LAW ON CLASSIFIED INFORMATION (*)

CHAPTER ONE
GENERAL PROVISIONS

Article 1

The Law shall herein regulate the classification of information, conditions, criteria, measures and the activities to be taken in the process for providing protection of classified information, the rights, the duties and the obligation of the originators and the users of such information, the national and international exchange, the inspection supervision over the implementation of this Law, as well as other issues pertaining to the access to and handling of classified information.

Article 2

Responsibility for the protection of classified information, in line with this Law, shall apply to all users of classified information who have had access to such information and/or have become acquainted with the contents thereof.

Article 3

The aim of this Law is to ensure lawful use of classified information and to prevent any type of illegal or unauthorized access, misuse and compromise of such information.

Article 4

The provisions of this Law shall be applied for the protection of national classified information as well as for the protection of classified information received from foreign states and international organizations or created during joint efforts of cooperation, unless otherwise regulated by international agreements ratified in line with the Constitution of the Republic of North Macedonia (hereinafter referred to as: ratified international agreements).

Article 5

For the purposes of protecting the classified information and implementing the international standards, carrying out the exchange of classified information in line with

* This law is compliant with the EU Council Decision of 23 September on the security rules for protecting EU classified information, CELEX: 32013D0488

the ratified international agreements, perfoming inspection supervision over the implementation of the provisions of this Law and the other regulations related to classified information as well as for accomplishing other tasks regulated by this Law, the Directorate for Security of Classified Information (hereinafter referred to as the Directorate) shall be the responsible body.

Meaning of the expressions used in this Law

Article 6

Individual expressions used in this Law shall have the following meaning:

1. **"Information"** shall refer to any knowledge that can be communicated in any form.

2. **"Information of interest for the Republic of North Macedonia"** shall refer to any information produced by the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entity established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje, natural person or legal entity, as well as foreign state body, i.e., foreign natural person or foreign legal entitiy, related to the security and defence of the state, its territorial integrity and sovereignty, constitutional order, public interest, freedoms and rights of the human and the citizen.

3. **"Classified information"** shall refer to any information from the scope of work of a body of the state and local administration established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje or other legal entities, relating to the public security, defence, foreign affairs or the security and intelligence activities of the country, which shall be protected against unauthorized access in accordance with law and which has been marked with an appropriate level of classification in accordance with this Law. Classified information may also include documents, technical devices, any machinery, equipment or separate components thereof or weapons or tools, manufactured or in the process of manufacturing as well as the classifed innovations pertaining to the defense and are of interest to the security of the state.

4. **"Document"** shall refer to any written matter, draft or sketch, reproduction, copy, photography, audio, video, magnetic, electronic, optical or any other type of record which contains information.

5. **"Damage"** shall refer to a violation of the interests of the state as a consequence from endangering the security of classified information of interest to the Republic of North Macedonia or the information that the Republic of North Macedonia is obliged to protect according to the ratified international agreements.

6. **"Security risk"** shall refer to likelihood for security infraction of the classified information.

7. **"Security of classified information"** shall refer to a set of activities and measures applied for protection of classified information against unauthorized access and unauthorized handling of such information.

8. **"Personnel security clearance"** shall refer to a document confirming that there is no security risk for the natural person to have access to and to handle classified information.

9. **"Facility security clearance"** shall refer to a document confirming that there is no security risk for the legal entity and that it possesses physical or organizational capacities for handling and/or keeping classified information, according to law.

10. **"Access permit"** shall refer to a document confirming that the foreign natural person or legal entity has a security clearance issued by the home-country and is eligible to have access to and use classified information in the Republic of North Macedonia.

11. **"Need to know"** shall refer to a principle according to which the user is determined on the basis of his/her/its requirement for access to classified information in order to perform the function or the official duty and authorizations as well as to carry out the activity or the classified contracts.

12. **"Originator of classified information"** shall refer to an authorized creator of classified information. Originators of classified information are the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje and other natural persons or legal entities that create information of interest to the public security, defence, foreign affairs or the security and intelligence activities of the state.

13. **"Dissemination of classified information"** shall refer to distribution of classified information to individuals who have an appropriate security clearance according to the "need-to-know" principle.

14. **"User of classified information"** shall refer to a natural person or a legal entity which has a requirement for access to classified information in order to perform the function, the official duty and official authorizations or to carry out classified contracts, and which has a security clearance appropriate to the classification level of the information.

15. **"Handling classified information"** shall refer to a process comprising of any treatment of classified information for the duration of its existence. It includes: creating, recording, recording, transmitting, using, reclassifying, declassifying, archiving and destructing classified information.

16. **"Security perimetar"** shall refer to the area around the building that represents the minimum distance from which the building or the classified information therein could be threatened.

17. **"Security area"** shall refer to the area or room within the building where information classified up to "TOP SECRET" is handled and stored and requires an approapriate physical protection.

18. **"Administrative zone"** shall refer to a visiby defined perimetar established around or leading up to security areas within which the possibility exists for the control of individulas and vehicles.

19. **"Classified contract"** shall refer to any form of contract or contract deriving therefrom, including the negotiations leading to its conclusion, which contains or enables access to classified information.

20. **"Officer for security of classified information"** shall refer to an individual authorized by the responsible person in the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje or by the legal entity, who is obliged to take care of the efficient and coordinated execution of the rights and responsibilities deriving from this Law.

21. **"Cryptographic security"** shall refer to a component of the communication and information system security, comprising of cryptographic protection, management of cryptographic material and development of methods for cryptographic protection, which are carried out by using password, code and digital signature.

22. **"Cryptographic protection"** shall refer to an operational planning activity within the system of cryptographic materials and products used for protection of classified information against unauthorized access, in the course of the process of creating, handling and storing of such information.

23. **"Cryptographic product"** shall refer to a software, system or device with which cryptographic protection is provided.

24. **"Cryptographic (crypto) materials"** shall refer to cryptographic algorithms, cryptographic hardware and software modules, crypto keys, implementation guidelines and associated documentation;

25. **"Security accreditation of communication and information systems"** shall refer to a process of formal approval of communication-information systems to operate up to a specified classification level in special security conditions in its operational environment and at an acceptable level of risk.

26. **"Security risk management process"** shall refer to a process of identifying, controlling, minimizing or eliminating events that may affect the security of an organization or the system used thereof.

27. **"Communication and information system (CIS)"** shall refer to any system that enables the creation, storage, processing or transmission of information in electronic form. The CIS includes all the means necessary for its functioning, such as infrastructure, organization, personnel, information, communication and other electronic resources.

CHAPTER TWO
Classification of information and levels of classification

Article 7

The classification determines the level of protection of the information that should match the degree of the damage that would result for the Republic of North Macedonia from unauthorized access to that information or its unauthorized use.

Information subject to classification shall particularly refer to: public security, defence, foreign affairs, security, intelligence and counterintelligence activities of the state, systems, devices, innovations, projects and plans of importance for the public security, defence, foreign affairs, scientific research, technological, economic and financial affairs of importance for the Republic of North Macedonia.

Article 8

The classification of the information shall be granted according to its contents.

The level of classification of the information shall be marked by the originator of the information and by another person authorized by him in written.

