



Strasbourg, 7 February 2012

Opinion no. 669/2012

CDL-REF(2012)005
Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

DRAFT LAW

ON AMENDMENTS TO THE

LAW ON CLASSIFIED INFORMATION

AND

THE LAW ON CLASSIFIED INFORMATION

OF MONTENEGRO

DRAFT LAW ON AMENDMENTS TO THE LAW ON CLASSIFIED INFORMATION

Article 1

The Law on Classified Information (Official Gazette of Montenegro 14/08, 76/09 and 41/10 is hereby amended:

Article 3(1) shall be replaced by the following:

"Classified information shall be any information whose disclosure to an unauthorized person has or might have harmful consequences onto security and defense, foreign affairs, monetary and economic policy of Montenegro."

Article 2

Article 4 is amended/reworded as follows:

"Information shall not be determined as classified in order to conceal crime, endangering the environment, limiting competition, exceeding or abuse of authority, or other illegal act or behavior or administrative error."

Article 3

In Article 8, points (1) and (2) are replaced by the following:

- "1) Information shall be the fact emerged in the work of bodies and organizations referred to in Article 2 irrespective of the source, time of origin, place of storage and way of cognizance;
- 2) Document shall be any kind of recorded information.

Points (3) and (4) shall be deleted.

Point 6 is reworded as follows:

"6) security clearance is an act by which access and use of classified information is granted to legal and physical entity;

The present points 5 to 18 shall become points 3 to 16.

Article 4

In Article 10, after paragraph 2 the new paragraph shall be inserted:

"By way of exception to paragraph 2 of this Article, a person authorized for determining classification level within a body where the same type of classified information is being produced and repeatedly used in continuity may by special act designate those information as classified and determine its classification level".

Paragraph 3 shall become paragraph 4.

Article 5

In Article 11. after paragraph 1 the new paragraph shall be inserted to read:

"The Government of Montenegro shall define more detailed criteria of informations for determining the "TOP SECRET", "SECRET" and "CONFIDENTIAL" levels of classification.

Article 6

Article 12 paragraph 1 shall be replaced by the following:

"The base for security classification of informations shall be the content of classified information and its importance for the security and defense, foreign affairs, monetary and economic policy of Montenegro."

Article 7

Article 18 paragraph 1 shall be replaced by the following:

"During the determination of security classification, person authorized to determine level of security classification of informations, shall also decide on manner of declassification by setting the date of declassification within the timeframe laid down in Article 19a as well as identifying declassification events".

Article 8

After Article 19 the following two new Articles shall be added:

"Article 19a

If declassification is not defined in accordance with Article 18 of this Law, the classified status shall cease after expiration of the term of:

- 1) 30 years - for information marked as TOP SECRET,
- 2) 15 years - for information marked as SECRET,
- 3) Five years - for information marked as CONFIDENTIAL,
- 4) Two years - for information marked as RESTRICTED.

The terms from paragraph 1 of this Article shall be computed from the date on which the secrecy label is attached.

The authorized person may prolong the term of the classified status if there are reasons the information remain classified before the expiration of the term from paragraph 1 of this Article for the term set for individual degrees of secrecy referred to in paragraph 1 of this Article the most.

Article 19b

The person authorized to determine level of security classification shall perform periodical assessment of classified information based on which the level of secrecy can be changed or declassification can be done, as follows:

- 1) for TOP SECRET informations at least once every 10 years,
- 2) for SECRET informations at least once every 5 years,
- 3) for CONFIDENTIAL informations at least once every 3 years, and
- 4) for RESTRICTED informations at least once a year.

Article 9

Article 20 shall be deleted.

Article 10

In Article 26 paragraph 1 point 5 shall be replaced by the following:

“5) state prosecutor.”

Point 6 shall be replaced by the following:

“6) judges”.

After point 7, the new point shall be inserted:

“8) members of the Council of the independent supervisory body for protection of personal data and access to information.”

Article 11

In Article 28, paragraph 3 shall be deleted.

Article 12

Article 31 shall be replaced by the following:

“The Directorate shall enable the access to classified information to foreign physical and legal entity if such entity holds security certificate issued by the State of his/her citizenship or principal place of business and/or by the international organization whose member he/she is and if in line with international agreement.”

Article 13

In Article 35 point 11 after the words “information about”, the words “present and” shall be inserted.

In point 15 after the words “intelligence” the words “and security” shall be inserted.

Article 14

: Article 39 paragraph 2 shall be replaced by the following:

“If the vetting procedure is not carried out within the deadline referred to in paragraph 1 of this Article, the deadline for the vetting procedure may be extended until the competent body get information related to vetting procedure.”

Article 15

In point 43(1) point 3 after the words “sources” the words “collecting” shall be inserted.

Article 16

In point 45 the word “inspect” shall be replaced by the word “collecting”.

Article 17

Article 47 shall be replaced by the following

“ The Directorate shall by decision refuse a request for issuing security clearance to legal entity if it does not fulfill conditions referred to in Articles 30 and 30a of this Law.”

Article 18

Article 51 shall be replaced by the following:

The applicant is entitled to submit the request for the prolongation of validity of security clearance at least 180 days before the expiry date of security clearance.

Based on the request for the prolongation of validity of security clearance referred to in paragraph 1 of this Article, the Agency shall carry out new vetting procedure.

Article 19

In Article 53 paragraph 1 point (3) shall be replaced by the following:

"3) ceased performing tasks demanding access to classified information within the body or organization;

Article 20

After Article 53 the following new Article shall be added:

"Article 53a

"Security clearance holder shall be obliged to return the it to the Directorate within eight days from bringing a decision referred to in Article 52 paragraph 1 of this Law and/or after the conditions for its issue referred to in the first paragraph of Article 53 no longer apply."

Article 21

In Article 55, the words translated as "holding security clearance or security permission" shall be replaced by the words "referred to in Article 31 of this Law".

Article 22

In article 67 point 5 shall be replaced by the following:

"5) establishing special procedures during the international visits".

Article 23

In Article 68 paragraph 2 after the words "information" the words "as well as conditions and the manner of providing the cryptographic protection of classified information" shall be added.

