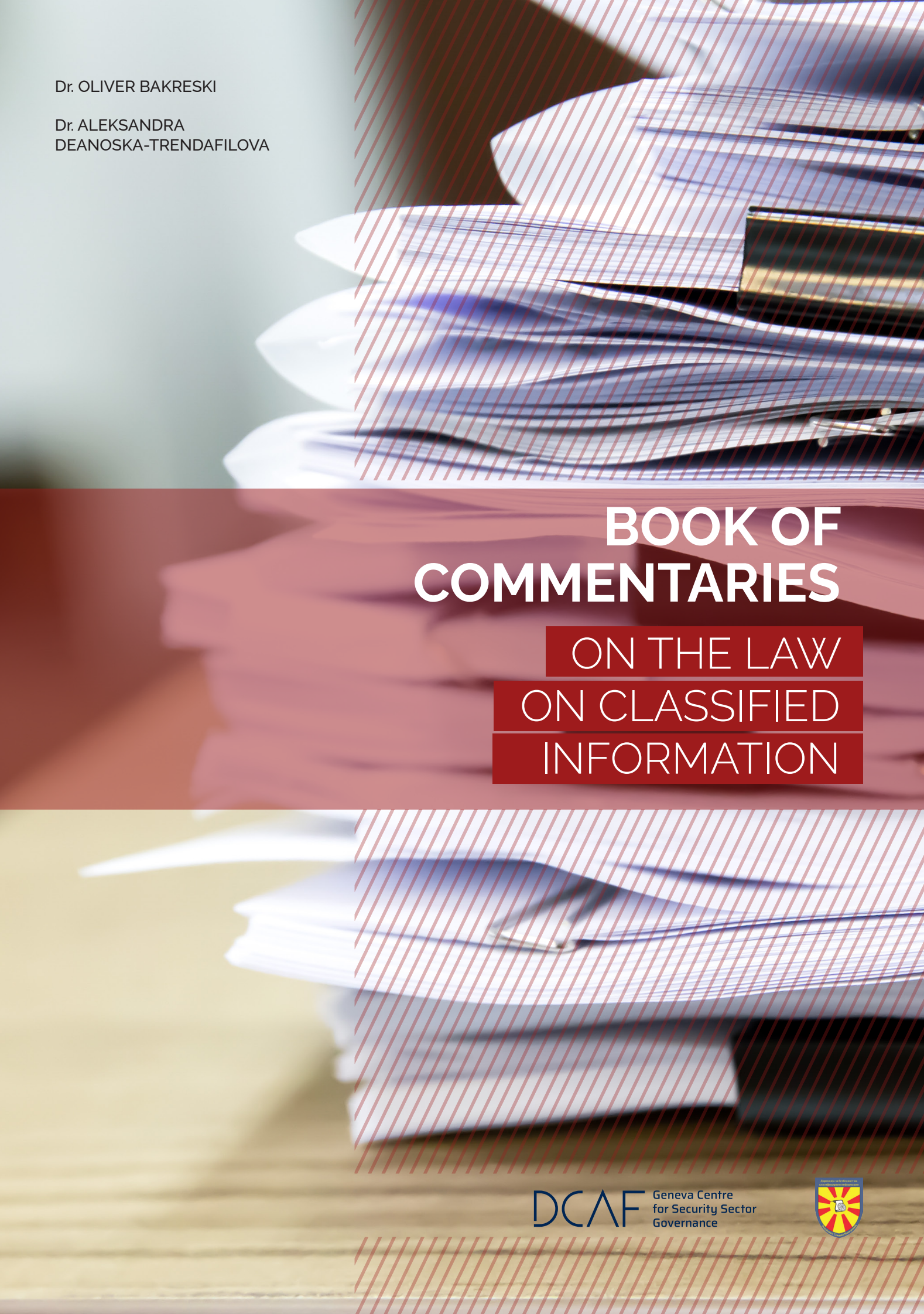
Dr. OLIVER BAKRESKI

Dr. ALEKSANDRA
DEANOSKA-TRENDAFILOVA



BOOK OF COMMENTARIES

ON THE LAW ON CLASSIFIED INFORMATION

DCAF Geneva Centre for Security Sector Governance

Dr. OLIVER BAKRESKI
Dr. ALEKSANDRA DEANOSKA-TRENDAFILOVA

BOOK OF COMMENTARIES
ON THE LAW ON CLASSIFIED INFORMATION

Skopje, 2021

BOOK OF COMENTARIES ON THE LAW ON CLASSIFIED INFORMATION(*)

Authors:
Dr. Oliver Bakreski
Dr. Aleksandra Deanoska-Trendafilova

DCAF Geneva Centre for Security Sector Governance

Publisher:

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity- building of both state and non- state security sector stakeholders.

DCAF's Foundation Council is comprised of representatives of about 60 member states and the Canton of Geneva. Active in over 80 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva

Kingdom of the Netherlands

Sweden Sverige

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Swiss Agency for Development and Cooperation SDC

The content of this publication does not necessarily reflect the views and the opinions of the donors or DCAF.

CONTENTS

PREFACE

With the establishment of the legal and institutional framework for protection of classified information in the Republic of North Macedonia, the existing system for protection of information of interest to the state was strengthened and a solid basis for credible cooperation with international organizations and foreign countries on sensitive security related issues was established. The regulation on protection of classified information was adopted in order to establish a positive practice for the protection of national security interests, to prevent damage to national security policy and the interests of the state, to clearly define the division of competencies and responsibilities, to exclude possible abuse in the performance of work tasks and duties, to provide effective control and sanctioning system, as well as to ensure obtaining the necessary credibility in the work and in the operation.

The legislation of the Republic of North Macedonia for protection of classified information is in line with NATO and EU standards. Its implementation, as well as the good results of the work of the Directorate for Security of Classified Information, as the only body for implementation of the established national policy and international standards for protection of classified information and realization of the exchange of classified information according to established procedures, contribute to raising the degree of security and protection of classified information and to the promotion of a security culture among public administration employees handling such information. This confirms the fact that during the preparations of the Republic of North Macedonia for NATO membership, great importance was attached to the promotion of the exchange of classified information as one of the privileged types of cooperation with international organizations and foreign countries. The security of classified information is also one of the key issues in Chapter 31 - Foreign Security and Defense Policy under the National Program for Adoption of the Acquis Communautaire (NPAA).

The Law on Classified Information was first adopted in March 2004, and then in accordance with the needs seen through its direct application in the area it regulates or due to harmonization with other laws whose provisions need to be implemented in the legal text, amendments were made several times (Official Gazette of the Republic of Macedonia No. 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18). During the implementation of the Law, the need aroused for the introduction of legal solutions for harmonization with the existing regulations in other areas (eg. Inspection supervision), to regulate issues that have not been covered in the regulations previously (eg. the use of classified information in court or other procedure), as well as for introducing a legal basis for adoption of a bylaw that regulates crypto protection in the country. At the same time, in accordance with the country's integration processes in NATO and the EU, there was a need for more precise determination of the competencies of the Directorate for Security of Classified Information in the field of exchange and protection of classified information with international organizations.

In order to properly implement the accepted international standards for security of classified information, during 2018, the Directorate for Security of Classified Information conducted a comparative analysis of the legal solutions of 12 NATO and EU member states with which the Government of the Republic of Macedonia had signed bilateral agreements on the exchange and mutual protection of classified information. Based on the results of the analysis, from the exchanged experiences with related services of the countries in the region with which the Directorate has developed close cooperation, as well as based on the experiences gained from lessons learned from the application of the Law since its adoption in 2004, in 2018 an initiative was launched to draft a new text of the law on classified information.

The new Law on Classified Information(*) transposing the Council Decision of 23 September 2013 on the security rules for protecting EU classified information, CELEX 32013D0488, was adopted at the end of December 2019 (Official Gazette of Republic of North Macedonia No. 275/19), and it entered into force on January 3, 2020.

The Law regulates the system for protection of classified information in the Republic of North Macedonia, emphasizing the classification of information, determining the classification levels, criteria, measures and activities for protection of classified information, exchange of classified information with foreign countries and international organizations, procedures for issuance and duration of security clearances, bodies for protection of classified information, work plans and programs of the Directorate, supervision, misdemeanor and penal provisions for unauthorized disclosure of classified information, and other issues related to the protection system of classified information.

The intention to explain in more detail the novelties introduced by this Law, as well as the desire to interpret it correctly in terms of its basic ideas and value determinations emphasized the need to write the commentaries on the Law. In it, in addition to the interpretation of the provisions governing some of the more significant innovations in the Law, due attention will be paid to the issues that indicate the need for their additional regulation in order not to cause misinterpretations and dilemmas in the application of the Law. For that reason, although this Book of commentaries is made immediately after the adoption of the Law, the intention with this first version is to encourage further discussion which, supplemented by practical experiences from the application of the Law, will undoubtedly improve the quality of a future edition.The Book of commentaries is primarily intended for the users of classified information, but the text will undoubtedly be a useful read for all others who are yet to be trained in handling classified information, for the security staff, for the law and security students, as well as for the academics.

As authors, we would like to thank the Geneva Centre for Security Sector Governance (DCAF) for its support in assisting this project, as well as for all well-meaning readers and users of the Book of commentaries who will contribute to the constructive critique of the commentaries in the process of expert analysis of the provisions contained in the Law on Classified Information(*).

The Authors

Skopje, March 2021

LAW ON CLASSIFIED INFORMATION (1*)

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.

Within the first article, the issues subject to regulation by the Law (ratione materiae) are regulated in principle. Obviously, this Article explicitly defines the main purpose, content and issues according to which criteria, measures and activities undertaken for protection and security of information, rights, obligations and responsibility of originators and users of classified information, national and international exchange, inspection supervision of the implementation of this Law, as well as other issues related to the access and handling of classified information are regulated. However, the content of this Article largely depends on the law in a broader sense, i.e. on other laws that regulate numerous issues related to the status and legal standing of all natural persons and legal entities. Thus, the issues regulated by this Law determine the status and the legal position and causality of all relations that occur in the entire process of implementation of measures and activities to the final recipients of classified information that are explicitly listed in this Article. The clear need for exchange of information is emphasized explicitly from national to international level and vice versa where there is an obvious expression of clear dominance of such concepts in all modern national legislations, but also in international acts related to this matter.

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.

The Law determines the obligation or duty of all users of classified information who have had access and/or were acquainted with its content to protect the content of the information. The obligation to protect also entails the responsibility of a person in a situation when the prescribed rules are not complied with or if that person does not perform or recklessly protects the information and if it allows intentionally or unintentionally other entities to be acquainted with the content of the information that he or she has a general obligation to protect. Having a lapidary nature, the provision of Article 2 is essential because the weight and significance of the obligation is a necessary

precondition for the conscientious conduct of the said persons.

The obligation to protect classified information is particularly important within the classical approach in which elements of professional attitude and a high degree of security culture prevail, which means that protection should be viewed through the prism of cognitive processes which, in essence, imply knowledge, knowledge of security, protection, meaning of information, etc. These are value judgments about the sensitivity of work and handling of information that mainly involve combinations of values, standards and criteria.

In order to reduce the potential insufficiency of responsible behavior, while emphasizing the protection of information, the approach itself is important to this problem which implies a complex process within the very institution/institutions and the individuals, and what is the security orientation of the users which has numerous dimensions that affect the political and security processes. The only relevant interpretation implies an orderly democratic-security environment in which a hierarchical structure is built. Here the security culture implies respect for the order, the state, the institution, the values, the interests, etc. So, the ambivalences mentioned here inevitably reflect on the individuals themselves, the social groups and especially the social elites, which influences the formation of their approach and the implementation of that approach in the security practice. Hence, only a socially active attitude towards this issue will contribute to the affirmation and development of the basic postulates in which the security aspect will make the necessary step to lead to the accumulation of security and cultural capital from the individual to society itself.

The fact that the obligation to protect classified information as referred to in Article 2 is incumbent on all users of classified information who had access to and/or were familiar with its content entails liability and is relevant from a criminal law perspective, i.e. entails criminal liability for persons and legal entities that will commit an illegal act of abuse and unauthorized disclosure of information and consequently, they may be held responsible for the act committed, which will allow the content of the information to become known to the persons who should not normally come in contact with such information.

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 3 explicitly defines the purpose of the Law which is aimed at ensuring the lawful use of classified information and disabling, preventing any kind of illegal or unauthorized access, misuse and compromising of information. The purpose describes, inter alia, a kind of imperative in the work of all legal entities that have contact and powers in the field of classified information, and they are a challenge and obligation for all who work and are attached to the institution that is most called upon to lead the whole process of ensuring the overall protection of the information, because they can identify themselves with its purpose and reason for existence.

The goal set in this Law is defined as a specific condition, situation or result, but there are also mechanisms by which its achievement is measured. The goal set in this way provides the expediency that should prevent illegality, unauthorized access, abuse and compromise, which means that a single approach to security should be provided, and that requires organizational coexistence.

Achieving the goal means participatory approach and contribution, but also an idea

of how to encourage creativity, which will basically mean innovation, determination, as well as taking action to enable changes in the security sense of the word. Exceeding the strict legal framework and conditions for action will mean illegal, unauthorized use and misuse of information, and in some cases can lead to even the most serious consequences, public scandals, etc., which imposes the need for serious sanctioning of perpetrators of illegal actions. The responsibilities, powers and functions of the responsible bodies need to be clearly defined so that the work at different levels of the hierarchy can be successfully monitored and evaluated.

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).

The connotation of Article 4 is to determine the scope, i.e. the limit that the application of the provisions of this Law extends to, so, as stated in Article 4, the provisions are not limited only to the national classified information, but also to the wider, i.e. to the classified information received from foreign countries and international organizations, as well as classified information created in cooperation with each other unless otherwise regulated by international agreements ratified in accordance with the Constitution of the Republic of North Macedonia, given the fact that ratified international agreements become part of domestic positive law.

The basis laid in this way provides a broad framework for cooperation and exchange of classified information. This specification of the application of the provisions in terms of implicit prohibition in different situations provides the framework of application and the entities that directly cooperate and exchange classified information with the intention of ensuring the preventive function in order to prevent possible abuse.

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 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.

Article 5 establishes the basic competence of the Directorate for Security of Classified Information, i.e. the right and obligation (from which the competencies arise further) of the Directorate for Security of Classified Information to protect classified information is emphasized. Namely, due to the specificity of the matter and the great importance, primarily from a security aspect, the existence of a special institution is envisaged that will support and maintain a comprehensive system for protection of information (which means application of a dynamic and specific approach to work that should be in correlation with a well-thought-out policy and strategy that will enable the

overall action and work to be based on professional, ethical, legitimate and experiential knowledge and premises). This is followed by the need for clear synergy and dialectics for effective implementation of the principles of work necessary for the successful execution of specific tasks. In particular, the management structures in the Directorate for Security of Classified Information are required to carefully and unconditionally create a climate for acceptance and organization of work tasks in a timely manner and at all hierarchical levels.

In that sense, in order to ensure protection of classified information and application of international standards, as well as to realize the exchange of classified information in accordance with ratified international agreements, to inspect the implementation of the provisions of this Law and other regulations in the field of the classified information, as well as for performing other activities determined by this Law, the competence of the Directorate is established, as stated above. The readiness to operationalize the specific tasks in order to ensure the necessary protection of the information whose confidentiality should be ensured, in fact, largely depends on the work of the Directorate.

In terms of achieving the protection of classified information, the Directorate for Security of Classified Information must have sufficient power and authority to carry out its work, but not to the extent that it would impose itself on the system or would remain out of any control. Hence, the normal answer to this dilemma emphasizes three aspirations: legitimacy, professionalism and responsibility. Hence, the main goals are aimed at constant legitimacy, constant professionalism and constant responsibility. All three conditions must be cumulatively met in order to talk about the existence of democratic governance. The professional conduct and responsibility underpin legitimacy, while accountability enables professionalism, and legitimacy itself provides the required degree of professional independence to the Directorate.

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.*

Article 6 of the Law is a glossary, i.e. it contains definitions of terms that make up the categorical system established in the Law on Classified Information(*).

The existence of a glossary or special article for «meaning of expressions» used in the Law is a grounded practice of the legislator at the beginning of the legal text, in the part of the general provisions to define the basic terms, concepts and expressions that the proper application of the Law depends on. This will prevent different, too broad or completely incorrect interpretations from occurring in practice; in fact, in such cases the legislator himself, who is most called upon authority in that sence, gives the necessary interpretation, so in the legal literature this is one of the forms of legal, i.e. authentic interpretation or interpretation through the so-called legal definitions.[2] In this particular case, as it is emphasized, it is about the terminological divergences about the terms that are directly correlated with the legal matter and are obviously in function of clarifying the basic categories and terms, which will directly contribute to shaping the whole picture to avoid doubts in the implementation of the Law. This provision is, indeed, more than necessary, given that the law governs an extremely specific and sensitive area.

The glossary of the Law on Classified Information(*) defines terms related to information and classified information, security terminology, entities that create, use and handle information, security areas, terms related to the security of communication and information systems, etc. So, many terms and concepts have been defined that the Law further operates and which are extremely important for a conceptual understanding of the overall reality defined in the legal text.

The practical application has yet to show (given the fact that this Law was adopted at the very end of 2019) whether the legislator has failed to define another term that will appear in practice as necessary.

The central terms in this Law, such as: information, information of interest to the Republic of North Macedonia and classified information, are first on the list of 27 terms. The first definition gives an idea and a theoretical explanation of the term information as knowledge in any form.

Paragraph 4 and paragraph 5 of Article 6 define the document as a form of a written text, draft or sketch, reproduction, etc., which contains information; and the damage that is a violation of the interests of the state as a consequence of endangering the

[2] Камбовски Владо, Казнено право - општ дел, Скопје, 2011, 114.

security of the classified information of interest to the Republic of North Macedonia or the information that the Republic of North Macedonia is obliged to protect in accordance with the ratified international agreements.

In the following paragraphs, security is broken down through the prism of security risk and security of classified information. In general, the changing nature of security risks has conditioned the need to redefine security, but has also led to the adoption of new approaches to security. Accepting this reality, states must adapt to new circumstances in order to protect national interests and to guarantee the optimal level of security. The adaptation to the security risks also expresses the high level of security of classified information, which is a set of activities and measures that ensure the protection of classified information from unauthorized access and unauthorized handling. This requires general comprehensive inclusion of all entities involved and exercising the protective component.

Paragraphs 8 and 9, which refer to the security clearance as a document confirming that there is no risk for the natural person or the legal entity to access and handle classified information, specifies that the security clearance for individuals, in fact, in the sense of the Law, means issuing document that the natural person meets the conditions to access and handle classified information, while the security clearance for legal entities is very precise in the argumentation, i.e. it is a legal entity that has physical and organizational capacity to handle and/or store classified information. This means that there is no risk (threats to information) and there is no danger of destruction, illegal action, abuse and other forms of harmful actions.