Information shall be marked with one of the levels of classification as follows:

- TOP SECRET;
- SECRET;
- CONFIDENTIAL and
- RESTRICTED.

Article 9

The information classified TOP SECRET shall be the information the unauthorized disclosure of which would put in jeopardy and cause irreparable damage to the permanent interests of the Republic of North Macedonia.

The information classified SECRET shall be the information, the unauthorized disclosure of which would result in exceptionally serious damage to the vital interests of the Republic of North Macedonia.

The information classified CONFIDENTIAL shall be the information, the unauthorized disclosure of which would result in serious damage to the interests of importance for the Republic of Macedonia.

The information classified RESTRICTED shall be the information the unauthorized disclosure of which would result in damage of the work of the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje that is of interest to the public security, defence, foreign affairs and the security and the intelligence activities of the state.

Article 10

In determining the classification level of the information, the originator, i.e., the person authorized by them, should designate the classified information with the most

appropriate level of classification that shall ensure the necessary protection of the state interests and the security referred to in Article 9 of this Law.

The appropriate level of classification of the information shall be determined on the basis of an assessment of the possible damage and consequences arising from the unauthorized access thereto.

Article 11

The TOP SECRET classification level can be granted to an information by the President of the Republic of North Macedonia, the President of the Assembly of the Republic of North Macedonia, the President of the Government of the Republic of North Macedonia, the President of the Constitutional Court of the Republic of North Macedonia, the President of the Supreme Court of the Republic of North Macedonia, the ministers within their sphere of activity, the Public Prosecutor of the Republic of North Macedonia, the Chief of the General Staff of the Army of the Republic of North Macedonia, the Director of the Intelligence Agency, the Director of the National Secutrity Agency, the Director of the Operational Technical Agency, the Director of the Crisis Management Centre, the Director of the Directorate for Security of Classified Information and the persons authorized by the abovementioned entities.

If otherwise regulated by law, ratified international agreement or another regulation, the persons envisaged therein can give TOP SECRET classification to information.

Article 12

The information the disclosure of which would result in decreased efficiency of the work of the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the City of Skopje, shall be marked with UNCLASSIFIED.

The UNCLASSIFIED designation is not a level of classification, however, a free access to such information shall not be granted.

The Government of the Republic of North Macedonia shall prescribe with a decree the manner of storing and handling information marked with UNCLASSIFIED.

Article 13

If the information includes data with different levels of classification, the originator shall be obliged to determine the level of classification for each data separately.

The information as a whole shall be classified according to the highest classification level, and the other parts with classification levels belonging to the information shall be indicated on the front page of the material.

If a part of the document contains classified information with a higher level of classification, that part may be extracted as a separate document with an appropriate level of classification.

The footnotes of the classified information shall not be classified, unless containing or disclosing classified information.

In order to avoid security risks, inserting footnotes should be minimized.

Article 14

The originator of the classified information shall mandatorily mark its level of classification on a visible place, according to this Law.

Article 15

If the information has not been marked with a level of classification, and the originator cannot be determined or has ceased to exist, the classification of the information shall be made by the legal successor of the originator.

In case the legal successor of the originator, referred to in paragraph 1 of this Article, cannot be determined either, the Directorate itself shall mark the classification level of the information.

Article 16

The reclassification shall change the classification level of the information.

The originator, or another person with his written authorization, shall make the change of the classification level.

The users of the information shall necessarily be informed about the change of its classification level.

The Government of the Republic of North Macedonia shall prescribe with a decree the manner of change of the classification level.

Article 17

The classification of the information shall terminate:

- on the date specified in the document;
- with the advent of the event specified in the document;
- with the expiry of the time period specified in the document; and
- with declassification.

Article 18

Declassification shall change the classified information into unclassified information.

The originator of the information or another person authorized by him/her shall make the declassification referred to in paragraph 1 of this Article and shall inform the users thereof.

The Government of the Republic of North Macedonia shall prescribe with a decree the manner of declassification of the information.

Article 19

The originator of the classified information shall mark the time period or the event after which the information can be reclassified or declassified.

The time period or the event after which the information can be reclassified or declassified may not be longer than ten years, except in cases where the classified information requires a longer protection regulated by law.

Article 20

The originator shall review and evaluate the TOP SECRET information in a period not exceeding ten years in order to assess the need for further retention of the classification level.

The information classified SECRET is reviewed and evaluated in a period not exceeding five years to assess the need for further retention of the classification level.

The information classified CONFIDENTIAL is reviewed and evaluated in a period no longer than three years to assess the need for further retention of the classification level.

The information classified RESTRICTED is reviewed and evaluated in a period not exceeding two years to assess the need for further retention of the classification level.

Article 21

The classified Information shall not be considered classified if it is concealing an overstepping of authorization, misuse of official function or any other illicit action i.e., a punishable act.

The persons who shall make the disclosure referred to in paragraph 1 of this Article to competent body according to the Law on Protection of Whistleblowers shall be guaranteed protection according to law.

Classified information of foreign states or international organizations

Article 22

Classified information from foreign states or international organizations with which the Republic of North Macedonia has entered into international agreements or to which the Republic of North Macedonia has become a member, shall keep the marking of the classification level used in that state or international organization.

Article 23

Foreign classified information shall be disseminated on the basis of “need-to-know” principle and provided that the user holds an appropriate security clearance.

The Government of the Republic of North Macedonia shall prescribe with a decree the manner of determining the users and the dissemination of the received foreign classified information.

CHAPTER THREE
Criteria, measures and activities for protection of classified information

Article 24

In order to protect the classified information, measures and activities shall be taken for administrative, physical and industrial, communication and information systems security, as well as for personnel security.

Article 25

Criteria that shall particularly be taken into account while determining the measures for protection of classified information shall be as follows:

- level of classification;
- scope and shape of the classified information; and
- risk assessment for the security of the classified information.

Administrative security

Article 26

Measures and activities for administrative security shall be as follows:

- determining the classification level and marking of the classified information accordingly;
- receipt and recording of the classified information;
- determining a manner of storing, handling and controlling classified information;
- reproductions, translations and excerpts of the classified information and designation of the number of copies and the users;
- dissemination of the classified information;
- transmission of the classified information,
- disposal and destruction of the classified information.

The Government of the Republic of North Macedonia shall prescribe with a decree the measures and activities for administrative security.

Physical security

Article 27

Physical security shall be carried out by applying physical and technical measures in order to prevent unauthorized access to classified information.

Physical security measured should deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorized actions and to allow for segregation of personnel in their access to classified information on a need-to-know basis.

Physical security measures shall be put in place for premises, buildings, offices, rooms and other areas in which classified information is handled, stored or processed electronically.

Areas in which information classified CONFIDENTIAL and above is stored, shall be established as security areas.

In order to protect the information classified CONFIDENTIAL and above, equipment, systems or other technical devices meeting the minimum standards prescribed by the Director of the Directorate, shall be used.

Article 28

Measures and activities for physical security shall be as follows:

- assessment of the possible security breach of the classified information;
- establishing a security area around the facility;
- definition of security and administrative zones;
- organizing physical protection and application of technical and other security devices for buildings and rooms where classified information is held;
- control of entry, movement and exit of individuals and vehicles for transportation of classified information; and
- physical safeguarding during transportation of classified information outside of the security areas.

