 9

3.3. Strategic response of Montenegro to the threat of terrorism 11

3.4. Contribution to international counter-terrorism efforts 11

3.5. Informing the public 12

3.6. The goals of fight against terrorism 12

3.6.1. Prevention of terrorism..12

3.6.2. Suppression of terrorism 12

3.6.3. Protection against terrorism...13

3.6.4. Remediation of damage from terrorist attacks...13

3.6.5. Criminal prosecution...13

4. MONEY LAUNDERING AND TERRORIST FINANCING........ 13

4.1. Money laundering...14

4.2. Terrorist financing..14

4.3. Analysis of the situation...15

4.3.1. National legal framework..16

4.3.2. International legal framework...18

4.3.3. Institutional framework 19

4.4. Strategic response of Montenegro to the threat of money laundering and terrorist financing...............21

4.5. The goals of fight against money laundering and terrorist financing...21

5. CONCLUSION.. 22

SUMMARY

In line with its basic goal, the Strategy defines the framework of action of Montenegro in the fight against terrorism, money laundering and terrorist financing, which is aimed at improving the existing and developing new measures, mechanisms and instruments, the purpose of which is to ensure stability and security of Montenegro, the region and beyond.

The Strategy is based on the analysis of the situation and recommendations of relevant international institutions, on the basis of which strategic goals have been defined and further activities required to achieve the vision that describes a future situation in the field of preventing terrorism, money laundering and terrorist financing in Montenegro have been planned.

The analysis of the current situation shows that Montenegro was not confronted with the criminal act of terrorism in the previous period. However, the approach of Montenegro to the fight against terrorism takes into account that modern terrorism knows no national borders and that it is therefore considered international in terms of its goals and modalities of action. Therefore, the responds to the causes, occurrences and consequences should be an expression of joint action with the international community.

Establishing a modern and comprehensive legislative framework in accordance with relevant international standards presents one of the key conditions for efficient prevention and suppression of terrorism, as well as the promotion of legal measures for suppression of the criminal acts of money laundering and terrorist financing.

The number of state authorities and institutions involved in counter-terrorist actions and suppression of money laundering and terrorist financing requires the establishment of an effective mechanism of coordination in the formulation and implementation of comprehensive policy in these fields.

ABBREVIATIONS

CTC – Counter-Terrorism Committee

EGMONT GROUP – The international gathering of financial intelligence units

EU - European Union

EUROPOL - European Police Office

FATF – Working group for financial measures against money laundering – Organization for Control and Prevention of Money Laundering

INTERPOL - International Criminal Police Organization

MONEYVAL - The Committee of Experts on the Evaluation of Anti-Money Laundering Measures of the Council of Europe

NATO – The North Atlantic Treaty Organization

OUN - Organization of the United Nations

OSCE - Organization for Security and Co-operation in Europe

OECD – Organization for Economic Co-operation and Development

SC – Security Council

CoE – Council of Europe

SEPCA – Southeast Europe Police Chiefs Association

SELEC – Southeast European Law Enforcement Center

SALW – Strategy for Control of Small Arms and Light Weapons

IBASE – An analytical tool that allows quality national and international cooperation in exchanging information with other bodies responsible for law enforcement

NSA – The body responsible for the protection of classified information

Pursuant to Article 12 paragraph 3 of the Decree on the Government of Montenegro (Official Gazette of Montenegro 80/08), the Government of Montenegro, at its session held on 30 September 2010, adopted the following

2010-2014 STRATEGY FOR PREVENTION AND SUPPRESSION OF TERRORISM, MONEY LAUNDERING AND TERRORIST FINANCING

1. INTRODUCTION

The Strategy for Prevention and Suppression of Terrorism, Money Laundering and Terrorist financing (hereinafter: the Strategy) is the first strategic document, which in a unique and comprehensive manner provides the answer in the field of fight against terrorism, money laundering and terrorist financing in Montenegro.

Terrorism, money laundering and the financing of terrorist activities may jeopardize national, security and economic interests which, among other things, require a stable constitutional order, rule of law, development of democracy, strengthening peace and stability as prerequisites for the development of society, financially strong business sector, a stable financial system, fair and free labor market and a functioning market economy. These phenomena can also jeopardize all social structures.

The main goal of the Strategy is to establish priorities based on the need to develop effective and functional mechanisms of the relevant institutions and the need to improve procedures to prevent and suppress terrorism, money laundering and terrorist financing. The Strategy shows the commitment of Montenegro to work jointly, through the European and Euro-Atlantic integration, with other countries and international organizations, with a view to strengthening national, regional and global security.

In line with its basic goal, the Strategy defines the general framework of action and response of Montenegro to current and future challenges and threats, through the promotion of existing and development of new measures, mechanisms and instruments, the purpose of which is to ensure stability and security, implying the realization of the following vision:

“Montenegro has a coordinated and efficient system for the prevention of terrorism, money laundering and terrorist financing based on international standards and cooperation between the competent institutions.”

In this sense, the strategic directions of actions of Montenegro are:

- Adoption and implementation of the Strategy;
- Promotion of cooperation and exchange of information with regional and international partners in the fight against terrorism, money laundering and terrorist financing;
- The adoption and application of international standards;
- Defining the principles and methods of improving cooperation between the competent institutions.

2. METHODOLOGY

The Strategy is based on the analysis of the situation and the projection of developments in the field of international security integrations, the characteristics of modern challenges and threats in the fields of terrorism, money laundering and terrorist financing, which is a prerequisite for the determination of strategic goals, as well as for planning future activities necessary to achieve the vision. The analysis of the situation was carried out through: reports and recommendations of relevant institutions; analysis of statistical data from reports, on: suspicious cash transactions, criminal acts, the crime situation and its manifestations, the predicate criminal acts, etc.

The Strategy is harmonized with other strategic documents of Montenegro, primarily with the National Security Strategy, Defense Strategy and the 2010-2014 Strategy for the Fight against Corruption and Organized Crime. In addition, the Strategy follows those goals and values that are defined in the Global Counter-Terrorism Strategy of the United Nations and the European Union Counter-Terrorism Strategy, as well as in other basic counter-terrorism documents of the United Nations (UN), European Union (EU), North Atlantic Treaty Organization (NATO), the Organization for Security and Co-operation in Europe (OSCE) and Council of Europe (CoE).

3. TERRORISM

3.1. The basic characteristics of terrorism

Terrorism presents one of the major global security threats in the 21st century and shows an upward trend in all of its forms, which is manifested through an increased number of terrorist acts, endangering human lives, causing increased public fear of the consequences of terrorist acts, larger destructions of material goods, etc.

In preparing the terrorist acts, terrorist organizations and individuals use wide availability, complexity and openness of communication and information technologies, especially Internet, to attract extremists, as well as for communication and dissemination of terrorist ideology. In this sense, knowledge of terrorist methods and techniques is of utmost importance for the prevention of all forms of terrorist acts.

Activities of terrorist organizations and terrorists are aimed at:

- attracting, to their cause, those individuals and/or groups who feel ignored or rejected in their society, or those individuals who do not manage to find socially and democratically acceptable forms of resolving their discontent and problems;

- deliberate and distorted interpretation of specific social, economic, religious and political issues, in order to cause inter-national, inter-religious, inter-cultural and other forms of intolerance and conflict, spreading, in this manner, terrorist propaganda and trying to gain support for their radical views, activities and goals, and recruiting new members;

- establishing a decentralized organizational structure, through creation of new and largely autonomous terrorist cells, protecting, in this manner, the security and the resilience of the terrorist organization itself, particularly the leaders and ideologists of terrorism.

Terrorist activities are conducted in an organized manner and are associated with other threats and risks, such as: trans-national organized crime, the spread of chemical, biological, radiological, and nuclear weapons and materials, smuggling: small arms and light weapons, explosive devices, man-portable missile systems, narcotic drugs, supplies of military and dual use, counterfeiting documents and money, illegal migration and human trafficking.

Terrorist groups and organizations are developing alternative ways of organizing and financing and they use elaborate logistical organization, especially in the acquisition of weapons and weapons of mass destruction, supplies of military and dual use, equipment and other assets that can be used for terrorist purposes.

It is the obligation of all state authorities and public administration bodies to, in accordance with their responsibilities, continually analyze and monitor all aspects of potential terrorist threats with which Montenegro could face, and to act, in an appropriate manner, to prevent them.

3.2. Legal and institutional framework for prevention and suppression of terrorism

3.2.1. National legal framework

Establishing a modern and comprehensive legislative framework, in accordance with relevant international standards, is one of the key prerequisites for efficient prevention and suppression of terrorism. Authorities responsible for prevention and suppression of terrorism are

carrying out a permanent evaluation of the efficiency of the legal framework and take care of its promotion as needed.

Jurisdiction, competences and actions of state authorities participating in the fight against terrorism are regulated by several laws which are related to this criminal-law field or refer to it:

- Criminal Code (Official Gazette of the Republic of Montenegro 70/03 and 47/06 and Official Gazette of Montenegro 40/08 and 25/10); Criminal Procedure Code (Official Gazette of Montenegro 57/09 and 49/10); Law on Public Prosecution Office (Official Gazette of the Republic of Montenegro 69/03 and 40/08); Law on Courts (Official Gazette of the Republic of Montenegro 5/02, 49/04 and Official Gazette of Montenegro 22/08); Law on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro 14/07 and 4/08); Law on Police (Official Gazette of the Republic of Montenegro 28/05 and 88/09); Law on the Agency for National Security (Official Gazette of the Republic of Montenegro 28/05); Law on Asylum (Official Gazette of the Republic of Montenegro 45/06); Law on Border Control (Official Gazette of Montenegro 72/09); Law on Foreigners (Official Gazette of Montenegro 82/08 and 72/09); Law on Travel Documents (Official Gazette of Montenegro 21/08 and 25/08); Law on the Protection of Personal Data (Official Gazette of Montenegro 79/08 and 70/09); Law on Data Confidentiality (Official Gazette of Montenegro 14/08 and 76/09).

According to the Criminal Code of Montenegro**, the criminal act of terrorism is made by any person who, with the intent to seriously intimidate citizens or to coerce Montenegro, a foreign country or an international organization, performs one of the following acts:**

1) Attack against the life, body or freedom of others,
2) Kidnapping or hostage taking,
3) The destruction of state or public buildings, transportation systems, infrastructure including information systems, fixed platforms in the epicontinental shelf, a public good or private property that may endanger human lives or cause significant damage to the economy,
4) Hijacking an airplane, ship, other means of public transport or transport of goods that may endanger human lives,
5) Manufacture, possession, acquisition, transport, supply or use of weapons, explosives, nuclear or radioactive materials or devices, nuclear, biological or chemical weapons,
6) Research and development of nuclear, biological or chemical weapons,
7) The discharge of dangerous substances, or causing fires, explosions or floods, or taking other generally dangerous action that may endanger human lives,
8) Disruption or suspension of water, electricity or other energy source supply that may endanger human lives.

With regard to the latest amendments to the Criminal Code from 2010, a special emphasis was placed on the harmonization with the standards in the field of fight against organized crime, corruption and terrorism. The above-mentioned amendments to the Criminal Code provide for an entirely new conception of criminal acts of terrorism, which are, in the corpus of criminal acts against humanity and other goods protected by international law, in accordance with the tendency of full compliance with international standards. The basic criminal act of terrorism (regardless of whether the act is directed against Montenegro, a foreign state or international organization) is

prescribed by Article 447 with numerous forms of the act of commission. This criminal act, as well as the new criminal acts of terrorism such as the public calls to commit acts of terrorism (Article 447a of the Criminal Code), recruitment and training for terrorist acts (Article 447b of the Criminal Code), use of a lethal device (Article 447c of the Criminal Code), destroying and damaging a nuclear facility (Article 447d of the Criminal Code), threatening an internationally protected person (Article 448), as well as the financing of terrorism (Article 449) were provided for and harmonized with a number of conventions aimed at preventing acts of terrorism, especially the Council of Europe Convention on the Prevention of Terrorism from 2005, which Montenegro has ratified in 2008.

With regard to the **Criminal Procedure Code** (Official Gazette of Montenegro 57/09 and 49/10), a special emphasis was placed on confiscation of property and material benefits acquired through a criminal act. The Code provides for a procedure of seizure of property and a financial investigation for the purpose of extended seizure of property. Through enactment of this Code, a confiscation procedure is introduced for property whose legal origin has not been proved. Through adoption of the institute of extended seizure of material benefits and the reverse burden of proof, efficient suppression of terrorism, money laundering and terrorist financing has been enabled. The procedure for confiscation of property whose legal origin has not been proved and the financial investigation for the purpose of extended seizure of property are significant changes in comparison to the previous legal text, which can be of great influence on the court practice. The measures of secret surveillance (special investigative means) may be applied to a larger number of criminal acts than before, and among these acts, the following are specified: criminal acts with elements of corruption (money laundering, causing false bankruptcy, abuse of evaluation of assets, passive bribery, active bribery, disclosure of an official secret, trading in influence, abuse of authority in economy, abuse of an official position and fraud in the conduct of an official duty). The measures of secret surveillance may also be applied for criminal acts against the security of computer data that are difficult to prove and complicated to detect due to the use of sophisticated computer technology, which will further contribute to the efficient fight against organized crime, terrorism, money laundering and terrorist financing.

3.2.2. International legal framework

Montenegro is a signatory to a large number of conventions regulating the area of fight against terrorism, which were adopted by the Organization of the United Nations and the Council of Europe. With a view to joining the European Union, Montenegro is implementing Common Position 2001/931/CFSP relating to the application of specific measures to combat terrorism. In this field, Montenegro is also promoting the cooperation in accordance with Resolution 1373 (2001), Resolution 1535 (2004), Resolution 1624 (2005) and other relevant UN resolutions, international conventions and other instruments. Montenegro is, through its Permanent Representative, actively cooperating with the Counter-Terrorism Committee of the UN Security Council, set up by the Resolution 1373 (2001). Acting within different international organizations, especially the United

Nations and the Council of Europe, Montenegro has become a signatory to a series of international - legal instruments, as presented in Annex I.

3.2.3. Institutional framework

The Ministry of Interior and Public Administration supervises and controls the work of the Police Directorate and performs tasks related to the preparation of strategies, laws, secondary legislation, projects and programs in the field of fight against terrorism. Within the Ministry of Interior and Public Administration, the Department for Emergency Management plays a significant role in the remediation of consequences of possible terrorist attacks.