In paragraph 10, the permit for access to classified information clearly confirms that the foreign natural person or legal entity has a security clearance issued in the home country and determines that they are eligible to access and use classified information in the Republic of North Macedonia. The permit has far-reaching implications for the performance of the activity, i.e. the lack of an appropriate permit will prevent the natural person and legal entity to use classified information in the country. If the foreign natural person or legal entity needs to use classified information of the Republic of North Macedonia, they must obtain the relevant permit.

Paragraph 11 sets out the "need to know" principle that determines the user who needs access to classified information in order to perform a function or execute an official duty and authority, to pursue activity or to implement classified agreements. The application of this principle ("need to know") is extremely important in providing access to classified information because having a security clearance or a high position, rank or function of a person does not imply direct access to certain classified information.[3]

Paragraph 12 defines the originator of classified information who is an authorized creator of classified information. Originators of classified information include state and local administration bodies established in accordance with the Constitution of the Republic of North Macedonia and 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 generate information of interest to the public security, defense, foreign affairs and security and intelligence activities of the state. Any other information that is not created by the originator of the information in the sense of the Law has no legal basis and credibility and in no case can obtain a classification level.

The following paragraphs define the dissemination, the user and the process of

3 Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, Enclosure "C", 20 November 2020, p. C-1, paragraph 4.

handling classified information, i.e. distribution of classified information to persons who possess an appropriate security clearance and handling classified information for the duration of its existence.

Paragraphs 16, 17 and 18 define the respective perimeter, areas and zones that prescribe the minimum distance defined as a safety belt, the space or room in the building designated as a security area where the classified information is handled and stored, and the protection space designated as an administrative zone to be established around and in front of the security areas.

Paragraph 19 specifies what is meant by "classified contract", which implies that for this legal relationship to be considered legally valid it must be created in writing and it must meet all other characteristics provided by other provisions of other relevant acts regarding how it is concluded between the contracting parties, if it contains or provides access to classified information, but it is especially emphasized that in addition to the contract, the negotiations leading to its concluding can be classified, because knowledge related to classified information can be obtained therefrom.

Paragraph 20 determines the significance of being a classified information security officer as a person who has the duty to take care of efficient and coordinated execution of the rights and obligations arising from the Law and is a person authorized by the responsible person in the state body, the legal entity or another entity from the relevant scope of entities determined by the Law. Paragraphs 21, 22, 23 and 24 define the terms "cryptographic security" which is a component of communication and information systems, meaning "cryptographic protection" as an operational-planning activity, then the "cryptographic product" and "cryptographic materials" which are cryptographic algorithms, cryptographic hardware and software modules, crypto keys, implementation guidelines and accompanying documentation.

Paragraph 25 explains the term "security accreditation of communication and information systems" and the legislator explains that it is a process of formal approval of communication and information systems to work to a certain classification level, in special security conditions in its operational environment and at an acceptable level of a security risk; and paragraph 26 explains the security risk management process with its determinant elements.

The last one, paragraph 27 explains the term "communication-information system" which is especially important in terms of enabling the creation, storage, processing or transmission of information in electronic form.

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 7 stipulates that the classification of information is done by determining a certain classification level and it is set down that it should be appropriate to the degree of damage that would occur to the Republic of North Macedonia in case a person would have an unauthorized access to that information or would use that information without been authorised accordingly. Thus, there is a correlation between the classification level and the potential damage that would result from its non-classification.

The second paragraph of the article stipulates that the classification level is determined for the information related to public security; the defence; foreign affairs; security, intelligence and counterintelligence activities of the state; systems, devices, inventions, projects and plans relevant to public security, defence, foreign affairs; scientific research and technological, economic and financial matters of importance for the Republic of North Macedonia.

In the context of the conditions associated with the global health pandemic with the COVID-19 virus, the question arises about the scope of the term security and what aspects it should cover, as well as the question about the need to protect information relating to or affecting public population health. In a broader discussion on whether such information should have a security classification level, i.e. whether it can be considered as information related to public security, one should take into account the broader context of the term security that includes the concept of human or individual security which, simply put, focuses on the safety and well-being of people. Human security recognizes a number of security threats, including threats to human health, together with various infectious and parasitic diseases, health and social problems caused by lack of clean water and air pollution, lack of adequate health care and the like. Consequently, the security nature of the information related to the health and health care of the population could be recognized and as such be subject to appropriate protection.

In the Law on Crisis Management,[4] the risks that endanger the health and life of the people are correlated with the term "endangerment of the security of the Republic".

At the same time, the National Security and Defense Concept from 2003,[5] which defines the interests of the state, in the vital interests that improve the security situation and create conditions for better life of citizens and functioning of the state and society, among others, also includes the interests for "protection and promotion of peace and security, life, health, property and personal security of the citizens of the Republic of Macedonia".

Consequently, in the context of a global health pandemic that could lead to disruption of the internal situation in the country and its relations at the international level, if we take into account that the degree of endangerment and damage to vital interests of the state affects the determination of the classification level of information, the legislator should recognize the security character of information related to human health care and regulate their protection.

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 8 stipulates that the classification of information is performed according to its content and that the originator determines the classification level, and with their written authorization, another person. It is a generally accepted rule in the security policies for handling classified information of NATO and the EU, as well as in the security policies of their member states, i.e. in the national security policies. This article also determines the classification levels: TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED.

With the adoption of the Law on Classified Information in 2004, a significant step forward was made in terms of harmonization of the classification levels with the internationally accepted classification levels and the revocation of the existing types of classification.

The new Law on Classified Information(*) follows that solution, but it remains for the criminal-legal protection and possibly some solutions in other laws to be harmonized for consistency. Namely, the disclosure of a Top Secret is criminalized in Article 317 of the Criminal Code, but other classification levels are not covered, while there are incriminations for protection of Military Secret, etc., which is a reflection of

4 Law on Crisis Management, Official Gazette of the Republic of Macedonia No. 29/05, Article 3, paragraph 1, point 1.

5 National Security and Defence Concept, Official Gazette of the Republic of Macedonia No. 5/03, Chapter I. Interests of the Republic of Macedonia, point 7 paragraph 2 line 1.

previous solutions currently unsupported by the positive legislation.[6]

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 9 regulates in more detail the classification levels according to the severity of the consequences of the unauthorized disclosure of the content of the information with each separate classification level. Thereby, the interests of the Republic of North Macedonia, which would be endangered by the unauthorized disclosure of classified information, are in line with the interests defined in the National Security and Defense Concept.[7]

By that, it is regulated that the TOP SECRET level is granted to information whose unauthorized disclosure would cause endangerment and irreparable damage to the permanent interests of the Republic of North Macedonia; the SECRET level is granted to information whose unauthorized disclosure would cause extremely serious damage to the vital interests of the Republic of North Macedonia, and the CONFIDENTIAL level is granted to information whose unauthorized disclosure would cause serious damage to important interests of the Republic of North Macedonia.

It is also regulated that the lowest classification level RESTRICTED is assigned to information whose unauthorized disclosure would cause damage to the operation of state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established by the Republic or municipalities, the City of Skopje and the municipalities in the City of Skopje, which are important for the public security, defence, foreign affairs and security and intelligence activities of the state.

6 See Criminal Code, Official Gazette of the Republic of Macedonia No. 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 41/14, 115/14, 132/14, 160/14, 199/14, 196/15, 226/15, 97/17 and 248/18, Articles 281, 349 and 360.

7 National Security and Defence Concept, Official Gazette of the Republic of Macedonia No. 5/03, Chapter I. Interests of the Republic of Macedonia, point 7.

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.

In Article 10, the legislator regulated the obligation of the originattor of the information, i.e. the person authorized by them, to mark the classified information with the most appropriate classification level which will provide the necessary protection of the state interests and security defined in Article 9. He pointed out that the determination the appropriate classification level of the information is made on the basis of an assessment of the possible damage and the consequences that would result from the unauthorized access to it.

The purpose of the provisions of this Article is to reduce the tendency of over-classification of information which then results in serious obligations for the users of classified information in terms of its handling and storage. At the same time, it means giving more weight to the process of accurate assessment of possible damages that will result in the most correct choice of the classification level.

This solution has been introduced by the new law as a result of the knowledge from the analyzes and the experiences gained from the applied practices for handling classified information in the Republic of North Macedonia, which indicated that the originators of classified information, for greater security or insufficient knowledge, often assign a higher classification level to the of information or, in rare cases, even unnecessarily classify information. In order to assist the users of classified information in determining the appropriate classification level to the information, the Directorate for Security of Classified Information has developed a Guide for determining the classification level of the information.[8]

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.

8 Guide for determining the classification level of the information (available at: https://www.dbki.gov.mk/files/pdf_files/Vodic_za_odreduvanje_stepen_na_KI.pdf).

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

Article 11 defines the entities that according to the Law are authorized to classify information with the highest level – TOP SECRET. Thereby, the holders of the highest public office in the country are listed, i.e. the President of the Republic of North Macedonia, the President of the Assembly of the Republic of North Macedonia, the Prime Minister 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 and the Chief of the General Staff of the Army of the Republic of North Macedonia, as well as the directors of state bodies with competencies in the field of security and state protection, i.e. the director of the Intelligence Agency, the director of the National Security Agency, the director of the Operational-Technical Agency, the director of the Crisis Management Center and the director of the Directorate for Security of Classified Information.

This provision stipulates that the TOP SECRET level can be determined by other persons authorized by the above-mentioned entities.

The second paragraph of this Article leaves the possibility for classified information with the TOP SECRET level to be determined by persons who are explicitly determined by law, ratified international agreement or other regulation.

The question is whether the possibility that the legislator has stipulated with another regulation to determine persons who will determine classified information with the level of TOP SECRET is a good solution, because it would actually mean by bylaws that are much easier to pass (do not pass through a law-making procedure) and are more often and potentially more easily changed, to expand the scope of persons who would classify information with the highest classification level.

The legislator has not specified the entities that are authorized to classify information with the levels of SECRET and CONFIDENTIAL, but in accordance with the positive regulations for organization and work of the state administration bodies it is understood that it is the responsible person in the entity or the person authorized by him for signing acts, resolving certain issues or performing other activities within the competence of the body.[9]

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

9 Law on for organization and work of the state administration bodies, Official Gazette of the Republic of Macedonia No. 58/00, 44/02, 82/08, 167/10, 51/11 and Official Gazette of the Republic of North Macedonia No. 96/19, 110/19, Article 47 and Article 52.

the manner of storing and handling information marked with UNCLASSIFIED.

Article 12 defines the awarding of the designation UNCLASSIFIED (***translator's note: in original ЗА ОГРАНИЧЕНА УПОТРЕБА***) to information the disclosure of which would reduce the efficiency of the work of state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the City of Skopje. As regulated by the second paragraph of this Article, the designation does not represent a classification level, but restricts public access to such information.

Namely, the designation UNCLASSIFIED is assigned to the information used for official purposes and although it does not impose the need for strict measures for handling and storage of such information, it still indicates the necessary protection from their publication in public. Namely, this clearly delimits such information from those to which free access may be allowed.[10]

In NATO security policy such information is marked UNCLASSIFIED, and in the EU such information is marked LIMITE. In addition, the security policies of both NATO and the EU emphasize that the marks are not a classification level but a mark for the distribution of the information which implies the handling of such information by persons within the organization for official purposes.

Due to the specific nature of the information marked UNCLASSIFIED, the third paragraph of this Article envisages the Government of the Republic of North Macedonia to regulate the manner of storage and handling of such information in more detail with a decree.

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 13 regulates the classification manner of an information which is composed of parts that are designated with different classification levels.

10 For more details on the information regarded as public information to which free access is allowed, see Law on Free Access to Public Information, Official Gazette of the Republic of North Macedonia No. 101/19.

The provisions of the article indicate the duty of the originator to determine the classification level of each part of the information separately, and to classify the whole information according to the highest classification level. In addition to the highest level with which he classifies the information, the originator is obliged to mark the other parts with classification levels that belong to the information on the front page of the document. This will make it clear to the future users of classified information, depending on the highest classification level, how the whole information is handled, and that its content is different in terms of classification.

The third paragraph of this Article determines the possibility that part of the document containing classified information with a higher classification level can be extracted as a separate document with an appropriate classification level. Namely, if it is necessary to apply strict protection measures for only one part of the classified information, its extraction in a separate document enables easier handling of the remaining parts of the classified information that do not have or have a lower classification level.

In practice, when working with national classified information, it is rare for parts of classified information to be set apart as a distinctive document, but this is a common practice when working with NATO classified information.[11]

This Article also regulates the use of footnotes, stating that as a rule they should not be classified unless they contain or reveal classified information, and in order to avoid a security risk, the provision of the fifth paragraph of this Article indicates that their use should be minimized.

The fact that the footnotes are references, i.e. they are always related to the basic text, it is practically difficult to perform all the protection in practice if the text is classified and the footnote itself is not, or if hypothetically there are different classification levels of the footnote text. Hence, the direction given in the last paragraph of this Article to avoid the use of footnotes in the classified information is pragmatic.

Article 14

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

In Article 14, the legislator envisagred the obligation of the originator of the classified information to obligatorily mark its classification level in a visible place. This is important in terms of faster and easier detection of the fact that this is classified information and its classification level, which would prevent cases of negligent access.

The marking of the classified information is regulated in more detail in a bylaw which prescribes the measures in the field of administrative security of the classified information.

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.

11 Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, Enclosure "E", 20 November 2020, p. E-2, paragraph 12.

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.

In case the information has not been marked with a classification level, and the originator could not be determined or has ceased to exist, the legislator in Article 15 provided that the classification of information is performed by the legal successor of the originator, and if the legal successor cannot be determined, the legislator established that the indication of the level of classified information is made by the Directorate for Security of Classified Information.

The basis for the justification of such a decision of the legislator lies in Article 5 of the General Provisions in which the Directorate is recognized as a competent body for implementing security policy regarding the protection of classified information and performing activities regulated by this law, and the goal is whenever necessary to classify certain information to have a ready-made solution on who will be the authorized entity in case of inability to determine or in case of actual absence of the originator of the information.

The legislator did not foresee here the role of the Directorate in case it is necessary to reclassify or declassify classified information whose originator cannot be identified or has ceased to exist.

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 16 actually defines the term reclassification and regulates the reclassification procedure, i.e. the change of the classification level of information, which is made by the originator of the information or a person authorized by him. Thereby, the legislator does not indicate precisely in which direction the change should take place, i.e. that the change in the classification level of information should go from a higher to a lower classification level, which is actually the intention of the reclassification procedure. It is not logical for information that is marked with a lower classification level, and as such has been available to a certain circle of users, to be additionally protected with a higher classification level, and thus with additional protection measures and access restrictions.

The third paragraph of the Article stipulates the obligation to inform all users of the classified information about the change. This obligation is given in order to ensure adequate protection of the classified information, especially if the level of protection has been raised, but also to avoid the use of larger resources than necessary for that

purpose or in general, if a lower classification level is given.

The provision from the fourth paragraph of this Article envisages the Government of the Republic of North Macedonia to regulate the manner of changing the information classification level with a decree, thus giving an opportunity for more detailed regulation of the procedure and operationalization of this provision and procedure in a bylaw. The manner of changing the classification level of information is subject to regulation in the bylaw which prescribes the measures in the field of administrative security of classified information.

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.

In Article 17, the legislator determines the ways in which the classification of an information can be terminated, i.e. when the classification of an information ends, and thus determines that the classification of the information terminates on the date indicated on the document, with the occurrence of the event that the document refers to, with the expiration of the time period indicated on the document and with declassification.

In fact, these are the few ways in which the classification ends, and not the cumulatively set conditions that need to be met for a classification to end. Namely, for some information it is possible to indicate the exact date when the classification will stop, but for others that is not possible because they are related to an event that can not be known in advance when it will happen, for some other information a time period will be determined, and some information will be declassified.

By regulating the termination of the classification of information, an opportunity is given to make it available to the public because there is no longer a danger that a certain interest of the state will be endangered or violated, and additionally by that to save resources that would have been allocated to its further protection. Accessibility to the public means, in particular, availability of information for scientific purposes, research and analysis.

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 18 regulates the procedure for declassification of classified information, which makes it non-classified. This is actually one of the many ways in which the classification of information ceases.

As a rule, a change in the level of classified information can be made by the originator or a person authorized by him, so consequently the legislator stipulates that the declassification itself is made by the originator of the information or a person authorized by him. As in the case of the procedure for reclassification of classified information, the provision of the second paragraph of this Article stipulates that users must be notified of the declassified information. In order to regulate the declassification procedure in more detail, the third paragraph of this Article stipulates that the Government of the Republic of North Macedonia will regulate the manner of declassification of information with a bylaw. This is subject to regulation in the bylaw which prescribes the measures in the field of administrative security of classified information.

Practice shows that the declassification procedure is not carried out often, but experiences from working with classified information in NATO are known, where there is a special Committee through which the declassification of NATO classified information is carried out. [12]

For the needs of court proceedings (more precisely - criminal proceedings), in our country we often declassify the evidence provided by the use of special investigative measures (PIM) and which are previously, as a rule, classified. With this de facto they become non-classified information, so in order to prevent free access, i.e. to restrict the access to them, it happens that they are mark as UNCLASSIFIED. However, this designation is not a classification level. We believe that additional discussions and trainings are needed in this domain of all relevant entities, because here several questions are legitimately asked: first, whether this mark, for example, is in itself a sufficient basis for exclusion of the public from proceedings and, secondly, whether there is the need to declassify all previously classified information in these cases (criminal proceedings), when the law provides that they can be used as classified with the exclusion of the public from proceedings?

For this, the judicial authorities, as well as the originators of classified information for the needs of criminal justice, should particularly take into account the provisions of Articles 63 and 104 of the Law on Classified Information(*) and Article 354 of the Law on Criminal Procedure.

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 19 emphasizes the obligation of the originator of the classified information to indicate the time period or event after which the information may be reclassified or declassified, stating that it may not exceed a period of ten years, unless the classified information needs longer-term protection provided by law.

12 ARCHIVES COMMITTEE, Directive on the Public Disclosure of NATO Information, AC/324-D(2014)0010-REV2, 16 January 2018

The purpose of this provision is in fact to direct the originators of classified information to the need to reconsider their decision and set a time limit for the above.

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 20 clarifies the provision of the previous article and determines the time period according to the classification level for which the originator reviews and evaluates certain classified information in order to determine the need to further retention of the existing classification level.

Thus, the legislator regulates that for the information classified TOP SECRET that period is not longer than ten years, for the information classified SECRET it is not longer than five years, for the information classified CONFIDENTIAL that period is not longer than three years, and for the information classified RESTRICTED that period is not longer than two years. However, further in the misdemeanor provisions, the legislator does not provide for liability for the originator if he does not consider and assess the need to further maintain the classification of information within the specified period.