The Government of the Republic of North Macedonia shall prescribe with a decree the measures and activities for physical security.

Personnel security

Article 29

Measures and activities for personnel security shall be as follows:

- designating a classified information security officer;
- security vetting;
- issuing a security clearance;
- issuing an access permit for classified information; and
- verifying and evaluation of the ability to handle classified information.

The Government of the Republic of North Macedonia shall prescribe with a decree the measures and activities for personnel security.

Security of communication and information systems

Article 30

Security of communication and information systems shall refer to the application of security measures for the protection of communication, information and other electronic systems as well as for the protection of classified information that is stored, processed or transmitted through these systems, thereby ensuring confidentiality, integrity, availability, authentication and non-repudiation of such information.

For the purposes of acomplishung the goals referred to in paragraph 1 of this Article and creating a secure environment in which to operate communication, information and other electronic systems, an appropriate set of security measures for

administrative and physical security, security of communication and information systems and for personnel security shall be implemented.

The set of security measures of the communication and information systems shall be based on a security risk management process.

Article 31

Measures and activities for communication and information systems security shall be as follows:

- accrediatation of communication and information systems and processes;
- assessment for possible breach of the security of the classified information by an unauthorized intrusion into the communication and information systems in which classified information is stored, transmissed and processed;
- identification of methods and security procedures for receiving, processing, transmission, storing and archiving of electronic classified information;
- protection in the process of creating, storing, processing and transmitting classified information in the communication and information systems;
- cryptographic security of communication, information and other electronic systems used for creating, storing, cryptographic processing and transmitting classified information;
- protection from compromising electromagnetic emissions;
- determination of zones and rooms protected from compromising electro-magnetic emission; and
- installation of storage devices for classified information.

The Government of the Republic of North Macedonia shall prescribe with a decree the measures and activities for communication and information systems security.

Article 32

Measures and activities for cryptographic security shall be as follows:

- planning, organization and implementation of cryptographic security;
- evaluation and approval of cryptographic materials and products;
- production and development of cryptographic algorithms and products;
- planning, organization and management of cryptographic materials;
- implementation of appropriate measures and procedures for recording, safety handling, storing and distribution of cryptographic materials and products;
- training of personnel to operate cryptographic materials and products;
- control of the implementation of the measures and procedures for cryptographic security and the mode of operation of the cryptographic materials and products.

The Government of the Republic of North Macedonia shall prescribe with a decree the measures and activities for cryptographic security.

Article 33

Transmission of classified information via communication systems outside of the security areas shall be exclusively made by using cryptographic protection.

Industrial security

Article 34

Measures for industrial security shall be applied to ensure the protection of classified information by contractors and entities involved in pre-contract negotiations and throughout the life-cycle of classified contracts.

The measures for industrial security shall ensure the protection of classified information during transportation and over the course of establishing procedures for visits of foreign natural persons and legal entities to facilities where classified information is handled.

The natural persons and legal entities referred to in paragraphs 1 and 2 of this Article are required to possess an appropriate security clearance or acess permit to classified information in order to have access to and handle classified information in carrying out classified contracts, transporting classified information and visiting facilities where classified information is handled.

In order to classify the contract and the stages preceeding the conclusion of the contract including the public call for participation in public procurements, the legal entity is required to present an opinion provided by the classified information security officer affiliated to the entity that announced the public call.

Measures and activities set forth in paragraphs 1 of Articles 26, 28, 29, 31 and 32 respectively, are integral part of the measures and activities for industrial security.

The Government of the Republic of North Macedonia shall prescribe with a decree the measures and activities for industrial security.

Exchange of classified information with foreign states and international organizations

Article 35

Classified information of a foreign state or international organization is an information or material, which the competent agency of the foreign state or the international organization has released to the Republic of North Macedonia with an obligation to ensure its protection.

The classified information received from a foreign state or an international organization shall be handled as determined with a ratified international agreement.

If the international agreement referred to in paragraph 2 of this Article does not include provisions on the way of handling classified information, it shall be handled in line with the provisions of this Law.

Article 36

In the event of a state of emergency, military or crisis situation in the Republic of North Macedonia, the Directorate may exchange classified information with foreign states and international organizations with which it has not entered into international agreements, provided that such exchange is requested by competent bodies according to the Constitution of the Republic of North Macedonia and regulated by law, a prior consent is given by the Governement of the Republic of North Macedonia and it is of interest to the Republic of North Macedonia.

Upon termination of the state of emergency, military or crisis situation referred to in paragraph 1 of this Article, the Directorate shall provide the Government of the Republic of North Macedonia with a report pertaining to the exchanged classified information with foreign states and international organizations with which it has not entered into international agreements.

Article 37

According to the assumed obligations from the ratified international agreements, the Directorate shall ensure exercising control by authorized representatives of foreign states and international organizations for the way of use and protection of the classified information they have released to the Republic of North Macedonia.

In line with this Law and the ratified international agreements, the Directorate shall control the way of use and protection of the released classified information from the Republic of North Macedonia to the foreign states and international organizations.

Use of classified information

Article 38

User of classified information may be a body of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entity established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje or a natual person or legal entity in the Republic of North Macedonia that has a security clearance or a foreign state body, institution or foreign natural person or legal entity that has a security clearance issued by the home-country and an access permit for classified information issued by the Directorate, according to the “need to know” principle.

Article 39

For the purposes of accomplishing the official tasks, a security clearance shall be issued to the employees handling classified information in the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, to legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje, as well as to other natural persons and legal entities according to the “need-to-know” principle.

A security clearance shall be issued for access to an appropriate level of classified information.

For the purpose of issuing a security clearance for access to an approapriate level of classified information, the interested natural person or legal entity shall submit a written request to the Directorate.

The request for issuing a security clearance referred to in paragraph 3 of this Article shall be submitted through the officer for security of classified information within the legal entity.

The procedure for issuing a security clearance for the persons employed by the Directorate shall be carried out through the officer for security of classified information within the Directorate.

Security clearance referred to in paragraph 2 of this Article shall be issued by the Director of the Directorate after security vetting and assessment for existence or non-existence of security risk for handling classified information have been carried out.

Article 40

For the purpose of unencumbered exercising of the official function from the day of election until the end of the mandate, security clearance for access to and use of classified information of any level of classification, without previous security vetting, shall be issued to: the President of the Republic of North Macedonia, the President of the Assembly of the Republic of North Macedonia, the President of the Government of the Republic of North Macedonia, the Deputies of the President of the Government of the Republic of North Macedonia, the President of the Constitutional Court of the Republic of North Macedonia and the President of the Supreme Court of the Republic of North Macedonia.

Article 41

Security clearance shall be issued to a natural person if:

- s/he is a citizen of the Republic of North Macedonia;
- there is a justified reason for using classified information according to the “need-to-know” principle;
- there are no security obstacles for having access to and handling classified information which is determined by a security vetting;
- s/he has legal capacity;
- s/he is 18 years old, and for using information classified TOP SECRET, 21 years old;
- there is no sanction for imposing a ban on practicing a profession, activity or duty;
- to have a non-conviction certificate, with validity not exceeding six months;
- there are no security obstacles for having access to and handling classified information which is being determined by a security vetting for the persons listed in the security questionnaire;

Prior to issuing the security clearance, the person shall be trained in handling classified information.