Article 24

In Article 69 paragraph 3 after the words "shall immediately" the words "inform the Directorate and" shall be added.

Article 25

In Article 72 after paragraph 1 the new paragraph shall be inserted:

"Records referred to in the paragraph 1 of this Article shall be the classified information for which the level of security classification is determined in line with this Law."

Present paragraph 2 shall become paragraph 3.

Article 26

In Article 74 point 4 after words “international organisations“ the words “and proposes measures to improve the protection of classified information“ shall be added

Point 7 shall be replaced by the following:

“7) establishes and maintain the Central Registry and sub-registries of classified information referred to in Article 77 paragraph 1 of this Law”.

Point 8a shall be replaced by the following:

“8a) prepare instructions for handling NATO and EU classified information“.

Article 27

After artical 75c the following two paragraphs shall be inserted:

Article 75d

Employment with the Directorate may be established without public announcement subject to prior confirmation of secured funding from the Minister in charge of budgets.

Jobs that are filled without public announcement shall be the act on internal organization and civil service positions in the Directorate.

Employment decision shall be made by the Director of the Directorate.

Article 75e

The employee of the Directorate shall be issued an official identity card.

The form and the content of the official I identity card shall be determined by the director of the Directorate.

Article 28

Article 76 paragraph 1 shall be replaced by the following:

“Exchange of classified information with NATO and EU shall be performed through the Directorate, in line with international agreements“.

Article 29

Article 77 paragraph 1 shall be replaced by the following:

“For the purpose of exchanging classified information with NATO and EU, the Directorate shall establish and manage registry of those information (Central Registry) as well as sub-registries of classified information regarding missions of Montenegro with NATO and EU”.

In paragraphs, 2 and 3 the word “foreign” shall be deleted.

Article 30

In Article 82 paragraph 1, after the point 2 following 2 new points shall be added, worded as follows:

“2a) fails to remove the secrecy label upon the expiration of of the term of the classified status (Art. 18 and 19a);

2b) fails to change or remove the secrecy label when the conditions laid down in Article 21a are being met.“

Point 4 shall be amended to read:

"4) fails to inform all the bodies and organizations that use information on its declassification or reclassification (Article 180 paragraph 4 and article 21 paragraph 5,"

In point 5 the word "realize" shall be replaced by the word "enable",

Point 7b shall be deleted.

In point 9 the words "level of security classification" shall be replaced by the word "secret".

In point 12 after the words "classified information" the words "and Directorate" shall be added.

Article 31

After Article 87 a new Article shall be added:

"Bylaws for the implementation of this law shall be adopted within six months from the day of its entry into force.

Article 32

This Act shall enter into force on the eighth day following the date of its publication in the "Official Gazette of Montenegro".

LAW ON CLASSIFIED INFORMATION

I GENERAL PROVISIONS

Article 1

This law regulates the unique system for determination of classified information, access, use, storage, recording, and protection of classified information.

Article 2

State bodies, State administrative bodies, local self government, and other legal entities that are entrusted for carrying out public authorization (hereinafter referred to as bodies) as much as legal and physical entities, who take cognizance of classified information while performing their legal or contracted jobs, shall be obliged to act in accordance with this law (hereinafter: organizations).

Article 3

Classified information is information whose disclosure to unauthorized persons has or might have harmful consequences onto security, political or economic interests of Montenegro and is related to:

- 1) Defense;
- 2) Public Security;
- 3) Foreign Affairs;
- 4) Intelligence and security activities of the State bodies of Montenegro;
- 5) Scientific, research, technological, economic and financial State interests in the fields of Defense, Public Security, Foreign Affairs, and intelligence and security activities of the State bodies of Montenegro;
- 6) Systems, devices, projects and plans in the fields of Defense, Public Security, Foreign Affairs, intelligence and security activities of the State bodies of Montenegro;

Classified information shall be determined under conditions and in a manner specified by this law.

Article 4

Information shall not be determined as classified if it has been done in order to cover up a criminal offence, the exceeding or abuse of competence, or other illegal act or behavior or administrative error.

Article 5

Classified information shall be used only for the purpose for which it has been collected and within the time necessary for its achieving.

Article 6

Access to classified information shall be restricted and granted only in a manner and under conditions specified by this law, the regulations based on it, and international agreements signed by Montenegro.

The access to classified information means to inform persons about content of classified information.

Article 7

Classified information shall be stored and used in accordance with the protection measures prescribed by this law.

Due to this law, every person who uses such information or is familiar with its content shall be obliged to safeguard and protect secrecy of such information after cessation of duty or service, as long as the information is marked as classified or until the person becomes released from the obligation to keep information secret.

Article 8

Individual terms used in this law shall have the following meaning:

1) Information: document, its content and supplements, objects, measures or procedures, as much as an oral communication or information with classified content originated from the work of bodies referred to in Article 2 or other legal or physical entities, irrespective of the source, time of origin, place of storage and way of cognizance;

2) Document: written, copied, drawn, pictured, printed, recorded, photographed, magnetic, optical or any other recorded information;

3) Object: dummy, model, specimen, photograph, film, microfilm or any other notes recorded by optical, sound, machine, manual or other way;

4) Building: all kinds of buildings, over ground and underground buildings, likewise other artificial and natural buildings (buildings, roads, tunnels, bridges, pits, airports, sea and river ports or docks, places for storage of devices and military equipment, plans, cryptographic devices and documents, natural underground passages, channels etc.);

5) Classified information of a foreign state and international organization: information which will be kept classified in accordance with international agreement between Montenegro and the foreign country or international organization;

6) Security clearance: an act by which access and use of classified information is granted to legal and physical entity likewise the foreign legal and physical entity;

7) Security permission is an act by which access and use of classified information of foreign country and international organization is granted to legal and physical entity;

8) Person authorized for handling of classified information is a person in the body responsible for receipt, recording, storage, giving to use, exchange, and other activities of classified information processing.

