LAW NO. 08/L-175

ON PROTECTION OF CLASSIFIED INFORMATION

Assembly of the Republic of Kosovo;

Based on Article 65 (1) of the Constitution of the Republic of Kosovo,

Adopts:

LAW ON PROTECTION OF CLASSIFIED INFORMATION

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose

1. The purpose of this Law is the determination of basic principles, minimum security standards and the unique system for protection of classified information related to the security interests of the Republic of Kosovo.

2. This Law establishes the Agency for Protection of Classified Information (hereinafter referred to as APCI), whereby determining its mission, structure, functioning, duties and responsibilities.

3. This Law is in line with the EU legislation, as follows:

3.1. Council decision of 23 September 2013 on the security rules for protecting EU classified information.

Article 2
Scope

This Law applies to all public institutions exercising executive, legislative and judicial competencies and natural and legal persons, which based on the need-to-know principle could, while discharging their duties, have access to classified information of the Republic of Kosovo, other states and international organizations.

Article 3
Protection of classified information

1. Classified information is protected in accordance with this law.

2. Any person entrusted with classified information or is familiar with its content is responsible for its protection in accordance with this law.

3. The entirety of classified information is protected by the highest classification level that its component possesses.

Article 4
Definitions

1. Terms used in this Law shall have the following meanings:

1.1. **Classified information -** any information or material for which a certain classification level has been set, the unauthorized disclosure of which would affect to various degrees the security interests of the Republic of Kosovo;

1.2. **Need-to-know –** the need of access to classified information in the light of a certain position and for the purpose of fulfilling a specific duty;

1.3. **Classification** – the act or process of determining the level of classification and the time period for maintaining such classification;

1.4. **Agency – Agency for Protection of Classified Information (**hereinafter **APCI);** means the National Security Authority responsible for the protection of Classified Information in the Republic of Kosovo;

1.5. **Vetting authority** - the Agency for Protection of Classified Information, as a structural unit specialized for conducting security clearances for individuals who will obtain knowledge, produce, store, administer, transport and transmit classified information;

1.6. **Security Clearance Questionnaire** - the form completed by any individual requiring access to classified information, and serves as the base for security clearance and assessment of data for the issuance or rejection of "Personnel Security Clearance" certificate;

1.7. **Personnel Security Clearance (PSC)** - the official document of APCI, or competent security authority of another country, which confirms, in terms of security, that a person meets the conditions set for obtaining knowledge, storing, administering and transferring classified information valid for a certain time and a certain level of access;

1.8. **Security breach** - an act or omission in contradiction with the applicable legislation that results, or may result in theft, loss, damage, compromise or unauthorized disclosure of classified information;

1.9. **Security Clearance** - the set of measures and procedures applied to a natural or legal person, and which serve as the basis for issuance, rejection, temporary suspension or withdrawal of "Personnel Security Clearance" certificate;

1.10. **Unacceptable Security Risk** - circumstances described in this Law, based on which APCI refuses the granting of PSC, or considers that the measure of its withdrawal or temporary suspension should be taken;

1.11. **Circumstances of Urgency** – conditions of objective inability to follow normal procedures for issuing a PSC due to the exercise of a short-term official duty of participation in an unpredicted international activity, extending military missions in various countries;

1.12. **Security Officer** (hereinafter SO) - the employee responsible for, or the structure charged by the head of the ministry, or state institution, for supervising and implementing requests for personnel security, and other disciplines of classified information;

1.13. **Classified Contract –** any contract concluded by a public institution with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves the access or creation of classified information or material classified under this Law;

1.14. **Classified Subcontract** - any contract signed by a contractor of a public

institution with another contractor (ie subcontractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves the entry or creation of information; classified;

1.15. **Declassification** - removal of any classification level;

1.16. **Document** - any information recorded regardless of its physical form or characteristics;

1.17. **Downgrading –** a decision that information classified and safeguarded at a set level is classified and safeguarded at a lower level of classification.

1.18. **Material** - any document, data carrier, parts of machinery, equipment produced or in the production process;

1.19. **Authorized holder of classified Information -** a natural person or a legal person possessing classified information has valid security PSCs and meets other conditions that allow access to Classified Information, unless otherwise provided by law;

1.20 **Industrial Security Clearance** certificate (hereinafter ISC), is an official document of APCI, or competent security authority of another country, whereby confirming, in terms of security, that an economic operator has organizational, technical, physical capacities and abilities and fulfils standards set for access, storage and administration of classified information in a project/program, or classified contract/sub-contract;

1.21. **Classifying authority** – any person defined in Article 5 of this Law, that has an original or delegated competence to classify information.