Article 42

Facility security clearance shall be issued to a legal entity if:

- it is registered in the Republic of North Macedonia;
- there is a justified reason for access to and handling classified information according to the "need-to-know" principle;
- there is no sanction for imposing a ban on practicing an activity;
- it has ensured physical security, administrative security and/or communication and information systems security, if stipulated in the classified contract;
- it has secured a security clearance for the officer for security of classified information employed therein;
- it is financially and economically stable; and
- there are no security obstacles for handling classified information which is being determined by a security vetting.

The financial and economic stability referred to in paragraph 1, line 6 of this Article shall be confirmed upon submitting the following documents, the issuance date of which should not exceed six months:

- excerpt from the professional activity register;
- document about the business success issued by a competent authority;
- evidence from a competent authority for nonexistence of bankruptcy or liquidation proceedings;
- evidence from a competent authority that no security measure for prohibition from practicing a profession has been delivered; and
- certificate from a competent authority for paid taxes, contributions and other public duties.

Article 43

The legal entity shall be considered eligible to provide protection of classified information in case it has provided conditions for application of the measures and activities for protection of classified information, regulated by this Law.

Procedures for issuing security clearances

Article 44

The fulfilling of the conditions for issuing a security clearance shall be determined through a security vetting.

The security vetting referred to in paragraph 1 of this Article shall be conducted on the basis of a prior written consent from the natural person or legal entity that has submitted a request for issuing a security clearance, which is a part of the request referred to in Article 39 paragraph 3 of this Law.

If the natural person or the legal entity withdraws his consent during the vetting procedure with a written statement, another security vetting cannot be conducted before the expiry of one-year period starting from the day of the withdrawal of the consent.

Article 45

For the purpose of determining the existence or nonexistence of a security risk, security vetting shall be conducted before a security clearance is issued to natural persons and legal entities for access to and handling classified information.

The security vetting shall begin after the request referred to in paragraph 3 of Article 39 of this Law, has been submitted to the Directorate.

The data collected from the questionnaire represent a part of the contents of the security vetting.

The Director of the Directorate shall prescribe the form and contents of the security questionnaire referred to in paragraph 1 of this Article upon prior coordination with the competent authorities responsible for conducting security vettings.

Article 46

The questionnaire filled out for a security vetting shall be marked with UNCLASSIFIED.

The data collected from the questionnaire referred to in paragraph 1 of this Article shall be used for the purposes of the security vetting and handled in line with a law.

Article 47

For using RESTRICTED information, no security vetting shall be conducted nor a security clearance shall be issued.

The natural person or the responsible person in the legal entity shall be briefed about the obligation to protect the classified information referred to in paragraph 1 of this Article that s/he has been given access to or a permission to handle such information.

Article 48

Depending on the level of the classified information for which a request for a security clearance for natural person has been filed, different vetting procedures, appropriate to the classification level of the information shall be conducted, as follows:

a) first level vetting for information classified CONFIDENTIAL;
b) second level vetting for information classified SECRET; and
c) third level vetting for information classified TOP SECRET.

Article 49

The first level vetting shall verify the following:

- identity of the individual (based on the submitted written documentation and the operational verification of the data about the individual conducted by a competent body);
- age of at least 18 years;
- citizenship of the Republic of North Macedonia;
- legal capacity of the individual (based on a certificate from a relevant court);
- existence of security obstacles for the individual for access to and handling classified information (determined with operational vetting conducted by a competent body).

Article 50

The second level vetting shall verify the following:

- identity of the individual (based on the submitted written documentation and the operational verification of the data about the individual conducted by a competent body);
- age of at least 18 years;
- citizenship of the Republic of North Macedonia;
- legal capacity of the individual (based on a certificate from a relevant court); and
- existence of security risk or security obstacles to the individual-requestor of security clearance and the persons listed in the security questionnaire for access to and handling classified information (determined with operational vetting conducted by a competent body).

Article 51

The third level vetting shall verify the following:

- identity of the individual (based on the submitted written documentation and the operational verification of the data about the individual conducted by a competent body);
- age of at least 21 years;
- citizenship of the Republic of North Macedonia;
- legal capacity of the individual (based on a certificate from a relevant court); and
- existence of security risk or security obstacles to the individual-requestor of security clearance and the persons listed in the security questionnaire for access to and handling classified information (determined with operational vetting conducted by a competent body);
- ability of the person to handle classified information, which is being determined with an interview conducted by an authorized person from the competent authorities carrying out the security vettings.

Article 52

Upon a request by the Directorate, the security vetting procedures for determining the existence of security obstacles for access to and handling classified information shall be carried out by:

- the National Security Agency for all natural persons and legal entities, with the exception of the ones indicated below in line 2 of this paragraph; and
- the competent services of the Ministry of Defence for all personnel employed at Ministry of Defence and the Army of the Republic of North Macedonia.

Article 53

The security vetting procedure shall last no longer than:

- four months for first level vetting for natural persons;
- six months for second level vetting for natural persons;
- six months for third level vetting for natural persons, and
- six months for vetting for a legal entity.

With the exception of paragraph 1 of this Article and in accordance with the Law on Interception of Communications, the third level security vetting procedure for the persons appointed in the supervisory bodies that supervise the application of the measures for monitoring of communications, as well as for the accredited national and international technical experts engaged in those bodies shall last one month from the date of submitting the request for conducting security vetting.

With the exception of paragraph 1 of this Article and in accordance with the Law on operational and technical agency, the second level security vetting procedure for persons, prior entering into employment relationship with the Operational Technical Agency, shall last one month from the day of submitting the request for conducting security vetting.

Validity of the security clearances

Article 54

Validity of the security clearance issued for TOP SECRET information shall not exceed five years.

Validity of the security clearance issued for SECRET information shall not exceed five years.

Validity of the security clearance issued for CONFIDENTIAL information shall not exceed ten years.

The Director of the Directorate shall prescribe the contents and pattern of the security clearances referred to in the paragraphs 1, 2 and 3 of this Article.

Article 55

The user of classified information shall be obliged to file a new request for extending the validity of the security clearance six months the latest before the day of the expiry of its validity.

For the natural person and legal entity who file a request for extension of the validity of the security clearance, a new vetting procedure according to the classification level of the information to be released to him shall be carried out, in accordance with this Law.

Article 56

In case it is determined that the natural person or the legal entity does not handle classified information according to this Law or that any of the conditions, on the basis of which the security clearance has been issued, is no longer met, the Director of the Directorate shall bring a decision to revoke the security clearance before the expiry of its validity.

The decision referred to in paragraph 1 of this Article shall not include a rationale about the reasons of revoking the security clearance.

The individual whose security clearance has been revoked before the expiration of its validity, has the right to appeal to the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes against the decision referred to in paragraph 1 of this Article, i.e. the procedure for revoking the security clearance.

Article 57

Unless the conditions of this Law are met, the Director of the Directorate may bring a decision to refuse the request for issuing a security clearance for natural persons and legal entities.