9) "Need to know": a principle which establishes justified need of the person to use classified information in the conduct of his/her official duties based upon issued security clearance;

10) Vetting procedure: the procedure of establishing the facts significant for the issuing of security clearance;

11) Security restriction: information or a fact established through the vetting procedure on the ground of which is based suspicion into loyalty or trustworthiness of the person subject to the issuing of security clearance;

12) Family: includes spouses, their children as much as the parents of the spouses;

13) Use of classified information: usage of classified information in the purpose of performing duties within the body or for the body;

14) Safeguarding of classified information: set of measures and activities used in order to prevent loss, disclosure, destruction and abuse of classified information.

15) Protection of classified information: set of physical, organizational and technical measures or activities used in order to prevent destruction, transfer or abuse of classified information;

16) Security perimeter: an area around the building which marks minimal distance from the building from which the building or classified information in it cannot be endangered.

17) Security area: an area or premise inside the building, where information classified "CONFIDENTIAL" or of a higher classification level is safeguarded and which requires appropriate physical protection.

18) Administrative zone: an area or premise inside the building where information classified "RESTRICTED" is safeguarded and which requires appropriate physical protection.

II PROCEDURE FOR SECURITY CLASSIFICATION

Article 9

The procedure for security classification shall include determination of classification levels and manner of declassification, likewise classification marking.

Article 10

Information shall be designated as classified if such is necessary in the democratic society and if the interest referred to in Article 3 paragraph 1 of this law prevails over the interest for free access to information.

The person authorized for determining classification level shall by decision designate the information as classified and determine its classification level.

If a document contains information which may be designated by different classification levels, the authorized person shall be obliged to designate each of the information with appropriate classification level.

Article 11

Classified information referred to in Article 3 of this law shall be given one of the following security classification levels:

1. TOP SECRET;
2. SECRET;
3. CONFIDENTIAL;
4. RESTRICTED

Article 12

The base for security classification shall be content of classified information and its importance for the security of Montenegro and its political or economic interests.

"TOP SECRET" shall be applied to classified information whose unauthorized disclosure could endanger or make unrecoverable harmful consequences to the security and interests of Montenegro;

"SECRET" shall be applied to classified information whose unauthorized disclosure could seriously harm the security or interests of Montenegro;

"CONFIDENTIAL" shall be applied to classified information whose unauthorized disclosure could harm the security or interests of Montenegro;

"RESTRICTED" shall be applied to classified information whose unauthorized disclosure could harm the body function.

Article 13

In classifying information or document, especially information bound for cooperation with intelligence, defense or security organizations of foreign countries, international and regional organizations, markings referred to in Article 11 of this law may also be used in English.

Article 14

Persons authorized for determining classification level "TOP SECRET" are: the President of Montenegro, the President of Parliament of Montenegro, the Prime Minister and members of Government of Montenegro, the director of Police Directorate, the head of the Administration for the Prevention of Money Laundering and Terrorism Financing, the director of the National Security Agency (hereinafter: the Agency), the Supreme State Prosecutor and the President of the Supreme Court.

Article 15

Persons authorized for the determining classification levels "SECRET", "CONFIDENTIAL" and "RESTRICTED", are the heads of the bodies referred to in Article 2 of this law or persons appointed by them.

Article 16

The obligation of classification and the designation of classification level shall begin at the moment of creating or cognizance of such information i.e. at the moment of preparing for creating the information.

Personnel from the body or organization shall be obliged, within their area of responsibility, to assess the security importance of the information and propose its classification level to the authorized person.

Article 17

During the determination, person authorized to determine classification levels shall be obliged to assess potential harmful effects to the security of the State and its interests.

Article 18

During the determination, person authorized to determine classification levels, shall also decide on manner of declassification by setting the date, event or deadline of the declassification.

Person authorized to determine classification levels, could declassify the information before the deadline referred to in paragraph 1 of this Article.

Person appointed by the head of the body as a person authorised to determine classification levels in accordance with Article 15 of this law, may declassify information only with the consent of the head of the body.

The authorised person referred to in paragraph 1 of this Article shall be obliged to inform about declassification all of the bodies and organizations who use such information.

Article 18a

The body or organization shall not be bound to confirm or deny the existence of classified information if the confirmation or denial could negatively influence security and interests of Montenegro.

Article 19

The information that requires to be protected in accordance with this law may be created by linking two or more information determined as unclassified.

In the case referred to in paragraph 1 of this Article, the authorized person shall be obliged to decide on security classifications.

If only a smaller part of information referred to in paragraph 1 of this Article requires to be protected, the authorized person shall be obliged to detach that part from the remaining document and determine its level of classification.

Article 20

If according to the content of classified information it is not possible to determine the manner of declassification, secrecy of such information shall cease on the expiry date and after that the archive shall start to be available for use in accordance with regulations on archival activities.

Article 21

The classification level is subject to the change.

Reclassification may be applied to the whole information or its classified piece.

Reclassification may be performed solely by the person authorized to determine classification levels.

Person appointed by the head of the body as a person authorised to determine classification levels may in accordance with Article 15 of this law reclassify information only with the consent of the head of the body.

The authorized person referred to in paragraph 3 of this Article shall inform the bodies and organizations using such information, about the change.

Article 22

Classified information shall be marked by:

- 1) classification level;
- 2) manner of declassification;

- 3) data about person authorized to determine classification levels (hereinafter: the authorized person);
- 4) data about the body whose authorized person determined the classification level.

Exceptionally from paragraph 1 of this Article, the information shall be considered as classified if it is designated only by the classification level.

The manner and procedure for security classification shall be prescribed by the Government of Montenegro (hereinafter: the Government).

III CLASSIFIED INFORMATION OF FOREIGN COUNTRIES AND INTERNATIONAL ORGANIZATIONS

Article 23

The classification markings of a foreign country or an international organization shall remain in the form in which they are used in that country or the international organization.

Article 24

Classified information shall be transmitted according to the principle "need to know".

Persons responsible for receipt and exchange of classified information, employed in the Directorate for protection of classified information (hereinafter: the Directorate), shall take the measures and activities necessary for receipt, determination of users and transmission of classified information to such users.

IV CONDITIONS AND PROCEDURE FOR ISSUING, RESTRICTION, AND VALIDITY OF THE SECURITY CLEARANCE

Article 25

Access to information classified TOP SECRET, SECRET, and CONFIDENTIAL shall be granted to a person holding security clearance or security permission, unless otherwise regulated by this law.