The assessment of the need to maintain the classification level is provided in order to reduce protection measures or to provide access to information that no longer needs to be protected. This will enable greater economy in the use of resources and greater transparency in the work of the state bodies and institutions.

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.

In order to prevent concealing an oversight, abuse of office or any other illegal act, i.e. a criminal offense behind classified information, Article 21 stipulates that such information shall not be considered classified.

Namely, it is hypothetically possible for a person authorized to grant a classification

level to information, to abuse such authority in order to conceal certain illegal actions, and therefore, this Article prevents such protection of information through classification to be used for illegal and illegitimate purposes.

Compared to the Law on Classified Information from 2004, this Law also introduces a provision for protection of persons who will report classified information that conceals illegal action, i.e. their protection is guaranteed by the Law on Whistleblower Protection[13] as a new mechanism for combating against corruption and crime.

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 22 defines that the foreign information released to the Republic of North Macedonia, which belongs to foreign countries or international organizations with which it has concluded international agreements or to which it has acceded, retains the original classification level, i.e. the level used in that country or international organization.

This provision emphasizes the compliance of the national standards for ensuring the protection of classified information with the internationally accepted standards and also confirms the determination of the state to ensure equal protection of foreign classified information as well as of the national classified information that has the same classification level. In case of change in the classification system of information in a foreign country with which the Republic of North Macedonia has concluded an international agreement, this provision of the Law provides continuity in the protection of the exchanged information.[14]

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.

Article 23 regulates the dissemination, i.e. the distribution of foreign classified information to persons who have an appropriate security clearance and in accordance

13 Law on Whistleblower Protection, Official Gazette of the Republic of Macedonia No.196/15 and 35/18.

14 Some time ago France has changed the legal framework for protection of national secret information which envisages narrowing down the number of its classification levels, so instead of three levels, as of July 1, 2021 it will use a system based on two classification levels. As a result, the Agreement between the Government of the Republic of Macedonia and the Government of the French Republic on Exchange and Mutual Protection of Classified Information, signed in Skopje on July 5, 2010 will be subject to relevant amendment in line with the procedure envisaged to that purpose.

with the principle "need to know". This means that it is not enough for a certain person to just have an appropriate security clearance, because in that case the foreign classified information would be distributed to all persons holding a security clearance with the appropriate classification level. On the contrary, by acting on the principle of "need to know", such (foreign) classified information will be distributed only to those persons who really need to know the content of the relevant information.

Dissemination of classified information as a term is introduced for the first time in this Law due to its generally accepted application among the users of classified information.

The second paragraph of this Article envisages the Government of the Republic of North Macedonia to further regulate the manner of determining the users and the dissemination of the received foreign classified information with a decree. This matter, more specifically, is subject to regulation in the bylaw which prescribes the measures in the field of administrative security of 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.

Chapter Three of the Law focuses on the criteria, measures and activities for protection of classified information. As a result, Article 24 defines the domains in which the measures and activities are applied, i.e. the domain of administrative security, physical security, industrial security, security of communication-information systems, as well as the domain of personnel security.

This definition of measures and activities is in line with internationally accepted standards for protection of classified information.

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.

Article 25 defines the minimum criteria to be taken into account when determining the measures for protection of classified information. The very expression "shall particularly be taken into account" means that when determining protection measures, as many as possible criteria relevant to the specific information should be taken into account, but the above are mandatory for consideration.

The first criterion is the classification level on which further depends the scope and seriousness of the measures and activities that will be taken to protect the classified information. As a rule, a higher classification level implies stricter protection measures, and consequently, engagement of greater resources.

The scope and shape of the classified information is the next criterion that is taken into account when determining the measures for protection of the classified information. If the classified information has a large "size", is in the form of a machine or an other device, etc., the user of such classified information should provide an appropriate storage space, as well as protection measures. In case it is classified information in electronic

form, the user of the information will have to take appropriate measures to protect the communication and information systems in which such information is processed and stored.

The risk assessment for the security of classified information is the third and no less important criterion in determining the measures for protection of classified information. It is a comprehensive analysis of all the factors that could impair the security of classified information, the results of which further indicate the extent and level of protection that should be provided for that 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.

Article 26 sets out the measures and activities for administrative security, i.e. information security as referred to in NATO and EU directives and acts.[15]

The first line of paragraph 1 of this Article refers to the determination of the classification level and its appropriate marking. When determining the classification level, indicators are taken into account that more closely indicate the degree of possible damage that would occur to the Republic of North Macedonia or to a foreign country or an international organization with unauthorized access to classified information or its unauthorized use. After determining the classification level, the originator of the classified information should mark it properly in order for the information to receive the appropriate protection.

15 For more details on the determining of the classification level and marking of the classificed information, receipt and recording of the classified information, reclassification and declassification of classified information, transmission and storage of classified infomation, translaions, reproductions, etc. see Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, Enclosure "E", 20 November 2020; Council Decision of 23 September 2013 on the security rules for protecting EU classified information 32013D0488 (Official Jornal of the European Union L274/1), Annex III).

The second line refers to the receipt and recording of classified information which are performed in accordance with the existing rules of office and archival work and represent an important step in protecting the information because the proper recording of information and "monitoring" of its movement are some of the prerequisites for providing adequate protection.

The third line of paragraph 1 of this Article refers to the determination of the manner of storing, handling and control of the classified information. The way in which classified information will be stored, handled and controlled depends on the classification level of that information and its scope and shape.

Reproduction of classified information and making translations and excerpts therefrom, as well as determining the number of the copies and the users are the following administrative security measures and activities listed in this Article. The internationally accepted standard in this case is that all reproductions, translations and copies bear the same markings and have the same protection as the original classified information, and in order to enable their proper protection and control, their number should be limited to the number required to perform official duties, and their users should to be properly registered.

The fifth line refers to the dissemination of classified information, i.e. its distribution to the end users, which means delivering the classified information to persons who have an appropriate security clearance according to the "need to know" principle. Consequently, the transfer of the classified information is regulated, while taking into account the manner of its packaging, according to its classification level.

The disposal and destruction of classified information is the last step in its "life cycle" and is carried out in accordance with the existing national office and archival rules and NATO and EU regulations on the handling of their classified information.

The second paragraph of this Article envisages the Government of the Republic of North Macedonia to further regulate the measures and activities for administrative security of classified information with a decree.

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.

The first paragraph of Article 27 stipulates that physical security is achieved by applying physical and technical protection measures in order to prevent unauthorized access to classified information.

Furthermore, the provisions of the article point to the results that should be achieved by applying the measures for physical security, which are prevention of covert or violent intrusion by an unauthorized person, deterrence, prevention and detection of unauthorized activities, as well as enabling staff segregation in their approach to classified information according to the "need to know" principle.

The third paragraph of the article indicates the comprehensiveness of the application of the measures for physical security, i.e. their application in all locations, facilities, buildings, offices and premises, where classified information is handled, stored or processed electronically.

The last two paragraphs of the article emphasize the establishment of security areas in the premises where information classified CONFIDENTIAL and higher is stored, as well as the use of equipment, systems or other technical means for protection of such information. The legislator, therefore, considers that the premises for the information classified CONFIDENTIAL, SECRET and TOP SECRET should be established as security areas, i.e. the premises for those levels for which the person is required to hold an appropriate security clearance in order to handle such information. Hence, this provision is exclusive in the opposite direction, i.e. ***argumentum a contrario*** the premises where the information classified RESTRICTED is stored are not established as security zones.

Thereby it is stipulated that the aforementioned equipment, systems and assets should meet the minimum standards prescribed by the Director of the Directorate. Basically, the prescribing of those standards is based on the internationally accepted standards of NATO and the EU, i.e. the lists of recommended products that meet the prescribed standards of those international organizations for the protection of classified information.

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.

Article 28 emphasizes the measures and activities for physical security, and it is no coincidence that the assessment of possible breaches of the security of classified information is placed in the first place. The results of the assessment of the possibility of endangering the security of the classified information and the sources from which it may originate, provide a solid basis for determining the measures and activities for physical security for the protection of the classified information. This primarily refers to the determination of a security perimeter around a given object, the determination of security areas and administrative zones in a given object, as well as the organization of physical protection and the application of technical means for securing objects and premises in which classified information is held.

Physical security measures and activities include, in addition to the above, the provision of control of entry, movement and exit of persons and vehicles for the transportation of classified information, as well as physical safeguarding during transportation of classified information outside the security areas. Given that the security environment and the sources of threats are constantly changing, and the technology is advancing rapidly, opportunity should be given to upgrade and supplement the envisaged measures and activities for physical security of classified information.

The second paragraph of this Article provides a basis for further more detailed determination of the identified measures and activities for physical security of classified information in a decree to be adopted by the Government of the Republic of North Macedonia.

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.

The measures and activities for personnel security are listed in detail in Article 29 and are regulated in more detail below in the Law.

The appointment of a classified information security officer and his/her responsibilities are elaborated in detail in Chapter Four of this Law. Classified information security officers are key personnel for the sustainability, enforcement and oversight of

security policies for working with classified information in each of the relevant state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established. from the Republic or from the municipalities, the City of Skopje and the municipalities in the City of Skopje and other legal entities, where classified information is handled and stored.

Together with the vetting of persons in order to issue a security clearance for access to classified information, the issuance of security clearances, the issuance of access permits to foreign individuals and legal entities for access to classified information of the Republic of North Macedonia, as well as the verification and evaluation of the ability to handle classified information as measures and activities for personnel security, the legislator envisaged the Government of the Republic of North Macedonia to regulate them in more detail by a decree.

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.

In Article 30, the legislator defines the security of communication-information systems (CIS) and determines that it is the application of security measures for protection of communication, information and other electronic systems and of the classified information that is created, stored, processed or transmitted in these systems, in order to ensure their confidentiality, integrity, availability, authenticity and irrevocability.

The second paragraph of this Article emphasizes the need to implement a comprehensive system of security measures for administrative and physical security, CIS security, and for personnel security, in order to create a security environment in which the communication, information or other electronic systems operate. The legislator thus points out the complexity of the measures and activities needed to achieve CIS security and leads to raising security awareness among the users of classified information when handling and storing such information in electronic form.

Therefore, in the third paragraph of this Article, the legislator indicates that the system of CIS security measures must be based on a process of security risk

management. Given that security risk management is already defined as the process of identifying, controlling, minimizing, or eliminating events that may affect the security of an organization or the system it uses, it can be concluded that the legislator once again emphasizes the complexity of this matter and the need to maintain a high level of security awareness of the changing security environment and the rapid development of technology, especially of the information technology and the expansion of cybercrime.

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.

The measures and activities for security of the communication-information systems (CIS) are listed in detail in Article 31, whereby the legislator envisaged their closer regulation by a decree to be passed by the Government of the Republic of North Macedonia. When enumerating the measures and activities for CIS security, the legislator denotes the accreditation of CIS and their operting processes and thus points towards the requirement a for formal approval of CIS for operating up to a certain level of classification. The formal approval of the CIS as a competence of the Directorate for Security of Classified Information is regulated below in this Law, in Article 69 paragraph 2 line 9.

The next measure of CIS security is the assessment of the possible breach of the security of the classified information by unauthorized entry into the CIS in which the classified information is stored, processed and transmitted. The purpose of such an assessment is to determine the risk, to assess the risk that cannot be avoided, to assess the vulnerability and threats, as well as to determine the consequences of the realization of certain threats.

The third line refers to the establishment of methods and security procedures for receiving, processing, transmitting, storing and archiving classified information in electronic form. It is a comprehensive procedure in which care should be taken to apply the appropriate measures and activities in the field of administrative security when receiving, processing and transmitting classified information, then in the field of physical security in terms of determining the security areas in which the CIS are located depending on the level of classified information processed in them, as well as measures and activities in the field of personnel security according to which access to CIS in which classified information is processed can only have a user who has an appropriate security clearance of the classification level commensurate to the CIS classification level and who is properly acquainted with the obligations arising from the CIS security and operational procedures.

Furthermore, the legislator points out the measures for protection during the creation, storage, processing and transmission of classified information in CIS, the cryptographic security of communication, information and other electronic systems through which classified information is created, stored, processed with cryptography and transmitted, as well as the protection from compromising electromagnetic emission and determination of zones and rooms protected from compromising electromagnetic emission. Measures for protection against compromising electromagnetic emission imply technical measurements that determine zones in the facilities where CIS are located and consequently to the obtained results, appropriate protection measures are determined from the aspect of the physical security.

As a last measure of CIS security, the legislator denotes the installation of storage devices for classified information, which means that they should be installed by experts and authorized persons.

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.

Cryptographic security is one of the measures and activities for security of communication and information systems. Article 32 exhaustively lists the measures and activities for cryptographic security, whereby the legislator provided for their closer

regulation in a decree by the Government of the Republic of North Macedonia. This does not presuppose that this matter has not been regulated at all so far, but that the existing Decree, adopted in 1995 and classified as TOP SECRET, should be replaced by a new decree which will reflect current trends in the field of cryptographic protection and that will clearly regulate the relations between all stakeholders of cryptographic protection in the country.

Considering that the legislator defines cryptographic security as an operational-planning activity in the system of cryptographic materials and products used for protection of classified information from unauthorized access during the creation, handling and storage of classified information, all listed measures and activities point to a complex matter for the implementation of which technically educated and properly trained staff is required. The legislator has recognized several measures and activities for cryptographic security which in themselves are separate processes that involve multiple activities. Such processes are the planning, organization, and implementation of cryptographic security; evaluation and approval of cryptocurrencies and crypto products used to ensure cryptographic protection; the production and development of cryptographic algorithms and products; planning, organization and management of crypto products; the application of measures and procedures for recording, safe handling, storage and distribution of cryptographic materials and crypto products; training of persons to work with cryptographic materials and cryptocurrencies, as well as exercising control over the implementation of cryptographic security measures and activities and the manner of use of cryptographic materials and products.

Due to the specific nature of the matter, the adoption of a special bylaw that will regulate the relations between the state administration bodies that have competencies in the field of cryptographic protection is of exceptional importance for the Republic of North Macedonia.

Article 33

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

In this Article, the legislator prescribes that the transmission of classified information through communication systems outside the security areas is done exclusively with the application of cryptographic protection, but has not envisaged a limit to the classification level of information to be transmitted electronically. This means that classified information of all classification levels can be transmitted electronically with the mandatory application of 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.

In Article 34, the legislator stipulates that the measures and activities for industrial security are applied in order to ensure protection of the classified information by the contractors and the entities involved in the negotiations before concluding the contract and during the realization of the classified contract. This means protection that covers all stages, even those that precede the conclusion of the contract. This is justified because even in those stages information that is and/or should be protected can be used and exchanged.

In addition, it is stipulated that industrial security measures ensure the protection of classified information during transportation and while establishing procedures for the visit of natural and legal persons to facilities where classified information is handled. Here, the legislator points out the connection of industrial security with the measures and activities for personnel security by stipulating that for access to and handling of classified information in the implementation of classified contracts, during transportation of classified information and in visits to facilities where classified information is handled, the individuals and legal entities need to have an appropriate security clearance or access permit to classified information.

The fourth paragraph of this Article stipulates that when classifying a contract and the stages preceding the conclusion of the contract, including the public call for

participation in public procurement, the legal entity should provide an opinion from the classified information security officer affiliated to the entity that announced the public call.

In this Article, the legislator does not explicitly list the measures and activities for industrial security as it does before with the other measures and activities because industrial security covers all prescribed measures and activities in the field of administrative security, personnel security, physical security and CIS security.

Such comprehensiveness of the measures and activities for industrial security, the legislator envisaged to be more closely regulated in a decree by the Government of the Republic of North Macedonia.

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.

In the first paragraph of Article 35, the legislator defines the classified information of a foreign state or international organization as information that the competent body of the foreign state or international organization has released to the Republic of North Macedonia with an obligation to ensure its protection.

Consequently, the second paragraph recognizes the obligation of the users of classified information in the country to handle such information in a manner provided by a ratified international agreement. And if the agreement does not contain provisions on the manner of handling the classified information, the legislator provided that the provisions of this Law shall be applied. This, above all, excludes the application of the relevant provisions of this Law in a case when the ratified international agreement determines the manner of handling such information. The application of our domestic legislation comes into play when the international agreement has not provided provisions for the manner of action.

By accepting such a solution, the serious attitude towards the protection of classified information and the compliance of the national legislation with the prescribed international standards and measures for protection of classified information are demonstrated.

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 36 contains provisions which for the first time regulate the actions of the Directorate for Security of Classified Information regarding the exchange of classified information in case of emergency, military or crisis situation in Republic of North Macedonia with foreign countries and international organizations with which no international agreements have been concluded.

So, this is an exceptional case (exchange of classified information with foreign countries and international organizations in the absence of an appropriate international agreement) in exceptional circumstances (state of emergency, military or crisis situation).

Namely, the first paragraph of the article stipulates that the Directorate may exchange classified information in such a case, if it is in the interest of the Republic of North Macedonia, at the request of the competent authorities in accordance with the Constitution of the Republic of North Macedonia and by law, and with prior consent of by the Government of the Republic of North Macedonia. In the second paragraph of this Article, the legislator undelines the obligation of the Directorate upon termination of the state of emergency, military or crisis situation in the country to submit a report to the Government on the exchanged classified information with foreign states and international organizations with which no international agreements have been concluded.

With this solution, the legislator regulates the relations and obligations of the Directorate in the context of the above and in case of emergency, military or crisis situation in the Republic of North Macedonia with emphasis that they put into effect if it is in the interest of the state.

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.

The provision of this Article is a kind of continuum of the provision of Article 35 and in it the legislator recognizes the undertaken obligations from the ratified international agreements as a basis for regulating the control over the use and protection of the exchanged classified information between the Republic of North Macedonia and other foreign countries and international organizations. In doing so, the principle of reciprocity is expressed.

Consequently, the legislator provided that authorized representatives of foreign countries and international organizations can control the manner of use and protection of classified information released by them to the Republic of North Macedonia, while in relation to the national classified information released by the Republic of North Macedonia to them, the legislator envisaged the control over the way that information is used and protected to be performed by the Directorate for Security of Classified Information.

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.

In Article 38, the legislator prescribes who can be a user of classified information, emphasizing the need to comply with the "need to know" principle. Thereby, it is provided that a state and local government body established in accordance with the Constitution of the Republic of North Macedonia and by law, a legal entity established by the Republic or the municipalities, the City of Skopje and the municipalities in the City of Skopje or a natural or legal person in the Republic of North Macedonia should have a security clearance, while a foreign state body, institution or a foreign natural or legal person should have a security clearance of the home country and an access permit to classified information issued by the Directorate. In other words, the legislator stipulates two cumulative conditions that a person (natural or legal) must meet in order to be a user of classified information, namely: 1. possession of an appropriate security clearance / security clearance and an access permit (for foreign natural or legal person) and 2. to be able to apply the "need to know" principle in the specific case.