The decision referred to in paragraph 1 of this Article shall not include a rationale about the reasons for refusing the request for issuing a security clearance.

The individual whose request has been refused may appeal to the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes against the decision referred to in paragraph 1 of this Article, i.e. the procedure for issuing the security clearance.

Article 58

The appeal referred to in paragraph 3 of Article 56, and paragraph 3 of Article 57 of this Law shall be filed within 15 days from the day of the receipt of the decision to the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes.

The decision on the appeal referred to in paragraph 1 of this Article brought by the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes shall be final.

Article 59

A new request for issuing a security clearance of the same or higher level of classification may be submitted:

- after the expiration of one year from the date of the decision for refusal of the request for issuing a security clearance has become effective or final, and

- after the expiration of three years from the date of the decision to revoke the security clearance before the expiry of its validity has become effective or final.

The validity of the reissued security clearance for the persons referred to in paragraph 1 of this Article shall not exceed one year.

Article 60

Security clearance shall cease to be valid upon expiry of its validity as well as if:

- the official function of the individuals referred to in Article 40 of this Law has ended;
- the requirement for having access to classified information according to the "need-to-know" principle has terminated;
- the mental capacity to handle classified information has diminished;
- the natural person deceased or the legal entity has stopped to exist.

In the cases referred to in paragraph 1, line 1, 2, 3 and 4 of this Article, the officer for security of classified information shall return the security clearances for natural persons and/or legal entities to the Directorate within 15 days from the day of the acknowledgment thereof.

Article 61

The validity of the access permit for classified information shall terminate:

- upon expiry of the validity period indicated in the access permit;
- upon accomplishing the relevant task;
- if the requirement for issuing the access permit has ceased to exist or has been changed;
- if it is determined that the legal entity and the natural person does not handle the classified information in accordance with law.

Article 62

The obligation for protection of the secrecy of the classified information shall continue beyond the termination of the validity of the security clearance.

Article 63

For the purposes of court proceedings or procedure in front of another relevant body in which classified information is used, the entities are required to possess a security clearance.

The procedure referred to in paragraph 1 of this Article shall be conducted in the presence of the person whose rights, obligations or responsibility are decided within its framework as well as when the person does not have a security clearance.

The person referred to in paragraph 2 of this Article shall be responsible for fulfilling the obligation for protection of the classified information according to this Law.

In conducting the procedure referred to in paragraph 1 of this Article, the public shall be excluded.

In case the classiffied information is not submitted by the originator in the procedure referred to in paragraph 1 of this Article, the relevant court, i.e., the competent body shall be obliged to inform the originator and the Directorate of its use therein, within 15 days from the day of the receipt of the classified information.

Article 64

The Directorate shall keep records of the issued security clearances and the filled out security questionnaires.

The Directorate shall keep a separate record of the issued access permits for classified information in the Republic of North Macedonia.

The contents, form and way of keeping the records referred to in paragraphs 1 and 2 of this Article shall be prescribed by the Director of the Directorate.

CHAPTER FOUR
BODIES FOR PROTECTION OF CLASSIFIED INFORMATION

Classified Information Security Officer

Article 65

The bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entity established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje and other legal entities shall be obliged to create conditions necessary for protection of classified information and to take on measures for eliminating the negative consequences should such information be disclosed.

In order to ensure efficient and coordinated execution of the rights and obligations concerning the classified information, the entities referred to in paragraph 1 of this Article shall designate a classified information security officer.

Article 66

The responsible person in the entities referred to in Article 65, paragraph 1 of this Law shall designate one or more officers for security of classified information depending on the number and scope of classified information being handled therein.

With the exception of paragraph 1 of this Article, depending on the number and scope of classified information, the responsible person of the entity may perform the duties of a classified information security officer.

With the exception of the case referred to in paragraph 2 of this Article, the classified information security officer is obliged to prepare and submit quarterly reports on the classified information related work and the conditions thereto, directly to the responsible person.

In case more classified information security officers are identified in the entity, the responsible person shall designate one of them to coordinate the classified information related activities with the Directorate.

Article 67

The classified information security officer may be designated if s/he meets the following requirements:

- s/he is a citizen of the Republic of North Macedonia,
- s/he is not a citizen of another state;
- s/he has been given access to appropriate level of classified information in accordance with the conditions and the procedure determined by law;
- s/he has completed a training for officer for security of classified information;
- s/he possesses an appropriate security clearance.

Article 68

The classified information security officer shall be obliged:

- to ensure application of the provisions of this Law and the ratified international agreements related to the security of classified information in the entity;
- to verify quarterly the records and the flow of materials and documents;
- to ensure proper and timely archiving and destruction of classified information;
- to carry out the procedure for submitting requests for issuing a security clearance within the entity and to keep records of persons with respect to whom, the procedure has been carried out;
- to notify the Directorate of the expiry of the security clearances, termination of the employment or reassigning the users of classified information;
- to notify the Directorate of the necessity to change the level of security clearance;
- to notify the Directorate in written of any change in the data listed in the security questionnaire or change in the conditions for issuing a security clearance which change s/he been aware of or could have been aware of;
- to record cases of unauthorized access to or compromising of classified information as well as actions undertaken, and to immediately notify the Directorate thereof;
- to inform the users of classified information at least once a year about the rights and obligations in handling classified information;
- to provide expertise in determining the classification level of the information within the entity;
- to organize training on the protection of classified information for the users of classified information within the entity.

For the purpose of accomplishing the working activities referred to in paragraph 1 of this Article, the classified information security officer shall prepare an annual working plan, which shall be submitted to the responsible person for approval. In case where the responsible person performs the duties of a classified information security officer, s/he shall prepare the annual working plan her/himself.

Directorate for Security of Classified Information

Article 69

The Directorate shall be a standalone body of the state administration with capacity of a legal entity.

The Directorate shall:

- ensure continuous application of the international standards and norms while taking on measures and activities for the protection of classified information;
- coordinate the activities for ensuring protection of the classified information with the state bodies and the institutions that exchange classified information with foreign states and international organizations;
- prepare, organize, apply and monitor the application of the measures and activities for ensuring protection of classified information that has been released to the Republic of North Macedonia by foreign states and international organizations;
- take on activities for protection of the classified information that the Republic of North Macedonia has released to foreign states and international organizations;
- participate in the process of developing plans and programs of the Republic of North Macedonia for membership in international organizations related to the protection of classified information;
- plan and accomplish international cooperation for protection and exchange of classified information;
- recommend measures for enhancing the protection of classified information;
- plan and accomplish international cooperation for protection and exchange of classified information;
- recommend measures for enhancing the protection of classified information;
- initiate entering into international agreements with foreign states and international organizations related to the exchange of classified information;
- perform accreditation of communication - information systems and processes
- organize and carry out trainings for protection of classified information;
- perform inspection supervision over the implementation of the provisions of this Law and
- accomplish other tasks regulated by Law.

The Directorate shall prepare an annual plan and report for its work that shall be subject to adoption by the Government of the Republic of North Macedonia.