The Ministry of Justice is carrying out tasks of the state administration relating to: criminal legislation, international legal assistance; the preparation of strategies, projects and programs and monitoring their implementation; preparation of necessary reports and measures for the implementation of ratified conventions in the field of judiciary; preparation and implementation of international agreements in the field of international assistance; preparation of laws and secondary legislation and their implementation, which are related to the organization, jurisdiction and work of courts, public prosecutor and misdemeanor authority, attorneys and legal assistance.

The Ministry of Defense proposes and implements the established defense policy; prepares the Plan of Defense of Montenegro and harmonizes Plans of Defense of other proponents of defense preparations; assesses war and other dangers; realizes multilateral and bilateral cooperation in the field of defense; conducts affairs of organization, equipping, arming, development and use of the Armed Forces and other activities in accordance with the Constitution.

The Agency for National Security collects data and information, through the use of special methods and means determined by law, on potential threats, plans or intentions of organizations, groups and individuals that are directed against the territorial integrity, security and the national legal order determined by the Constitution, and draws attention to the potential challenges, risks and threats to security.

The Armed Forces of Montenegro, in accordance with the Defense Strategy of Montenegro and the Law on Defense, among other things, are responsible for tasks relating to: assisting the Police Directorate in the fight against terrorism and supporting civil authorities during natural or man-made disasters and other emergencies.

The Police Directorate provides for general, personal and property safety and protection of citizens. The Police Directorate is responsible for internal security, preventing and suppressing all forms of crime, especially organized crime and corruption, protection of human rights, monitoring and control of the state border, ensuring public peace and order, the safety of citizens and traffic safety, and assisting the civil authorities during natural or man-made disasters. The Police Directorate is one of the most important bodies in the fight against terrorism, proliferation of weapons of mass destruction, corruption and drugs.

The Administration for Prevention of Money Laundering and Financing Terrorism, in accordance with the Law on Prevention of Money Laundering and Terrorist Financing, performs tasks of the Administration related to detecting and preventing money laundering and terrorist financing determined by this Law and other regulations. The Administration for Prevention of Money Laundering and Financing Terrorism is organized as a financial intelligence service of an administrative type. The Administration is responsible for tasks related to detecting and preventing money laundering and terrorist financing related to gathering, analyzing and submitting to the competent bodies of data, information and documentation necessary for the detection of money laundering and terrorist financing.

The Directorate for Protection of Classified Data in accordance with the Law on Data Confidentiality, organizes performance of tasks related to sharing classified information with foreign countries and international organizations, through the Central Registry, performs the tasks of issuing permits for access to classified data of natural (Personal Security Clearance) and legal persons (Facility Security Clearance), as well as inspection control of the implementation of the Law and the application of international agreements. In accordance with the Agreement on Security of information, in its part related to the exchange and protection of NATO classified information, the Directorate has been marked as NSA (National Security Authority).

The Supreme Public Prosecutor's Office established, for the tasks of suppressing corruption, the **Division for Suppressing Organized Crime, Corruption, Terrorism and War Crimes**, headed by the Special Prosecutor, which acts before the High Courts. The Division manages the pre-trial proceedings, directs the work of the Police Directorate and takes the necessary measures for the purpose of detection of criminal acts within its jurisdiction; requires an investigation, brings and represents indictments, and takes other actions stipulated by law, with a view to seizure and confiscation of assets and material benefits acquired through criminal acts.

The Specialized Division of the High Court in Podgorica and Bijelo Polje is responsible for trials in criminal cases of organized crime, corruption, terrorism and war crimes.

Other government authorities participate, within the scope of their jurisdiction and if necessary, in prevention and suppression of terrorism.

3.3. Strategic response of Montenegro to the threat of terrorism

So far, Montenegro has not been confronted with the criminal act of terrorism. However, given that global terrorism and organized crime pose a serious threat to international peace and security, these phenomena, regardless of their real source, are considered serious security risks and threats to Montenegro.

Therefore, Montenegro is trying to contribute, to the greatest extent possible, to general security at the regional and global level. In this context, the greatest attention is being paid to preventive mechanisms in the fight against terrorism: the strengthening of international cooperation, prevention of radicalization, monitoring movement of people and goods across land and sea borders, and exchange of information through information and intelligence connections.

With a view to coordinated and efficient implementation of strategic measures for the fight against organized crime and terrorism, the Government of Montenegro has adopted, in the previous period, a significant number of strategic documents and laws in the field of illegal migration, human trafficking, drugs and arms trafficking and other forms of cross-border crime. These are primarily the Criminal Procedure Code, Criminal Code, Strategy for the Reform of Judiciary, Strategy for the Fight against Human Trafficking, Strategy for the Control of Small Arms and Light Weapons (SALW), Strategy for Integrated Border Management, Strategy for Integrated Migration Management, National Strategic Response to Drugs, Strategy for the Fight against Corruption and Organized Crime, etc.

3.4. Contribution to international counter-terrorism efforts

Montenegro will continue to actively participate in the prevention and suppression of terrorism at global and regional level, particularly within the system of UN, EU, NATO, OSCE, Council of Europe, Interpol, Europol, and other relevant organizations and initiatives, as well as to contribute to strengthening and developing the counter-terrorism cooperation on the inter-regional level.

In the prevention of terrorism, Montenegro places special emphasis on cooperation with other countries, particularly in the area of South-Eastern Europe. This action consists of two

components. The first one encompasses cooperation of security sectors of countries in the region in the prevention of terrorism, which takes place through the police, intelligence and border control cooperation. In this regard, it is important to emphasize successful cooperation of Montenegrin institutions with SEPCA and SELEC. The second component is the cooperation among the countries of the region, aimed at developing political, economic, social and cultural relations, as a means of achieving long-term stabilization of the whole region. Montenegro will continue to pay particular attention to international cooperation in the field of adopting international-legal instruments, through the implementation of conventions and protocols, exchange of information, experiences and good practices in the implementation of counter-terrorism measures, strengthening cooperation in terms of international-legal assistance and extradition matters, researching into possible new terrorist threats and developing appropriate counter-measures and mechanisms and strengthening professional-technical and scientific-educational dimensions.

3.5 Informing the public

Modern terrorism misuses, for its own purposes, free and unhindered dissemination of information to spread its ideas, attract militants, and carry out operations. It is therefore necessary to take all measures to prevent the spread of terrorist ideas through any media of transmission.

Free and unhindered dissemination of information and ideas is one of the most effective means of promoting understanding and tolerance, which should be effective in preventing and suppressing terrorism as well. The public should be competently informed about all forms of terrorism, its criminal nature, the threats it presents and the responsibility that everyone has in its prevention and deterrence.

3.6. The goals of fight against terrorism

In the fight against terrorism the goals are achieved through implementation of the measures of prevention, suppression, protection and remediation of damage from terrorist attacks, the measures of criminal prosecution of individuals and entities linked to terrorism, strengthening inter-agency coordination and international cooperation.

The main goal of the prevention and suppression of terrorism is to achieve the highest possible level of protection of Montenegro, its citizens and all the people residing in it, its values, interests and resources from the threat and consequences of terrorism, while simultaneously

providing the most effective possible contribution to international efforts in the fight against terrorism.

3.6.1. Prevention of terrorism

Goals in the field of prevention include:

- improved normative-legal framework;

- developed personnel, administrative and material-technical capacities;

- implemented new programs of training and vocational training;

- improved cooperation among all relevant institutions in the country, region and at international level;

- improved mechanisms for prevention of propaganda, calling for terrorism, and inciting terrorism in any way.

3.6.2. Suppression of terrorism

Goals in the field of suppression of terrorism include:

- improved mechanisms for prevention of organizational and logistics activities with terrorist intentions;

- improved mechanisms for the detection and prosecution of all persons who are associated with terrorism or the disclosure of all activities directed against Montenegro, other countries and/or international organizations;

- improved mechanisms for prevention of the movement and residence of all persons associated with terrorism in the territory of Montenegro;

- improved mechanisms for prevention of criminal activities that may be directly or indirectly related to terrorism (transnational organized crime, the spread of chemical, biological, radiological, nuclear weapons and items, smuggling weapons and explosives, goods of military and dual use, narcotic drugs and other goods, counterfeiting documents and money, illegal migration and human trafficking).

3.6.3. Protection against terrorism

Goals in the field of protection against terrorism include:

- improved mechanisms for developing and strengthening the protection of infrastructure facilities of special importance on the territory of Montenegro;

- improved mechanisms for strengthening the system of protection and surveillance of the state border;

- improved system of control of traffic, warehousing and storage of weapons, explosives and other assets that can be used for terrorist attacks;

- improved mechanisms for strengthening surveillance of traffic and the use of dual-use goods;

- improved mechanisms for informing citizens and legal entities on the level of terrorist threats.

3.6.4. Remediation of damage from terrorist attacks

Goals in the field of remediation of damage from terrorist attacks include:

- improved and developed national capacities necessary for remediation of consequences of attacks and rehabilitation of damaged systems;

- developed mechanisms for rescuing people, material and cultural resources and the environment.

3.6.5. The criminal prosecution

Goals in the field of criminal prosecution of persons and entities associated with terrorism include:

- efficient criminal prosecution of the perpetrators, accomplices and other persons who are in any way associated with terrorist activities.

4. MONEY LAUNDERING AND TERRORIST FINANCING

One of the key requirements for the preparation of terrorist activities and their implementation is the provision of financial resources, acquired in an illegal manner. Money laundering and terrorist financing are global problems, which have negative effects on economic, political, security and social structure of each country. The consequences of money laundering and terrorist financing are: undermining the stability and efficiency of the financial system of the country, economic disruptions and instability, jeopardizing the planned reforms, a decrease of investment security and investment and jeopardizing both, national and international security.

4.1. Money laundering

According to the Criminal Code of Montenegro, the criminal act of money laundering is committed by any person who performs the conversion or transfer of money or other property with the knowledge that they were acquired through criminal activity, with the intent to conceal or misrepresent the origin of money or other property, or who acquires, holds or uses money or other property with knowledge, at the time of their admission, that they were acquired through criminal activity, or who conceals or misrepresents the facts about the nature, origin, place of deposit, movement, disposition or ownership of money or other property, knowing that they were acquired through criminal activity.

Money laundering, according to the Law on Prevention of Money Laundering and Terrorist Financing, includes:

1) Conversion or other transfer of money or other property acquired through criminal activity;

2) Acquisition, possession or use of money or other property acquired through criminal activity;

3) Concealing the nature, origin, place of deposit, movement, disposition, ownership or rights over money or other property acquired through criminal activity.

Money laundering can be divided into three basic stages: investment, stratification and integration, while it is important to note that in practice these stages are very difficult to observe and differentiate. During the first stage, the money, which is acquired through criminal activity, is introduced in the financial system. Afterwards, after the investment of cash, the stage of concealment is underway, when, by transferring to different accounts, an attempt is made to conceal the source of funds and their owner. At the same time, an attempt is made to conceal the link between the money and criminal activity from which the money originated. In the third stage, or the integration stage, the money is invested in legitimate businesses, or investments are made, so that it is considered to be acquired in a lawful manner.

Looking at these stages, in the fight against money laundering, the most can be done at the stage of investment, in which the institutions that take deposits are especially jeopardized. The European Community adopted regulations requiring the identification of the party that opens the account and makes payments, the obligatory keeping of appropriate records of deposits, and the notification of the competent authorities of suspicious financial transactions.

4.2. Terrorist financing

Terrorist financing, according to the Law on Prevention of Money Laundering and Terrorist financing, refers to providing or collecting, or an attempt of providing or collecting money or other property, directly or indirectly, with the goal or the knowledge that they will be used, as a whole or partially, for carrying out a terrorist act or used by terrorists or terrorist organizations, as well as inciting or assisting in providing or collecting funds or property.

Terrorist financing has several stages, namely: raising funds from legitimate businesses, storage and transfer of funds. In the first stage, funds are gathered from legitimate business companies, which are linked to terrorist organizations or individuals. In the next stages, the funds gathered are stored in different ways and transferred to terrorist organizations or individuals, for the purpose of implementing terrorist activities.

4.3. Analysis of the situation

On its way towards improving the legislative framework and accepting international standards in the fields of prevention and suppression of money laundering and terrorist financing, the starting point for Montenegro will be the exchange of existing experiences and information on the types and ways of sharing intelligence information of relevant institutions of the countries of the region. Bearing in mind that these phenomena exceed national borders, the countries of the region took a unique position that financial intelligence services shall be the proponents of the development of systems for the fight against money laundering and terrorist financing. In this regard, the financial intelligence services will, among other things, constantly work, through the media, on raising awareness of the professional and general public on the establishment of an effective system for the fight against money laundering and terrorist financing.

The Ministry of Finance issued the Rulebook on the guidelines for risk analysis in order to prevent money laundering and terrorist financing, on the basis of which the authorities who supervise the implementation of the Law on Prevention of Money Laundering and Terrorist financing

establish guidelines for risk analysis. In accordance with established guidelines, the obligated parties prepare the internal regulation on risk analysis.

The Law on Prevention of Money Laundering and Terrorist FINANCING from 2007 was brought in line with relevant international standards. The Law provides for a list of obligated parties who are required to submit, to the Administration for Prevention of Money Laundering and Financing Terrorism, reports on any cash transaction in the amount of EUR 15.000 or more, at the latest within three days from the date of the transaction, as well as on any transaction (regardless of the amount and type) for which there is suspicion of money laundering or terrorist financing, before the transaction itself is processed. The largest number of reports on suspicious transactions is submitted to the Administration for Prevention of Money Laundering and Financing Terrorism by banks. The Customs Administration also submits information on any cross-border transfer of cash, checks, bearer securities, precious metals and stones, the value of which is EUR 10.000 or more, as well as information on the transfer or attempted transfer of money, checks, etc., with a value or an amount less than EUR 10.000, if in relation to the specific person, there are reasons to suspect money laundering or terrorist financing. The Administration for Prevention of Money Laundering and Financing Terrorism can order a temporary (up to 72 hours) suspension of a transaction, if it assesses that there is a suspicion of money laundering or terrorist financing, notifying the competent authorities to take measures within their competence. The law defines the authorities who supervise the implementation of this Law in relation to different categories of obligated parties.