This solution once again affirms the above-mentioned principle which has long been known and applied in the security theory and practice, and has been apostrophized in many NATO documents, but also theoretically prevents any person with an appropriate security clearance from accessing all classified information to the appropriate classification level. In this way, the confidentiality of the information is additionally ensured, and access to it is limited only to persons who really need to know the content of the specific information in order to exercise their functions, tasks and powers.

The legislator did not provide here (nor anywhere else in the Law) the conditions that need to be met for the access permit to classified information to be issued by the Directorate.

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 39 focuses on a range of issues related to the security clearance as a necessary precondition for access to classified information to the users of classified information.

In the first paragraph, the legislator prescribes that the security clearance is issued to persons who handle classified information to execute their duties in accordance with the "need to know" principle, and in the second paragraph, stipulates that the security clearance is issued to access an appropriate level of classified information. This means that the classification level of the security clearance should correspond, i.e. be at least equal to the classification level of the information to which the user needs access to. It does not restrict the user from accessing information with a lower classification level than the classification level of the security clearance that they possess, but does not allow access to information with a higher classification level than the one of the security clearane. In other words, a security clearance for a higher classification level covers the lower levels, but not the higher ones.

Furthermore, the legislator stipulates that the interested natural person or legal entity should submit a written request to the Directorate in order to start the procedure for issuing a security clearance and prescribes that the request is submitted through a

classified information security officer in the legal entity. The designation of a classified information security officer as one of the key elements of the classified information protection system, which has been introduced in order to enable efficient and coordinated execution of the rights and obligations related to classified information, has been regulated in more detail by the legislator from Article 65 to Article 68 of this Law.

For the employees of the Directorate for Security of Classified Information in the fifth paragraph of this Article it is prescribed that the procedure for issuing a security clearance is conducted through the classified information security officer in the Directorate.

This means that the "communication" regarding the request for issuance of a security clearance to a certain person carried out through the security officers, i.e. the security officer of the legal entity where the interested person works forwards the request to the Directorate for further action.

The provision from the last paragraph of this Article regulates that the security clearance is issued by the director of the Directorate on the basis of a previously conducted vetting procedure and assessment of the existence or non-existence of a security risk for handling classified information.

The issuance of a security clearance to the users of classified information is regulated in more detail in a bylaw.[16]

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 40 prescribes an exception to the provision of the previous article, i.e. provides a list of the persons who due to smooth execution of their function from the day of election to the end of their mandate receive a security clearance for access and use of classified information of all levels without prior security vetting. The legislator, as we have said, lists the holders of the highest public functions in the country, namely: the President of the Republic of North Macedonia, the President of the Assembly of the Republic of North Macedonia, the Prime Minister of the Republic of North Macedonia, the Deputy Prime Ministers 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.

This list of exceptions has been prepared in accordance with the existing prescribed international standards that refer to the procedure for issuing security clearances for access to classified information of holders of high state positions. The law on this issue is quite restrictive compared to the legislation of other foreign countries, but experience

16 Decree on Personnel Security (Official Gazette of the Republic of Macedonia No. 82/04). The procedure for passing a new Decree on Personnel Security is currently underway.

shows that international factors view the short list of exceptions positively, because the large number of exceptions can pose a greater security risk to classified information.

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.

In Article 41, the legislator defines the conditions for issuing a security clearance to a natural person.

In the first line, the legislator determines that the natural person should be a citizen of the Republic of North Macedonia, but further in the second line it stipulates that for a security clearance with the level of TOP SECRET the person should not have dual citizenship, i.e. not be a citizen of another state, while in the third line specifies that for a security clearance with the level of SECRET the natural person should not be a citizen of a non NATO member country. In these two lines, the legislator defines the position regarding the possession of dual citizenship when handling information with a higher classification level. Namely, persons with dual citizenship will not be issued a security clearance for the highest level of classification by any exception, while for the lower level - SECRET as an exception, a security clearance for this level can be issued to persons with dual citizenship, but only to those persons whose other citizenship is that of a NATO member state.

Then, other conditions that a natural person must meet in order to obtain a security clearance are listed, i.e. to have a justified need to use classified information in accordance with the "need to know" principle, to have no security obstacles for having access to and handling of classified information which is determined by an operational vetting, the natural person to have a legal capacity, to have reached 18 years of age, and for using information classified TOP SECRET to have reached 21 years of age, not to have sanctions imposing a ban on a profession, activity or duty, to have a non-conviction certificate with validity not exceeding six months, and the results of the operational vetting for the persons listed in the security questionnaire (family members, etc.) not

to imply existence of any security obstacles for access to and handling of classified information.

In the second paragraph of this Article, the legislator stipulated that before issuing the clearance, the person must be trained in handling classified information, but did not regulate the conditions, i.e. did not envisaged what kind of training it is and who conducts it. For that reason, the article should be supplemented with provisions that will additionally regulate the issuance of a certificate or another type of document as a confirmation of the completed training, as well as to regulate the duration, i.e. the time of validity of such a document.

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.

In Article 42, the legislator regulates the conditions for issuing a security clearance to a legal entity. He states enumeratively that: the legal entity should be registered in the Republic of North Macedonia, there should be a justified need for access and handling of classified information in accordance with the principle "need to know", not to have sanctions imposing a ban on the activity, to have provided conditions for physical security, administrative security and / or security of communication-information systems if required by the conditions of the classified agreement, to have provided a security clearance for the security officer of classified information in the legal entity,

to be financially and economically stable and that there are no security obstacles for handling classified information which is being determined by an operational vetting. Here it is necessary to emphasize that the fulfillment of the prescribed conditions by the legal entity is checked by the Directorate with its expert teams, while the operational vetting is carried out by a competent body, i.e. the National Security Agency.

Furthermore, the legislator regulates in more detail the evidence that determines the financial and economic stability of the legal entity, i.e. the documents that should be attached to the application for a security clearance as evidence of the financial and economic stability of the legal entity and the validity of which should not exceed six months. Thus, the legislator stipulated that the legal entity should submit an excerpt from the professional activity register, a document for solvency from a competent authority, proof from a competent authority that no bankruptcy or liquidation proceedings have been opened – activity ban, as well as a certificate from a competent body 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.

With the provision from Article 43, which is general and indicative in its nature, the legislator regulates that the legal entity is considered eligible of providing protection of classified information if it provides the conditions for implementation of measures and activities for protection of classified information determined by this Law. This means fulfilling the measures and activities in the field of administrative security, personnel security, physical security, industrial security and security of communication-information systems, depending on the scope of work and the need and scope of access to classified information. The mentioned security domains are regulated in other provisions of 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 44 stipulates that the fulfillment of the conditions for issuing a security clearance is determined by a security vetting for which the natural person or the legal entity that has submitted a request for issuance of a security clearance has previously given a written consent to be conducted. Such consent is a logical condition because the security vetting involves actions that penetrate deep into the realm of privacy and include sensitive personal data. Hence, the person has the right to withdraw the consent during the procedure. However, it also causes a certain consequence, namely, in case the natural person or the legal entity withdraws its consent for verification in writing during the procedure, the legislator provided that the re-examination procedure cannot be conducted before the expiration of one year from the day of 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.

The legislator regulates in detail the security vetting procedure in Article 45 and stipulates that it is carried out before issuing a security clearance to legal entities and individuals for access to and handling of classified information, in order to determine the existence or non-existence of security risk, and that it begins with the very submission of a request to the Directorate. Furthermore, the legislator regulates that the completed data from the security questionnaire, the form and content of which are prescribed by the director of the Directorate, is a part of the procedure for issuing a security clearance. Here, he envisaged to prescribe the content and form of the security questionnaire forms, but did not specify how many and what patterns were in question. Based on the other provisions of the law and the current practice, it can be concluded that separate forms are prescribed for different classification levels (depending on the request) and depending on whether it is a natural person or a legal entity.

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.

In Article 46, the legislator provided that the completed security vetting questionnaire is marked UNCLASSIFIED which means that the questionnaire cannot be

made available to the public and is used only for official purposes, in compliance with the provisions of the Law on Personal Data Protection.[17] The mark UNCLASSIEID limits the distribution of the security questionnaire and indicates that it will be used only for the purposes for which it is intended, i.e. for the needs of the security vetting. In that direction is the provision from the second paragraph of this Article which regulates that the data from the completed security questionnaire is used for the vetting purposes and it is treated in accordance with the law. This means that, for example, personal data is protected in accordance with personal data protection regulations, etc.

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.

In Article 47, the legislator provided that for the use of information classified RESTRICTED no security vetting is carried out and no security clearance is issued, but the natural person or the responsible person in the legal entity is informed about the obligation to protect the classified information made known to them, i.e. released to them for handling. That means the so-called security briefing conducted by an authorized person in the body, i.e. the security officer of classified information, by which the person is informed about the security measures and procedures and his obligations in handling and storing the classified information. At least once a year, and as needed and more often, the classified information security officer re-briefs the users of classified information on their obligations under the Law on Classified Information(*). After the initial and the re-acquaintance with their obligations, the users of the classified information sign a statement confirming that they have fully understood the provisions of the Law.

If the rules for handling and protection of this information are violated, the person should be subject to appropriate liability and sanction, depending on whether it is a minor violation, misdemeanor or other illegal act or abuse committed with intent that would be treated as crime. Although this is the lowest level of classification, it should be noted that such classified information should also be protected and handled with seriousness and responsibility.

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.

In Article 48, the legislator determines three levels of security vetting for a natural person that correspond to the level of the classified information that the request for

[17] Personal Data Protection Law, Official Gazette of the Republic of North Macedonia No. 42/20.

issuance of a security clearance has been submitted for. As a result, the legislator envisages: first level vetting for information classified CONFIDENTIAL, second level vetting for information classified SECRET and third level vetting for information classified TOP SECRET.

The various levels of security vetting are further regulated in the following articles of the Law.

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).

With regard to the first vele of vetting, in Article 49 the legislator provided that the following elements are checked: identity of the person (based on the attached written documentation) and operational verification of the data on the person by a competent authority, age of at least 18 years, citizenship of the Republic of North Macedonia, the legal capacity of the person (based on a certificate from a competent authority) and the existence of security obstacles for the individual to have access to and handle classified information (determined by an operational vetting conducted by a competent authority).

Analogous to the verification of the legal capacity of the person on the basis of a certificate issued by a competent authority, the legislator did not envisage here a verification of the conviction of the person on the basis of a non-conviction certificate, with validity not exceeding six months, whose possession as a condition for obtaining a security clearance has been prescribed in 41 paragraph 1 line 9. But, of course, it should be borne in mind that the non-conviction of the person is also checked during the operational vetting.

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).

In Article 50, the legislator, having in mind the Decision of the Constitutional Court of the Republic of Macedonia of 20 April 2011, provided for a wider range of second level vetting, so that in addition to checking the security clearance applicant, the operational vetting also includes vetting of the persons listed in the security questionnaire.[18] Thus, the second level vetting verifies: the identity of the person (based on the attached written documentation) and the operational verification of the data about the individual done by a competent authority, age of at least 18 years, citizenship of the Republic of North Macedonia, legal capacity of the person (on the basis of a certificate issued by a competent authority), the existence of security obstacles for the person to have access to and handle classified information (determined by an operational vetting conducted by a competent authority), as well as the person's possession of a citizenship of another non-NATO country which is also checked with the operational vetting.

In this Article as well, the legislator did not envisage the vetting to include verification of the conviction of the person on the basis of a non-conviction certificate, with validity not exceeding six months, whose possession as a condition for obtaining a security clearance has been prescribed in 41 paragraph 1 line 9, as provided for the verification of the legal capacity of the person on the basis of a certificate issued by a competent authority. However, as we stated in the commentary on Article 49, the non-conviction of the person is checked during the operational vetting.

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.

[18] Following an initiative, at its session held on April 20, 2012, the Constitutional Court of the Republic of Macedonia adopted a Decision (U.No.209/2010) (Official Gazette of the Republic of Macedonia No. 61/11) to revoke Article 7 paragraph 2 lines 2 and 3 of the Decree Personnel Security (Official Gazette of the Republic of Macedonia No. 82/04) which contained provisions providing that the existence of security risk for the person for whom the issuance of an appropriate security clearance is required, is determined on the basis of an operational vetting of the candidate, his children and spouse, for the second level vetting, while for the third level vetting, based on the operational vetting of the candidate, his children and spouse, the parents and other persons living with the candidate in a same household. The reasoning of the Constitutional Court for such a Decision states that in the absence of a legislation stipulating that the vetting should also include the mentioned persons, it cannot be regulated by a bylaw passed by the Government. With this in mind, when drafting the new text of the Law on Classified Information, the legislator envisaged that the second level vetting should also include the persons listed by the security clearance candidate in the security questionnaire, as a general term whicn includes the parents, the spouse and the immediate family members, as well as the persons older than 18 years living in the same family and the spouse's parents for whome there are separate sections in the security questionnaire.

The scope of the third level vetting has been foreseen by the legislator in Article 51. He determined that the following elements are checked: the identity of the person - based on attached written documentation and operational verification of the data about the individual done by a competent authority, age of at least 21 years, citizenship of the Republic of North Macedonia, the legal capacity of the person requesting a security clearance and the persons listed in the security questionnaire[19] (based on a certificate issued by a competent authority), the existence of security obstacles for the person to have access to and handle classified information (determined by an operational vetting conducted by a competent authority), determining the ability of the person to handle classified information through an interview conducted by an authorized person from the competent services who carry out the vetting, as well as the person's possession of a citizenship of another non-NATO country which is also checked with the operational vetting.

Determining the ability of a person to handle classified information through an interview by the competent services is a novelty introduced by this Law. The previous practice included a conversation/ an interview with the person requesting a security clearance with the level of TOP SECRET by the director of the Directorate for Security of Classified Information as assessed if certain knowledge obtained by the operational vetting of the person need to be clarified.

In terms of non-conviction, it is checked during the operative vetting, and the legislator here did not envisage checking the non-conviction of the person based on the non-conviction certificate, with validity not exceeding six months, which the person submits and whose possession is a condition for obtaining security clearance in accordance with Article 41 paragraph 1 line 9.

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 52 identifies the security services that, at the request of the Directorate, carry out the operational vetting for the existence of security obstacles for access to and handling of classified information.

It is stipulated that the National Security Agency conducts the vetting of all individuals and legal entities, except for the persons employed in the Ministry of Defence and the Army of the Republic of North Macedonia, for which vetting is done by the competent services of the Ministry of Defence for all employees in the Ministry of Defence and the Army of the Republic of North Macedonia.

In case of vetting of persons employed in the Intelligence Agency or diplomats, i.e. persons who have resided and worked abroad, the Intelligence Agency may submit information on the persons concerned to the competent services, and that information

19 In the context of the Decision of the Constitutional Court - U.No. 209 /2010 (see previous footnote), the legislator envisaged that the third level vetting should also include the persons listed by the candidate for security clearance in the security questionnaire.

will be taken into account in the overall security vetting.[20]

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.

In Article 53, the legislator provided the deadlines for the security vetting procedure and determined that the first level vetting procedure for natural persons lasts up to four months, while it lasts up to six months for the second level vetting procedure for natural persons, for the third level vetting procedure for natural persons and the vetting procedure for a legal entity.

The legislator also provided for exceptions, thus stipulating that the deadline for the third level vetting procedure for the persons appointed to the supervisory bodies supervising the implementation of the measures for interception of communications, as well as for the hired accredited national and international technical experts from those bodies, in accordance with the Law on Interception of Communications, lasts one month from the day of submitting the request. The second exception is the procedure for second level vetting for persons before getting employed by the Operational Technical Agency, in accordance with the Law on Operational Technical Agency,[21] which the legislator has determined to last one month from the date of submission of the request. In the exceptions, the legislator did not provide for the procedure for third level vetting for the employees of the Operational Technical Agency.

It is a matter of envisaging faster procedures (implemented in shorter deadlines) for certain categories of persons where it is necessary to complete the procedure faster, i.e. the absence of such a solution could lead to blocking the work in these extremely important areas.

20 Intelligence Agency Law, Official Gazette of the Republic of North Macedonia No. 21/21, Article 83.

21 Law on Operational Technical Agency, Official Gazette of the Republic of Macedonia No. 71/18 and Official Gazette of the Republic of North Macedonia No. 98/19, Article 17, paragraphs 4 and 6.

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.

In Article 54, the legislator provided for the validity of security clearances. He determined the different duration of the security clearances issued for different levels of classification. Thus, the security clearance issued for information classified TOP SECRET is valid for five years, and for information classified SECRET and CONFIDENTIAL, the clearance is valid for ten years. With a provision in the fourth paragraph of this Article, the legislator provided for the content and the form of the security clearance form to be prescribed by the director of the Directorate.

The legislator did not provide for the validity of the security clerance during the duration of an activity or service, for example going on a mission and the like. This is because in such a case the "need to know" principle is complied with, even though the person received a security clearance valid for ten years, after the cessation of the need for it, i.e. after the completion of the activity or mission for which the clearance was issued in the first place, the validity of the security clearance will expire in accordance with Article 60 paragraph 1 line 2 of this Law.

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.

In Article 55, the legislator regulated the obligation of the user of classified information to submit a new request for extension of the validity of the security clearance no later than six months before the day of its expiration. The purpose of this obligation is to prevent a kind of vacuum that would occur if the person waits for the validity of the security clearance to expire, before requesting its extension, given, above all, that the Law does not provide for the possibility of issuing a temporary security clearance. Given the fact that the extension presupposes the implementation of a new appropriate

security vetting, it is clear that this process should start earlier. Therefore, this period of six months is harmonized with the deadlines for the duration of the security vetting procedure defined above in Article 53.

In the second paragraph of this Article, the legislator indicates that with the request for extension of the validity of the security clearance, for the natural person and the legal entity who submits the request, a new vetting is carried out appropriate to the level of the classified information released to him. Once performed vetting does not mean that it gives results that cannot be changed, hence, every person who has access to classified information should be periodically subject to an appropriate control (and according to appropriate indications and more often), so the legislator envisaged an obligation for a re-vetting at each request for extension of the validity of the clearance.

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 56 regulates the procedure for revocation of the security clearance and before its expiration by the Director of the Directorate in case it is determined that the natural person or the legal entity does not handle the classified information in accordance with law or no longer meets any of the conditions based on which the security clearance had been issued. This is determined by the classified information security officer in the body in which the natural person is employed or the inspector for security of classified information who can supervise the work of the natural person, i.e. the legal entity, with the classified information. The legislator provided for the director of the Directorate to make a decision for revocation of the security clearance which does not provide an explanation for the reasons for revocation of the security clearance.[22] The reasons why no explanation is given, the legislator probably sees in the possibility with the explanation itself to reveal information that should remain secret at that moment.