Article 70

In the exchange and protection of classified information with NATO and the European Union, the Directorate shall:

- coordinate and implement NATO and European Union security policies in the Republic of North Macedonia in order to ensure an appropriate level of protection of the classified information in accordance with the ratified international agreements;
- provide security of the communication for selection, management and maintenance of the cryptographic equipment for transmitting, processing and storing classified information;
- conduct security accreditation of the communication-information systems and processes in which classified information is used;
- take on measures and activities for protection of the communication – information systems against compromising electromagnetic emission.

Article 71

In the exchange and protection of classified information with NATO, the Ministry of Defence and the Army of the Republic of North Macedonia shall manage the materials for cryptographic security of classified information, thereby ensuring safety handling, storage, distribution and recording of the crypto materials.

In the framework of managing the materials for cryptographic security of classified information and ensuring safety handling, storage, distribution and recording of the crypto materials, the Directorate shall perform supervision over the implementation of the measures carried out by the competent body.

Registries and control points

Article 72

For the purpose of accomplishing the works concerning NATO classified information, classified information of the European Union and other foreign classified information within the scope of responsibility of the Directorate, registries, subregistries and control points shall be established.

The registry shall be established at the Directorate, while subregistries and control points shall be established within the organs of the state administration established in accordance with the Constitution of the Republic of North Macedonia and regulated by law, the legal entities established by the Republic and other legal entities where NATO classified information, classified information of the European Union and other foreign classified information is handled and stored.

The subregistries and control points referred to in paragraph 1 of this Article shall forward information necessary for accomplishing the work of the Directorate and the exchange of classified information with foreign countries.

Upon a request by the users of classified information, the Directorate shall give a consent of fulfilling the conditions for establishing subregistries and control points.

The exchange of classified information between the Republic of North Macedonia and foreign states and international organizations shall be accomplished via the Directorate, unless otherwise regulated by law, ratified international agreement or another arrangement.

Article 73

The Directorate shall inform the competent bodies of the foreign states and international organizations about the security of the classified information exchanged and shall be informed by them about the security of the classified information released to them by the Republic of North Macedonia, in accordance with the ratified international agreements.

Article 74

Upon a request by the Directorate, the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje and other legal entities and natural persons shall provide information necessary for accomplishing the works within the competence of the Directorate.

Article 75

The Directorate for Security of Classified Information shall be managed by a director who shall be appointed and discharged by the Government of the Republic of North Macedonia.

The director shall be appointed for a mandate of four years.

The director shall have a deputy who is appointed and discharged by the Government of the Republic of North Macedonia for a term of office of four years. The deputy director shall replace the director in the cases of his/her absence or when due to illness or other reasons he/she is not able to perform his/her duties, and shall have all his/her management powers and responsibilities.

The director and the deputy director shall be selected at a public announcement which is published in three daily newspapers that are printed on the whole territory of the Republic of Macedonia one of which is a newspaper printed in a language spoken by at least 20% of the citizens who speak an official language other than the Macedonian.

A person who meets the following requirements may be appointed as a director and deputy director of the Directorate:

1) to be a citizen of the Republic of Macedonia;
2) not to have a citizenship of another state;
3) not to be issued an effective injunction banning him/her from exercising a profession, business or office;
4) to have at least 240 credits under ECTS or completed VII/1 degree;
5) to have at least five years of work experience;
6) to hold one of the following internationally recognized certificates for active knowledge of English language which is not older than five years:
   - TOEFL IBT - at least 74 points,
   - IELTS - at least 6 points,
   - ILEC (Cambridge English: Legal) - at least B2 level,
   - FCE (Cambridge English: First) - passed,
   - BULATS - at least 60 points, or

- APTIS - at least B2 level and

7) to have a TOP SECRET security clearance.

The term of office of the director and deputy director shall be terminated before the expiry of the mandate for which they were appointed:

- if s/he resigns;
- on a personal request;
- due to fulfillment of the requirements for old-age pension defined by law, with the right to an extension in accordance with the labour regulations;
- due to death;
- s/he is sentenced to prison for more than six months by means of an effective court decision.

The Government of the Republic of North Macedonia shall discharge the director and the deputy director of the Directorate if one of the following conditions has been met:

- it is established that s/he does not meet one of the requirements defined in Article 74, paragraph 5 of this Law;
- s/he refuses to submit a statement on property ownership and interests pursuant to the law or the data provided therein are false and;
- s/he evidently violates the rules of conflict of interest, that is, an exemption in situations when the director was aware or should have aware of the existence of any of the grounds for conflict of interest, that is, an exemption stipulated in the law.

Article 76

The employees of the Directorate shall have the status of administrative servants. With respect to their rights and responsibilies arising from employment, the provisions of the Law on Administrative Servants shall be applied.

The employees of the Directorate shall be appointed to perform duties in the missions of the Republic of North Macedonia to NATO and EU, according to the signed agreement on joint cooperation with the Ministry of Foreign Affairs.

During the appointment, the employees shall be given a title, according to the provisions of the Law on foreign affairs.

The employees of the Directorate shall be required to have a relevant security clearance for access to classified information. The level of the security clearance shall be defined with the act on systematic design of posts of the Directorate.

The employee of the Directorate whose validity of the security clearance is not extended during the employment or it is established over the course of the vetting procedure that a security clearance cannot be issued to him/her due to existence of a security risk for access to and handling classified information, shall be permanently transferred to another state body or institution at a position of a same level for which s/he meets the general and specific conditions defined with the jobs systematization act of the other institution.

The transfer shall be made on the grounds of an agreement signed by the managing persons of both institutions.

The employee being transferred shall have his/her employment terminated unless s/he signs the new employment contract within 15 days from the submission day thereof.

The employees of the Directorate shall have official identification cards issued by the Director of the Directorate.

The Director of the Directorate shall prescribe the form of the official identification card the manner of issuing thereof.

CHAPTER FIVE
PLANS AND PROGRAMS FOR THE WORK OF THE DIRECTORATE AND BUDGETING OF THE DIRECTORATE

Article 77

The work of the Directorate shall be guided and accomplished according to the relevant principles, norms and procedures of the Planning, Programming and Budgeting System.

Article 78

The finances necessary to meet the requirements of the Directorate shall be provided from the Budget of the Republic of North Macedonia.

The finances necessary to meet the requirements of the Directorate may also be provided from other sources, according to law.

The finances for the state bodies necessary for the protection, use and international exchange of the classified information shall be provided from the Budget of the Republic of North Macedonia within the framework of the budgets of those bodies.

For the purposes of protection, use and international exchange of classified information, the bodies of the local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje shall provide finances from their own sources and from the financial and material assets of the Republic of North Macedonia.

CHAPTER SIX
SUPERVISION

Article 79

Inspection supervision over the implementation of this Law and the regulations adopted on the basis of this Law, shall be performed by the Directorate via the inspectors for security of classified information (hereinafter referred to as inspectors).

The supervision works shall be exercised in a separate organizational unit within the Directorate.

Article 80

In the procedure of perfoming inspection supervision, the provisions of this Law shall apply, while the provisions of the Law on Inspection Supervision and the Law on General Admisnistrative Procedure shall apply for the issues that are not regulated by this Law.

The director of the Directorate shall prescribe the manner of performing inspection supervision with a rulebook.