In practice, cases of money laundering are mainly based on: drugs and arms trafficking, corruption, abuse of an official position and abuse of authorizations in economy, fraud, counterfeiting documents, tax fraud, etc., as well as predicate criminal acts.

Potential threats in the field of money laundering can be: the creation of fictitious companies; investments in the construction industry; investments in real estate; investments in the privatization process.

In the MONEYVAL report on the third round of a detailed assessment of Montenegro in the field of money laundering and terrorist financing, the compliance with international standards was evaluated and out of 49 FATF recommendations, Montenegro has brought in line its system of prevention of money laundering and terrorist financing with 41 recommendations or - 83.67% (some 12% or 6 recommendations were not harmonized and 2 recommendations, or about 4% are not applicable). In March 2010, in the Council of Europe, a Progress Report for Montenegro in the field of money laundering and terrorist financing for last year was adopted.

4.3.1. National legal framework

Given that money laundering is a criminal activity with a high degree of social danger, and that this criminal act is very difficult to detect and prove, the fight against money laundering and terrorist financing also includes strengthening administrative, technical, personnel and material conditions for work of the institutions for fight against money laundering and terrorist financing. Montenegro is making great efforts to create appropriate legal requirements and to strengthen the institutions involved in the system for prevention of money laundering and terrorist financing. These institutions are: the judiciary and prosecutor's office, Police Directorate, Administration for Prevention of Money Laundering and Financing Terrorism, Agency for National Security, Customs Administration, Tax Administration.

Jurisdiction, competences and actions of the above-mentioned state authorities participating in the fight against money laundering and terrorist financing are regulated by several laws related to this criminal-law field:

Law on Prevention of Money Laundering and Terrorist Financing (Official Gazette of Montenegro 14/07 and 4/08); Criminal Code (Official Gazette of the Republic of Montenegro 70/03, 47/06 and Official Gazette of Montenegro 40/08, 25/10); Criminal Procedure Code (Official Gazette of Montenegro 57/09 and 49/10); Law on Banks (Official Gazette of Montenegro 17/08, 44/10); Customs Law (Official Gazette of the Republic of Montenegro 7/2002, 38/2002, 72/2002, 21/2003, 29/2005, 66/2006 and Official Gazette of Montenegro 21/2008); Law on Insurance (Official Gazette of the Republic of Montenegro 78/06 and Official Gazette of Montenegro 19/07, 53/09); Law on Voluntary Pension Funds (Official Gazette of the Republic of Montenegro 78/06 and 14/07); Law on Financial Leasing (Official Gazette of the Republic of Montenegro 81/05); Law on Games of Chance (Official Gazette of the Republic of Montenegro 52/04 and Official Gazette of Montenegro 13/07); Law on Securities (Official Gazette of the Republic of Montenegro 59/00, 10/01, 43/10, 28/06 and 53/09); Law on Investment Funds (Official Gazette of the Republic of Montenegro 49/04); Law on Education in Judicial Bodies (Official Gazette of the Republic of Montenegro 27/06); Law on Accounting and Auditing (Official Gazette of the Republic of Montenegro 69/05 and Official Gazette of Montenegro 80/08); Law on Payment System (Official Gazette of Montenegro 61/08); Law on State Audit Institution (Official Gazette of the Republic of Montenegro 28/04, 27/06, 78/06 and Official Gazette of Montenegro 17/07); Law on the Central Bank of Montenegro (Official Gazette of the Republic of Montenegro 52/00, 53/00, 47/01 and Official Gazette of Montenegro 40/10 and 46/10); Law on International Legal Assistance in Criminal Matters (Official Gazette of Montenegro 4/08); Law on Managing Seized and Confiscated Assets (Official Gazette of Montenegro 49/08); Law on Criminal Liability of Legal Persons (Official Gazette of Montenegro 2/07); Law on the State Property (Official Gazette of Montenegro 21/09).

A series of by-laws were adopted which were passed under the Law on the Prevention of Money Laundering and Terrorist Financing, Law on Banks and the Law on International Current and

Capital Transactions: Rulebook on the indicators for identifying suspicious customers and transactions (Official Gazette of Montenegro 69/09); Rulebook on drafting guidelines for risk analysis in order to prevent money laundering and terrorist financing (Official Gazette of Montenegro 20/09); Rulebook on the manner of submission of data on cash transactions valued at 15.000 euro or more and suspicious transactions to the Administration for Prevention of Money Laundering and Financing Terrorism (Official Gazette of Montenegro 79/08); Rulebook on the manner of work of authorized persons, manner of implementation of internal control, data storage and protection, manner of keeping records and training of employees (Official Gazette of Montenegro 80/08); Decision on the banking ombudsman (Official Gazette of Montenegro 15/09); Decision on the amount of cash that can be brought in and out of the Republic of Montenegro without reporting (Official Gazette of the Republic of Montenegro 58/05); Decision on records of accounts for performing international payment transactions (Official Gazette of Montenegro 09/24); Decision on internal audit in banks (Official Gazette of Montenegro 60/2008); Decision on minimum standards for managing interest rate risk, which does not derive from commercial activities of the bank (Official Gazette of Montenegro 60/2008); Decision on minimum standards for managing liquidity risk in banks (Official Gazette of Montenegro 60/2008); Decision on the basis of the internal control system in banks (Official Gazette of Montenegro 60/2008); Decision on minimum standards for market risks management in banks (Official Gazette of Montenegro 60/2008); Decision on minimum standards of bank operations with entities related to the bank (Official Gazette of Montenegro 60/2008); Decision on records of accounts for performing international payment transactions (Official Gazette of Montenegro 24/2009); Decision on the minimum elements of credit and debit orders (Official Gazette of Montenegro 24/2009 and 41/2009); Decision on conditions and manner of performing certain tasks in carrying out transfers of funds by an agent (Official Gazette of Montenegro 24/2009); Decision on the manner of exercising payment systems control (Official Gazette of Montenegro (24/2009); Decision on minimum standards for risk management in micro-lending financial institutions (Official Gazette of Montenegro 24/2009 and 41/2009); Decision on methods for making consolidated financial statements of banking groups (Official Gazette of Montenegro 24/2009); Decision on minimum standards for operational risk management in banks (Official Gazette of Montenegro 24/2009).

New regulations in the Criminal Code, in accordance with MONEYVAL recommendations and regulations laid down, inter alia, in the UN Convention against Transnational Organized Crime with Protocols thereto (Palermo Convention) and the United Nations Convention on the Unlawful Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) amended the definition of the crime of money laundering referred to in Article 268. The new definition in the Criminal Code abolished earlier restriction of the crime of money laundering as operations which covered "banking, financial and other business operations". The definition includes every aspect of exchange (conversion) and transmission, as well as acquisition, possession and use of money or other assets acquired through crime. Concealment and misrepresentation of facts concerning the nature, origin, place of deposit, movement, ownership or disposition of money or other property obtained by crime were also criminalized.

Amendments to the Criminal Code in Article 449 revised the definition of act of terrorist financing, which includes activities that contribute to the financing of terrorism and which are not strictly raising money and securities. The definition includes provision of funds or property for the purposes of terrorist financing. The terms "funds" and "property" are interpreted broadly in line with ratified international conventions.

The new definition of terrorism financing lays down imprisonment sentences ranging from one to ten years for anyone who in any way provides or collects money, securities, other assets or property which is intended to be wholly or partly used for financing criminal acts referred to in Art. 447 (terrorism), 447a (public calls to commit acts terrorism), 447b (recruitment and training for terrorist acts), 447c (use of a lethal device), 447d (destroying and damaging a nuclear facility) and 448 (threatening an internationally protected person) of the Criminal Code or for financing either organizations that aim to carry out such crimes, or members of such organizations.

Montenegro has ratified the Convention for the Suppression of the Financing of Terrorism (Official Gazette of the FRY – International Treaties 7/02), as well as the Palermo Convention and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention). Bearing in mind the hierarchy of normative acts stipulated by the Constitution, the terms "funds", "property", "confiscation", "seizure", "predicate offense" and other defined in that Convention are an integral part of our law and order and are applicable in case law.

Measures to detect and prevent money laundering and terrorist financing are undertaken by obligated parties before and during all activities of receiving, investing, exchanging, storing or other disposition of money or other property, other transactions in accordance with this Law and regulations adopted pursuant to this Law, and during all transactions for which there are grounds to suspect that they are of money laundering and terrorist financing nature.

Law on the Prevention of Money Laundering and Terrorist Financing has been harmonized with the requirements of international organizations and institutions and relevant regulations on the prevention of money laundering and terrorist financing, as follows:

1. Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering;

2. Directive 2001/97/EC of the European Parliament and of the Council;

3. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;

4. FATF (40 +8 +1) Recommendations;

5. UN Convention against Corruption.

4.3.2. International legal framework

Montenegro contributes to suppressing money laundering and terrorist financing at the regional and global levels by fulfilling the obligations arising from membership in international organizations, as well as via intensive cooperation with the competent authorities of other countries through exchange of information. As a member of the United Nations, Montenegro implements measures pursuant to UNSC Resolutions 1267 (1999), 1333 (2000), 1390 (2002), 1455 (2003), 1526 (2004) and 1373 (2001). Montenegro is a member of the Egmont Group (world association of financial intelligence units), a full member of MONEVAL, and in June 2010 Montenegro was admitted as a member of the Eurasian Group (EAG), with the status of observer.

The list of international legal instruments ratified by Montenegro and the list of bilateral treaties on the prevention of money laundering and terrorist financing are given in Annexes I and II.

4.3.3. Institutional framework

The competent national authorities, parties subject to the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing and otfher natural and legal persons are engaged in the fight against money laundering and terrorist financing.

The Division for suppressing organized crime, corruption, terrorism and war crimes was established within the **Supreme Public Prosecutor's Office**. The Special Prosecutor is a coordinator in resolving issues related to money laundering and setting up cooperation with relevant national and international institutions.

Specialized divisions for trials in cases of organised crime, corruption, terrorism and war crimes were established in **High Court in Podgorica and High Court in Bijelo Polje**. Trials for money laundering and terrorist financing are under the jurisdiction of these specialized divisions.

Specialized divisions, which administer justice in cases related to crimes of money laundering and terrorist financing, have trained personnel and they are equipped to work effectively.

From an organizational point of view, the **Police Directorate** is divided into several departments. As regards fight against money laundering and terrorist financing, the most important is the Criminal Police Department, parts of which are the Division for Combating Organized Crime and Corruption and the Division for Combating Economic Crimes.

According to the Law on the Prevention of Money Laundering and Terrorist Financing, **Administration for Prevention of Money Laundering and Financing Terrorism** performs administrative functions related to detecting and preventing money laundering and terrorist financing, as laid down in law and other regulations. Administration for Prevention of Money Laundering and Financing Terrorism was organized as a financial and intelligence administrative type unit, whose work is supervised by the Ministry of Finance. The Administration is responsible for tasks related to detecting and preventing money laundering and terrorist financing, related to collecting, analyzing and disseminating to the competent bodies data, information and documentation necessary for the detection of money laundering and terrorist financing.

Tax Administration performs tasks related to: initiating and conducting first instance misdemeanor proceedings and imposing penalties and protective measures for tax violations and preventing and detecting crimes and corporate offences in misdemeanor procedure.

Customs Administration carries out: customs supervision; clearance of goods; control of goods whose import or export are specially regulated; foreign exchange control in international travel and cross-border traffic with foreign countries; prevention and detection of customs violations and conducting administrative and first instance misdemeanor procedures; prevention and detection of crimes and corporate offences in customs procedures; preventing and detecting foreign exchange related violations in international travel and cross-border traffic; processing and monitoring statistical data on imports and exports, as well as other duties placed under its competence.

Supervision over the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing is carried out by:

Ministry of Finance, which monitors the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing in cases of audit companies, independent regime and legal relations of natural persons engaged in accounting and tax consulting services.

Through an authorised official and in accordance with the law governing inspection control, **Administration for Prevention of Money Laundering and Financing Terrorism** carries out inspection control over the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing in: humanitarian, nongovernmental and other nonprofit organizations and business associations, legal persons, entrepreneurs and natural persons engaged in the activity or activities of: buying and selling receivables; factoring; asset management for third parties; issuing payment and credit cards and carrying out transactions with those cards; financial leasing; organizing travels; trade in real estate; trade in motor vehicles; trade in vessels and aircraft; storage in safes; issuing guarantees and other warranties; lending and loan brokering; lending and mediation in contracting lending; brokerage or representation in life insurance; insurance; organizing and conducting auctions, trade in works of art, precious metals and precious stones and articles made from precious metals and stones, and other goods, if payment is in cash in the amount of 15,000 euro or more, in one or a number of related transactions.

In accordance with the Law on the Central Bank of Montenegro, among other things, **Central Bank of Montenegro** monitors the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing in banks, branches of foreign banks, other financial organizations, organizations engaged in payment transactions, savings banks, saving-banks, exchange offices and companies for the issuance of electronic money.

Securities Commission, among others, performs supervision over the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing, in: investment funds management companies and branch offices of foreign companies for managing investment funds, pension funds management companies and branch offices of foreign companies for managing pension funds, as well as stockbrokers and branch offices of foreign stockbrokers.

In accordance with the Law on Electronic Communications, among others, **Agency for Electronic Communications and Postal Services** performs supervision over the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing by the national postal service.

Insurance Supervision Agency monitors the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing in insurance companies and branch offices of foreign insurance companies engaged in life insurance activities.

Administration for Games of Chance supervises the implementation of the Law on the Prevention of Money Laundering and Terrorist Financing on the part of organizers of classical and special games of chance.

In addition to these bodies and institutions, the Banking Association of Montenegro, Institute of Accountants and Auditors, etc. also deal with issues of money laundering.

4.4. Strategic response of Montenegro to the threat of money laundering and terrorist financing

Montenegro has made significant progress, especially in terms of creation of legal and institutional measures for suppressing the crimes of money laundering and terrorist financing.