However, in the third paragraph of the article, the legislator regulated the right of the person to appeal such a decision before the the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes regarding the

22 Following an initiative, at the session held on September 21, 2005, the Constitutional Court of the Republic of Macedonia adopted a Decision (U.No.213 / 2004) that no procedure for assessing the constitutionality of Article 54 paragraph 2 and Article 55 paragraph 2 of the Law on Classified Information is initiated (Official Gazette of the Republic of Macedonia No. 9/04) which contained provisions that no explanation is given for the reasons for the termination of the validity of the security clearance. The explanation of the Constitutional Court for such a decision states that "given that the security clearance is not a classic administrative act that addresses the individual rights of citizens, but the right of access and use of classified information to access a specific matter - area such as the security of the state defense, the Court found that the question of the conformity of the disputed legal provisions with the Constitution of the Republic of Macedonia could not be raised.

procedure for revoking the security clearance. This means that the State Commission primarily considers the manner of conducting the procedure for its revocation and, as a rule, does not go into the reasons for revoking the security clearance. However, if the members of the Commission become aware of the content of some classified information during the procedure itself, they are obliged to keep such information secret in accordance with Article 104 of this Law.

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.

In Article 57, the legislator also regulated the possibility for the director of the Directorate to be able to make a decision to reject the request for issuance of a security clearance for individuals and legal entities if the conditions prescribed by this Law are not met. This decision does not provide an explanation for the rejection of the request, and the person has the right to appeal it before the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes in relation to the procedure for issuing the security clearance.

The rejection of the request for issuance of a security clearance, as it can be concluded, although it is unexplained, it is not a discretionary decision without grounds, i.e. it is a result of non-fulfillment of the legal requirements, but most often the reasons for refusal in a particular case should remain secret as to why they are under investigation, for example, or pose detected risks or threats that need to be properly addressed, hence the need not to be explained in the explanation.

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.

In the first paragraph of Article 58, the legislator determines the deadline of 15 days for submitting the appeal to the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes, while in the second paragraph it stipulates that

the decision made by the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes in the second instance is final.

The above-mentioned Commission was established by the Law on the Establishment of a State Commission for Decision-Making in Second Instance Administrative and Employment Disputes.[23] An administrative dispute may be initiated before a competent court against its decision, in accordance with Article 10 paragraph 1 of the Law on Establishment of a State Commission for Decision-Making in Second Instance Administrative and Employment Disputes.

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.

In Article 59 the legislator defines the deadlines when a request for re-issuance of a security clearance with the same or higher classification level can be submitted when a person was denied to be issued a security clearance or when he had received a clearance but it was revoked. Depending on the reason for which the "negative" decision was made, the legislator provided different deadlines, thus determining that it can be submitted after one year from the validity or finality of the decision to reject the request for issuance of a security clearance and after the expiration of three years from the validity or the finality of the decision for revocation of the security clearance before the expiration of the validity. The reason for determining a different time limit when the person can apply for re-issuance of a security clearance with the same or a higher classification level lies in the greater seriousness of the reasons for which the decision to revoke the security clearance is made.

In case of a positive answer, the issued clearance is expected to be valid for one year. This is because although it is currently established that the conditions for issuing a security clearance are met, the reasons why a person has previously been denied or revoked a clearance remain "hanging" in the air as an indication that the person may pose a potential risk, so the validity of the clearance is shorter than that according to the basic decision, which means a re-vetting if after the expiration of the validity of that clearance of one year, the person requests its extension. Given the fact that the person should request an extension at least six months before the expiration of the validity, this means that the next vetting prcedure would begin six months after the issuance of the clearance referred to in Article 59, paragraph 2.

23 Law on the State Commission for Decision-Making in Second Instance Administrative and Employment Disputes, Official Gazette of the Republic of Macedonia No. 51/11, 148/13, 41/14, 130/14, 53/16 and 11/18.

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 60 stipulates when the security clearance ceases to be valid. In addition to the main grounds for termination of validity, which is after the expiration of the deadline, the legislator has provided for several more cases.

The first refers to persons who according to law receive a security clerance for access and use of classified information of all levels, without prior vetting, for uninterrupted performance of the function from the day of election to the end of the term (Article 40). Thus, after the end of their function, i.e. at the end of the mandate, the security clearance issued to them for performing their duties ceases to be valid.

The second case concerns the termination of the need for access to classified information in accordance with the "need to know" principle. This means that a person who needed access to classified information at a given time in order to perform tasks that required access to classified information, in the event of his/her reassignment to a job that does not require access to classified information, no longer needs security clearance and thus the security clearance, which was issued when the "need to know" principle was met for that person, ceases to be valid. The same applies when a person moves to a job position from one institution to another because even in that case the "need to know" principle on the basis of which the security clearance was issued may cease to apply.

The legislator provided for the validity of the security clearance to cease in case of reduced mental capacity to handle classified information determined by a competent medical institution. This case is not regulated in more detail in the Law which does not contain provisions regulating the manner of determining the reduced ability of a person who holds a valid security clearance or the procedure for obtaining an opinion from a competent medical institution. The given provision of the Law presupposes that in case of realization of a security risk for the classified information due to reduced mental capacity of the person handling it confirmed by a competent medical institution, the issued security clearance will cease to be valid.

The last case in which the security clearance is expected to cease to be valid is the death of the natural person or termination of the legal entity.

The last paragraph of this Article regulates the obligation of the security officer of classified information to return the security clearances for natural persons and/or legal

entities to the Directorate within 15 days from the ascertainment of the termination of their validity.

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 61 regulates the termination of the validity of the permit for access to classified information, whereby the legislator provided for it to cease to be valid upon the expiration of the validity period specified in the permit, by performing the task for which it was issued, in case the need for issuance of the permit has ceased to exist or has been changed and if it is determined that the legal entity and the natural person do not handle the classified information in accordance with the law. In fact, through an inspection by the inspector for security of classified information, it is determined that the legal entity and the natural person do not handle the classified information in accordance with the law.

The access permit for information, in fact, according to Article 6, paragraph 1, line 10, is a document confirming that the foreign natural person or legal entity has a security clearance issued in the home country and has the right to access and use classified information in the Republic of North Macedonia, based on this Article (61), we indirectly come to the conclusion that it is issued to foreign persons who need it, i.e. there is a need for them to have access to classified information in our country, it is related to some task etc. Hence, the termination of the existence of such grounds, as well as the failure to act with the classified information in accordance with the law is the basis for termination of the validity of the access permit.

Termination of the access permit does not terminate the validity of the security clearance issued in the home country, but it alone is not sufficient for a foreign natural person or alegal entity to have access to classified information, so that the access permit is a ***conditio sine qua non (a condition without which one cannot do).***

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 62 regulates the obligation to protect the confidentiality of classified information after the expiration of the validity of the security clearance. This provision implies that the user of classified information has an obligation to protect it even after the termination of his need for access to classified information in accordance with the "need to know" principle, i.e. to keep all information about them secret.

The violation of this obligation, depending on the circumstances, may constitute a specific crime.

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 classified 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 63 regulates the need for possession of a security clearance by entities/persons participating in court proceedings or proceedings before another competent authority in which classified information is used.

In order to respect the right to defense which is one of the basic rights of the accused and it is a constitutionally guaranteed principle (Article 12 of the Constitution), the legislator provided for the procedure to be conducted before the person whose liability is decided within it and when the person does not have a security clearance. However, in the area of the court proceedings, this is not limited to criminal proceedings, but refers to any court proceedings where decisions are made about the rights and obligations of a person (for example, civil dispute, labor dispute), and not only for liability. Additionally, other procedures before the competent authorities are covered. The use of classified information in any procedure should not ***per se*** be a basis for its declassification, but its protection the legislator continues to provide by providing liability for the person in terms of fulfilling the obligation to protect classified information in accordance with this Law. This means that all entities and persons who hold a security clearance and persons who are part of the procedure, and do not hold such a clearance, based on the provisions of this Law are obliged to protect classified information, i.e. their confidentiality.

In order to achieve the pre-stipulated protection of classified information used in various court or other proceedings before competent state bodies, in the fourth paragraph the legislator stipulated that the public is excluded in proceedings using classified information, in order to restrict access to classified information by unauthorized persons, i.e. a wider circle of persons.

In order to regulate the situation when the originator of the classified information did not submit the classified information in the procedure, the legislator provided that the court or the competent authority has a duty within 15 days from the receipt of the classified information to inform the originator and the Directorate for Security of Classified Information about its use in the procedure.

The issue of using classified information in a court procedure or procedure before another competent body is regulated for the first time in this Law, although Article 354 of the Law on Criminal Procedure provides for the possibility of excluding the public, among other things, for keeping "state, military, official or an important business secret."[24] As we can see, the Law on Criminal Procedure still uses old terminology, although since 2004 the Law on Classified Information has determined the four levels of classification "top secret", "secret", "confidential" and "restricted". Undoubtedly, it is necessary to harmonize such solutions and to ensure the consistency of the relevant legislation.

As mentioned above in this commentary, the occurrence of awarding a classification level to evidence provided by the use of special investigative measures (PIM) is common. Then they are most often declassified and marked "UNCLSSIFIED (court proceedings)".

We emphasize once again that if there is a need for further protection of the information, it does not need to be declassified, but as such (classified) can be part of the procedure of exclusion of the public from proceedings.

If the originator of the information thinks that he should declassify it, it primarily means that it will be used in a procedure where the public is not excluded. Hence, it is clear that these issues require discussions and training that will involve all relevant entities. It should not be forgotten that the classification of PI-measures (especially the ones with the highest levels of TOP SECRET or SECRET) implies the fulfillment of strict conditions for protection of any kind, including cryptographic protection if the information is transmitted electronically, strict regulations for copies, reproductions, etc. The originators of classified information should take into account all legal requirements, and it is recommended to take into account the more specific guidelines and examples given in the Guide for determining the level of classification of information of the Directorate for Security of Classified Information, especially if the originator has dilemmas about the classification level that he is to determine and the consequences resulting therefrom.

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.

Article 64 regulates the obligation of the Directorate for Security of Classified Information to keep records of the issued security clearances and the completed security questionnaires, as well as special records of the issued permits for access to classified information in the Republic of North Macedonia. The access permits to classified information are subject to special records because they are issued to foreign individuals or legal entities that already hold a security clearance from the home country.

The legislator envisaged the content, form and manner of keeping such records to be prescribed by the director of the Directorate with a bylaw.

[24] Law on Criminal Procedure, Official Gazette of the Republic of Macedonia, No. 150/10, 100/12, 142/16 and 198/18.

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.

In Article 65, the legislator regulates the obligation of the state and the local government bodies established in accordance with the Constitution of the Republic of North Macedonia and 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 to create conditions necessary to protect classified information and to take measures to eliminate the negative consequences if classified information is disclosed. Within that duty, the legislator provided that the mentioned entities should appoint a security officer for classified information who will enable efficient and coordinated execution of the rights and obligations related to classified information.

The network of the classified information security officers is an important segment of the system for protection of classified information as the classified Information security officers are considered key personnel for the sustainability, enforcement and oversight of security policies for working with classified information in each of the relevant entities where classified information is handled and stored.

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.

In Article 66, the legislator envisaged that the responsible person in the entities in which classified information is handled and stored, i.e. in the entities listed in the previous article, will appoint one or more officers for security of classified information, depending on the number and scope of classified information which is handled in the entity.

An additional basis for appointing more classified information security officers in one entity that the legislator has not identified, could be the large number of employees who need access to classified information as it presupposes an increased range of tasks and activities for the security officer. The experience shows that the large users of classified information, i.e. entities with a large number of employees where a large number of classified information is handled and stored, need more officers for security of classified information.

On the other hand, the legislator provided for an exception in which, depending on the number and scope of classified information, the responsible person in the entity may perform the duties of a classified information security officer.

Further in the same article, the legislator regulated the obligation of the classified information security officer to prepare and submit quarterly reports on his work and the situation with the classified information directly to the responsible person. It is stipulated that this obligation does not apply to the officer for security of classified information who is also a responsible person in the entity.

In order to better coordinate the work of the entity in the area of protection of classified information with the Directorate for Security of Classified Information, the legislator stipulated that if the entity has several officers for security of classified information, the responsible person should appoint one of them for coordination 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 67 regulates the conditions that a person must meet in order to be appointed as a classified information security officer. Namely, it is necessary to be a citizen of the Republic of North Macedonia, not to be a citizen of another country, to be granted access to an appropriate level of classified information according to the conditions and procedure established by law, to have passed training for a security officer of classified information and have an appropriate security clearance. The legislator does not specify here the level of the security clearance that the classified information security officer should possess, but it is assumed that this is the level that corresponds to the level of classified information handled within the entity.

The training for a classified information security officer is not regulated in more detail by the legislator, i.e. the legislator does not indicate who conducts the training and what evidence the security officer should present in confirmation of the completed training. An obligation remains for the legislator in the future to fill this legal gap, i.e. to further regulate the matter on this issue.

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.

In Article 68, the legislator regulated the duties of the classified information security officer and enumerated them exhaustively. He envisaged that the security officer should take care of the implementation of the provisions of this Law and the ratified international agreements regarding the security of the classified information in the entity. This means that the classified information security officer is in direct line of communication with the Directorate for Security of Classified Information regarding the measures and activities that the entity undertakes to protect the classified information. In addition to the general obligation of the classified information security officer to implement the provisions of the Law, the legislator further provides for certain more specific duties and responsibilities. He stipulates that the officer should check the records and the flow of materials and documents on a quarterly basis, to take care of the correct and timely implementation of the archiving and destruction of classified information, to conduct the procedure for submitting requests for issuance of security clearance within the entity and to keep records of the persons for whom a procedure has been conducted, to inform the Directorate about the expiration of security clearances, termination of operation or redeployment of users of classified information, to inform the Directorate about the need to change the classification level of the security clearance, to inform the Directorate, in writing for any change in the data in the security questionnaire or change in the conditions for obtaining a security clearance that he was aware of or could have known that it has occurred, to record cases of unauthorized access to classified information or their compromising and actions taken and to immediately inform the Directorate for such case and action, to inform the users of classified information at least once a year about the rights and obligations in handling classified information, to provide professional assistance in the classification of information in the entity, to organize training for users of classified information in the entity for protection of classified information.

In the second paragraph of the article, the legislator provided for the classified information security officer to prepare an annual work plan which will include the activities that he has to fulfill in accordance with the given obligations and which is approved by the responsible person. The legislator also regulated the case when the responsible person performs the duties of an officer for security of classified information and at the same time regulated that s/he prepares the annual work plan her/himself.

Failure to perform the duties by the security officer stipulated by this Article may constitute a misdemeanor, and the deliberate and intentional omission of his duties in order to cause a certain harmful consequence may even constitute a criminal offense, depending on the circumstances of the case, the harmful consequences, etc.

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 69 regulates the status of the Directorate for Security of Classified Information as an independent body of the state administration with the capacity of a legal entity. It was established as an independent body in 2004 after the adoption of the Law on Classified Information in the same year and is a continuation of the former National Security Authority in NATO context as a professional service of the Government.[25]

In addition, the competencies of the Directorate are regulated, whereby: it ensures continuous implementation of the international standards and norms in undertaking the measures and activities for protection of the classified information, coordinates the activities in providing protection of the classified information with the state bodies and institutions that exchange classified information with foreign countries and international organizations, prepares, organizes, implements and monitors the implementation of measures and activities for ensuring protection of classified information released to the Republic of North Macedonia by foreign countries and international organizations, undertakes activities for protection of classified information released by the Republic of North Macedonia to foreign countries and international organizations, participates in the preparation of plans and programs of the Republic of North Macedonia for membership in international organizations in the field of protection of classified information, plans and accomplishes international cooperation for protection and exchange of classified information, proposes measures for promotion of the protection of classified information, initiates international agreements with foreign countries and international organizations in the field of exchange of classified information, carries out accreditation of communication-information systems and processes, organizes and conducts trainings for security of classified information, executes inspection supervision over the implementation of the provisions of this Law and performs other activities determined by law.

The legislator envisaged the Directorate for its work to endorse an annual plan and prepare a report to be adopted by the Government of the Republic of North Macedonia. Consequently, after the endorsement of the annual plan, it is published on the official website of the Directorate, and the report is submitted to the Government for consideration and adoption.

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.

25 Directorate for Security of Classified Information, History, available at: https://www.dbki.gov.mk/?q=node/129

Article 70 regulates in more detail the tasks of the Directorate for Security of Classified Information regarding the exchange and protection of classified information with NATO and the European Union, which recognize the roles that the Directorate has in relation to cooperation with those international organizations.

Namely, as the highest body in the country in the field of protection of classified information, by coordinating and implementing the security policies of NATO and the European Union in the Republic of North Macedonia, in order to ensure an adequate level of protection of classified information in accordance with the ratified international agreements, the Directorate is recognized as the National Security Authority (body) for the implementation of policy in the field of exchange and protection of classified information with the international organizations. By performing the tasks of communications security for the selection, management and maintenance of cryptographic equipment for transmission, processing and storage of classified information, the Directorate is recognized as the National Communication Security Authority. Performing the tasks for conducting security accreditation of the communication-information systems and the processes in which the classified information is used, the Directorate has the role of the National Accreditation Authority, and by taking measures and activities for protection of the communication-information systems from compromising electromagnetic emission, the Directorate is recognized as the National TEMPEST Authority.[26]

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.

Article 71 regulates the competence of the Ministry of Defence and the Army of the Republic of North Macedonia in the exchange and protection of classified information with NATO for the management of materials for cryptographic protection of classified information and secure handling, storage, distribution and recording of cryptographic materials.

In the second paragraph of the article, the legislator envisaged the competence of the Directorate for Security of Classified Information to supervise the implementation of the measures applied by the competent body in the area of material management for cryptographic security of classified information and secure handling, storage, distribution and recording of cryptographic materials. The supervisory role of the Directorate here is focused on its competence to monitor the application of the applicable legislation and to continuously implement international standards and norms in undertaking measures and activities for protection of classified information while the competent entities have the competence to perform the operational work.

26 See, Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, 20 November 2020

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 72 regulates the establishment of the registration system for executing activities within the competence of the Directorate for Security of Classified Information with NATO classified information, classified information of the European Union and other foreign classified information. It is composed of a registry established at the Directorate for Security of Classified Information and sub-registries and control points established within the entities in which NATO classified information, European Union classified information and other foreign classified information is handled and stored.