CHAPTER II
INFORMATION SECURITY

Article 5
Classification Authority

1. The authority of classifying information shall be exercised by:

1.1. President;

1.2. The President of the Assembly and the members of the Presidency of the Assembly;

1.3. Prime Minister and other members of the Government;

1.4. President of the Supreme Court;

1.5. Chief State Prosecutor;

1.6. Director of KIA;

1.7. Commander of KSF;

1.8. Police General Director;

1.9. The heads of Independent Institutions.

2. Authorities responsible for information classification provided for in paragraph 1 of this Article shall be entitled to transfer the classification competence to the heads of their subordinate

institutions, as executives are informed of the rules and procedures for the security of classified information protection and have individually admitted their responsibilities with regard to the protection of such information.

3. The request for granting authorization by the Classification Authority shall be submitted to APCI, which after reviewing and assessing, recommends for granting authorization or not.

4. Any authorization of the competency to classify information shall be done in writing and clearly identify the title holder by name and the title of the position. This authorization shall be valid only for the duration of the position as the head of relevant institution.

5. APCI shall draft, maintain and regularly update a register with the data of the persons that have competence for classification.

Article 6
Categories of information to be classified

1. The information shall be classified only if necessary and if it falls within one or more of these categories:

1.1. projects, plans, systems or operations related to the protection and security of the constitutional order of the Republic of Kosovo;

1.2. information from foreign states and international organizations, relations or activities of the Republic of Kosovo, which will be protected against unauthorized exposure.

1.3. activities, information sources and methods of intelligence institutions related to the security of the Republic of Kosovo.

1.4. systems, installations, infrastructure, projects, plans or services of protection related to the security interests of the Republic of Kosovo;

1.5. scientific, technological, economic and financial activities related to the security interests of the Republic of Kosovo;

1.6. cryptologic systems; cryptologic issues/problems;

1.7. plans on operation and use of the system of communication of classified information and cryptology;

1.8. risk assessments/inspection reports related to the shortcomings in cryptology system;

1.9. plans for identification, reduction and management of the risk that occurs in the electronic communication system;

1.10. plans, projects and programs for securing systems of communication for classified information;

1.11. information collected through specific operations and electronic interceptions, dealing with the protection and security of the Constitutional order of the Republic of Kosovo.

Article 7
Prohibition of information classification

1. The classification of information is prohibited when done for the purpose of:

1.1. hiding law violation, abuse of authority, lack of efficiency or administrative error,

1.2. depriving the right to recognize a person, organization or institution,

1.3. hampering or delaying the provision of information that is not required to be protected in the interest of security of the Republic of Kosovo;

1.4. limiting the competition.

Article 8
Classification levels

1. In terms of content, value and state interest, the information shall be classified in one of the following levels:

1.1. “TOP SECRET” - unauthorized disclosure of which, under reasonable assessment, could result in exceptionally grave damage to the security interests of the Republic of Kosovo;

1.2. “SECRET” – unauthorized disclosure of which would seriously damage security interests of the Republic of Kosovo;

1.3. “CONFIDENTIAL” – unauthorized disclosure of which would damage security interests of the Republic of Kosovo;

1.4. “RESTRICTED” – unauthorized disclosure of which would be unfavourable for security interests of the Republic of Kosovo.

2. The Classification Authority shall avoid over-classification of information and shall assign to them only a level of classification that is necessary to protect interests of the Republic of Kosovo.

Article 9
Duration of classification

1. Information shall be classified insofar as it is in the interest of security of the Republic of Kosovo.

2. Terms for classification of information shall be as follows:

2.1. information classified as “RESTRICTED”, one (1) year;

2.2. information classified as “CONFIDENTIAL”, five (5) years;

2.3. information classified as “SECRET”, fifteen (15) years; and

2.4. Information classified as “TOP SECRET”, fifty (50) years.

3. The calculation of the term for classification of information shall start from the date of production of classified information.

4. If the Classification Authority considers that information should be protected for a period longer than provided for in paragraph 2 of this Article, it shall issue a new decision for classification in accordance with Article 8 of this Law. Such a decision shall not be taken earlier than six (6) months before the date foreseen for declassification under paragraph 1 of this article.

Article 10
Conditions for the administration of classified information

1. Production of classified information shall take place only based on the list of classified information approved by the Classification Authority, in compliance with the procedure determined by the applicable legislation.