Owing to the adoption of the Criminal Procedure Code (Official Gazette of Montenegro 57/09 and 49/10), secret surveillance measures can be applied in relation to a higher number of crimes compared to the past, and such offences are enumerated so as to include, inter alia, corruption crimes (money laundering, causing false bankruptcy, abuse of evaluation of assets, passive bribery, active bribery, disclosure of an official secret, trading in influence, abuse of authority in economy, abuse of an official position and fraud in the conduct of an official duty). In fact, under the previous Code, it was not possible to apply secret surveillance measures for certain criminal offenses, which would be more difficult to prove without the application of these measures. The application of measures of secret surveillance is provided for criminal acts against the security of computer data that are difficult to prove and complicated to detect precisely due to the use of sophisticated computer technology, which will further contribute to a more efficient fight against organized crime, terrorism, money laundering and terrorist financing.

By-laws necessary to implement the Law on the Prevention of Money Laundering and Terrorist Financing were adopted. Rules and procedures were established for reporting transactions executed in cash amounting to 15.000 euro and above, as well as for reporting suspicious transactions to the Administration for Prevention of Money Laundering and Financing Terrorism, which also relates to rules for organizing records and manner of keeping them, professional development of staff and performance of internal control within entities obliged to report to the Administration for Prevention of Money Laundering and Financing Terrorism. Rulebook on the development of risk analysis in order to prevent money laundering and terrorist financing was drawn up in March 2009, as well as Rulebook revising the list of indicators for identifying suspicious customers and transactions. Administration for Prevention of Money Laundering and Financing Terrorism has databases of suspicious transactions and cash transactions higher than the statutory

limit. Management has made the purchase of an important analytical tool (IBASE), which will allow for better national and international cooperation and data exchange with other law enforcement authorities.

It is necessary to further improve the legal, institutional, personnel, administrative, material and technical capacities of the competent authorities in the fight against money laundering and terrorist financing, in accordance with new threats and challenges.

4.5. The goals of fight against money laundering and terrorist financing

are implemented via:

- improvement of normative and legal framework;
- developed human resources, administrative, material and technical capacities;
- improved institutional cooperation aimed at effective exchange of information;
- improved international cooperation;
- established centralized information system between the competent authorities;
- conducted new programs, trainings and specializations;
- applied MONEYVAL recommendations;
- prepared and adopted risk analysis.

5. CONCLUSION

Adoption of the Strategy is one of the key conditions for more effective prevention and suppression of socially dangerous phenomena of terrorism, money laundering and terrorist financing and represents a response to new challenges and threats to stability and peace in the country.

Implementation of the Strategy involves coordinated action by all actors involved in combating terrorism, money laundering and terrorist financing. National Commission for the implementation of

the Strategy for the Prevention and Suppression of Terrorism, Money Laundering and Terrorist Financing will carry out control of the implementation of this Strategy in the period 2010-2012, during which the Action Plan will be implemented.

Objectives, specific activities of all the authorities competent for implementation of the Strategy and time-frame for implementation of objectives and measures envisaged in the Strategy will be laid down in the 2010-2012 Action Plan.

Annex I

United Nations conventions:

United Nations Convention against Transnational Organized Crime with Protocols thereto (Official Gazette of FRY 6/2001) assumed by succession, entered into force on 03/06/2006
United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), (Official Gazette of SFRY - International Treaties 14/90), assumed by succession, entered into force on 03/06/2006
Convention on Offences and Certain Other Acts Committed on Board Aircraft (Official Gazette of SFRY - International Treaties 47/70), assumed by succession, entered into force on 03/06/2006
International Convention against the Taking of Hostages (Official Gazette of SFRY - International Treaties 09/84), assumed by succession, entered into force on 03/06/2006
Criminal Law Convention on Corruption (Official Gazette of FRY - International Treaties 02/02 and Official Gazette of the Republic of Montenegro 18/05), assumed by succession, entered into force on 03/06/2006
International Convention for the Suppression of the Financing of Terrorism (Official Gazette of FRY 07/02), assumed by succession, entered into force on 03/06/2006
International Convention for the Suppression of Terrorist Bombings (Official Gazette of FRY 12/02), assumed by succession, entered into force on 03/06/2006
UN Convention against Corruption (Official Gazette of Serbia and Montenegro - International Treaties 11/05), assumed by succession, entered into force on 03/06/2006

International Convention for the Prevention of Acts of International Terrorism (Official Gazette of Serbia and Montenegro - International Treaties 06/02), assumed by succession, entered into force on 03/06/2006
International Convention for the Suppression of Acts of Nuclear Terrorism (Official Gazette of Serbia and Montenegro - International Treaties 2/2006), assumed by succession, entered into force on 03/06/2006
Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Official Gazette of SFRY - International Treaties 14/89); assumed by succession, entered into force on 03/06/2006
Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organized Crime (Official Gazette of Serbia and Montenegro - International Treaties 11/05), assumed by succession, entered into force on 03/06/2006
Montenegro ratified
Additional Protocol to the Criminal Law Convention on Corruption (Official Gazette of Montenegro 11/07)
Convention on Cluster Munitions (Official Gazette of Montenegro, International Treaties 4/09)

Council of Europe conventions:

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Official Gazette of FRY 01/92), assumed by succession, entered into force on 03/06/2006
European Convention on Extradition, with Additional Protocols thereto (Official Gazette of FRY 10/01), assumed by succession, entered into force on 03/06/2006
European Convention on the Transfer of Sentenced Persons with Additional Protocol thereto (Official Gazette of FRY 01/04), assumed by succession, entered into force on 03/06/2006
European Convention on the Suppression of Terrorism (Official Gazette of FRY 10/01), assumed by succession, entered into force on 03/06/2006
European Convention on the Transfer of Proceedings in Criminal Matters (Official Gazette of FRY 10/01), assumed by succession, entered into force on 03/06/2006
European Convention on Mutual Assistance in Criminal Matters with Additional Protocol thereto (Official Gazette of FRY 10/01 and Official Gazette of Serbia and Montenegro - International

Treaties 2/06), assumed by succession, entered into force on 03/06/2006
European Convention on the International Validity of Criminal Judgments with Annexes thereto (Official Gazette of SFRY - International Treaties 13/02 and 02/06), assumed by succession, entered into force on 03/06/2006
Agreement on Cooperation to Prevent and Combat Trans-border Crime (Official Gazette of Serbia and Montenegro - International Treaties 05/03), assumed by succession, entered into force on 03/06/2006

Montenegro has ratified the following Council of Europe conventions and protocols:

Civil Law Convention on Corruption (Official Gazette of Montenegro - International Treaties 1/08)
Council of Europe Convention on Action against Trafficking in Human Beings (Official Gazette of Montenegro, International Treaties 4/08)
Council of Europe Convention on the Prevention of Terrorism (Official Gazette of Montenegro, International Treaties 5/08)
Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Official Gazette of Montenegro, International Treaties 5/08)
Convention on Cybercrime (Official Gazette of Montenegro, International Treaties 4/09)
Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (Official Gazette of Montenegro, International Treaties 4/09)
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Official Gazette of Montenegro, International Treaties 5/08)
Police Cooperation Convention for Southeast Europe (Official Gazette of Montenegro 1/08)
Agreement on Strategic Cooperation between Montenegro and the European Police Office (Official Gazette of Montenegro, International Treaties 2/09).

Annex II

List of bilateral treaties on cooperation in the fight against organized crime

Treaties signed by the Government of Montenegro

Cooperation Agreement between the Government of the Republic of Bulgaria and the Government of the Republic of Montenegro on Cooperation in Fighting Terrorism, Organized Crime, Illicit Traffic in Narcotics, Psychotropic Substances and Precursors, Illegal Migration and Other Criminal Offences (2005);
Agreement between the Government of the Republic of Albania and the Government of

Montenegro on Cooperation in Fighting Terrorism, Organized Crime, Trafficking and Other Illegal Activities (2003);
Agreement between the Government of Montenegro and the Government of the Republic of Turkey on Police Cooperation (2007);
Agreement between the Government of the Republic of Slovenia and the Government of Montenegro on Cooperation in the Fight against Organized Crime, People Trafficking and Illegal Migration, Trafficking in Illegal Drugs and Precursors, Terrorism and Other Forms of Crime (2006);
Agreement between the Government of Montenegro and the Council of Ministers of Bosnia and Herzegovina on Cooperation in Combating Terrorism, Organized Crime, Trafficking in Drugs, Psychosomatic Substances and Precursors, Illegal Migration and Other Criminal Acts (2007);
Agreement between the Government of the Republic of Montenegro and the Government of the Republic of Macedonia on Cooperation in Combating Terrorism, Organized Crime, Illegal Trafficking in Narcotics, Psychotropic Substances and Precursors, Illegal Migration, and Other Crimes (2003);
Memorandum of Understanding on Police Cooperation between the Government of the Republic of Montenegro and the United Nations Interim Administration Mission in Kosovo (2003).

Agreements signed by MoI&PA / Police Directorate

Agreement between the MoI of Montenegro and the MoI of the Republic of Croatia on Police Cooperation (2005);
Agreement between the MoI of Montenegro and Federal MoI of the Republic of Austria on Police Cooperation (2004);
Protocol on Police Cooperation between the Ministry of Interior of Montenegro and the Ministry of Interior of Romania (2006);
Protocol between the MoI of Montenegro and the MoI of the Republic of Serbia on Cooperation in Combating Terrorism, Organized Crime, Illegal Trafficking in Narcotics, Psychotropic Substances and Precursors, Trafficking in Human Beings, Illegal Migration and Other Criminal Acts, as Well as on Cooperation in Other Areas under Their Competences (2003);
Agreement on Cooperation between the Ministry of Interior of Montenegro and the Ministry of Interior of the Russian Federation from 2008.

THE FIELD OF PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Agreements signed by the AfPMLaFT

Agreements
Agreement on Mutual Cooperation with FIU Serbia, 16/04/2004,
Agreement on Mutual Cooperation with FIU Albania, 16/04/2004,
Agreement on Mutual Cooperation with FIU B&H, 19/04/2005,
Agreement on Mutual Cooperation with FIU Macedonia, 29/10/2004,
Agreement on Mutual Cooperation with FIC - Financial Information Centre UNMIK – Kosovo, 07/12/2004,
Agreement on Mutual Cooperation with FIU Slovenia, 28/12/2004,
Agreement on Mutual Cooperation with FIU Croatia, 24/03/2005,
Agreement on Mutual Cooperation with FIU Bulgaria, 11/04/2006,
Agreement on Mutual Cooperation with FIU Portugal, 11/06/2007,
Agreement on Mutual Cooperation with FIU Russia, 07/09/2007,
Agreement on Mutual Cooperation with FIU Poland, 15/11/2007,
Agreement on Mutual Cooperation with FIU Romania, 10/10/2008,
Agreement on Mutual Cooperation with the Financial Crimes Enforcement Network - FinCEN, 22/10/2008,
Agreement on Cooperation with the FIC of EULEX Mission in Kosovo, 20/02/2009,
Agreement on Mutual Cooperation with the State Committee for Financial Supervision of Ukraine, 27/05/2009,
Agreement on Mutual Cooperation with the Unit for Preventing Money Laundering and Suspicious Cases - FIU of the United Arab Emirates, 06/07/2009,
Regional Protocol on Combating Money Laundering in Order to Promote Regional Cooperation, was signed by representatives of FIUs of Montenegro, Serbia, Albania, Slovenia, Croatia, B&H at the II

Regional Conference of Financial Intelligence Units, in April 2008.

CUSTOMS COOPERATION

Agreement between the Government of the SFRY and the Government of the Polish People's Republic on Cooperation and Mutual Assistance in Customs Matters (signed on 9 May 1967 in Warsaw),
Agreement on Administrative Assistance in Preventing, Detecting and Combating Customs Offenses between the Government of the SFRY and the Government of the Republic of France (signed on 28 April 1971 in Belgrade),
Treaty between the Socialist Federal Republic of Yugoslavia and the Federal Government of the Republic of Germany on Mutual Administrative Assistance in Prevention, Investigation and Suppressing Violations of Customs Regulations (signed on 2 April 1974, in Bonn),
Agreement between the Socialist Federal Republic of Yugoslavia and the Republic of Austria on Administrative Assistance in Customs Matters in Suppressing Violations of Customs Regulations (signed on 15 March 1978, in Belgrade),
Agreement between the Federal Executive Council of the Socialist Federal Republic of Yugoslavia Parliament and the Government of the Republic of Greece on Cooperation and Mutual Assistance in Customs Matters (signed on 4 October 1983, in Athens),
Agreement between the Federal Executive Council of Socialist Federal Republic of Yugoslavia Parliament and the Government of the People’s Republic of China on Cooperation in Customs Matters (signed on 23 January 1989, in Belgrade),
Agreement between the Federal Executive Council of the Socialist Federal Republic of Yugoslavia and the USA Government on Mutual Assistance between their Customs Administrations (signed on 11 April 1990, in Belgrade),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Russian Federation on Cooperation and Mutual Assistance of Customs Services (signed on 6 November 1996, in Moscow),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Republic of Macedonia on Customs Cooperation and Mutual Assistance (signed on 4 September 1996, in Skopje),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Republic of Bulgaria on Customs Cooperation and Mutual Assistance (signed on

4 June 1997, in Belgrade),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Czech Republic on Mutual Assistance in Customs Matters (signed on 9 September 1998 in Belgrade),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of Romania on Customs Cooperation and Administrative Assistance in Preventing, Investigations and Suppression of Customs Offences (signed on 14 January 1998, in Belgrade),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of Republic of Hungary on Cooperation and Mutual Assistance in Customs Matters (signed on 24 September 1998, in Belgrade),
Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Republic of Slovakia on Customs Cooperation (signed on 28 March 2001, in Belgrade),
Agreement between the Federal Republic of Yugoslavia and Bosnia and Herzegovina on Customs Cooperation and Mutual Assistance (signed on 18 December 2001 in Sarajevo),
Agreement on Mutual Administrative Assistance between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Republic of Italy in Prevention, Investigating and Suppression of Customs Offences (signed on 10 November 1965, in Belgrade),
Agreement on Mutual Administrative Assistance between the Federal Government of the Federal Republic of Yugoslavia and the Government of the Republic of Turkey in Prevention, Investigating and Suppression of Customs Offences (signed on 6 February 2002, in Istanbul),
Agreement between the Government of the Republic of Montenegro and the Government of the Republic of Croatia on Mutual Assistance in Customs Matters (signed on 9 December 2005, in Podgorica),
Agreement between the Government of the Republic of Montenegro and the Council of Ministers of the Republic of Albania on Mutual Assistance in Customs Matters (signed on 26 December 2005, in Tirana),
Agreement between the Government of the Islamic Republic of Iran, Government of the Republic of Serbia and the Government of the Republic of Montenegro on Mutual Assistance and Cooperation in Customs Matters (signed on 1 June 2005, in Teheran),
Memorandum of Understanding between the Customs Administration of Montenegro and the Customs Service of United Nations Interim Administration Mission in Kosovo (UNMIK) on Cooperation and Mutual Administrative Assistance in Customs Matters (signed on 19 November 2004 in Podgorica),
Customs Administration exercises cooperation pursuant Annex 5 on Mutual Administrative Assistance in Customs Matters of the Agreement to Amend and Enlarge the Central European Free

Trade Agreement – CEFTA 2006. CEFTA signatories which exercise cooperation pursuant to the afore-mentioned Annex are: Republic of Albania, Bosnia and Herzegovina, Republic of Croatia, Republic of Macedonia, Republic of Moldova, Montenegro, Republic of Serbia and UNMIK /Kosovo. This Agreement represents amendment to the agreements on mutual assistance in customs matters, which may be or have already been concluded between the CEFTA signatories.