Before issuing a security clearance a vetting procedure shall be carried out.

Article 26

Access to classified information without security clearance shall be granted to:

- 1) The President of Montenegro;
- 2) The President of Parliament of Montenegro;
- 3) The Prime Minister;
- 4) Deputy Prime Ministers and Ministers competent for interior, foreign affairs, finance and defense.
- 5) Members of the Committee for Defense and Security
- 6) The Supreme State Prosecutor, and
- 7) The President of the Supreme Court

Persons referred to in paragraph 1 of this Article shall solely access to classified information within their area of responsibility, in accordance with the law.

Entering the duties persons referred to in Paragraph 1 of this Article shall sign a statement by which they are bound to handle classified information in accordance with the law and other appropriate regulations.

Article 27

Access to information classified "RESTRICTED" is granted to all employees within the body or organization.

Article 28

Security clearance for the information classified "TOP SECRET", "SECRET" and "CONFIDENTIAL" shall be issued by the Directorate.

Request for issuing security clearance referred to in paragraph 1 of this Article shall be submitted to the Directorate, namely:

- 1) For person handling of classified information or other person employed in the body, by the head of the body;
- 2) For legal entity or other person employed by legal entity, by its own legal representative

A request for issuing security clearance for foreign legal and physical entity shall be submitted by the entity.

Article 29

A request for issuing a personnel security clearance shall contain: identification data (name and surname) of the person for whom the request is submitted and residence, duties, jobs and activities related to the access to classified information, likewise the classification level for the requested security clearance.

In addition to the request referred to in paragraph 1 of this Article, physical entity shall enclose the documentation confirming:

- 1) he/she is Montenegrin citizen;
- 2) He/she disposes with justified request for the use of classified information according to the principle "need to know";
- 3) he/she has reached the age of 18 or 21 years in order to access classified information designated "TOP SECRET";

In addition to evidences referred to in paragraph 2 of this Article, an entrepreneur shall enclose the evidence that he/she has not rendered the protection measure on prohibition of performing activities.

Article 30

Request for issuing a facility security clearance shall contain: name, seat and activity, personal name and residence of the legal representative, likewise classification level of the information for which security clearance is required.

In addition to the request referred to in paragraph 1 of this Article, legal entity shall enclose the evidences confirming that:

- 1) The measures and activities for physical and information security of classified information are provided;
- 2) Employees, who require access in order to perform contracted job, hold security clearance.

Prior to the issuing a facility security clearance, the Directorate shall check whether the measures on protection of classified information within the legal entity are established."

Article 30a

Besides conditions referred to in Article 30, paragraph 2 of this law, legal entity must fulfill the following conditions confirming:

- 1) It has been registered for carrying out appropriate activity;
- 2) there are no criminal procedures for criminal offences with elements of corruption against the authorized person and that he has not been legally convicted for criminal offences;
- 3) Alignment procedure is not initialized likewise insolvency or bankruptcy;
- 4) It defrays tax liability;
- 5) it disposes with evidences on ownership;
- 6) there is no security risk for using classified information.

Fulfillment of conditions referred to in paragraph 1 of this Article shall be confirmed through the vetting procedure.

Article 31

Security clearance shall be issued to foreign physical and legal entity if such entity holds security certificate issued by the State of his/her citizenship, or residence or by the international organization whose member he/she is and if in accordance with the international treaty he/she may access to classified information in Montenegro.

Article 31a

The Directorate shall at the request of head of the body issue security permission for access to classified information of foreign country or international organization of the appropriate classification level, to an employee who requires access in the performance of his/her duties for the time needed for access to such information.

Security permission may be issued to an employee holding personnel security clearance.

Article 31b

The Directorate shall at the request of responsible person within the legal entity issue security permission for access to classified information of foreign country or international organization of the appropriate classification level, to legal entity who requires access in the performance of his/her duties for the time needed for access to such information.

Security permission may be issued to the legal person holding facility security clearance. "

Article 32

Vetting procedure shall be carried out by the Agency.

The request for vetting procedure shall be submitted by the Directorate.

Vetting procedure shall be carried out only according to the written consent of the person cleared.

If the person cleared refuses to give the written consent, the Agency shall not carry out the vetting procedure.

Vetting procedure may also include family members of the person cleared if estimated they may influence to the behavior of such person.

Vetting procedure shall be carried out in the place of birth, residence and employment of the person cleared.

Article 33

Due to the classification levels, the following vetting procedures shall be carried out:

1. basic vetting procedure, for the information classified "CONFIDENTIAL";
2. special vetting procedure, for the information classified "SECRET";
3. special vetting procedure, which also includes additional vetting procedure, for the information classified "TOP SECRET".

Article 34

Before carrying out the vetting procedure, the Agency shall deliver to physical and legal entity subject to clearance, a questionnaire for the vetting procedure.

The questionnaire referred to in paragraph 1 of this Article may be basic or special security questionnaire.

Legal and physical entity shall fill in the basic security questionnaire, but if the clearance is requested for access to the information classified "TOP SECRET" and "SECRET", they shall also fill in the special security questionnaire.

Completed basic and special security questionnaire shall be classified as "RESTRICTED".

Article 35

The basic security questionnaire for physical entities shall be completed with the following data:

1. identification data (name, surname, including previous);
2. personal identification number;
3. date and place of birth;
4. citizenship, including the data on previous or double citizenship;
5. permanent and temporary residence;
6. previous visits abroad lasting at least three months;
7. marital status and number of children;
8. level of education and profession;
9. military service;

10. professional training in Montenegro and abroad;
11. previous employments;
12. criminal offences and ongoing criminal proceedings;
13. alcohol and drug addiction;
14. medical data on addiction or mental diseases;
15. contacts with foreign intelligence services;
16. membership and participation in activities of organizations with prohibited aims;
17. liability for violation of regulations on classified information;
18. previous vetting procedures
19. property right onto real estate registered into real estate cadastre or real estate onto which the applicant disposes with legal basis for the acquisition of property, likewise the annual tax on total citizen's income for previous year.