2. Production, usage, multiplication, transfer, physical transportation, archiving, storage and destruction of classified information shall take place in compliance with the following standards:

2.1. Personnel Security - consists of the selection of natural persons who should have access to classified information, the verification of the conditions for access to classified information and their education in the field of security;

2.2. Physical Security - is a system of measures designed to prevent or impede unauthorized access to Classified Information, or to provide evidence of any access or any unauthorized access attempt;

2.3. Information security - system of measures for the origin, receipt, registration, handling, dispatch, transport, transfer, handover, storage, removal, archiving or any other method of handling classified information, as the case may be;
2.4. Industrial Security - is the implementation of measures to ensure and verify the conditions for access to the classified information in the classified information and to ensure the treatment of classified information by the facility in accordance with this Law;

2.5. Security of Information Communication Systems - a system of measures to ensure the confidentiality, integrity and availability of classified information addressed by these systems and the responsibility of the administration and users for their implementation in information or communication systems using cryptographic methods and materials in the processing, transmission or storage of classified information;

2.6. the heads of public institutions that produce and administer classified information are required to undertake all necessary actions to prohibit the unauthorized access of classified information throughout the life cycle of such information from production, multiplication, distribution, transfer, processing and archiving them, registering in the relevant books for the management of classified information.

3. Procedures for implementation of this article shall be governed with a sub-legal act proposed by APCI and adopted by the Government.

Article 11
Declassification

1. Information shall be declassified when there is no longer a need for protection and when its publication no longer poses a risk to the security of the Republic of Kosovo.

2. The Classification Authority, from which the classified information is originated, shall carry out its declassification.

3. Cases of declassification of classified information shall be:

3.1. when its publication is dictated by state interests that are more important than the need to keep it classified;

3.2. when an event or a particular date occurs as determined by the classification authority.

4. Unauthorized disclosure of classified Information shall not constitute a cause for declassification.

5. The Classification Authority which has declassified information shall be obliged to notify all institutions that possess the classified information.

6. The procedures for the implementation of this Article shall be regulated by a sub-legal act, proposed by APCI and approved by the Government.

Article 12
Disposal and Destruction of Classified Information

1. In any state institution, the head of the institution or its authorized representative shall establish the commissions for disposal and destruction of classified information.

2. The commission for disposal shall review and decide on the disposal of classified information, in cases when this information is of no value for further retention and shall not be declassified.

3. Commission for destruction, based on the Decision of the Commission for Disposal, shall carry out all procedures regarding the destruction of classified information and prepare the final report.

4. Information that shall be submitted to the archive network should not be disposed and destroyed but declassified.

5. Procedures for implementation of this Article shall be regulated by a sub-legal act proposed by APCI and approved by the Government.

Article 13
Downgrading and Upgrading of Classification Level

1. The Classification Authority, which has originated classified information, shall be responsible for the downgrading of the classification level of such information.

2. The competent classification authority shall downgrade or upgrade the classification level if it becomes aware of facts that clearly indicate that the classified information does not require the level of protection associated with the existing level of classification.

3. Information classification procedures, including the classification of parts of documents, separate documents and markings that keep classified information, declassification and revision of the classification level are defined by sub-legal act proposed by APCI and approved by the Government.

Article 14
Citizens Proposals

1. When a citizen or employee of the Republic of Kosovo, who has no classification authority, considers that particular information under the state's control has the necessary values to be classified, he or she shall propose the classification of this information to the relevant institution. This institution shall decide within ten (10) days whether the information will be classified or not and shall notify the citizen or the employee of the decision taken.

2. From the moment of the proposal on the classification of relevant information, its possessor shall be obliged to protect the information from unauthorized access.

CHAPTER III
PERSONNEL SECURITY

Article 15
Personnel Security

Personnel security shall mean the set of measures and procedures based on which is assessed on whether a person, while maintaining his loyalty, reliability and security, can be authorized to access classified information without jeopardizing the security of said information.

Article 16
Personnel Security Clearance

1. The Vetting Authority shall issue the PSC only to the person who, after carrying out a security clearance procedure in accordance with the legislation into force, is designated as an acceptable security risk.

2. PSC shall clearly show the level of classified information, in which the person who has passed the security clearance procedure, can access. The PSC, for a certain level of classification, shall give the title holder access to information with the lowest classification level.