In the third paragraph of this Article, the legislator provided that the sub-registries and control points submit information necessary for the execution of the activities of the Directorate and exchange classified information with abroad. The legislator also regulated the procedure for establishing sub-registries and control points by stipulating that they are established after obtaining the consent of the Directorate for fulfilling the conditions required for establishing sub-registries and control points upon request from users of classified information. In this Article, however, the legislator did not specify in detail what are the conditions that need to be met for the establishment of sub-registries and control points. In order to regulate this issue in more detail, the legislator should prescribe them or give a legal basis to do so with a bylaw.

The last paragraph of this Article stipulates that the exchange of classified information between the Republic of North Macedonia and foreign countries and international organizations is done through the Directorate, unless otherwise regulated by law,

ratified international agreement or another arrangement.

The sub-registry network enables proper distribution of the foreign classified information to the users and control over their movement in the entities in which they are established. In accordance with ratified international agreements, the register, sub-registries and control points are subject to supervision by the competent services of NATO and the EU (Article 37 paragraph 1 of this Law).

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.

In Article 73, the legislator regulated the cooperation between the Directorate for Security of Classified Information and the competent authorities of foreign countries and international organizations, which is based on ratified international agreements, for mutual reporting on the security of the exchanged classified information.

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.

In Article 74, the legislator regulated the obligation of the state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and 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 persons and natural entities upon request to provide the Directorate for Security of Classified Information with the information necessary for for accomplishing the works within its competence. This cooperation of the Directorate with the entities is especially expressed in the framework of the vetting procedure of the natural persons and the legal entities that request to be issued a security clearance.

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.

In Article 75, the legislator stipulated that the Directorate is managed by a director. He is appointed and dismissed by the Government of the Republic of North Macedonia for a term of four years. For the first time with this Law, the legislator envisages a deputy director who is obliged to replace the director in case he is absent or when due to illness and other reasons he is not able to perform his function with all his powers and responsibilities in the management. The deputy director is also appointed and dismissed by the Government of the Republic of North Macedonia for a term of four years.

This article also prescribes the procedure for election of director and deputy director, which begins with publishing a public announcement in three daily newspapers that are published throughout the Republic of North Macedonia, one of which is published in the language spoken by at least 20% of the citizens speaking an official language other than the Macedonian.

The conditions that both officials have to meet in order to be elected for the positions of director and deputy director are also prescribed, as follows: to be a citizen of the Republic of North Macedonia; not to have citizenship of another state; with a final court decision not to have been sentenced with a ban on performing a profession, activity or duty; to have obtained 240 credits according to ECTS or VII / 1 degree of education; to have at least five years of work experience; to have one of the following internationally recognized certificates or official attestation document for active knowledge of English 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 level B2 and to have a TOP SECRET security clearance.

In this Article, the legislator also provided the conditions when the function of the director and of the deputy director of the Directorate respectively terminate before the expiration of the mandate for which he was appointed, i.e.: if he resigns, at his own request, due to fulfillment of conditions for old-age pension determined by law, with right of extension in accordance with the labor regulations, due to death and if by a final court decision he is sentenced to imprisonment of more than six months. The conditions according to which, if one of them is fulfilled, the Government of the Republic of Northern Macedonia dismisses the director and the deputy director of the Directorate. Namely, the director and deputy director of the Directorate can be dismissed if it is determined that he does not meet one of the conditions set out in Article 75 paragraph 4 of this Law *(a technical error was made here in the Law - paragraph 5)*, if he refuses to submit a statement on property ownership and interests in accordance with the law or if the data contained in the statement are untrue and obviously violate the rules for conflict of interest, i.e. exemption in situations in which the director/deputy director knew or should have known about the existence of one of the grounds for conflict of interest, i.e. exemption provided by law. The last two grounds are in fact indications of corrupt practices that in themselves make the official unworthy of executing this very important function.

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.

The provisions of Article 76 apply to employees in the Directorate for Security of Classified Information. The legislator prescribed that the employees of the Directorate have the status of administrative civil servants, and in accordance with such a status, he prescribed that the provisions of the Law on Administrative Servants apply to their employment rights and responsibilities.[27] With this status, the employees of the Directorate remain the only ones within the state bodies that have competencies in the

27 Law on Administrative Servants, Official Gazette of the Republic of Macedonia No. 27/14, 199/14, 48/15, 154/15, 5/16, 142/16 and 11/18 and Official Gazette of the Republic of North Macedonia No. 275/19 and 14/20.

security sector that do not have the status of persons with special duties and powers.[28] Such status of the employees in the Directorate, unfortunately, is a reason for increased outflow of staff in other institutions and directly affects its personnel capacity to implement the legal competencies.

In the second paragraph of this Article, the legislator provided that the employees of the Directorate are sent to work in the permanent missions of the Republic of North Macedonia to NATO and the EU, in accordance with a signed agreement for joint cooperation with the Ministry of Foreign Affairs, and during the referral, get a title in accordance with the provisions of the Law on Foreign Affairs.

This article also regulates the condition for the employees in the Directorate to have an appropriate security clearance for access to classified information, which is determined by the jobs systematization rulebook of the Directorate. This issue is regulated in this way because all employees in the Directorate do not need access to classified information with the same level of classification as they do not have the same need to access classified information of NATO and/or the EU.

The legislator in the fifth paragraph of this Article provided for the procedure in case when an employee of the Directorate during the employment will not be extended the validity of the security clearance or during the vetting it will be determined that he can not obtain a security clearance due to security risk of access to and handling of classified information. In such a case, he provided that the employee be permanently transferred to another state body or institution, to a job at the same level for which he meets the general and special conditions prescribed in the act for systematization of the other institution. The transfer of the employee to another institution is arranged to be based on an agreement signed by the managers of both institutions. If the employee who is taken over does not sign the new employment contract within 15 days from the date on which it was submitted, his employment is terminated. This decision is in line with the current legislation on mobility of administrative servants.[29]

For the employees of the Directorate, the legislator envisaged for them to have an official identification card issued by the director of the Directorate who prescribes its form and issuance in a bylaw. The envisaged Rulebook on the Form of the Official Identification Card of the Employees in the Directorate for Security of Classified Information and on the Manner of its Issuance was adopted and published in the Official Gazette of the Republic of North Macedonia No. 53/2021.

28 Law on National Security Agency (Official Gazette of the Republic of Macedonia No. 108/19) Article 65; Law on Operational Technical Agency (Official Gazette of the Republic of Macedonia No. 71/18 and Official Gazette of the Republic of North Macedonia No. 98/19) Article 11, paragraph (1) and Article 20 paragraph (1); Law on Intelligence Agency (Official Gazette of the Republic of North Macedonia No. 21/2021), Article 25.

29 Law on Administrative Servants (Official Gazette of the Republic of Macedonia No. 27/14, 199/14, 48/15, 154/15, 5/16, 142/16 and 11/18 and Official Gazette of the Republic of North Macedonia No. 275/19 and 14/20), Article 30; and Law on Public Sector Employees (Official Gazette of the Republic of Macedonia No. 27/14, 199/14, 27/16, 198/18 and Official Gazette of the Republic of North Macedonia No. 14/20), Articles 42,43 and 44.

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.

For more efficient realization of the work of the Directorate, with the provisions of this Article, the legislator determines that it should be guided and accomplished according to the principles, norms and procedures valid in the planning, programming and budgeting system. As can be seen in the comment for the next article, it is prepared in accordance with the instructions and guidelines for preparing budget requests from the budget circular prepared by the Ministry of Finance.

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.

Article 78 of the Law legally regulates the issue of financing the Directorate for Security of Classified Information and financing of the protection, use and international

exchange of classified information undertaken by other state bodies, local government bodies, legal entities, etc.

According to paragraph 1 of this Article, the Directorate is financed from the Budget of the Republic of North Macedonia. It is an independent body of state administration and hence, its financing and work are not coordinated through a ministry, for example, but directly from the state budget.[30]

The amount of funds allocated to the Directorate is an issue that can be discussed a lot, although it goes beyond the narrow pragmatic framework of a commentary on a law. It depends on many important elements. First of all, the nature and the changing amplitude of the challenges faced by the Directorate in its current work, as well as the sensitive sphere of action dictate in some way the volume of funds needed for efficient functioning of this institution. Second, almost all European countries, even the most developed ones, face the challenge of high spending on security institutions. In accordance with the modern understanding of the protective component of the entities in charge of it, as is the case with the Directorate, it is necessary to build a system that will ensure the necessary information to reach the end user and to be protected. The clearly defined position on the need for existence, construction and development of an appropriate system for protection of classified information, in itself raises the question of expenditures, i.e. how much financial resources are needed to secure this segment.

Hence, one of the most frequently cited arguments for ensuring the required functionality of the system is the cost, i.e. the price, consistently understood as the volume of funds needed to be provided to achieve the desired goal, including the funds to be provided for better organization and operation.

The Directorate, according to the Law, can be financed from other sources of financing, and they are not specifically listed in the article, but such a possibility is explicitly provided by the Law.

Regarding the financial means for the state bodies for the needs of protection, use and international exchange of the classified information, the provision from paragraph 3 of this Article determines that such funds are provided from the Budget of the Republic of North Macedonia within the financial resources of those bodies. This means that funds are allocated to them for that purpose from the state budget, and not through the Directorate and the funds intended for it.

Local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established by the municipalities, the City of Skopje and the municipalities in the City of Skopje for the needs of protection, use and international exchange of classified information provide funds from own sources and from the financial and material assets of the Republic of North Macedonia in accordance with paragraph 4 of this Article.

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.

Pursuant to this Article, it is envisaged to carry out inspections on the implementation of the entire legislation for protection of classified information. This means that the inspectors during the supervision will check the entities from the aspect of application of the provisions of the Law, but also the provisions of the bylaws adopted on the basis of the Law, i.e. the decrees and the rulebooks.

The primary role in performing the inspection is entrusted to the inspectors for security of classified information of the Directorate. In conducting the supervision, their task is to determine whether the Law and the regulations adopted on the basis of this Law are being implemented, i.e. to consider the situation and to evaluate the total operation of the relevant entities. Inspection in legal science is also called repressive supervision because it expresses certain powers of a coercive nature that are applied in order to ensure consistent compliance with the legality of operations and the legal order in general.[31]

It is a systematic activity to perceive how the established legal standards and norms for ensuring the legal use of classified information are respected, how classified information is handled during their lifecycle, what are the conditions under which classified information is handled and stored and how the security space is secured, the classified contract, etc. The inspectors for security of classified information should take action to inspect the actual situation and evaluate the overall operation. This feedback also means comparing actual results with pre-defined operating standards. So, the supervision is in function of the assessed and objective perception of the situation on whether there are shortcomings in the implementation and enforcement of legal norms that are based on certain standards by which the actual execution is carried out.

The provisions of paragraph 2 of this Article stipulate that the activities of the inspection should be performed in a special organizational unit within the Directorate. Basically, it is the real place and element of the above synthesized analysis which says that it is naturally predestined for the organizational unit to conduct inspections in this

[31] Давитковски, Б., Павловска – Данева, А., Административно право – прв дел, Скопје, 2018, 309.

area, because it is the entity that is in charge and really knows the implementing side of the law and the essence of supervision. From the aspect of the systematic connection of the people working in a legal entity with the goals, each organizational unit is composed of people who are grouped according to certain criteria. Within the Directorate they are given in Article 81. The organizational unit for inspection is composed of professionals who know the subject of inspection in general, but also the sensitive area of protection of classified information.

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.

Inspection supervision, as we have previously emphasized, is of great importance in the process of information protection for at least two reasons, namely: one is aimed at understanding how the provisions of the Law on Classified Information(*) are applied and the relevant regulations that have been adopted and that result from the Law in concreto and secondly, to detect weaknesses and omissions in the operation in order to take certain actions in order to improve it.

Article 80 paragraph 1 defines the legal bases for conducting inspections in this area, i.e. it is clearly stated that in the procedure for conducting inspections the provisions of this Law are primarily applied, which is an essential provision, because such a solution was not contained in the previous Law on Classified Information and exclusively the provisions of the Law on Inspection were applied. This means that for matters regulated by this Law, it is a ***lex specialis*** and it is applied primarily, while the Law on Inspection (as well as the Law on General Administrative Procedure) is a ***lex generalis*** and its provisions apply to matters that ae not regulated with the Law on Classified Information(*) as ***lex specialis***.

Obviously, the situation is significantly different and justified due to the specificity of this area, so the provisions of the Law on Inspection Supervision, in accordance with Article 2, paragraphs 1, 2 and 3 of the Law[32] relating to the procedure, obligations and conditions for inspection, apply to the inspection services organized as bodies within the ministries or as organizational units, within the bodies of the state administration, the municipalities, the municipalities in the City of Skopje and the City of Skopje, but not for the Directorate for Security of Classified Information, and also are not applied to the Ministry of Finance, including the Public Revenue Office and the Customs Administration, the Ministry of Defence and the Ministry of Interior.[33] This means that the Directorate for Security of Classified Information has the original right to conduct inspections through its inspectors. This achieves a dual goal, on the one hand, it provides the necessary independence due to the nature of the matter, and on the other hand, it certainly ensures legality in acting in order to direct the work in accordance with the legislation.

The legislator envisaged that the manner of conducting inspections will be regulated

32 Law on Inspection Supervision, Official Gazette of the Republic of North Macedonia No. 102/19, Article 2.

33 Ibid, Article 2, paragraph 4.

in more detail by a rulebook, but has also left room to apply the provisions of the Law on Inspection Supervision and the Law on General Administrative Procedure for issues not regulated by this law. The application of the provisions of the mentioned laws is only an addition in the implementation of the necessary supervision due to the complementarity of the matter. Thus, the Law on General Administrative Procedure regulates the issues that regulate the procedure for accomplishing the protection of the rights and legal interests of natural persons, legal entities and other parties, as well as protection of the public interest, which the ministries, bodies of the state administration, the organizations determined by law, other state bodies, legal entities and natural persons entrusted by law to perform public authorizations, as well as the bodies of the municipality, the City of Skopje and the municipalities in the City of Skopje, when in performing their legal competencies, act, decide and undertake other administrative actions in administrative matters[34] and most importantly this Law applies to all administrative actions of the public bodies and service providers.[35]

The above-mentioned rulebook aims to fully develop the manner of performing inspections in this area and should certainly be in correlation with the Law on Classified Information(*) and other ***inter alia*** legal regulations that are in conjunction with the Law on Classified Information(*). In other words, the provisions of this Rulebook reflect the firm and clear determination of the Law on Classified Information(*) and the prescribed provisions that in practice should create easy concretization of supervision, i.e no different interpretations of the same and similar issues in the proceedings or, which is especially important, not to create space for subjective thinking. This means that the provisions should be clear, precise and applicable. Norms in law that can be interpreted in different ways are considered not to meet the requirement for clear and precise provisions: ***lex certa et stricta*** which is a consequence of the principle of legality.

The Rulebook on the Manner of Performing Inspection Supervision was adopted on the basis of Article 80, paragraph 2 of this Law and was published in the Official Gazette No. 246/20.

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.

34 Law on General Administrative Procedure, Official Gazette of the Republic of Macedonia No. 124/15, Article 1.

35 Ibid, Article 2.

A person who will perform inspection, i.e. the inspector, must meet certain conditions that are clearly and explicitly stated by the Law. Namely, the inspector performing the inspection in the field of protection of classified information must first meet the general conditions prescribed by the Law on Administrative Servants and special conditions prescribed in the Law on Classified Information(*).

All conditions are a prerequisite for a competitive person who is expected that with his purposeful action and individual behavior will make the tasks visible and contribute to their concretization and achievement.

There is no doubt that for the inspector performing the inspection in the field of protection of classified information in terms of qualifications, competencies, training, etc., in addition to the general conditions set by the Law on Administrative Servants, the legislator believes that he should meet special requirements due to the specificity of the matter. Regarding the general conditions, in accordance with the Law on Administrative Servants where the job classification of administrative employees is given, the general competencies are determined in the framework of the general competencies for administrative employees,[36] while the legislator provided the special conditions such as the necessary professional qualifications, work experience in the profession, as well as the passed professional exam for inspector for classified information to be determined as special conditions at the workplace. The category of jobs of administrative employees according to the responsibility, goals, type and complexity of work and tasks in the job, is in accordance with Article 22 of the Law on Administrative Servants. The positions of administrative staff are classified into four categories: Category A - secretaries, Category B - senior administrative staff, Category C - professional administrative staff and Category D - auxiliary professional administrative staff.[37] The filling of vacancies of administrative employees and employment of administrative employees are defined in Chapters VI and VII of the Law on Administrative Servants.[38]

It must be emphasized that education is key to acquiring the necessary competencies and skills and that leaving room in the Law on Classified Information(*) as defined in paragraph 1 line 1 for potentially every education profile to be competitive, relativizes the general commitment to man the organizational unit for inspection with professional and above all competent staff who have the necessary knowledge and skills acquired in the process of education.

In addition to proper education, an important prerequisite for successful performance of this work is professional work experience. The three-year work experience listed in line 2 leaves room for serious discussion. There are opinions that inspectors need to have much more professional work experience to be able to get to the heart of the problem in order to understand the changing amplitude of work in this area, which would fulfill the main goal of being a catalyst for the overall situation in detecting the irregularities in the operation of the legal entities and the natural persons that are in contact with classified information and taking actions to remove and/or sanction them.

Paragraph 2 of this Article regulates the obligation of the Directorate to adopt a Rulebook on the Manner of Taking the Professional Exam for Inspectors for Security of Classified Information (the third special condition) which prescribes in more detail the conditions and the manner of taking the exam which will check the theoretical

36 Law on Administrative Servants, Official Gazette of the Republic of Macedonia No. 27/14, 199/14, 48/15, 154/15, 5/16, 142/16 and 11/18 and Official Gazette of the Republic of North Macedonia No. 275/1019 and 14/20, Article 21, paragraph 2.

37 Ibid, Article 22.

38 Ibid, Article 30-47.

knowledge of the candidates who have applied for inspectors, as well as checking the competitiveness and competences of the candidates.

The Rulebook on the Manner of Taking the Professional Exam for Inspectors for Security of Classified Information was adopted and published in the Official Gazette of the Republic of North Macedonia No. 219/20 and it stipulates that the exam consists of a general part (questions from the areas of general administrative procedure, inspection procedure and misdemeanor procedure) and a special part (issues in the field of regulations on security of classified information).[39] The candidate who has answered correctly at least 70% of the questions for each section separately, is considered to have passed the exam and receives an appropriate certificate for that.

Paragraph 3, which refers to the salary supplement of the inspectors, stipulates that it is 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.

This article specifies, as stated, which entity will be subject to inspection, i.e. that inspection supervision will be carried out in the state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, in legal entities established by the Republic or from the municipalities, the City of Skopje and the municipalities in the City of Skopje, as well as other legal entities and natural persons. Of course, these are not all such entities, but those whose work is related to the classified information.