Article 36

The basic security questionnaire for legal entities shall be completed with the following data:

- 1) name and seat including previous;
- 2) identification number of the legal entity and tax-identification number;
- 3) personal name of the representative;
- 4) the date and place of establishing ;
- 5) the origin of the establishing capital including changes within the period of the last three years;
- 6) the number of employees;
- 7) the number of employees for which security clearance is requested and kind of jobs they perform;
- 8) the data on legal responsibility of legal entity and responsible persons within the legal entity, likewise the data on ongoing procedures;
- 9) contacts with foreign intelligence services;
- 10) membership and participation in activities of organizations with prohibited aims;
- 11) liability for violation of regulations on classified information;
- 12) previous vetting procedures;
- 13) property right onto real estate registered into real estate cadastre or real estate onto which the applicant disposes with legal basis for the acquisition of property, likewise the information on the annual financial report for previous year according to the Law on accounting and auditing.

In addition to the questionnaire referred to in paragraph 1 of this Article, the representative of the legal entity shall also fill in the basic security questionnaire for physical entity.

Article 37

In order to conduct special vetting procedure regulated by Article 33, points 2 and 3 of this law, in addition to the basic, a special security questionnaire shall be filled in, too.

The special security questionnaire includes the data on:

- 1) participation in foreign armed forces and para-military formations;
- 2) the other characteristics, except those referred to in Articles 35 and 36 of this law which makes physical or legal entity accessible to influences and pressures representing security risk;
- 3) obligations resulted from the financial debts or taken guarantees.

Article 38

An additional vetting procedure shall be carried out if security clearance is requested for the information classified "TOP SECRET".

Beside clearing the facts from the basic and special vetting procedures the additional vetting procedure also includes clearing all those facts, circumstances and events from the private life of the person subject to the vetting procedure within the period of the last ten years from the day of submitting the request for security clearance, which might be the reason for suspicion into his/her reliability, and especially if his/her activities are contrary to the interests of Montenegro or if he/she is in contact with foreign persons who can endanger the foreign policy and security of Montenegro.

Article 39

The period for carrying out vetting procedure shall start from the day of filling in the questionnaire in the Agency up to:

- 1) 30 days for the basic vetting procedure;
- 2) 90 days for the special vetting procedure and
- 3) 180 days for the special vetting procedure including the additional vetting procedure.

If the vetting procedure is not carried out within the deadline referred to in paragraph 1 of this Article, the deadline for the vetting procedure may be extended for 30 days.

Article 40

Vetting procedure shall be carried out:

- 1) by means and methods in accordance with the law, not requiring the Court permission,
- 2) by the cooperation with administration body responsible for police affairs, judicial bodies, likewise the companies or organizations and other legal entities employing the person (or who were employing the person) and if it is necessary with other bodies and organizations in order to provide certain information from the questionnaire.

Article 41

The Agency may, during the vetting procedure, cooperate with bodies of foreign countries and international organizations responsible for vetting procedures, in accordance with the international treaties concluded between these bodies and Montenegro likewise regulations on protection of personal data.

Article 42

Due to the request of the Agency and in accordance with the law, the bodies and legal entities referred to in Article 40, point 2 of this law shall be obliged to deliver requested information.

Article 43

During the vetting procedure the Agency is obliged to:

- 1) provide exactness and objectivity of information regarding the vetting procedure;

- 2) prevent violation of the dignity of person cleared by using the data from the vetting procedure.
- 3) prevent the disclosure of methods, means and sources of information.
- 4) provide that the information from the vetting procedure shall be used solely for the purpose of its collecting.

Article 44

The Agency shall submit to the Directorate report on vetting procedure or additional vetting procedure with the recommendation for issuing or refusing of the security clearance.

In addition to the report referred to in paragraph 1 of this Article, the Agency shall also deliver to the Directorate filled in security questionnaires referred to in Articles 35-38 of this law.

The report with the recommendation of the Agency shall be considered classified and marked "CONFIDENTIAL".

Article 45

A person subject to the vetting procedure shall be entitled to inspect the collected information, except the information regarding the sources and the manner of their clearance.

Article 46

The Directorate shall by decision refuse a request for issuing a personnel security clearance if the person does not fulfill conditions referred to in Article 29 of this law and if vetting procedure confirms the following security restrictions:

- 1) indictment for criminal offences prosecuted ex officio or conviction for such criminal offences with the exception of those where as the main sentence a fine or imprisonment up to three years is regulated, if not erased from criminal record;
- 2) registration in the records of alcohol or drug addiction;
- 3) excessive debts indicating possible extortion and other forms of pressure onto person subject to clearance;
- 4) relations or having the relations with: persons who on unauthorized way collect classified and other information, terrorists, saboteurs, members of organized criminal groups justifiably suspected to be members of such groups;
- 5) unauthorized contacts and collaboration with intelligence-security or military structures of foreign countries;
- 6) membership in organizations which threaten security of Montenegro;
- 7) drug addiction and use of psychoactive substances or tendency to excessive use of alcohol;
- 7a) the existence of addictions or any other diseases that could endanger secure handling of classified information;
- 8) violent behavior and provoking conflicts in working or living environment;
- 9) hiding or giving incorrect personal information or the information about family members;
- 9a) infractions of regulations pertaining to the secrecy of information;
- 10) the other security restrictions defined by the Law and confirmed by international treaties.

Article 47

The Directorate shall by decision refuse a request for issuing security clearance to:
-legal entity if it does not fulfill conditions referred to in Articles 30 and 30a of this law;

-foreign legal and physical entity if it does not fulfill conditions referred to in Article 31 of this law.

Article 48

The reasons for the refusal of issuing security clearance shall be listed in the decision referred to in Article 46 of this law.

The information about source and manner of vetting procedure shall not be listed in the decision referred to in paragraph 1 of this Article.

Against the decision referred to in paragraph 1 of this Article a complaint shall be submitted to the Ministry competent for the defense affairs (hereinafter: the Ministry).

Article 49

When delivering security clearance or security permission, the Directorate shall inform the user about regulations regarding handling of classified information, as much as the legal or other consequences of its unauthorized disclosure.

A security clearance shall be issued to the person who previously signs a statement that he undertakes to handle classified information in accordance with this law.

If a person refuses to sign the statement referred to in paragraph 2 of this Article, he/she shall not be issued a security clearance.