Agreements signed by the Supreme Public Prosecutor's Office

- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and the Public Prosecutor's Office of the Republic of Croatia on the Fight against Organized Crime
- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and the Public Prosecutor's Office of Bosnia and Herzegovina,
- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and the Public Prosecutor's Office of the Republic of Serbia,
- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and the Public Prosecutor's Office for War Crimes of the Republic of Serbia,
- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and EULEX Office - Special Public Prosecutor's Office of the Republic of Kosovo,
- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and the General Prosecutor's Office of the Republic of Albania,
- Cooperation Agreement between the Supreme Public Prosecutor's Office of Montenegro and the General Prosecutor's Office of Ukraine.

THE 2010-2012 ACTION PLAN FOR PREVENTION AND SUPPRESSION OF TERRORISM, MONEY LAUNDERING AND TERRORIST FINANCING

	OBJECTIVE	MEASURE	COMPETENT BODY	TIME LIMIT	SUCCESS INDICATORS
I TERORISM					
1. TERRORISM PREVENTION					
1	Enhanced normative and legal framework	Analysis of the existing and drafting of new regulations	MoI & PA, Agency for National Security (AfNS), Police Directorate (PD)	2011	Analysis developed
		Developing a Rulebook on engagement of the Special Anti-terrorist Unit	PD	2011	Rulebook developed
		Developing a Rulebook on engagement of the Special Police Unit	PD	2011	Rulebook developed
		Developing a Rulebook on the use of ad hoc negotiating team	PD	2011	Rulebook developed

2	Developed human resources, administrative and material and technical capacities	Development of new rulebooks on organization and job descriptions	AfNS PD	2011	New rulebooks on organization and job descriptions adopted
		Recruiting the necessary staff	Ministry of Defence (MoD) AfNS PD	continuously	Achieved staffing, occupancy rate compared to the job descriptions
		Drafting the Needs Plan for the supply of missing material and technical resources and specialist equipment for Special Anti-terrorist Unit, Special Police Unit and Counter Terrorism Search Team	PD	2010/ continuously	Needs Plan developed
		Supply of technical equipment for measures of secret surveillance to be used by the Special Anti-terrorist Unit, Special Police Unit and Counter Terrorism Search Team	PD	continuously	Percentage of equipment procured compared to the planned equipment
		Strengthening intelligence system in the process of intelligence gathering	AfNS PD	continuously	
		Further improvement of existing technical solutions	AfNS	continuously	The level of upgraded technical equipment

3	New training and specialization programs conducted	Organise trainings for judges and public prosecutors in order for them to get acquainted with international conventions and laws	Coordinating Committee Judicial Training Center	continuously	Number of trainings organized
		Organise trainings for judges and public prosecutors in terms of enforcing statutory provisions	Coordinating Committee Judicial Training Center	continuously	Number of trainings organized
		Organize training to identify and prevent radicalization and extremism that can potentially grow into terrorism	AfNS PD	continuously	Number of organized trainings
		Needs assessment and training of personnel in the field of protection against sabotage and biochemical protection	PD	continuously	Report on the types and number of required trainings
		Conducting trainings of Criminal Police Department employees working on investigations of terrorism	PD	continuously	Number of trainings conducted, number of participants
		Strengthening the capacities of Special Anti-terrorist Unit and Special Police Unit by intensifying	PD	continuously	Number of trainings at the regional level

		specialized trainings and through cooperation and exchange of experiences with renowned special forces in the region and beyond			
		Participation in joint training with forces from other institutions in Montenegro; NATO forces and other foreign armed forces	PD MoD / Army of Montenegro	continuously	Number of trainings conducted, number of participants
		Intensifying specialist trainings of the Agency for National Security staff engaged in working field of combating terrorism	AfNS	continuously	Number of trainings conducted, number of participants
4	Improved cooperation among all relevant institutions in the country, within the regional and at international level	Organize meetings with relevant institutions in the country – signing of a protocol on cooperation	MoI & PA MoD AfNS PD	continuously	The number of organized meetings, the number of signed protocols
		Participation of employees in working bodies, groups and projects aimed at combating terrorism	MoI & PA MoD AfNS PD	continuously	The number of working groups and bodies in which representatives of MNE participate Reports from meetings
		Plan and implement joint activities in the country, within the region and at international level	MoI & PA MoD AfNS PD	continuously	Number of joint activities implemented

5	Improved mechanisms for preventing propaganda and public calls to commit acts of terrorism, and incitement of terrorism in any way	Analysis of existing statutory provisions, with proposed measures to prevent propaganda, public calls to commit acts of terrorism and inciting terrorism in any way	MoI & PA Ministry of Justice (MoJ)	2012	Analysis with proposed measures developed
2. SUPPRESSING TERRORISM					
6	Improved mechanisms for disabling the organizational and logistics activities having terrorist intentions	Analysis of possible organizational and logistics activities with terrorist intentions	AfNS PD	2012	Analysis developed
7	Improved mechanisms for detection and prosecution of all persons who are related to terrorism or for detection of all activities directed against Montenegro, other states and/or international organizations	It will be defined in the next 2012-2014 Action Plan	AfNS PD	2012-2014	
8	Improved mechanisms for preventing movements and stay of all persons associated with	Deployment of Interpol's services at border crossings, in order to perform direct searches in Interpol's databases and checks of	PD		Number of border crossings networked with NCB Interpol, compared to the total number of border crossings

	terrorism in the territory of Montenegro	persons, travel documents and vehicles at border crossings			
9	Improved mechanisms for the prevention of criminal activities that may be directly or indirectly linked to terrorism	Objective defined by the measures set out in part on terrorism prevention	PD		Reporting on the basis of measures to prevent terrorism
3. PROTECTION AGAINST TERRORISM					
10	Improved mechanisms for developing and strengthening the protection of infrastructure facilities of special importance to the territory of Montenegro	It will be defined in the next 2012-2014 Action Plan			
11	Improved mechanisms for strengthening the system of protection and surveillance of state borders	Procurement of necessary equipment	PD	continuously	Equipment procured
12	Improved control system of transport, storage and safekeeping of weapons, explosives and other devices that can be used for terrorist	Analysis of the existing control system of transport, storage and safekeeping of weapons, explosives and other devices	MoI & PA MoD	2011	Analysis developed

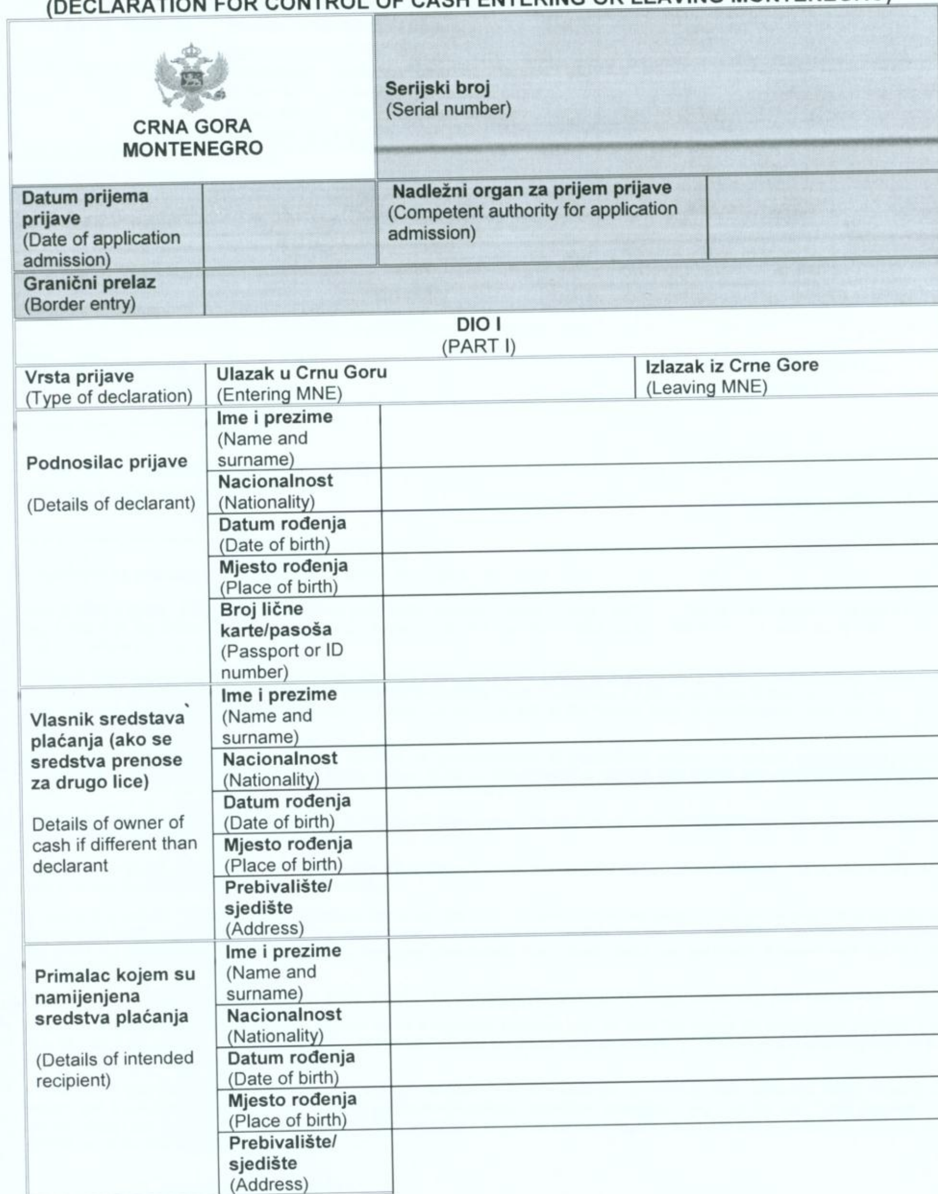
	attacks				
13	Improved mechanisms for strengthening supervision of trade in and use of dual-use goods	Analysis of the existing supervision system of trade in and use of dual-use goods	MoI & PA Ministry of Health (MoH)	2011	Analysis done
14	Improved mechanisms for informing citizens and legal entities on the level of terrorist threats	Enhance cooperation of state authorities with the media, which contributes to more objective public information	Competent bodies	continuously	Number of held press conferences
4. REPAIRING DAMAGE FROM TERRORIST ATTACKS					
15	Improved and developed national capacities necessary to redress the consequences of attacks and rehabilitation of damaged systems	It will be defined in the next 2012-2014 Action Plan		2012-2014	
16	Developed mechanisms of saving people, material and cultural resources and the environment	It will be defined in the next 2012-2014 Action Plan		2012-2014	
5. CRIMINAL PROSECUTION					
	Effective enforcement of criminal prosecution of	Analysis of harmonization of legislation with international	MoJ	continuously	Ensured compliance

17	perpetrators, accomplices and others who are in any way connected with terrorist activities	standards and conventions			
		Production of semi-annual analysis of statistical indicators concerning the number of cases in the field of terrorism	PD Supreme Public Prosecutor's Office High Public Prosecutor's Office	continuously	Joint report of institutions
		Conducting trainings in the field of financial investigations	MoJ PD Supreme Public Pros's Office High Public Pros's Office AfPMLaFT		Number of trainings conducted, number of participants per institutions
II MONEY LAUNDERING AND TERRORIST FINANCING					
18	Improvement of normative and legal framework	Analyze legislation and ensure its compliance with international standards and conventions	AfPMLaFT	continuously	The number of regulations that were analyzed and the number and names of conventions that were analyzed
		Drawing up new laws and by-laws that	Ministry of	2011	Number of adopted or amended

		comply with international standards and conventions	Finance (MoF), AfPMLaFT		regulations
		Making the amended list of indicators of suspicious transactions	MoF, AfPMLaFT, Central Bank of MNE, in cooperation with competent authorities referred to in Art. 86 of the Law	2011	Amended list of indicators of suspicious transactions adopted
19	Developed human resources, administrative and material and technical capacities	Amendments of and adoption of Rulebook on internal organization and job descriptions, in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing	AfPMLaFT	2011	Rulebook adopted
		Recruiting the necessary staff	AfPMLaFT PD	continuously	Achieved staffing, occupancy rate compared to the job descriptions
		Needs assessment and procurement of equipment needed for work, in accordance with recognized trends in the field of money laundering	AfPMLaFT	2010/ continuously	Needs estimated, the percentage of acquired equipment compared to the necessary equipment