Inspection supervision is more than obviously necessary, but its full effect requires a lot of knowledge and experience of inspectors, and the effectiveness of supervision depends on the anticipatory approach of all entities involved in this process such as state and local government, 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.

Paragraph 2 of Article 82 refers to the independence of the inspector in performing the work. Independence is an important and key component in ensuring that the inspector completes his or her task properly during the inspection. This means that no one should

39 See, Article 4 of the Rulebook on the Manner of Taking the Professional Exam of the Inspectors for Security of Classified Information, Official Gazette of the Republic of North Macedonia No. 219/20.

influence his work, and independence will allow him to solve the problem faster, more completely and more objectively, it creates objective conditions for impartiality and implies the absence of pressure to act according to someone's request and wishes. All this is a solid basis for the inspector to be able to objectify his view and to always strive for the situation to be considered neutrally.

However, in addition to the independence assessed and evaluated in value-ethical sense, as elaborated above, the understanding of independence in the context of this provision in terms of independent action versus team action should be taken into account.

Namely, due to the real needs or as a result of the workload, the legislator provided, at the proposal of the head of the organizational inspection unit, the director of the Directorate for Security of Classified Information to appoint an inspection team composed of administrative servants from the Directorate. In certain specific situations, there is a need to determine a team that will allow a more thorough and complex analysis of the problem; and that will mean more rationally to provide the necessary depth and breadth of knowledge and experience, which will mean faster and more complete knowledge of the character of the problem being solved; but this will sometimes mean the need to reconcile the opinions of the majority of those involved on a particular issue. This opportunity provided by the legislator – the director to appoint an inspection team at the suggestion of the head of the organizational inspection unit can be considered a positive solution because it means more people to unite thinking on one or more issues that allows to "illuminate" the problem element from different aspects, opinions, knowledge, etc. or because of the large scale. That is why there is a better chance of reaching a relevant opinion and conclusion. However, it must be emphasized that in teamwork it can happen to dilute the responsibility for the possible misinterpretation of the situation. From the above, it should be concluded that this possibility should be practiced by the director as an exception, as in fact the legislator himself indirectly pointed out, envisaging such a solution on an optional basis.

Paragraph 3 of the same article states that inspectors are obliged to act in accordance with the law and regulations. Inspectors should ensure objective application of the law and general legal action. This means that the inspectors in performing the inspection should implement objective, comprehensive, non-selective and non-discriminatory application of the law, which will mean that it will be well placed and adapted to the character and essence of the problems in the controlled entity and will emphasize the feedback expressed through the total relations of all entities involved in the inspection (the inspectors and the controlled entity). The inspection itself means supervision to determine whether someone's work is in accordance with the law, so it is expected and even more (***a fortiori***) emphasized that the inspectors themselves should legally perform their professional duties.

The illegal conduct of inspectors, given the supervisory and very specific nature of their work, should often be treated as serious abuse and legally qualified, depending on the circumstances of the case, as one of the offenses provided for in Chapter XX of the Criminal Code: Criminal acts against official duty.

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.

In this Article, the legislator has stated in the most general way the basic powers of the inspectors for security of classified information, and they are, above all, systematized in three areas: first, the inspectors supervise the implementation of the legislation on security of classified information, secondly, based on the conducted supervision ***in concreto***, they are authorized to propose measures to eliminate the identified shortcomings and irregularities in the application of the Law in a certain period of time (deadline) and thirdly, to take other actions in accordance with the law, which are usually provided in other more specific provisions. These powers naturally follow each other, namely, in order to propose, for example, measures to eliminate irregularities, an inspection must first be carried out within which such irregularities are identified, and so on.

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.

The legal provisions provided in paragraph 1 of this Article oblige the inspector during the inspection to obligatorily identify himself/herself, which will prove his/her official capacity. This means that the inspector must wear an official identification card and badge during the supervision and when referring to his work and official tasks he is obliged to show both the identification card and the badge. If this provision is interpreted consistently, it would mean the inspector when performing inspection, i.e. during each implementation of any of his tasks given as authorizations when in contact with the person being supervised, without exception to identify himself. In a situation where there is no specified work uniform, which identifies the inspector with the job, the requirement for regular identification is justified.

However, this provision should be interpreted restrictively, which is in correlation with the obligation of the inspector to legitimize himself at any request from the party that doubts his official action. The Law treats the identification card as proof of ability to perform inspections as a kind of a license for professional engagement in the work and the official tasks related to conducting inspections. The identification card obtained by the inspector by fulfilling the general and special conditions of the Law on Administrative

Servants and the Law on Classified Information(*) is a proof of passed professional exam in accordance with the Rulebook prescribed by the director of the Directorate, i.e. it is a kind of "diploma" which is acquired in order to gain legitimacy for performing the activities related to the inspection.

Paragraph 2 of this Article stipulates that the inspector is obliged to return the identification card and the badge at the request of the director of the Directorate when conditions are created for revocation of the identification card and the badge due to negligent behavior and other circumstances that are grounds for revocation.

Such circumstances make the inspector unworthy of further service, so they are grounds for revoking both the identification card and the badge. Of course, the issuing authority is also called upon to revoke the identification card and the badge. It is obvious and more than logical that the inspector must not behave in his work outside the prescribed standards of professional work and ethical norms for acting.

Pursuant to paragraph 3, the pattern, form and content of the official identification card and badge, as well as the manner of their issuance and revocation, are prescribed by the director of the Directorate.

If we generalize the analyzed position, we will come to the conclusion that the increasing specialization that is present in the inspection supervision requires conditional issuance of special identification cards and badges, and consequently they must be prescribed in a special pattern, form and content, with a rulebook adopted by the director of Directorate for Security of Classified Information.

The envisaged Rulebook on the Pattern, Form and Content of the Official Identification Card and Badge of the Inspector for Security of Classified Information, and on the Manner of their Issuance and Revocation was adopted and published in the Official Gazette of the Republic of North Macedonia No. 240/20.

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 85 paragraph 1 defines the obligation, for the purpose of the inspection, the state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the City of Skopje, as and other legal entities and natural persons to enable uninterrupted supervision in the field of security of classified information. That is, this means an obligation for all subjects of supervision to enable its smooth performance. This means that everything needed for the inspectors to see the real situation during the inspection should be made available, and if certain deviations are recorded, certain corrective actions should be taken. In order to ensure the smooth performance of supervision, there must be a certain type of cooperation. When it comes to the absence of cooperation of the legal entity or the natural person subject to supervision with the supervisor, several dilemmas arise. The first is in the direction of the so-called hidden absence of cooperation, i.e. it is always more difficult to measure the quantity of documentation required for the supervision that has not been submitted during the inspection (there is always the possibility for the documents to be additionally submitted). It is even more problematic and includes subjectivity because the attitude of the supervisor and the persons (legal and natural) where the supervision is performed may be objectively different. The supervisor, i.e. the inspector should be precise and specific in his requests, consistent, objective and impartial and finish the supervision at the moment when he analyzes the situation and assesses that it is enough to make an appropriate conclusion, instead of looking for new information, etc., when it is unnecessary and unjustified.

Obstruction or disabling of the supervision of legal entities and natural persons by the inspectors is not covered by the misdemeanor provisions of this Law. The existence of such a provision should be directly aimed at the responsible person in the legal entity, who commits the misdemeanor, which should be prescribed alternatively, as: obstruction of supervision, i.e. not enabling supervision; concealing the required documentation, i.e. not making it available to the supervisor in this case the inspector, or obstructing the supervision by not providing the necessary documents, data and information, for which the offender should be fined. However, the Law on Inspection Supervision, which applies to everything that is not covered by the provisions of the Law on Classified Information(*), envisages a misdemeanor for actions that mean obstruction of the inspection. Article 98 paragraph 1 of the Law on Inspection Supervision envisages as misdemeanor actions, inter alia, not providing access to premises, products, not

providing access to documentation, etc.[40]

Paragraphs 2, 3, 4 and 5 of this Article determine the manner of conducting the inspection supervision, which can be regular, ad hoc or control. Regular inspection includes supervision over the implementation of this Law and is performed according to the annual plan and monthly work plan of each inspector that the director of the Directorate adopts in accordance with the law. Thus, regular supervision is carried out continuously and is understood as part of a continuous process in which the supervision is established according to regularly determined dynamics. Such prerogatives are an integral part of the Law on Inspection Supervision, which in Article 69 paragraph 1 states that regular inspection is an inspection of the implementation of relevant laws and regulations adopted on the basis of those laws and is performed according to a pre-determined schedule in the annual plan.[41] This provision provides a broader framework and possibility if it is determined that additional supervision is needed and that both ad hoc and control supervision can be performed.

Pursuant to the Rulebook on the Manner of Conducting Inspection Supervision,[42] the regular inspection of the same entity is performed once a year.

Ad hoc supervision is usually conducted additionally, regardless of the planned dynamics for conducting supervision, or as stated in paragraph 4 of this Article, the ad hoc supervision is performed on the basis of an initiative submitted by state and local government bodies established in accordance with the Constitution of North Macedonia. and by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the City of Skopje, natural persons or lega entities, as well as in case of suspicion of the inspector (ex officio).

The ad hoc inspection is usually an unannounced inspection and it is carried out as soon as possible after receiving the initiative, i.e. as provided by the Rulebook in Article 2, paragraph 3, no later than 15 working days from the receipt of the initiative.

The control inspection is performed after the expiration of the deadline determined in the inspection act for elimination of identified deficiencies, i.e. the control supervision includes: direct inspection of the prescribed measures, inspection of the activities for elimination of irregularities, i.e. as prescribed in the Law on Inspection Superviion, control Inspection is an inspection that is performed ex officio in order for the inspector to determine whether the subject of the inspection, after the expiration of the term determined in the inspection act, during a previously performed regular or ad hoc inspection: acted in full after the inspection act; partially acted upon the inspection act or did not act upon the inspection act.[43]

Pursuant to paragraph 6, during the inspection, the inspectors have the right to access and inspect at any time and without notice, buildings, business premises, residential premises and premises where classified information is handled and stored and of course as stated. in paragraph 7 for performing the activities from paragraph 6 of this Article in residential premises, the inspectors are obliged to provide a court order. This is because the residential premises enjoy the constitutional and criminal protection of the inviolability of the home.

Establishing a system of supervision, which is both democratic and efficient, is

40 See, Law on Inspection Supervision, Article 98.

41 Ibid, Article 69.

42 Rulebook on the Manner of Conducting Inspection Supervision, Official Gazette of the Republic of North Macedonia No. 246/20, Article 2, paragraph 2.

43 Law on Inspection Supervision, Article 76 and Rulebook on the Manner of Conducting Inspection Supervision, Article 2, paragraph 4.

one of the more serious challenges. A positive step in the implementation of effective supervision is the right of the inspectors to have access and to inspect at any time without notice buildings, business premises, residential premises (by order only) and premises where classified information is handled and stored, i.e. inherent element of the supervision is that everything that is done has to be controlled. However, care should be taken and the work of inspectors should be transparent, demystified and should be aimed at detecting illegalities in the work. This creates a positive attitude of the controlled legal entities and individuals for their work and the tasks they undertake.

Paragraph 8 of this Article states that during the inspection, the inspectors may request the presence of an authorized person from the body of the state administration responsible for performing the activities in the field of police affairs, for their protection. Within the course of the action, there may be certain situations in which the inspectors during the inspection may face unpleasant situations, resistance, etc., especially when they have a legal opportunity to enter without notice into buildings, business premises, residential premises and premises in which classified information is handled and stored, but also in other situations when performing regular, ad hoc or control supervision. To prevent this from happening, after a preliminary assessment of the situation, the inspectors can request assistance from the Ministry of Interior in order to conduct the necessary inspections where planned.

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.

The importance of supervising legal entities and individuals is emphasized by the provision of Article 86 paragraph 1 of this Law. This provision is directly aimed at the identified deficiencies and irregularities related to the fulfillment of the security requirements of the classified information during the inspection. In case the inspector concludes that there are irregularities and shortcomings, i.e. that the controlled entities subject to inspection do not comply with the Law and other regulations governing this matter, then the inspector will issue a decision ordering the elimination of the identified deficiencies and irregularities within a certain period. This is a confirmation of the theoretical views that inspection, although ultimately repressive, is primarily preventive. Legal entities and individuals dealing with classified information should take concrete steps to eliminate any deficiencies.

The legislator did not «forget» the second instance here as well, so the subjects being supervised have the right to file a complaint, as stated in paragraph 2 of the same article, if they believe that the inspector's decision does not reflect the real situation in handling

the classified information and that they are damaged in the procedure by which it was determined that there was a deviation from the prescribed standards determined by the legal regulations, which would mean that certain inconsistencies ocurred in their work.

The deadline for submitting an appeal is 15 days from the day of receiving the decision, and the competent body for deciding on the appeal is the State Commission for Deciding in the Second Instance in the Area of Inspection and Misdemeanor Procedure.[44]

Pursuant to the Law on Establishing the State Commission for Decision-Making in the Second Instance in the Area of Inspection and Misdemeanor Procedure, the Commission applies the provisions of the Law on General Administrative Procedure, the Law on Inspection Supervision and the Law on Misdemeanors unless it is regulated otherwise with this or other law. According to Article 11 of the same law, an administrative dispute can be initiated against the decision of the State Commission before a competent court, and the lawsuit against such a decision of the State Commission does not delay its execution.

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 87 should also be read in the context of Article 86, as it regulates the situation referred to in paragraph 1 of that Article. These provisions of Article 87 are directly aimed at the legal entity and the natural person where the inspection is performed and refer to the ascertained shortcomings and irregularities that hinder the execution of the legal being. For the mentioned omissions and in general for any ascertained condition, the inspector is obliged to compile minutes with a finding on the situation and submit them in a manner and within a period provided by law. In this context, the provisions of the Law on Inspection Supervision are taken into account, which envisage the inspector compile the minutes on the spot and to record therein the performed supervision, the established factual situation, the ascertained and determined irregularities and shortcomings, remarks, statements and other relevant facts and circumstances.[45] The minutes are signed by the inspector and the subject of the inspection to whom a copy is handed over. If the subject of the inspection refuses to sign the minutes, the inspector will state the reasons for the refusal. Except when due to the scope and complexity of the inspection supervision, its nature and work circumstances, it is not possible to compile the minutes at the place of supervision, the minutes are compiled in the official premises of the inspection service within three days from the day of the inspection supervision with explanation of the reasons for that.[46]

44 Law on establishing the State Commission for Decision-Making in the Second Instance in the Area of Inspection and Misdemeanor Procedure, Official Gazette of the Republic of Macednia No. 130/14, 53/16 and 11/18.

45 Law on Inspection Supervision, Article 82, paragraph 1.

46 Ibid, Article 82, paragraph 2 and 3.

As usual, when certain inconsistencies and irregularities in the operation are ascertained, a decision is made to eliminate them. In the same Article 87, in the following paragraphs it is implicitly indicated that the responsible person in the subject of supervision is obliged to act according to the decision and to inform the inspector about the undertaken activities. In the decision, the inspector will determine deadlines during which the identified deficiencies and irregularities should be removed. As can be concluded, the deadlines in some way bind both parties. Basically, the intention of the legislator is to limit the time in which concrete measures should be taken to eliminate irregularities and inconsistencies. The entity should, as a rule, inform the inspector about the undertaken activities. Such decisions of the inspector are the basis for the so-called control inspection.

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.

The provisions of this Article stipulate the obligation of legal entities and individuals working with classified information to continuously take care of the prescribed security standards for the protection of classified information and not to allow the use of devices, technical means, installations and systems that do not comply with the prescribed standards. The provision that if such a situation is determined, a decision will be made to prohibit their use and will require their removal. Failure to meet any of the conditions is considered a serious violation of the Law.

The need for greater oversight of legal operations in the field of use of devices, technical means, installations and systems is the growing danger that comes from the development of techniques and technology, and especially of the information technology.

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.

This is a clear restrictive norm in relation to situations of imminent danger to security. Namely, if the inspector during the supervision determines that there is an immediate danger of violating the security of the facilities or premises, documents, equipment, systems and persons in the security perimetar, the security area or the administrative zone, with a decision pronounces a ban on using the space, facility or part of the building.

The essence of the decision imposing a ban on the use of space, object or part of an object, etc. is protection from harmful consequences, the occurrence of which is very probable and would mean violation and destruction of important legal goods, and the

urgency of the situation is the basis for the necessity of such a solution.

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.

The provision from paragraph 1 of this Article, envisages the inspector to seal the building or the premises in question in order to execute the decision from Article 86 paragraph 1 and Article 88 of this Law. This prevents their further use until the moment of elimination of the deficiencies. The sealing is performed by an inspector and in accordance with paragraph 2 of the same article it is done with a seal stamp of the Directorate, which in terms of form and content is regulated by a special rulebook which also regulates the manner of sealing. The Rulebook was adopted by the director of the Directorate and was published in the Official Gazette No. 187/2020.

According to its provisions, the seal stamp has the shape of a circle with a diameter of 30 mm, made of metal for stamping on printing wax, which is attached to a wooden hilt, and the stamping is done on red wax and yellow-red thread (tape).

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.

This article builds on the previous ones, i.e. it regulates that in case of elimination of the determined inconsistencies, due to which a ban measure has been imposed, and upon a previously written request of the entity to which the measure has been imposed, the inspector shall remove the wax stamp. The Directorate, more precisely its inspectors have complete supremacy in the part of sealing and seal removing, i.e. it is an established right that already exists and is executed according to really emerged need, so when the need for sealing falls away, the inspector should remove the 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.

Supervision over the legality of the operation of the entities that store and handle classified information is exercised by authorized supervisory officials, i.e. inspectors who can order the undertaking of several measures. Paragraph 1 of this Article lists the measures whose execution may be ordered by the inspectors in accordance with the provisions of the Law on Classified Information(*). These are measures that have a predominantly preventive character, as follows: dismantling, moving or removing equipment, devices, installations and systems that endanger the security of classified information; determination of security perimeters, security areas and administrative zones around the facility, space or room in the facility where classified information is handled or stored; installation of security information-communication equipment, systems and installations for security of classified information; relocation or removal of persons without an appropriate security clearance or without an appropriate permit for access to the security perimeter around the facility and to the security areas and administrative zones in the facility where classified information is handled or stored; moving or removing vehicles without proper permission to enter the security perimeter around the building and into administrative zones in the building where classified information is handled or stored; preparation of internal acts for security risk assessment for classified information and for their protection in case of emergency; updating and correcting records of classified information and their removal and destruction; providing prescribed conditions for dissemination and transmission of classified information; prohibition for receipt, handling, release and storage of classified information and other measures that the inspector determines to be in function of the protection of classified information in the subject of supervision. Obviously, these measures are in function of protection of the classified information in the subject of supervision.