The Directorate shall inform the applicant about issued security clearances and security permissions.

The content and form of security clearance shall be regulated by the Ministry.

Article 50

Security clearance for the information classified "TOP SECRET" shall be valid for 3 years.

Security clearance for the information classified "SECRET" shall be valid for 5 years.

Security clearance for the information classified "CONFIDENTIAL" shall be valid for 10 years.

Article 51

The Directorate shall inform the user, in written form, at least 180 days before the expiry date of security clearance, that he/she is entitled to submit the request for the prolongation of validity of security clearance.

Along with the request for the prolongation of validity of security clearance referred to in paragraph 1 of this Article, the user shall inform the Directorate about changes of the data from the previously submitted security questionnaire with evidences, and the Agency shall carry out new vetting procedure.

Article 52

The Directorate shall decide on restriction or termination of the security clearance even before its expiration, if establishes that person holding security clearance does not handle or

safeguard classified information in accordance with this law and other regulations or that he/she does not anymore fulfill conditions necessary for the issuing of security clearance.

If it is necessary, a part of the explanation of decision referred to in paragraph 1 of this Article that is classified "CONFIDENTIAL", shall not be transmitted to the user.

Article 53

A security clearance shall be revoked, if:

- 1) after the expiry date, its validity is not prolonged;
- 2) ceased the function of the person referred to in Article 26 of this law;
- 3) ceased the function of performing jobs of the employees within the body or organization;
- 4) based upon the decision of the Directorate, brought during the vetting procedure, and
- 5) physical or legal entity who holds issued security clearance, deceased or ceases to exist.

Validity of security permission expires after performing jobs it has been issued for, or after fulfilling certain conditions referred to in paragraph 1 of this Article.

Article 54

The head of the body shall temporarily restrict or disable the access to classified information to the person with issued security clearance, if such a person is the subject to:

- 1) a disciplinary proceeding due to the founded suspicion that he committed the infractions referred to in this law, and
- 2) a criminal proceeding for criminal offences referred to in Article 46, paragraph 1, point 1 of this law .

The restrictions referred to in paragraph 1 of this Article shall be applied until making the final decision on disciplinary measure, or final court decision.

V USE OF CLASSIFIED INFORMATION

Article 55

Users of classified information are: Montenegrin citizens and legal entities seated in Montenegro holding security clearance or security permission, foreign physical and legal entities holding security clearance, likewise the persons referred to in Article 26, paragraph 1 of this law.

Article 56

Bodies and organizations referred to in Article 2 of this law, who receive classified information from the authorized person, shall not be allowed to give it to the other bodies and organizations without consent, unless otherwise provided by this law and regulations based on it.

Article 57

A person holding security clearance and using classified information shall be obliged to immediately, in written form, notify the authorized person who determined classification level on noticed irregularities regarding protection of classified information and its disclosure.

An authorized person who determined classification level shall be obliged to (in cases referred to in paragraph 1 of this Article) immediately undertake the measures for the

elimination of noticed irregularities or prevention or reducing of possible harmful effects resulted from the disclosure of classified information.

Article 58

The authorized person, referred to in Article 57, paragraph 2 of this law, shall provide permanent monitoring over the use of classified information and keep regularly updated registry of the bodies and organizations who use such information and the persons who are granted access to classified information as much as the time of use and access to classified information.

VI SAFEGUARDING OF CLASSIFIED INFORMATION

Article 59

The obligation to keep information secret shall begin at the moment when authorized person referred to in Article 14 and 15 of this law, sets information as classified or designates its classification level.

Article 60

Release of the obligation to keep information secret, may be given by the authorized persons who determined the level of classification.

If the person appointed by the head of the body as a person authorised to determine classification levels, designates the information as classified, in accordance with Article 15 of this law, the head of the body shall be responsible for releasing from an obligation to keep the information secret.

The body that appointed or chose the head of the body may release him/her from an obligation to keep information secret, and shall inform the Directorate thereof.

The release of the obligation to keep information secret may be complete or partial.

The partial release shall regard a part of classified information or precisely defined body, organization or the person to whom classified information can be completely or partly released.

VII MEASURES FOR PROTECTION OF CLASSIFIED INFORMATION

Article 61

The criteria for determination of measures for protection of classified information are:

- 1) the level of classification, and
- 2) the content and form of classified information.

Article 62

In order to protect classified information the bodies and organizations are bounded to take measures and activities for providing administrative, physical, information and industrial protection of classified information.

Article 63

Measures and activities for administrative protection of classified information are:

- 1) determination and designation of classification levels;
- 2) receipt and recording of classified information;
- 3) safeguarding and handling of classified information;
- 4) coping, translating and making excerpts from classified information, setting the number of copies and users;
- 5) control and handling of classified information during its transmission to the users;
- 6) prevention from an unauthorized disclosure and publishing of classified information which would endanger security and other interests of Montenegro and its bodies;
- 7) prevention from disclosure
- 8) storage and destruction of classified information.

Article 64

Measures and activities for physical protection of classified information are:

- 1) Assessment of possible breaches of security of classified information resulted from intrusion or unauthorized access, use or destruction of classified information;
- 2) setting security perimeter around the building with classified information;
- 3) setting security and administrative zones;
- 4) organizing physical protection and application of technical and other means for protection of buildings and premises with classified information;
- 5) issuing security passes for access to buildings and premises;
- 6) entry and exit control and movements of persons and vehicles for transfer of classified information;
- 7) organizing secure transfer of classified information outside security areas.

Article 66

Measures and activities for providing information protection of classified information are:

- 1) certification of communication and information systems and processes;
- 2) the evaluation of possible endangering of security of classified information pertaining to the intrusion into information system and use and destruction of processed classified information stored in the communication and information systems;
- 3) establishing methods and security procedures necessary for receipt, processing, transmission, safeguarding and storage of classified information in electronic form;
- 4) making, distribution and storage of crypto keys and other crypto materials;
- 4a) protection of information during processing and storage in communication and information systems;
- 5) crypto protection of communication, information and other electronic systems for composing, transmission, processing and archiving of classified information;
- 5a) protection from risks of compromising electromagnetic radiation;
- 6) installation of the devices for safeguarding classified information.