Article 81

Aside from the general conditions regulated by the Law on administrative servants, the inspector who shall perfom the supervision, is required to fulfill the following special conditions:

- to have 240 credits under ECTS, that is, completed VII/1 degree;
- to have three years of work experience related to the security of classified information;
- to have passed a professional exam of inspector for security of classified information;

The director of the Directorate shall prescribe with a rulebook the manner of taking the professional exam of inspectors for classified information.

The supplement to the salary of the inspector shall be regulated by the Law on Inspection Supervision.

Article 82

The inspector shall perform supervision in the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje as well as in other legal entities and natural persons.

The inspector shall be independent in performing the inspection supervision. If necessary, upon proposal by the head of the organizational unit responsible for performing inspection supervision, the director may establish an inspection supervision team comprised of administrative servants of the Directorate.

The inspectors shall be obliged to act in accordance with the law and the regulations.

The inspectors are required to provide an objective application of the law.

Article 83

While exercising the inspection supervision referred to in Article 79 of this Law, the inspectors shall be authorized to:

- perform supervision over the application of this Law and the other regulations related to the security of classified information,
- recommend measures for removal of the occurred irregularities and deficiencies in an established time frame.
- undertake other actions in accordance with law.

Article 84

The official capacity of the inspector shall be proven with an official identification card and a badge.

While performing inspection supervision, the inspectors shall be obliged to identify themselves.

The official identification card and the badge referred to in paragraph 1 of this Article, shall be issued and revoked by the director of the Directorate.

The director of the Directorate shall prescribe the pattern, form and contents of the official identification card and badge as well as the manner of issuance and revocation thereof.

Article 85

For the purpose of performing inspection supervision, the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje as well as other legal entities and natural persons shall be obliged to ensure an unobstructed supervision related to the security of classified information.

The inspection supervision may be regular, ad hoc or control.

Regular inspection supervision shall entail supervision over the implementation of this Law and shall be performed according to an annual program and an individual montly working plan of each inspector adopted by the director of the Directorate according to law.

Ad hoc inspection supervision shall be performed on the basis of an initiative submitted by the bodies of the state and local administration established in accordance with the Constitution of the Republic of North Macedonia and determined by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the city of Skopje, legal entities or natural persons as well as in case of suspicion of the inspector (ex officio).

The control inspection supervision shall be performed upon the expiration of the deadline set in the decision for removal of identified deficiencies.

When performing inspection supervision, inspectors shall have the right of access to and inspect buildings, business offices, residential premises and premises where classified information is handled and stored, at any time and without previous notice.

For the purpose of performing the works in residential premises referred to in paragraph 6 of this Article, inspectors shall be obliged to provide a court warrant.

In order to be protected during inspection supervision, the inspectors may request the presence of an authorized person from the state administrative body competent for performing police affaits related activities.

Article 86

If during the performance of the inspection supervision, the inspector detects deficiencies and irregularities related to the fulfillment of the conditions for security of

classified information, s/he shall bring a decision ordering removal of the detected deficiencies and irregularities within a defined timeframe.

Complaint may be filed against the decision of the inspector referred to in paragraph 1 of this Article, within fifteen days as of receiving the decision.

The State Commission for Decision-Making in the Second Instance in the Area of the Inspection Supervision and Misdemeanor Procedures shall decide upon the complaint against the decision of the inspector.

Article 87

Upon the performance of the inspection supervision, the inspector shall compose minutes containing the findings on the situation, and shall submit it in the manner and within the timeframe regulated by law.

The inspector shall bring a decision containing deadlines within which the recommended measures for removal of the deficiencies and irregularities are to be implemented. The responsible person of the entity being subject of inspection shall be obliged to take up actions according to the minutes and to inform the inspector about the implemented activities.

Article 88

If the inspector determines that the devices, technical means, installations and systems in use do not correspond to the prescribed security standards and criteria for protection of classified information, s/he shall issue a decision to prohibit their use and to remove them.

Article 89

If during the performance of inspection supervision, the inspector determines the existence of an immediate danger violating the security of the buildings or the premises, documents, equipment, systems and persons within the security perimetar, security area or administrative zone, s/he shall issue a decision prohibiting the use of the area, the building or a part thereof.

Article 90

In order to enforce the decision referred to in the Article 86, paragraph 1 and Article 88 of this Law, the inspector shall seal the building or premises in question.

The sealing referred to in paragraph 1 of this Article shall be marked with a seal stamp of the Directorate.

The Director of the Directorate shall prescribe with a rulebook the contents and the shape of the seal stamp as well as the manner of sealing.

Article 91

After the detected deficiencies have been removed, because of which the measure of prohibition had been delivered and upon a written request from the entity to whom the measure had been delivered, the inspector shall remove the wax seal.

Article 92

During the performance of the supervision over the implementation of the provisions of this Law and the other regulations related to security of classified information, the inspectors may order the following measures to be undertaken:

1) dissembling, displacement or removal of equipment, devices, installations and systems endangering the security of classified information;
2) establishing of the security perimetar, security areas and administrative zones around the building, area or premises within the building where classified information is handled and stored;
3) setting-up of secure communication and information equipment, systems and installations for security of classified information;
4) displacement or removal of persons without appropriate security clearance or access permit from the security perimetar around the building, as well as from the security areas, administrative zones within the building where classified information is handled and stored;
5) dispalcement or removal of vehicles without appropriate access permit to the security perimeter around the building and the administrative zones within the building where classified information is handled or stored;
6) preparation of internal acts for security risk assessment and for protection of classified information in case of emergencies;
7) updating and correction of the records, disposal and destruction of classified information;
8) ensuring implementation of prescribed conditions for dissemination and transmission of classified information;
9) prohibition for receiving, handling, releasing and storing of classified information;
10) other measures determined by the inspector that are relevant for the protection of classified information in the supervised entity.

Article 93

If during the performance of inspection supervision, the inspector determines a violation of a law and other regulations which represents a misdemoneour, he shall file a request for commencing a misdemenour procedure in accordance with the provisions of this Law and the Law on Misdemenours.

If during the performance of inspection supervision, the inspector considers that the violation represents a criminal offence, he shall be obliged to inform immediately the Director of the Directorate in order to commence a procedure in front of a competent body.

CHAPTER SEVEN

MISDEMENOUR PROVISIONS

Article 94

Fine in amount from 3.000 to 5.000 Euro in Denar counter value shall be imposed on a legal entity – user of classified information for a misdemenour if it:

- does not implement the measures for administrative secuity, physical secuity, communication and information systems security, personnel security or industrial security of classified information, according to the provisions of Articles 26, 28, 29, 31, 32, and 33 of this Law;
- does not handle classified information according to the provision of Article 56 paragraph 1 of this Law (unless the action represents a criminal offence);
- does not inform about the cessation of fulfillment of some of the conditions on the basis of which a security clearance has been issued, according to the provisions of Article 42 of this Law;
- hinders the execution of the inspection supervision according to the provisions of Article 79 of this Law.

Fine in amount from 1.000 to 2.000 Euro in Denar counter value shall be imposed on a responsible person in the legal entity – user of classified information for the misdemenours referred to in paragraph 1 of this Article.

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on a natural person – user of classified information for the misdemenours referred to in paragraph 1 of this Article.