20	Improved institutional cooperation aimed at effective exchange of information	Analysis of the implementation of agreements on cooperation with other authorized state agencies and organizations and needs assessment for concluding new agreements	AfPMLaFT PD	2010/ continuously	Analysis made, the number of new agreements or revisions of the existing agreements
		Efficient data exchange among institutions	AfPMLaFT PD	continuously	The number of submitted reports on suspicious transactions to Prosecution Office and police which resulted in inter-institutional cooperation
21	Improved international cooperation	Analysis of the implementation of agreements on cooperation with financial intelligence units (FIU) in the region, and needs assessment to conclude new agreements	AfPMLaFT	2010/ continuously	Analysis made, the number of new agreements or revisions of the existing agreements
		Efficient exchange of financial and intelligence information, data and documentation with authorized bodies of other countries and international organizations	AfPMLaFT	continuously	The number of submitted reports on suspicious transactions to Prosecution Office and police which resulted in international cooperation
	Established centralized information system between the competent authorities	Providing links and connections to computer networks and databases of institutions	AfPMLaFT, PD in cooperation with the		Links provided, centralized information system established

			competent authorities		
22	New training and specialization programs conducted	Participation in seminars organized by international institutions as well as in working groups of the Egmont Group	AfPMLaFT	continuously	Number of seminars, number of meetings of EGMONT
		Organizing seminars and symposia for authorized persons of obligated parties and employees who have direct contact with clients	AfPMLaFT, PD, in cooperation with competent authorities	continuously	Total number of seminars and symposia by institutions and fields
23	Applied MONEYVAL recommendations	Realization of Government conclusions dated 23 April 2009	Competent bodies	continuously	Number of executed conclusions
24	Prepared and adopted risk analysis	Adopting guidelines on risk analysis	Supervisory authorities referred to in Art. 86 of the Law on PMLTF	2010	Guidelines adopted



OBRAZAC

PRIJAVA O FIZIČKOM UNOŠENjU ILI IZNOŠENjU SREDSTAVA PLAĆANjA
(DECLARATION FOR CONTROL OF CASH ENTERING OR LEAVING MONTENEGRO)

CRNA GORA MONTENEGRO		Serijski broj (Serial number)	
Datum prijema prijave (Date of application admission)		**Nadležni organ za prijem prijave** (Competent authority for application admission)	
Granični prelaz (Border entry)			

DIO I
(PART I)

Vrsta prijave (Type of declaration)	**Ulazak u Crnu Goru** (Entering MNE)	**Izlazak iz Crne Gore** (Leaving MNE)
Podnosilac prijave (Details of declarant)	**Ime i prezime** (Name and surname)	
	Nacionalnost (Nationality)	
	Datum rođenja (Date of birth)	
	Mjesto rođenja (Place of birth)	
	Broj lične karte/pasoša (Passport or ID number)	
Vlasnik sredstava plaćanja (ako se sredstva prenose za drugo lice) Details of owner of cash if different than declarant	**Ime i prezime** (Name and surname)	
	Nacionalnost (Nationality)	
	Datum rođenja (Date of birth)	
	Mjesto rođenja (Place of birth)	
	Prebivalište/ sjedište (Address)	
Primalac kojem su namijenjena sredstva plaćanja (Details of intended recipient)	**Ime i prezime** (Name and surname)	
	Nacionalnost (Nationality)	
	Datum rođenja (Date of birth)	
	Mjesto rođenja (Place of birth)	
	Prebivalište/ sjedište (Address)	

DIO II (PART II)		
Vrsta i iznos sredstava plaćanja (Description of cash)	**Iznos u valuti** (Amount and currenc	
	Efektivne banknote i kovani novac (Banknotes and coins)	
	Instrumenti plaćanja (čekovi, mjenice i sl.) (Cheques, promissory notes, and other physically transferable instruments of payment or other)	
Porijeklo sredstava plaćanja (Provenance of cash)		
Namjena korišćenja sredstava plaćanja (Cash destination)		

Vrsta prevoza (Means of transport)	a. **Vazdušni** (Air)	b. **Morski** (Marine)	**e. Drugo** (Other)
	c. **Drumski** (Road)	d. **Željeznički** (Rail)	

Mjesto i datum podnošenja prijave
(Place and date)

____

Potpis podnosioca prijave,
(Signature of declarant)

____

Potpis ili faksimil carinskog službenika
(Signature of customs officer)

____

***Uputstvo za popunjavanje obrasca prijave /** Important information for completion of the form

Sve rubrike u dijelu I i II Obrasca popunjava podnosilac prijave. Ostale rubrike popunjava carinski službenik. / (All requests in part I and II of the Form of Declaration have to be filled in by the declarant. Other parts of the Form are reserved for use by the Customs officer.)

Obrazac prijave popunjava se u tri primjerka, od kojih jedan primjerak zadržava podnosilac prijave, jedan primjerak zadržava carinski službenik, dok se jedan prijmerak dostavlja Centralnoj banci Crne Gore. / Application form is filled out in triplicate, one copy retains the Customs officer, second copy Customs Authority delivers to the Central Bank of Montenegro, while the third copy belongs to the applicant.

Prijava se popunjava velikim štampanim slovima na crnogorskom ili engleskom jeziku i potpisan predaje carinskom službeniku. / (Please fill in all parts using capital letters either in Montenegrin or English and signed form submit to the Customs officer.)

U Dijelu I Obrasca priave navode se podaci iz pasoša ili lične karte. / (in the Part I please indicate clearly your details as stated in your passport or your identity card.)

Ukoliko se prenose prenosiva sredstva plaćanja čiji je vlasnik drugo lice navode se i podaci o tom licu. / (If you carry cash on behalf of somebody else please indicate their details.)

U Dijelu II u rublici "Vrsta i iznos sredstava plaćanja" Obrasca prijave navodi se tačan iznos sredstava plaćanja koja se prenose uz korišćenje evropskog mjernog sistema (npr. 12.500,30). / (In the Part II in the box "Description of cash" please indicate the exact amount per instrument (if different monetary instruments were used) using the European measurement system, e.g 12.500,30.)

Valuta se označava velikim slovima (npr. EUR, USD). / (Indicate the currency clearly in capital letters (e.g. EUR, US dollars etc).)

U ribrici "Porijeklo sredstava plaćanja" navodi se da li sredstva plaćanja koja se prenose potiču od nasledstva, štednje, od prodaje, da li su podignuti sa računa itd. / (In the box "Source of assets" please indicate if the sum(s) declared originate from inheritance, savings, sale, bank account, etc.)

U rubrici "Namjena korišćenja sredstava plaćanja" navodi se svrha prenosa sredstava (npr. plaćanje robe, kupovina nekretnina, kupovina automobila, ulaganje, plaćanje raznih usluga, turistička potrošnja i sl.) / (In the box "Cash destination" please indicate the purpose of transferred funds (e.g, payments of goods, buying property, buying a car, investments, payment of various services, tourist spending, etc.)

ANNEX 3. TRAINING ATTENDED BY THE STAFF OF THE FIU

During 2009 APMLTF representatives attended:

• At the beginning of September - trainings for supervisory bodies under the Law on the Prevention of Money Laundering and Terrorist Financing were held for the following supervisors: APMLTF, Ministry of Finance, Insurance Supervision Agency, Department of Public Revenues, Central Bank, Administration for Games on Chance, Securities Commission.

• The workshop on Inter-agency co-operation in relation to organized crime and corruption was held in the period from 7th to 11th September. The participants at this workshop were representatives from: APMLTF, Police Directorate, Directorate for Anticorruption Initiative and Ministry of Internal Affairs and Public Administration.

• In July 2009 representatives of APMLTF participated at one- day workshop organised for employees from one commercial bank and its subsidiaries (14 participants)

• Within IPA 2007 Twinning project "Fight against organised crime and corruption" experts form United Kingdom and Northern Ireland, in co-operation with APMLTF, during May 2009 organised trainings for officers having a direct communication with customers. The training was conducted at 9 commercial banks with 100 participants.

During 2010 APMLTF representatives attended:

• 2 February, within IPA Twining project, EU organized a seminar: "EU Coordination, tables for legal complying with a view to complying the European law with the national law of Montenegro. The seminar was held in the Ministry of Finance (three participants from the FIU).

• 10-11th June, within TAIEX instruments, the EC Directorate General for Enlargement organized the seminar on combating terrorism, money laundering and terrorist financing. The seminar was held in Vienna (one participant from the FIU).

• 5-7th July, The Human Resources Management Authority in cooperation with the Judicial Training Center, UNDP, OSCD and USA Embassy in Podgorica organized the seminar: "Improving trainings on investigating corruption and related issues – financial investigation.'' The seminar was held in Budva(one participant from the FIU).

• 20-22 September, UNDP, OSCE, USA Embassy in Podgorica, the Government of Montenegro, the Human Resources Management Authority and the Judicial Training Center organized the seminar "Investigations on corruption and related issues – financial investigation.'' (two participants from the FIU).

• 4- 8 October, the IMF, together with the Basel Institute on Governance and International Institute of Higher Studies in Criminal Sciences, organized a five-day workshop: Cooperation between FIU and Law Enforcement Authorities in fighting money laundering and recovering illicit assets. The workshop was held in Syracuse (one participant from the FIU)

• 1-5 November - Police officers professional ethics and corruption prevention, held in Becici, Montenegro from.

• 10 November Training programme for the holders of judicial function on fight against corruption – Personal and institutional integrity, held in Kolašin and Budva organized by the Centre for training the holders of judicial function, UNDP and OSCE offices to Montenegro , State Department, US Department of Justice.

• 15 - 17 November - Human resources management in performing police duties, held in Danilovgrad, Montenegro

- 2 – 3 December Values –gender relations and corruption, held in Budva, Montenegro, , organized by Centre for training the holders of judicial function and UNDP
- 6-9 December , the World Bank and Egmont Group organized the Egmont Group Training – Tactical Analysis and Training for trainers. The training was held in Paris (two participants from the FIU).
- 9-10 December, within the ILECUs II project a two-day workshop: Development of economic-financial strategy", was held in Bečići (one participant from the FIU).

<u>During 2011 APMLTF representatives attended:</u>

- 8 – 19 January - Workshop on Preparing AML/CFT information material for public, financial and non-financial institutions.
- 18-19 January - Workshop on preparing AML/CFT information material for public, financial and non-financial institutions.
- 25- 26 January - AML/CFT supervision workshop for financial institutions
- 27-28 January - AML/CFT supervision workshop for non-financial institutions
- January - workshop named Developing a training program for obliged institutions within which a Commission's representative had a presentation for capital market participants regarding Instruction on risk analysis of money laundering , „know your client" procedures and other procedures for recognizing suspicious transactions
- January - study visit in the Bank of Italy, in order to get acquainted with the practice of that institution regarding preparation of material intended for the public, aimed at promoting activities related to money laundering and terrorist financing
- 21-22 February - workshop regarding preparation of Prevention of Money Laundering and Terrorist Financing Inspection Guide for the Commission's needs
- 1 -2 March- AMLCFT workshop for police and judicial institutions
- 7-8 March - Second Conference of the Parties to the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) held in Strasbourg.
- 17-18 March a Workshop on Criminal Money Flows on the Internet was organized in Belgrade
- 21-23 March - Tax and Crime Conference: A whole of government approach in fighting financial crime was held in Oslo
- 28-29 March - Human Resources Management Authority in cooperation with Judical Training Center of Montenegro and UNDP office in Podgorica organised training on Personal and institutional integrity and Corruption-Related Crimes" in Bečići, Montenegro
- In the period April – September, the Central Bank of Montenegro continued to strengthen its role in the area of prevention of money laundering and terrorism financing through the realization of new activities in the Twinning project MN 08 IB FI 01 –"Strengthening the regulatory and supervisory capacity of the financial regulators in Montenegro" financed by the European Commission and performed in cooperation with the De Nederlandsche Bank and the Bulgarian National Bank.
- On 18 April 2011- Within the Twinning project MN 08 IB FI

01 –"Strengthening the regulatory and supervisory capacity of the financial regulators in Montenegro" workshop for representatives of the competent state authorities included in the PML/CFT system in Montenegro, was held in Podgorica,MNE

- 19 – 21 April, within ILECUS project, a workshop on “Prevention of money laundering” was held in Becici, MNE.
- On 21 April - Human Resources Management Authority in cooperation with Directorate for Anti –corruption Initiative organised training on “Preparation and conducting Integrity Plans, in Podgorica, MNE
- 26 – 29 April, Human Resources Management Authority in cooperation with the Regional School of Public Administration(RESPA) organised workshop on “ Prevention of Corruption in State Administration” in Danilovgrad, MNE
- April - Meeting on domestic cooperation between AML/SFT authorities whose aim was a conclusion of Memorandum among supervisors in Montenegro
- 6 May - Human Resources Management Authority in cooperation with the Government of Norway organised the conference on “Public Administration Reforms in the process of accessing EU”, in Podgorica, MNE
- 9 -10 May - the Meeting of the South East European Co-operation Process Directors of National Institutions and Agencies for Combating Corruption and Organized Crime took place in Becici, MNE
- 9 – 13 May - within the Twinning project IPA 2009 “Strengthening capacities of the Police Directorate Montenegro” workshop on “Conducting financial investigations with the view of combating money laundering and terrorist financing” was held in Danilovgrad, MNE
- 24 – 26 May - within ILECUS 2 project, a workshop on “Investigations of the criminal offences related to narcotics and organized crime” was held in Budva, MNE
- 6 – 10 June 2011 - Rule of Law Assessment mission: Fight against Organised Crime and Corruption was carried out in Podgorica, MNE
- On 14 June - within ILECUS 2 project, a workshop on “Investigations of the corruptive criminal offences” was held in Kolasin, MNE
- 14 -17 June - EAG was held in Moscow, Russia
- 2-7 July - The Third The International Association of Anti-Corruption Authorities seminar was held in Shanghai, China
- 11-15 July - The 19th Egmont Group Plenary Meeting was held in Armenia
- 5 - 9 September - within the Twinning project IPA 2009 “Strengthening capacities of the Police Directorate Montenegro” workshop on “Money Laundering, Seizure And Confiscation of the Proceeds From Crime” was held in Danilovgrad, MNE
- 27-29 September, in Moldova, the Government of Moldova, in cooperation with OSCE and UN Office, organized the Workshop on Prevention and Fight against Terrorist Financing (one representative of the FIU attended the workshop).
- 10 – 14 October - within the Twining project IPA 2009 „Strengthening the capacities of the Police Directorate one representative of the FIU participated into study visit to the Criminal Police of the region Baden-Wurttemberg – in Germany.
- 12-14 October - The Fifth Regional Heads of FIUs Conference held in Otočec, Slovenia
- 1-3 November - MONEYVAL 10th Expert’s Meeting on Money Laundering and Terrorist Financing Typologies was held in Tel Aviv, Israel.
- 2 November - 10th MONEYVAL Typologies meeting was held in Tel Aviv, Israel from 30 October

- 23-24 November - The 15th Plenary meeting of the Eurasian group on combating money laundering and financing of terrorism (EAG) was held in Xiamen, China
- 22-24 November, within the ILECUs II project, a workshop:” Financial investigations and recovering illicit assets” was organized in Bečići.
- 13-14 December - UNODC and OSCE organized a workshop in Bucharest. The FIU representatives participated into this workshop for the purpose of training the employees and exchanging experience with other participants.