Article 67

Measures and actions for providing industrial protection of classified information are:

- 1) protection from loss and disclosure of classified information contained in service contracts;

- 2) issuing of security clearances for legal and physical entities who set, use or are in contact with classified information of the organizations;
- 3) protection from the loss and disclosure of classified information of foreign legal and physical entities;
- 4) providing protection during the transfer of classified information and
- 5) establishing special procedures during the visits of foreign legal and physical entities to the organizations that set, process and safeguard classified information.

Article 68

Classified information can be transmitted outside the premises of the bodies and organizations only by the application of prescribed protection measures which guarantee access to classified information solely to persons holding a security clearance.

More detailed conditions and means of implementing administrative, information, industrial and the measures pertaining to the protection of classified information shall be prescribed by the Government.

Article 69

Personnel holding security clearance and other employees in the bodies and organizations where classified information is set, shall in the case of loss or unauthorized disclosure of classified information immediately inform thereof the authorized person who determined the level of classification.

Personnel holding security clearance and other employees in a recipient bodies and organizations, shall in the case of loss or unauthorized disclosure of classified information immediately inform thereof the authorized person who determined the level of classification.

In cases 1 and 2 referred to in this Article, the authorized person shall immediately take all necessary steps to identify the circumstances that caused the loss of classified information or its unauthorized disclosure, remove harmful consequences, and prevent further losses and unauthorized disclosure of such information within bodies and organizations.

Article 70

Based upon special measures for the protection of classified information significant for Country's defense, protection shall be provided to:

- 1) devices and military equipment;
- 2) buildings for the purposes of Country's defense;
- 3) performing tasks of special importance for Country's defense;

The special protection measures referred to in paragraph 1 of this Article shall be prescribed by the Government.

Article 71

Bodies and organizations shall ensure the regular internal control over the protection measures prescribed by the law.

Control referred to in paragraph 1 of this Article shall be carried out by the heads of the bodies and the responsible personnel within organizations.

Control referred to in paragraph 1 of this Article shall be carried out inside the organizational units and organizations referred to in paragraph 2 of this Article or through the classification of job regarding protection of classified information.

The Government shall prescribe the method and content of internal control referred to in paragraph 1 of this Article.

VIII RECORDS ON CLASSIFIED INFORMATION

Article 72

Records shall be kept on: classified information, submitted requests for issuing security clearances and security permissions, issued and revoked security clearances and security permissions.

The Government shall prescribe the method and content of the record referred to in paragraph 1 of this Article.

IX THE DIRECTORATE

Article 73

The Directorate is an administrative body with characteristics of a legal entity.

Article 74

The Directorate shall perform the following tasks:

- 1) provides implementation of standards and regulations pertaining to the protection of classified information;
- 2) adopts the plan on protection of classified information in the events of emergency;
- 3) coordinates activities that ensure protection of classified information entrusted to Montenegro by other states and international organizations;
 - 3a) ensures adequate and efficient selection, installation and servicing of cryptographic systems, products and mechanisms;
 - 3b) handles NATO and EU crypto materials;
 - 3c) certificates communication and information systems and processes for processing, transmission and storage of classified information;
 - 3d) protects premises and equipment from the risk of electromagnetic radiation;"
- 4) acts according to the requests for issuing security clearances;
- 5) keeps records on issued security clearances;
- 6) establishes and keeps Central Registry and classified information of foreign state or international organization;
- 7) undertakes measures in order to train users of classified information and bodies for handling of classified information in accordance with standards and regulations;
 - 7a) prepares instructions for handling classified information of foreign state or international organization;
- 8) performs other tasks established by this law.

Article 75

The Government shall appoint and recall the Director of the Directorate (hereinafter: the Director) on the proposal of Minister of Defense.

The Director shall be a person who fulfills the conditions for work in the State bodies, with university degree and at least five years of working experience.

The Director is not allowed to be a member of any political party or act politically.

Article 75a)

Prior to the engagement in the Directorate, vetting procedure of the persons shall be carried out in accordance with this law.

Article 75b)

Persons employed in the Directorate cannot be members of any political party or act politically.

Article 75c)

Due to the complexity and nature of jobs, responsibilities, working conditions, risks, and special prohibitions and restrictions, the insurance of the persons employed in the Directorate shall be accounted with increased duration.

X OBLIGATIONS OF THE DIRECTORATE PERTAINING TO THE CLASSIFIED INFORMATION OF FOREIGN COUNTRIES AND INTERNATIONAL ORGANIZATIONS

Article 76

Exchange of classified information with foreign countries and international organizations shall be performed through the Directorate, unless otherwise provided by a specific law or international treaty.

Through the international cooperation, bodies may directly exchange classified information with bodies of foreign countries and international organizations in accordance with specific law or international treaty, and with prior consent of the Directorate.

Classified information provided by the foreign country and international organization shall be treated in accordance with international treaty.

If the international treaty referred to in paragraph 2 of this Article does not include provisions on manner of handling classified information, it shall be treated in accordance with provisions of this law. "

Article 76a)

During the international exchange and protection of classified information the Directorate shall perform the following tasks:

- 1) security authority for coordination and implementation of NATO and EU security policy in Montenegro, in order to provide adequate level of protection of classified information, in accordance with interstate treaties (NSA-National security Authority);
- 2) security of communications for selection, management and service of equipment used for transmission, processing and storage of classified information(NCSA National Communication Security Authority);
- 3) conducting security accreditation of communication and information systems and processes in which classified information are used (SSA- Security Accreditation Authority);

4) control of materials for cryptographic protection of classified information and safe handling, storage, distribution and recording of crypto materials (NDA National Distribution Authority).

State administrative body competent for informatics society, Ministry and the Agency, shall be bound to in order to perform tasks referred to in paragraph 1, points 2 and 3 of this Article, on the request of the Directorate, provide necessary professional and technical assistance. "

Article 77

In order to exchange foreign classified information the Directorate shall establish and manage registry of those information (Central Registry).

Bodies and legal entities that, in the conduct of jobs within their area of responsibility, continuously use foreign classified information shall establish and manage registry of classified information of foreign country.