Article 95

Fine in amount from 1.500 to 2.000 Euro in Denar counter value shall be imposed on a legal entity – user of classified information for a misdemenour if it does not undertake the activities necessary for reception, processing, identification of users and does not disseminate the classified information to them, according to the provisions of Article 26 of this Law.

Fine in amount from 1.000 to 1.500 Euro in Denar counter value shall be imposed on a responsible person in the legal entity – user of classified information for the misdemenour referred to in paragraph 1 of this Article.

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on a natural person – user of classified information for the misdemenour referred to in paragraph 1 of this Article.

Article 96

Fine in amount from 1.500 to 2.000 Euro in Denar counter value shall be imposed on a legal entity which shall act contrary to the obligation referred to in Article 47 paragraph 2 and with reference to Article 2 of this Law for protection of information classified RESTRICTED.

Fine in amount from 1.000 to 1.500 Euro in Denar counter value shall be imposed on a responsible person in the legal entity for the misdemenour referred to in paragraph 1 of this Article.

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on a natural person for the misdemenour referred to in paragraph 1 of this Article.

Article 97

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on a legal entity which shall act contrary to the Article 12 and shall disclose information marked with UNCLASSIFIED.

Fine in amount from 450 to 700 Euro in Denar counter value shall be imposed on a responsible person in the legal entity for the misdemenour referred to in paragraph 1 of this Article.

Fine in amount from 300 to 500 Euro in Denar counter value shall be imposed on a natural person for the misdemenour referred to in paragraph 1 of this Article.

Article 98

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on the officer for security of classified information for a misdemenour if s/he:

- does not fullfil any of his/her duties referred to in Article 68
- obstructs the performance of the inspection supervision according to the provisions of Article 79 of this Law.

Article 99

Fine in amount from 1.000 to 1.500 Euro in Denar counter value shall be imposed on the legal entity-originator of classified information which shall act contrary to the Article 10, paragraph 2 and does not make the necessary assessment of possible damage and consequences.

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on a responsible person in the legal entity for the misdemenour referred to in paragraph 1 of this Article.

Fine in amount from 300 to 500 Euro in Denar counter value shall be imposed on a natural person for the misdemenour referred to in paragraph 1 of this Article.

Article 100

Fine in amount from 1.500 to 2.000 Euro in Denar counter value shall be imposed on the legal entity-originator of classified information who shall act contrary to the Article 16, paragraph 3 and Article 18, paragraph 2 and does not notify the user of classified information for the change of the classification level or for its declassification.

Fine in amount from 1.000 to 1.500 Euro in Denar counter value shall be imposed on a responsible person in the legal entity for the misdemenour referred to in paragraph 1 of this Article.

Fine in amount from 500 to 1.000 Euro in Denar counter value shall be imposed on a natural person for the misdemenour referred to in paragraph 1 of this Article.

Procedure for settlement and issuing a misdemenour payment order

Article 101

For the misdemenours stipulated in this Law, the inspector shall be obliged, prior submitting a request for commencing a misedemenour procedure, to issue to the perpetrator a misdemenour payment order in accordance with the Law on Misdemenours.

The inspector shall be obliged to keep records of the issued misdemeanor payment orders and the outcome thereof.

The following data shall be collected processed and stored in the records referred to in paragraph 2 of this Article: first and last name, i.e., name of the perpetrator, permanent or temporary residence, address, type of misdemenour, number of the issued misdemeanor payment order as well as the outcome of the procedure.

The personal data referred to in paragraph 3 of this Article shall be kept for five years from the date of entry into the records.

The director shall prescribe the form and contents of the misdemeanor payment order.

If this Law does not entirely regulate the misdemenour payment order procedures, the Law on Misdemenours shall apply.

Article 102

For the misdemenours stipulated in this Law, the misdemeanor procedure shall be conducted and the sanction shall be imposed by a competent court.

CHAPTER EIGHT

PUNITIVE PROVISIONS

Disclosure of information classified SECRET and CONFIDENTIAL

Article 103

A person who tells, hands over or makes available an entrusted information classified SECRET to the public or to an unauthorized person, information to which s/he has an acess to according to law, and thereby endangers or violates the vital interests of the Republic of North Macedonia, shall be punished with imprisonment of one to five years.

A person who tells, hands over or makes available to the public or to an unauthorized person, information for which s/he knows is an information classifed SECRET, and which s/he acquired in an unlawful manner, shall be punished with imprisonment of one to three years.

A person who tells, hands over or makes available an entrusted information classified CONFIDENTIAL to the public or to an unauthorized person, information to which s/he has an acess to according to law, and thereby endangers or violates the

important interests of the Republic of North Macedonia, shall be punished with imprisonment of one to three years.

A person who tells, hands over or makes available to the public or to an unauthorized person, information for which s/he knows is an information classifed CONFIDENTIAL, and which s/he acquired in an unlawful manner, shall be punished with imprisonment of six months to three years.

If the crime referred to in paragrafs 1 and 3 of this Article is committed during a state of war, the perpetrator shall be punished with imprisonment of one to ten years.

The attempt of the crime referred to in the paragraphs 2, 3 and 4 of this Article shall be punishable.

If the crime referred to in paragrafs 1 and 3 of this Article is committed by negligeance, the perpetrator shall be punished with fine or imprisonment of up to one year.

Unauthorized disclosure of classified information used in court or other procedure

Article 104

A person who in violation of law discloses without authorization information classified TOP SECRET for which s/he found out about in court or other procedure shall be punished with imprisonment of up to five years.

If the information is classified SECRET or CONFIDENTIAL, the perpetrator shall be punished with imprisonment of one to three years.

The attempt of the crime referred to in paragraph 2 of this Article shall be punishable.

If the crime referred to in paragrafs 1 and 2 of this Article is committed by negligeance, the perpetrator shall be punished with fine or imprisonment of up to one year.

CHAPTER NINE

TRANSITIONAL AND FINAL PROVISIONS

Article 105

The by-laws envisaged by this Law, shall be passed within six months as of the day this Law enters into force.

The by-laws passed on the basis of the Law on classified information (“Official Gazette of the Republic of Macedonia”, No. 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18), shall be applied until the day the by-laws regulated by this law enter into force.

Article 106

The regulations regulating the issues on classified information shall be harmonized with the provisions of this Law in a period of one year starting from the day of entering into force of the Law.

Article 107

The security clearances issued until the day of entering into force of this Law shall be used until the termination of their validity.

Article 108

On the day of entering into force of this Law, the Directorate for Security of Classified Information, established with the Law on Classified Information (Official Gazette of the Republic of Macedonia, No. 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18), shall continue functioning as a Directorate for Security of Classified Information according to the competences regulated by this Law.

Article 109

The director of the Directorate for Security of Classified Information appointed until the day of entering into force of this Law, shall continue exercising the function until the expiration of the mandate for which s/he had been appointed.

Article 110

The validity of the Law on Classified Information (Official Gazette of the Republic of Macedonia, No. 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18) shall terminate on the day of entering into force of this Law.

Article 111

This Law shall enter into force on the eighth day from the day of its publication in the Official Gazette of the Republic of North Macedonia.