During 2012 APMLTF representatives attended:

- Within the Twinning Light Project „Strengthening the Fight against Money Laundering“, assisted by experts from Europe, there have been organized 8 seminars and trainings for the AML/CFT supervisory authorities, and 5 for compliance officers at reporting entities (banks, lawyers, notaries, casino representatives, betting offices and insurance companies) and employees that directly contact clients. Also, within this project, a two-week training related to conducting financial investigations was held for the employees of the APMLTF and Police Directorate.
- March and May 2012, participation in the negotiating teams for accession of Montenegro to the European Union, Working group for Chapter 23 – Judiciary and Fundamental Rights and Working Group for Chapter 24 - Justice, Freedom and Security, Brussels, Belgium;
- April 2012, workshop on fighting money laundering and terrorist financing, Skopje, Macedonia,
- April 2012, Training for inspection supervision – Podgorica, Montenegro
- April 2012, Training for public relations – Podgorica, Montenegro
- May 2012 Conference on strengthening the implementation of universal anti-terrorism instruments on explosive substances used by terrorists, organized by the OSCE and the UNODC, Vienna, Austria,
- May 2012, Montenegro on its path to NATO - Podgorica, Montenegro
- May 2012, Software Package For Project Management- Podgorica, Montenegro
- May 2012, Professional debate, organized by NGO Association of gambling providers of Montenegro on the topic of current developments in the field of games of chance – Podgorica, Montenegro
- May 2012, Plenary Session of the Group EAG, Moscow, Russia,
- May 2012, the OSCE seminar on crime analysis at the strategic level, Podgorica, Montenegro
- June 2012, Seminar: International Security and Montenegro, Podgorica, Montenegro
- June 2012, Seminar Safety forum 2BS (To be secure), entitled "Safety Challenges - Chicago summit: What can the Western Balkans offer. " Director participated in the session "The fight against corruption and organized crime - old and new models", Budva, Montenegro,
- June 2012, training for “Financial management and control in Montenegro”, Podgorica, Montenegro
- June 2012, First Conference of the National Convention on the European integration of Montenegro, Podgorica, Montenegro,
- June 2012, training on financial investigations for investigators, financial analysts, auditors and prosecutors working on financial crime cases, Bar, Montenegro,
- June 2012, within the Twinning Project with Germany a five-day seminar on "Money laundering and confiscation of property derived from felony" was organized, Danilovgrad, Montenegro

- June 2012, Panel discussion "The functioning of state authorities administration in the field of games of chance - monitoring, implementation of legislation, problems, effects and deviations“. Panel discussion was organized on the Initiative for the Adoption of the Strategic document on establishing the conditions in the field of games of chance and measures to be taken, addressed to the Government of Montenegro and the Parliamentary Committee on Economy, Finance and Budget, Podgorica, Montenegro,
- June 2012, Seminar on General Administrative Procedure, Podgorica, Montenegro,
- June 2012, Seminar on "Access to the web database of the EU", Podgorica, Montenegro,
- June 2012, Seminar on crime analysis on tactical / operational level - an analytical method that can be used to identify strategically important individuals within groups or networks of organized crime, Budva, Montenegro,
- June 2012, meeting of the Working group for Chapter 23 – Judiciary and fundamental rights that is held under the project of the National Convention of the European integration of Montenegro, Podgorica, Montenegro,
- June 2012, meeting of the Working Group for Chapter 24- Justice, freedom and security that is held within the project of the National Convention of the European integration of Montenegro, Podgorica, Montenegro.
- July 2012, Trainings for financial management and control –Ministry of Finance – Podgrica, Montenegro
- July 2012, 20th EGMONT GROUP Plenary , Sankt Petersburg, Russia;
- July 2012, Public procurement system - Podgorica, Montenegro,
- July 2012, identification, seizure and confiscation of assets which originates from various forms of human trafficking, OESCE – Prague, Czech Republic;
- September 2012, FATF Inter-session Meeting –WGEI, Paris, France;
- September 2012, Workshop organized by MONEYVAL and EAG: FATF standards, Strasbourg, France;
- September 2012, Rights and obligations of civil servants – Podgorica, Montenegro
- September 2012, Confiscation of assets – OESCE – Vienna, Austria;
- September 2012, Seizure of proceeds of crime and financial evidence– USA Embassy in Pristina, Kosovo;
- October 2012, Meeting of the project team- Typologies on money laundering, Warsaw, Poland,
- October 2012, Fight against money laundering and terrorist financing – TAIEX – Sarajevo, Bosnia and Herzegovina;
- October 2012, Implementation of the law on protection of personal data - Podgorica, Montenegro
- October 2012, Personal and institutional integrity – UNDP, OSCE - Podgorica, Montenegro
- October 2012 Fight against economic crime – OSCE in cooperation with Police and Prosecutors Office of Sweden– Budva, Montenegro
- November 2012, Money laundering, financial investigations and seizure of assets – Human Resources Administration, CENPF, UNDP, OEBS – Budva, Montenegro
- November 2012, Informatic Protection of Classified Information – Podgorica, Montenegro

- December 2012, Financial investigations with a focus on money laundering – TAIEX – Bruxelles, Belgium;
- December 2012 Money laundering, financial investigations and seizure of assets – CENPF, UNDP, OEBS – Bar, Montenegro

<u>During 2013 APMLTF representatives attended:</u>

- 29th January - Seminar "SPS information day", dedicated to the NATO program Science for Peace and Security (SPS) – organized by the Ministry of Foreign Affairs and European Integration, University of Montenegro and NATO program SPS – Podgorica, Montenegro
- 13-15th - Strategic priorities in the cooperation against cybercrime - Hosted by Minister of Interior and the Minister of Justice of Croatia – Dubrovnik, Croatia
- 27th February 2013 - Presentation on the subject" Suppression of organized financial crime" - Ministry of Interior and UK General Prosecutor's Office- Podgorica, Montenegro
- 7th March - Sharing alternatives practices for the utilization of confiscated criminal assets – European Commission and Local Democracy Agency Montenegro – Podgorica, Montenegro
- 14- 15. March - The fight against organized crime and corruption - Strengthening the Prosecutors' Network – Judicial Training Centre in cooperation with German organization for the International Cooperation and Dutch Centre for International Cooperation – Podgorica, Montenegro
- 13th March – Integrity Plan in State Administration , Podgorica, Montenegro
- 21-22nd March - Financial investigations and confiscations - experiences of Croatia and Great Britain - Human Resources Administration, Judicial Training Centre, United Nations Development Programme and OSCE– 2 officers
- 27th -28th March – Implementation of the supervision of the Law on prevention of money laundering and terrorist financing by the Securities Commission and Insurance Supervision Agency – organized by the APMLTF – Budva, Montenegro
- 1st -5th April - The five-day workshop in order to develop the Innovated Action Plan for the prevention of terrorism, money laundering and financing of terrorism for the period 2013-2014 - Police Administration in cooperation with OSCE Mission to Montenegro – Budva, Montenegro
- 1st -3rd April– FIU strategic analysis – World bank and Kazakhstan Ministry of Finance – Borovoe, Kazakhstan
- 17th -19th April – Models of communication between citizens and public administration in the information society - Ministry for Information Society and Telecommunications - Podgorica, Montenegro
- 29th -30th April – Cyber Crime @ IPA: "Closing Conference" – European Union and the Council of Europe -Budva, Montenegro
- 8th May- Constitutional System of Montenegro - Human Resources Administration – Podgorica, Montenegro
- 8th May –Prevention of Corruption - Human Resources Administration – Podgorica, Montenegro
- 17th May - The system of state administration - Human Resources Administration – Podgorica, Montenegro
- 24th May – European Union - Human Resources Administration – Podgorica, Montenegro
- 28th May– Public Finance System - Human Resources Administration – Podgorica, Montenegro

- 5th June - Free access to information correlated with personal and confidential data - Human Resources Administration – Podgorica, Montenegro
- 20th June– Business correspondence - Human Resources Administration – Podgorica, Montenegro
- 22nd – 24th June –Fifth International Association of Anti-Corruption Authority (IAACA) Seminar - IAACA and the Supreme People's Procuratorate of the People's Republic of China (SPP), - Jinan, the capital of Shandong Province, China
- 24th – 28th June - Seminar on financial investigations – British Embassy - Police Academy – Danilovgrad, Montenegro
- 4th June - Mobbing - Human Resources Administration – Podgorica, Montenegro
- 5th July – Code of Ethics - Human Resources Administration – Podgorica, Montenegro
- 8th June - Office Management - Human Resources Administration – Podgorica, Montenegro
- 10th July - Conflict Management - Human Resources Administration – Podgorica, Montenegro
- 4th -5th July– Multi-country Workshop on the implementation of international restrictive measures – European Commission's DG Enlargement – Podgorica, Montengro
- 26th -30th - The sixth regional - Euro Atlantic Camp REACT 2013 (NGO ALFA CENTAR) – Plav, Montenegro
- 4th and 5th September - Regional conference on money laundering and confiscation of property – Belgrade – USA Embassy in Belgrade, Office of the Legal Adviser of the Ministry of Justice USA and The OSCE Mission to Serbia
- 24th and 25th September 2013 – Judicial cooperation in criminal matters - The Ministry of Public Administration and Justice, Department of International Criminal Law of Hungary and Ministry of Justice of Montenegro - Podgorica, Montenegro
- 1st October - Drafting and adoption of a law - Human Resources Administration – Podgorica, Montenegro
- 3rd and 4th October - Assessment of opportunities for developing skills in public administration - Human Resources Administration in cooperation with ENA (French school for public administration)
- 8th -10th October - National workshop on the International Legal Framework against Terrorism and its Financing – Police Directorate and UNODC - Human Resources Administration – Podgorica, Montenegro
- 9th -10th October - The position of organizations performing public powers - SIGMA/OECD and Ministry of Interior - RESPA Danilovgrad, Montenegro
- 23rd -25th October – The role of FIU in the fight against money laundering linked with narco-traffic – institutional network and best practices – MILDT – Sofia, Bulgaria
- 4-8 November– training seminar organized by MONEYVAL – Strasbourg
- 12 – 13 November – Financing and budgeting of projects – Podgorica, Montenegro
- 2-3 December – National risk assessment - The implementation process of the new FATF recommendation No. 1 – OSCE and APMLTF – Budva, Montenegro

Training provided to supervisory staff in the APMLTF that is relevant to their oversight responsibilities under Article 4(1) items 15 and 16 of the LPMLTF and "co-ordination" role under Article 86 of the LMPLTF

- September 2009 - trainings for supervisory bodies under the Law on the Prevention of Money Laundering and Terrorist Financing were held for the following supervisors: APMLTF, Ministry of Finance, Insurance Supervision Agency, Department of Public Revenues, Central Bank, Administration for Games on Chance, Securities Commission;
- April 2012, Training for inspection supervision – Podgorica, Montenegro
- May 2012, Professional debate, organized by NGO Association of gambling providers of Montenegro on the topic of current developments in the field of games of chance – Podgorica, Montenegro
- May 2012, the OSCE seminar on crime analysis at the strategic level, Podgorica, Montenegro
- June 2012, training on financial investigations for investigators, financial analysts, auditors and prosecutors working on financial crime cases, Bar, Montenegro
- October 2012, Fight against economic crime – OSCE in cooperation with Police and Prosecutors Office of Sweden– Budva, Montenegro
- March 2013 – Implementation of the supervision of the Law on prevention of money laundering and terrorist financing by the Securities Commission and Insurance Supervision Agency – organized by the APMLTF – Budva, Montenegro

ANNEX 4. STATUS OF IMPLEMENTATION OF THE VIENNA CONVENTION, THE PALERMO CONVENTION AND THE UN INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM

Provisions of the Vienna Convention	**Legislative acts and regulations that cover requirements of the Vienna Convention**
Article 3 (Offences and Sanctions)	Criminal Code art. 447, 449, 449a, 23, 24 and 25
Article 4 (Jurisdiction)	Criminal Code art. 134, 135 and 137
Article 5 (Confiscation) - with regard to confiscation of proceeds derived from offences involving illicit trafficking of narcotic drugs or psychotropic substances; - with regard to seizure of property (assets); - with regard to rendering mutual legal assistance.	Criminal Procedure Code, as well as the Criminal Code (for example, in the article 300 paragraph 7 states that Narcotic drugs and the means used for their production shall be confiscated and destroyed
Article 6 (Extradition)	Law on MLA in criminal matters art. 10-33
Article 7 (Mutual Legal Assistance)	Law on MLA in criminal matters art. 1-8 and 42-53
Article 8 (Transfer of Proceedings)	Law on MLA in criminal matters art. 34-37
Article 9 (Other Forms of Cooperation and Training)	Law on MLA in criminal matters art. 42-53
Article 10 (International Cooperation and Assistance for Transit States)	Law on MLA in criminal matters art.2
Article 11 (Controlled Delivery)	Criminal Procedure Code, Article 157 paragraph 2
Article 15 (Commercial Carriers)	No information provided
Article 17 (Illicit Traffic by Sea)	No information provided
Article 19 (The Use of the Mails)	No information provided

Provisions of the Palermo Convention	Legislative acts and regulations that cover requirements of the Palermo Convention
Article 5 (Criminalisation of Participation in an Organized Criminal Group)	Criminal Code art. 401, 401a, 135, 136, 24 and 25
Article 6 (Criminalisation of the Laundering of Proceeds of Crime)	Criminal Code art. 268, 137 par. 2
Article 7 (Measures to Combat Money-Laundering)	Criminal Code art. 268
Article 10 (Liability of Legal Persons)	Law on criminal liability of legal entities art. 1
Article 11 (Prosecution, Adjudication and Sanctions)	Criminal Procedure Code art. 164, 165, 166, 170, 175
Article 12 (Confiscation and Seizure)	Criminal Code art. 113, 75 and 85
Article 13 (International Cooperation for Purposes of Confiscation)	Law on MLA in criminal matters
Article 14 (Disposal of Confiscated Proceeds of Crime or Property)	Law on MLA in criminal matters
Article 15 (Jurisdiction)	Criminal Code art. 134, 135 and 137
Article 16 (Extradition)	Law on MLA in criminal matters art. 10-33
Article 18 (Mutual Legal Assistance)	Law on MLA in criminal matters art. 1-8 and 42-53
Article 19 (Joint Investigations)	Regarding this provision, Montenegro do not have legal or other obstacles to conclude bilateral or multilateral agreements on forming JIT
Article 20 (Special Investigative Techniques)	Criminal Procedure Code art. 157
Article 24 (Protection of Witnesses)	Criminal Procedure Code art. 120 Law on witness protection
Article 25 (Assistance to and Protection of Victims)	Criminal Procedure Code chapter XV
Article 26 (Measures to Enhance Cooperation with Law Enforcement Authorities)	Criminal Procedure Code art. 125-132
Article 27 (Law Enforcement Cooperation)	No information provided
Article 29 (Training and Technical Assistance)	Law on education in judicial bodies
Article 30 (Other Measures: Implementation of the Convention through Economic	No information provided

Development and Technical Assistance)	
Article 31 (Prevention)	VDT, USPNFT, policija
Article 34 (Implementation of the Convention)	Provisions of the Convention are implemented in Montenegrin legislation such as CC, CPC, Law on MLA in criminal matters, Law on witness protection, Law on criminal liability of legal entities, Law on internal affairs, Law on Prevention of Money- Laundering and Terrorist Financing etc.