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.

With Article 93 paragraph 1 the legislator envisages the duty of taking actions in order to initiate an appropriate procedure which will ultimately sanction the violation of the Law and other regulations which repesens a misdemeanor or a crime.

Thus, the inspector is obliged to submit a request for initiating a misdemeanor procedure against a person who will violate the Law and who acts or has acted contrary to the Law and other regulations concerning classified information. It is obvious that in this case, the inspector has the sovereign right to assess whether the conditions are met for a request for initiating a misdemeanor procedure which requests a misdemeanor procedure to be initiated against the person, on the basis of which a misdemeanor sanction will be imposed. The procedure is conducted in accordance with the misdemeanor provisions of the Law on Classified Information(*) and the Law on Misdemeanors.

According to the provision from paragraph 2 of this Article, if during the supervision the inspector considers that the violation is a criminal act, he is obliged to immediately inform the director of the Directorate for initiating a procedure before a competent body. This means that the director of the Directorate is obliged to immediately take measures and inform the competent authorities for further action in accordance with law, i.e. to file criminal charges, to inform the Public Prosecutor's Office which will further investigate the allegations, facts and circumstances and decide whether to prosecute.

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.

In Article 94, as well as in the next six articles of this Law, the legislator provided fines for committed misdemenours in relation to the inappropriate application of this Law for the legal entity-user of classified information, the responsible person in the legal entity-user of classified information and for the natural person-user of classified information. Guided by the provisions of the Law on Misdemeanors, especially in the area of recognizing the areas in which higher fines for misdemeanors may be imposed than those provided by the Law (general law) for a natural person and the responsible person in a legal entity,[47] the legislator in this Article provided for higher fines for misdemeanors related to classified information due to the nature and seriousness of the damage to the state that could occur with the illegal handling of classified information and their release to unauthorized persons. Unauthorized disclosure of classified information could adversely affect the protection of human health, the protection of natural resources, the environment, the protection of cultural heritage, and classified information may be disclosed to unauthorized persons out of selfishness or cause greater property damage.

As a result, the legislator envisaged a fine in the amount of 3,000 to 5,000 Euro in Denar counter value for the legal entity-user of classified information, if: it does not implement the measures for administrative, physical, security of communication-information systems, personnel security or for industrial security of the classified information, in accordance with the provisions of Articles 26, 28, 29, 31, 32 and 33 of this Law; does not handle the classified information in accordance with the provision of Article 56 paragraph 1 of this Law (unless the action is not a crime); does not notify of termination of fulfillment of any of the conditions on the basis of which a security clearance has been issued, in accordance with the provisions of Article 42 of this Law, and obstructs the inspection supervision in accordance with the provisions of Article 79 of this Law.

In the second paragraph of this Article, the legislator provided a fine in the amount of 1,000 to 2,000 Euro in Denar counter value for a misdemeanor of the responsible person in the legal entity-user of classified information for the misdemeanors referred to in paragraph 1 of this Article. And in the third paragraph, it provided for a fine in the amount of 500 to 1,000 Euro in Denar counter value for a misdemeanor of the natural person-user of classified information for the misdemeanors 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.

In Article 95, the legislator prescribed the fines for misdemeanors of the legal entity-user of classified information, of the responsible person in the legal entity-user of classified information and of the natural person-user of classified information if they do not undertake the necessary activities for receipt, processing, determination to the users and did not disseminate the classified information to them, in accordance with the provisions of Article 26 of this Law. The amount of the prescribed fine for a misdemeanor of the legal entity is from 1,500 to 2,000 Euro in Denar counter value, for a misdemeanor of the responsible person is from 1,000 to 1,500 Euro in Denar counter value, and for a misdemeanor of a natural person from 500 to 1,000 Euro in Denar counter value.

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 96 prescribes the fines regarding the illegal handling of classified information marked with the level RESTRICTED, i.e. for acting contrary to the obligation for its protection, regulated in Article 47 paragraph 2 and in the sense of Article 2 of this Law. Thereby, a fine in the amount of 1,500 to 2,000 Euro in Denar counter value for a misdemeanor of the legal entity is prescribed, a fine in the amount of 1,000 to 1,500 Euro in Denar counter value is prescribed for a misdemeanor of the responsible person in the legal entity, and for a misdemeanor of the natural person, a fine from 500 to 1,000 Euro in Denar counter value is prescribed.

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 97 prescribes the fines for acting contrary to the provisions of Article 12 of this Law, i.e. for disclosing information marked UNCLASSIFIED. The amount of the prescribed fine for a misdemeanor of the legal entity is from 500 to 1,000 Euro in Denar counter value, for a misdemeanor of the responsible person is from 450 to 700 Euro in Denar counter value, and for a misdemeanor of a natural person from 300 to 500 Euro in Denar counter value.

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.

In Article 98, the legislator prescribed the fines for a misdemeanor to the security officer of classified information in the amount of 500 to 1000 Euro in Denar counter value if he does not fulfill any of his duties stated in Article 68 of this Law or if he obstructs the inspection in accordance the provisions of Article 79 of this Law.

It should be borne in mind that in each concrete case all the circumstances should be examined in order to determine whether a particular action can be treated as a crime, especially if the perpetrator acted intentionally or with special intent and caused a harmful consequence appropriate to the nature of the crime.

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.

The legislator envisaged fines for misdemeanors of the legal entity-originator of classified information, the responsible person in the legal entity and the natural person if they act contrary to Article 10 paragraph 2 of this Law, i.e. if they do not determine the appropriate classification level of the information based on the possible damage and the consequences that would result from unauthorized access to it. Thereby, for a misdemeanor of the legal entity-originator of classified information, the legislator envisaged a fine in the amount of 1,000 to 1,500 Euro in Denar counter value, for a misdemeanor of the responsible person in the legal entity envisaged a fine in the amount of 500 to 1,000 Euro in Denar counter value, and for the misdemeanor to the natural person envisaged a fine in the amount of 300 to 500 Euro in Denar counter value.

Failure to determine the appropriate classification level of a particular piece of information can have serious consequences because, instead of being adequately protected, the information remains fully or partially available to persons who should not be objectively aware of its content, so that may endanger the interests of the state and result in a harmful consequence and in such a case the possibilities for abuse, i.e. a crime should be investigated.

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.

Article 100 prescribes the fines for misdemeanor of the legal entity-originator of classified information, the responsible person in the legal entity and the natural person if they act contrary to Article 16 paragraph 3 and Article 18 paragraph 2 of this Law and do not inform the user of the classified information on the change in the classification level or on its declassification.

Thereby, for a misdemeanor of the legal entity-originator of classified information, the legislator envisaged a fine in the amount of 1,500 to 2,000 Euro in Denar counter value, for a misdemeanor of the responsible person in the legal entity envisaged a fine in the amount of 1,000 to 1,500 Euro in Denar counter value, and for the misdemeanor to the natural person envisaged a fine in the amount of 500 to 1,000 Euro in Denar equivalent.

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.

In Article 101, the legislator regulates the institute of "settlement" in the misdemeanor procedure. Pursuant to the Law on Misdemeanors,[48] the legislator stipulated that the inspector for classified information is obliged to issue a misdemeanor payment order to the perpetrator of the misdemeanor, before submitting a request for initiating a misdemeanor procedure. The second paragraph stipulates that the inspector keeps records of the issued payment orders in which the following data are collected, processed and stored: name and surname, i.e. name of the perpetrator of the misdemeanor, place

48 Law on Misdemeanors, Official Gazette of the Republic of North Macednia No. 96/19, Article 51.

of residence, seat, type of misdemeanor, number of the misdemeanor payment order issued to him and the outcome of the procedure. It is regulated that personal data are stored for five years from the date of entry in the records.

The legislator envisaged the form and the content of the misdemeanor payment order to be prescribed by the director of the Directorate with a bylaw, and for everything that is not determined by this Law regarding the misdemeanor payment order, to apply the provisions of the Law on Misdemeanors.

In fact, the Law on Misdemeanors as ***lex generalis*** applies whenever in the special law a certain institute or procedure of the misdemeanor law is not regulated differently.

The Rulebook on the Form and Content of the Misdemeanor Payment Order was adopted and published in the Official Gazette of the Republic of North Macedonia No. 181/20 and 285/20.

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.

In Article 102, the legislator provided that for the misdemeanors determined by this Law, a misdemeanor procedure is conducted and a misdemeanor sanction is imposed by a competent court.

This provision is in accordance with Article 54 paragraph 1 of the Law on Misdemeanors.

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.

Article 103 incriminates the disclosure of information classified SECRET and CONFIDENTIAL.

With the introduction of these provisions in the Law, the current vacuum is filled, i.e. the gap in the penal regulations regarding the illegal handling of information with the classification level SECRET and CONFIDENTIAL.

Namely, the Criminal Code contains provisions only in relation to the information that is considered a TOP SECRET and prescribes criminal sanctions for its disclosure under Chapter Twentyeight: Criminal acts against the state, in Article 317.[49]

For that reason, in the first paragraph of this Article, the legislator provided that the person who told, handed over or made available to the public or to an uninvited person information classified SECRET to which he has access in accordance with law and thus endangers or violates the vital interests of the Republic of North Macedonia, shall be punished by imprisonment of one to five years.

The second paragraph provided for liability for the person who told, handed over or made available information to the public or to an uninvited person that he knows is classified SECRET, and which he obtained in an illegal manner, whereby such action is punishable by imprisonment of one to three years.

The act from paragraph 1 according to the legislator is more severe than the act from paragraph 2, because in the first case the illegal action is committed by a person to whom the classified information is entrusted, which means that he abuses his duty, in conditions when he is expected to provide the necessary protection against unauthorized access. The act from paragraph 2 means that the perpetrator came in possession of the classified information in an illegal, i.e. impermissible, unlawful way, whereby he will make it available to an uninvited person or to the public.

In the third paragraph, the legislator provided that the person who told, handed over or made available to the public or uninvited person information that is classified as CONFIDENTIAL to which he has access in accordance with law and thus endangers or violates the important interests of the Republic of North Macedonia, shall be punished by imprisonment of one to three years. And, in the fourth paragraph, he found that a person who told, handed over or made available to the public or an uninvited person information that he knew was classified CONFIDENTIAL, and which he obtained in an illegal manner, shall be punished by a fine or imprisonment of six months to three years.

In the fifth paragraph, the legislator provided the so-called qualified form of the crime, more precisely if the crime from items 1 and 3 was committed during a state of war, the perpetrator will be punished with imprisonment of one to ten years.

At the same time, he explicitly provided that the attempt of the crime from paragraphs 2, 3 and 4 of this Article is punishable, because according to the prescribed punishment for the acts from the stated paragraphs the provision from article 19 of the Criminal Code for the punishment of the attempt cannot be applied. In fact, the attempt of all the acts from paragraphs 1-4 is punishable, only for paragraph 1 it is based on Article 19 of the Criminal Code, and for the other paragraphs it is explicitly provided.

The legislator also sanctions the act of negligence, so in the last paragraph of this Article he provided that if, due to negligence, the person tells, hands over or makes available to the public or to an uninvited person information that is classified SECRET or CONFIDENTIAL, to which he has access in accordance with the law, and thus endangers

49 Criminal Code, Article 316 paragraph 6 and Article 317.

or violates the vital, i.e. important interests of the Republic of North Macedonia, that he will be punished with a 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.

Article 104 contains an incrimination of the unauthorized disclosure of classified information that the person found out about in a court or other procedure, which is a novelty in relation to the current regulation on classified information in this sense.

Namely, instead of a classified information to be declassified in order to be used in court proceedings (as evidence or similar) which would lose the meaning of the classification because it would be a "small door" to access information that is important to be secret and protected, the legislator provides for an obligation for any person to keep confidential information that has been classified, and for which it has learned in some procedure. In doing so, he does not limit it only to court proceedings, but also to others, for example, administrative proceedings, in order to cover all possible cases, even those that are very rare in practice.

In fact, the judge handling such cases (as well as the public prosecutor, if it is a case in which he has jurisdiction) should have a security clearance, and this provision should cover other participants in the proceedings, depending on what procedure is in question, etc.

Violation of this prohibitive criminal norm is sanctioned according to the classification level of the information in question in the specific case, and based on that, several forms of the crime are detected.

Namely, the legislator stipulated that a person who, contrary to law, unauthorizedly discloses information classified TOP SECRET which he found out in court or other proceedings, will be punished with imprisonment of up to five years, which from a criminal point of view means a frame of 30 days up to five years in prison.[50] If the information is classified SECRET or CONFIDENTIAL, the legislator provided for the perpetrator to be

50 See, Criminal Code, Article 35. Namely, Article 35, paragraph 1 defines the general legal minimum and maximum of imprisonment which is 30 days, i.e. 20 years, and given the fact that in the incrimination of Article 104 of the Law on Classified Information(*) the legislator has determined only the legal maximum, and the minimum is the one provided as a general minimum, i.e. 30 days.

punished with imprisonment of one to three years.

The attempt of the crimes from paragraph 1 and 2 is punishable, whereby the attempt of the crime from paragraph 1 is punishable according to the general provision for attempt from Article 19 of the Criminal Code,[51] and the attempt of the crime from paragraph 2 does not fall within the scope of the mentioned provision from Article 19 of the Criminal Code, so the legislator in this Article explicitly provides for it.

If the crime is committed through negligence, the last paragraph of this Article stipulates that the perpetrator is punished with a fine or imprisonment of up to one year, which is completely justified, because it is a matter of committing the lesser form of guilt - negligence, while pragraphs 1 and 2 cover the premeditated forms of the criminal act.

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.

For successful implementation of the provisions of the Law on Classified Information(*), it is necessary to adopt bylaws that regulate certain actions in more detail. In the transitional provisions of Article 105, the legislator stipulates that such bylaws will be adopted within six months from the day this Law enters into force, and that by then the bylaws adopted on the basis of the Law on Classified Information (Official Gazette of Republic of Macedonia No. 9/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18) will be applied.

In relation to this provision, the following bylaws have been adopted so far:

- Rulebook on the form and content of the security questionnaire forms and security clearances;[52]
- Rule Book on the Content, Form and Manner of Keeping the Records of the Issued Security Clearances and the Completed Security Questionnaires and the Special Records for the Issued Permits for Access to Classified Information;[53]
- Rulebook on the Manner of Performing Inspection Supervision;[54]
- Rulebook on the Manner of Taking the Professional Exam of the Inspectors for Security of Classified Information;[55]
- Rulebook on the Form and Content of the Misdemeanor Payment Order;[56]
- Rulebook on the Pattern, Form and Content of the Official Identification Card and Badge of the Inspector for Security of Classified Information, and on the Manner of their Issuance and Revocation;[57]
- Rulebook on the Form and Content of the Wax Seal Stamp of the Directorate for Security of Classified Information and the Manner of Sealing;[58]
- Rulebook on the Form of the Official Identification Card of the Employees in the Directorate for Security of Classified Information and on the Manner of

its Issuance.[59]

- The draft texts of the following bylaws are in the phase of harmonization with the Secretariat for Legislation:
- Decree on the manner of storage and handling of Unclassified information, the manner of reclassification of information, the manner of declassification of information, the manner of determining the users and dissemination of the received foreign classified information and the measures and activities for administrative security of classified information
- Decree on Physical Security of Classified Information;
- Decree on Personnel Security of Classified Information;
- Decree on Industrial Security of Classified Information;
- Decree on Security of Communiction and Information Systems.

The draft text of the Guidelines for the process of risk management of physical security of the classified information has been prepared, which after the adoption of the new Decree on Physical Security will be subject to harmonization with the Secretariat for Legislation in the form of a Rulebook.

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 106 stipulates that the regulations governing issues in the field of classified information shall be harmonized with the provisions of this Law within one year from the day this Law enters into force.

This primarily means changes to other regulations, amendments to relevant provisions in other laws whose matter relates to the protection of classified information, but also indirectly means the need for possible changes and repealing provisions in the Criminal Code that will prescribe criminal sanctions for other levels of classified information (although this is now covered by this Law), and not only for information recognized as a TOP SECRET,[60] as well as the repealing provisions on disclosure of military secrets and similar obsolete provisions .

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.

In Article 107, the legislator provided that the security clearances issued until the day of entry into force of this Law continue to be valid until the expiration of their validity. This in fact prevents the valid clerances from ceasing to be valid only due to the adoption of a new law, especially since there is no reason to terminate their validity until its expiration after which the extension of their validity and issuance of new security clearances will be done in accordance with the new law. .

59 Official Gazette of Republic of North Macedonia No. 53/21.

60 Criminal Code, Article 317.

The non-existence of this provision would cause a crisis in the operation of the handlers of classified information because suddenly all valid security clearances of the relevant entities in the country would become invalid, the Directorate would be overwhelmed with requests for new clearances, and the work in many institutions would be blocked for months, taken the fact into account that the procedure usually takes longer.

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.

The legislator ensures continuity in the work of the Directorate for Security of Classified Information established by the Law on Classified Information (Official Gazette of the Republic of Macedonia No. 9/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18) by stipulating in Article 108 that from the day of entry into force of this Law it continues to operate as the Directorate for Security of Classified Information in accordance with the competencies determined by this (new) 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.

In Article 109, the legislator envisaged continuity in the work of the director of the Directorate for Security of Classified Information appointed until the day of entry into force of this Law by stipulating that he continues to perform the function until the expiration of the mandate for which he was 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.

In Article 110, the legislator provided that on the day of entry into force of this Law, the Law on Classified Information (Official Gazette of the Republic of Macedonia No. 9/04, 113/07, 145/10, 80/12, 41/14, 21/18 and 83/18), i.e. the previous law with all its amendments becomes invalid.

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.

The last Article 111 of this Law prescribes the so-called ***vacatio legis***, i.e. the period from the publication until the entry into force of the law, i.e. in this case it is stated that the entry into force will be the eighth day from the day of its publication in the Official Gazette of the Republic of North Macedonia.

CIP - Каталогизација во публикација

Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

351.083.8(497.7)(094.5.072)

342.738(497.7)(094.5.072)

BAKRESKI, Oliver

Book of commentaries on the Law on classified information [Електронски извор] / Oliver Bakreski, Aleksandra Deanoska-Trendafilova.

- Skopje : Geneva center for security sector governance - Skopje DCAF,

2021

Начин на пристапување (URL):

https://dcaf.ch/resources?type=publications. - Начин на пристапување

(URL): https://www.dbki.gov.mk. - Текст во PDF формат, содржи 108 стр. - Наслов преземен од екранот. - Опис на изворот на ден 01.07.2021. - Фусноти кон текстот

ISBN 978-608-66657-6-0

1. Deanoska-Trendafilova, Aleksandra [автор]

а) Класифицирани информации -- Заштита -- Македонија -- Коментирани закони

COBISS.MK-ID 54251013