Bodies and legal entities referred to in paragraph 2 of this Article may establish specific places for processing foreign classified information (Control points).

Article 77a

The Directorate shall conduct security accreditation of the registries and control points and approve their work. "

Article 78

The Directorate shall inform foreign state or international organization about security of the foreign classified information which foreign country or international organization delivered to Montenegro.

Article 79

Under extremely adverse political, economic or defense-security circumstances for Montenegro and if such is necessary in order to protect interests referred to in Article 3 of this law, the Directorate shall at the request of the body and without previously concluded international agreement exchange classified information with foreign state or international organization.

XI SUPERVISION OF THE IMPLEMENTATION OF THE LAW

Article 80

The Ministry shall conduct supervision of the legality of the work of the Directorate.

The Directorate shall be responsible through the competent inspectors and in accordance with the law for the inspection supervision over the law enforcement and implementation of the international agreements.

Article 81

Beside competences of inspectors regulated by the law on inspection supervision, the competent inspector referred to in Article 80 paragraph 2 of this law shall:

1) supervise implementation of laws and other regulations on classified information;

- 2) order measures for the elimination of irregularities pertaining to the exchange and other activities of classified information processing;
- 3) submit criminal charges and propose starting of misdemeanor and other procedures, in case of violation of regulations of this law;
- 4) assist in the implementation of this law and other regulations on classified information.

In carrying out the supervision, the competent inspector shall without previous notification to the body, competent person, operator or recipient, control the security, handling, exchange and other activities regarding processing of classified information.

The competent inspector shall order measures and set the deadline for elimination of irregularities pertaining to the use, exchange and other activities of classified information processing.

XII PENALTY PROVISIONS

Article 82

A body or legal entity in Montenegro shall be fined for infraction between twenty and three hundred times the minimum salary in Montenegro, if:

- 1) fails to set the information as classified and mark its classification level at the moment of establishing or receiving it, or at the moment of beginning with preparations for establishing such information (Article 16 paragraph 1);
- 2) during the designation of classification level it does not assess the harmful effects onto security of the State and its interests (Article 17);
- 3) fails to determine classification level of the information resulted by connecting two or more information, or does not separate a piece of information and determine its level of classification (Article 19);
- 4) fails to inform all the bodies and organizations using such information on its reclassification (Article 21 paragraph 4);
 - 4a) does not appropriately mark classified information (Article 22, paragraph 1)
- 5) accesses to classified information without a security clearance (Article 25);
- 6) carries out vetting procedure without written consent of the person cleared (Article 32 paragraph 3);
- 7) fails to provide insight into requested information, on the request of the Agency (Article 42)
 - 7a) delivers classified information to another user without previous consent of the authorized person who determined classification level of such information (Article 56);
 - 7b) fails to inform the Directorate about changes of information from previously submitted security questionnaire with evidences (article 51, paragraph 2);
- 8) fails to immediately inform the authorized person on noticed irregularities pertaining to the protection of classified information (Article 57 paragraph 1);
- 9) fails to immediately take measures in order to eliminate noticed irregularities, or measures for the prevention or reducing of possible harmful effects of disclosure of classified information (article 57 paragraph 2);
- 10) fails to ensure constant monitoring over classified information given to the use and keep updated records referred to in Article 58 of this law;
- 11) fails to take measures and activities providing administrative, physical, information and industrial protection of classified information (Article 62);
- 12) fails to immediately inform the authorized person who determined classification level on loss or unauthorized disclosure of classified information within the body or organization where such information is lost or within the body or organization to whom such information is delivered (Article 69, paragraphs 1 and 2);

- 13) fails to immediately take all necessary steps to identify the circumstances that caused loss of classified information or its disclosure to an unauthorized person, or remove any harmful effects, and prevent further losses and unauthorized disclosure of such information (Article 69 paragraph 3);
13a) fails to keep record on: classified information, issued and revoked security clearances, and security permissions (Article 72, paragraph 1)
- 14) fails to ensure the regular internal control over the implementation of protection measures regulated by the Law (Article 71 paragraph 1).

A responsible person within body or legal entity shall be fined for infraction referred to in paragraph 1 of this Article between two and twenty times a minimum salary in Montenegro.

A physical entity within body or legal entity shall be fined for infraction referred to in paragraph 1, points 5, 9, and 12 between two and twenty times a minimum salary in Montenegro.

XIII TRANSITIONAL AND FINAL PROVISIONS

Article 83

The Directorate referred to in Article 73 of this Law shall be established, no later than sixty days after this law enters into force.

Article 84

Bodies and organizations referred to in Article 2 of this law shall be obliged to harmonize the procedures of designation, access, handling and storage of classified information likewise the protection measures with provisions of this law, no later than six months after this law enters into force.

Article 85

Classification level determined before this Law enters into force shall be harmonized in accordance with this Law no later than two years from its entry into force, as follows:

- information designated "state secret" shall be treated as "TOP SECRET";
- information designated "official secret" or "military secret-highly confidential" shall be treated as "SECRET";
- information designated "official secret" or "military secret-confidential" shall be treated as "CONFIDENTIAL" and
- information designated "official secret" or "military secret-restricted" shall be treated as "RESTRICTED"

Actual markings shall be applied until harmonizing the classification levels (paragraph 1 of this Article).

Article 86

Previously initiated procedures for the determination of classification level shall be completed in accordance with this law.

Article 87

Bylaws for the implementation of this law shall be adopted within six months from the day of its entry into force.

Article 88

Entering into force of this law, the implementation of the Regulation on the Criteria for Determining the Information Significant for Defense Which Have to be Safeguarded as State or Official Secret and on Establishing Tasks and Jobs Especially Important for Defense of Country Which Have to be Protected by Applying Special Security Measures ("Official Gazette of FRY", Nr. 54/94) shall cease to have effect.

Article 89

This law shall enter into force on the eighth day following the date of its publication in the "Official Gazette of Montenegro" and start to be implemented 60 days after its entry into force.

SU-SK No. 01-9/9

Podgorica, February 13th, 2008

THE PARLIAMENT OF MONTENEGRO

PRESIDENT

Ranko Krivokapić

This law shall enter into force on the eighth day following the date of its publication in the "Official Gazette of Montenegro.