Provisions of the UN International Convention for the Suppression of the Financing of Terrorism	Legislative acts and regulations that cover requirements of the UN International Convention for the Suppression of the Financing of Terrorism
Article 2	Article 449 of the Criminal Code
Article 3	No information provided
Article 4	Criminal Code
Article 5	Law on criminal liability of the legal persons for the ciminal offences
Article 6	No information provided
Article 7	Criminal Code (article 134,135,136, 137)
Article 8	Criminal Procedure Code
Article 9	Article 5 of the Criminal Procedure Code
Article 10	Law on mutual legal assistance in criminal matters
Article 11	Law on mutual legal assistance in criminal matters
Article 12	Law on mutual legal assistance in criminal matters
Article 13	Law on mutual legal assistance in criminal matters and Criminal Code
Article 14	Law on mutual legal assistance in criminal matters and Criminal Code
Article 15	No information provided
Article 16	No information provided
Article 17	Criminal Procedure Code
Article 18	No information provided

Provisions of the Resolution 1267 (1999)	**Legislative acts and regulations that cover requirements of the Resolution 1267 (1999)**
subparagraph “a” of paragraph 4	Not implemented
subparagraph “b” of paragraph 4	Not implemented
Provisions of the Resolution 1333 (2000)	**Legislative acts and regulations that cover requirements of the Resolution 1333 (2000)**
subparagraphs “a”, “b”, and “c” of paragraph 5	Not implemented
subparagraphs “a”, “b”, and “c” of paragraph 7	Not implemented
subparagraphs “a”, “b” and “c” of paragraph 8	Not implemented
subparagraphs “a” and “b” of paragraph 10	Not implemented
subparagraphs “a” and “b” of paragraph 11	Not implemented
subparagraphs “a” and “b” of paragraph 14	Not implemented
Provisions of the Resolution 1363 (2001)	**Legislative acts and regulations that cover requirements of the Resolution 1363 (2001)**
paragraph 8	Not implemented
Provisions of the Resolution 1373 (2001)	**Legislative acts and regulations that cover requirements of the Resolution 1373 (2001)**
subparagraphs “a”, “b” and “c” of paragraph 1	Not implemented
Paragraph 2	Not implemented
Provisions of the Resolution 1390 (2002)	**Legislative acts and regulations that cover requirements of the Resolution 1390 (2002)**
subparagraphs “a”, “b” and “c” of paragraph 2	Not implemented
Provisions of the Resolution 1455 (2003)	**Legislative acts and regulations that cover requirements of the Resolution 1455 (2003)**
paragraph 1	Not implemented
paragraph 5	Not implemented
paragraph 6	Not implemented

Provisions of the Resolution 1526 (2004)	Legislative acts and regulations that cover requirements of the Resolution 1526 (2004)
paragraph 4	Not implemented
paragraph 5	Not implemented
Paragraph 17	Not implemented
paragraph 22	Not implemented

ANNEX 5. INTERNATIONAL AGREEMENTS SIGNED BY MONTENEGRO

1. Agreement between the Federative People's Republic of Yugoslavia and the Republic of Austria on the Mutual Recognition and Enforcement of Arbitral Awards and Arbitral Settlements in Commercial Matters, concluded on 18 March 1960 (taken by succession)
2. Agreement between the Federative People's Republic of Yugoslavia and the Republic of Austria on the Mutual Recognition and Enforcement of Decisions in Alimony Matters, singed on 10 October 1961 (taken by succession)
3. Agreement on Mutual Execution of Court Judgements in Criminal Matters between the Socialist Federal Republic of Yugoslavia and the Republic of Austria concluded on 1 February 1982 (taken by succession)
4. Agreement on Legal Cooperation in Criminal Matters between the Socialist Federal Republic of Yugoslavia and the Republic of Austria concluded on 1 February 1982. (taken by succession)
5. Agreement between Montenegro and Bosnia and Herzegovina on legal assistance in civil and criminal matters, signed on 9 July 2010.
6. Agreement between Montenegro and Bosnia and Herzegovina on Mutual Execution of Court Judgements in Criminal Matters, signed on 9 July 2010.
7. Convention on the issuance of birth certificates and the exemption of legalization between Socialist Federal Republic of Yugoslavia and the Republic of France, signed on 29 October 1969 (taken by succession)
8. Convention between the Socialist Federal Republic of Yugoslavia and the Republic of France on Mutual Legal Cooperation in Criminal Matters, signed on 29.10. 1969 (taken by succession)
9. Agreement on Facilitation of Application of the Hague Convention on Civil Proceedings from March 1, 1954 between the Socialist Federal Republic of Yugoslavia and the Republic of France signed on 29 October 1969. (taken by succession)
10. Convention on Jurisdiction and Law which applies to Personal and Family matters between the Government of Socialist Federal Republic of Yugoslavia and the Government of the Republic of France signed on 18 May 1971 (taken by succession)
11. Convention on Recognition and Execution of Court Judgements in Civil and Commercial Matters between the Government of the Socialist Federal Republic of Yugoslavia and the Government of the Republic of France signed on 18 May 1971 (taken by succession)
12. Agreement between the Federative People's Republic of Yugoslavia and the Kingdom of Greece on Mutual Recognition and Execution of Judicial Acts - Decisions, of 18 June 1959 (taken by succession)
13. Convention between FPRY and the Kingdom of Greece on Mutual Legal Relations, signed on 18 June 1959; (taken by succession)
14. Agreement on Mutual Execution of Court Judgements in Criminal Matters between the Government of Montenegro and the Government of Croatia, concluded on 9 September 2011.
15. Agreement between Socialist Federal Republic of Yugoslavia and the Republic of Cyprus on Legal Assistance in Civil and Criminal Matters, signed on 19 September 1984; (taken by succession)
16. Treaty between Montenegro and the Republic of Italy on facilitating the implementation of the European Convention on Mutual Legal Assistance in Criminal Matters, signed on 25 July 2013.
17. Treaty between Montenegro and the Republic of Macedonia on extradition and legal assistance in civil and criminal matters, signed on 20 December 2013.
18. Treaty between Federative People's Republic of Yugoslavia and Poland on Legal Communication in Civil and Criminal Matters, signed on 6 February 1960. (taken by succession)
19. Treaty on Mutual Execution of Court Judgements in Criminal Matters between Montenegro and the Republic of Macedonia signed on 20 December 2013.

20. Agreement between Socialist Federal Republic of Yugoslavia and Kingdom of Spain on Legal Aid in Criminal Matters and extradition, signed on 12 July 1980. (taken by succession)
21. Treaty between Montenegro and Serbia on Legal Aid in Civil and Criminal Matters, signed on 29 May 2009.
22. Treaty between Montenegro and Serbia on Mutual Execution of Court Judgements in Criminal Matters, signed on 29 May 2009.
23. Convention between the Kingdom of Serbs, Croats, and Slovenes and Italy on Legal and Court Protection of Citizens, signed on 6 April 1922. (taken by succession)
24. Convention between the Federal People's Republic Yugoslavia and the Republic of Italy on Mutual Legal Aid in Criminal and Administrative Matters, signed 3 December 1960 (taken by succession)
25. Agreement supplementing the Convention between Federal People's Republic Yugoslavia and the Republic of Italy on Mutual Legal Aid in Criminal and Administrative Matters, signed on 7 May 1962 (taken by succession)
26. Treaty between the Federal People's Republic of Yugoslavia and the People's Republic of Romania on Legal Aid, signed in Belgrade on 18 October 1960 (taken by succession)
27. Additional Protocol to the Treaty between Federal People's Republic of Yugoslavia and the People's Republic of Romania on Legal Aid, signed in Belgrade on 18 October 1960, signed in Bucharest on 21 January 1972. (taken by succession)

EXTRADITION AGREEMENTS

1. Convention between the Kingdom of Serbs, Croats, and Slovenes and Italy on Extradition, signed on 06 April 1922. (taken by succession)
2. Agreement on Extradition between the Socialist Federal Republic of Yugoslavia and the Republic of Austria concluded on 1 February 1982 (taken by succession)
3. Treaty on extradition of criminal offense perpetrators (Nederland), concluded on 11 March 1897 (taken by succession)
4. Extradition Treaty between Montenegro and Bosnia and Herzegovina signed on 15 November 2012.
5. Convention on Extradition between the Government of Socialist Republic of Yugoslavia and the Republic of France, signed on 23 September 1970 (taken by succession)
6. Extradition Treaty between the Government of Montenegro and the Government of the Republic of Croatia, signed on 1 October 2010.
7. Treaty between Montenegro and the Republic of Italy on facilitating the implementation of the European Convention on Extradition, signed on 25 July 2013.
8. Extradition Treaty between Montenegro and the Republic of Macedonia, signed on 4 October 2011.
9. Agreement between Socialist Federal Republic of Yugoslavia and Kingdom of Spain on Legal Aid in Criminal Matters and Extradition, signed on 12 July 1980. (taken by succession)
10. Extradition Treaty between Montenegro and the Republic of Serbia, signed on 29 May 2009.
11. Treaty between Montenegro and the Republic of Serbia on amendments to the Extradition Treaty between Montenegro and the Republic of Serbia signed on 29 October 2010.

COOPERATION AGREEMENTS IN THE AREA OF FIGHT AGAINST ORGANIZED CRIME, TERRORISM, TRAFFICING AND OTHER ILLEGAL ACTIVITIES

1. Cooperation Agreement between the Government of the Republic of Montenegro and the Government of Albania in the field of fight against terrorism, organized crime, trafficking as well as other illegal activities, signed on 31 October 2003.
2. Agreement between the Government of the Republic of Montenegro and the Council of Ministers of Bosnia and Herzegovina on cooperation in the fight against terrorism, organized crime, illegal trafficking in narcotics, psychotropic substances and precursors, illegal immigration and other criminal offences, signed on 7 September 2007.
3. Agreement between the Government of the Republic of Montenegro and the Government of the Republic of Bulgaria on cooperation in the fight against terrorism, organized crime, trafficking in narcotics, psychotropic substances and precursors, illegal immigration and other criminal offences, signed on 5 April 2005.
4. Cooperation Agreement in the area of crime between Montenegro and the Czech Republic, signed on 22 June 2012.
5. Agreement between the Government of the Republic of Montenegro and the Government of the Republic of Italy in the fight against crime, signed on 25 July 2007.
6. Agreement between Montenegro and the Republic of Macedonia in the area of cooperation in the fight against terrorism, organized crime, illegal trafficking in narcotics, psychotropic substances and precursors, illegal immigration and other criminal offences, signed on 10 June 2003.
7. Agreement between the Government of Montenegro and the Government of Malta on the fight against illegal trafficking in narcotics and psychotropic substances, organized crime and international terrorism, signed on 22 July 2010.
8. Agreement between the Government of Montenegro and the Government of the Republic of Slovenia on cooperation in the fight against organized crime, trafficking in human beings and illegal immigration, illegal trafficking in narcotics and precursors, terrorism and other forms of crime, signed on 13 October 2006.
9. Memorandum between the Ministry of Interior of Montenegro and the Ministry of Interior of Ukraine on cooperation in the area of fight against crime, signed on 13 June 2013.

ANNEX 6. MEMORANDUMS OF UNDERSTANDING SIGNED BY THE MONTENEGRIN FIU

	COUNTRY	Date
1.	FIU Serbia	15.04.2004
2.	FIU Albania	03.06.2004
3.	FIU Bosnia and Herzegovina	19.04.2005
4.	FIU Macedonia	29.10.2004
5.	FIC-UNMIK Kosovo	07.12.2004 (revised on 19.02.2009)
6.	FIU Slovenia	28.12.2004
7.	FIU Croatia	25.03.2005
8.	FIU Bulgaria	11.04.2006
9.	FIU Portugal	11.06.2007
10.	FIU Russia	07.09.2007 (revised 15.12.2010)
11.	FIU Poland	15.11.2007
12.	FIU UAE	06.07.2009
13.	FIU Ukraine	27.05.2009
14.	Fin Cen	21.10.2008
15.	FIU Romania	27.02.2009
16.	FIU Bermuda	21. 10. 2009
17.	FIU Moldova	12.10.2010
18.	FIU San Marino	12.10.2010
19.	FIU Israel	12.10.2010
20.	FIU Aruba	14.03.2011
21.	FIU Estonia	14.03.2011
22.	FIU Armenia	12.07.2011

23.	FIU British Virgin Islands	12.07.2011
24.	FIU United Kingdom	12.07.2011
25.	FIU Japan	31.01.2012
26.	FIU Canada	31.01.2012
27.	FIU Cyprus	10.07.2012
28.	FIU Panama	04.07.2013
29.	FIU India	04.07.2013
30.	FIU Saudi Arabia	04.07.2013