3. Each head of the public institution shall be obliged, within fifteen (15) days, to implement the decision of the Vetting Authority and shall not provide access to classified information to a person who has been denied a PSC.

Article 17
Criteria for knowing the classified information

1. The right to know, retain, manage and transfer classified information have only persons who:

1.1. obtain the right of knowing by the head of the institution or the Contractor's Industrial Security Officer due to the duty they perform;

1.2. are previously informed about the recognition of classified information security procedures and individual responsibilities for violations of security and have signed the statement of information retention;

1.3. are provided with PSC, except for cases with the recognition of classified information at the "restricted" level.

2. Only the President of the Republic of Kosovo, the President of the Assembly of Kosovo and the Prime Minister of the Government of the Republic of Kosovo shall be authorized to access classified information without being subjected to security verification provided that:

2.1. need to know such information;

2.2. be informed/briefed about the rules and security procedures for the protection of Classified Information;

2.3. have acknowledged that they have been notified of their responsibilities for the protection of classified information and have signed the statement of information retention.

Article 18
Lists of functions/positions for knowing the classified information

1. State institutions which, because of their activity, produce classified information or, while cooperating with other institutions benefit this category of information, have the duty to approve and send in writing to APCI a list of functions/positions that due to official duties can be acquainted with classified information and relevant PSC level.

2. The review of these lists shall be done periodically and in accordance with the changes in the organizational structure of the respective institution. For any eventual change, the head of the institution shall be obliged to notify APCI.

Article 19
Conditions for initiating the Security Clearance

1. Security Clearance procedure shall commence only after the applicant has accepted and

has given written consent to collect data and perform security clearance procedures, as per the security questionnaire requirements.

2. The handling of personal data and information collected in the Security Clearance process shall be carried out in accordance with the requirements of the applicable Law on the Protection of Personal Data.

Article 20
General Security Assessment Requirements

1. APCI, as the only Vetting Authority in the Republic of Kosovo responsible for conducting the Security Clearance Procedure, shall comply with the General Security Assessment Requirements, which include, but are not limited to the following:

1.1. the accurate verification of identity, generality and status of citizenship in the past and the present, for each person;

1.2. the data control, in function of the security of the Republic of Kosovo;

1.3. the applicant's financial status, in order to verify whether he may be under pressure due to instability, serious financial difficulties or the possession of any unjustified property;

1.4. the information on the education of a person after the age of eighteen (18) or for the period considered as appropriate by the vetting authority;

1.5. the information on the employment of the individual taking into consideration the references from previous jobs, based on employer reports;

1.6. the information on participation in military operations, the duration and the reason of termination of service in the military;

1.7. the overall assessment of whether a person may be pressured by an unfriendly foreign force.

Article 21
Essential Security Assessment Criteria

1. The essential criteria, used to assess existence or non-existence of an unacceptable security risk for classified information, which serve as the grounds for issuing, suspending or rejecting the equipment or holding of a PSC, are the cases where an individual result to:

1.1. have been, is or is trying to secretly engage, alone, in collaboration or as part composition of an illegal organization, in espionage, terrorism, betrayal, rebellion or armed violence against the constitutional order or has actively encouraged someone to engage in espionage, terrorism, betrayal, rebellion, sabotage or armed violence against the constitutional order;

1.2. has been or is a collaborator of espionage, terrorism, betrayal, rebellion, sabotage or armed violence against the constitutional order, there are suspicions that he/she has been a collaborator of representatives of organizations, foreign states, including intelligence services, which may violate the security of our country and/or NATO and EU Member States, unless such collaborations are authorized due to the duty;

1.3. has been or is a member of an organization that, by violent, hostile, illegal means, intends to overthrow the government or change the constitutional order;

1.4. has been or is a supporter of an organization as described in sub-paragraph

1.3 of this Article, or has been or is closely associated with any member of such an organization;

1.5. has intentionally concealed, misrepresented or falsified information of major importance, of a particular security nature or intentionally lied during the completion of a security questionnaire or a security interview;

1.6. has been convicted for one or more intentionally committed criminal offenses.

1.7. has a background of addiction to alcohol, use of illegal drugs, or abuse of legal drugs;

1.8. has bad ethics, criminal tendencies, and involvement in organized crime, which bears risk of weakness toward blackmail or can be seriously influenced under different pressures;

1.9. through concrete actions has expressed a lack of loyalty, trustworthiness, and security;

1.10. has committed a security breach or has repeatedly violated classified information security rules or has attempted and managed to perform an unauthorized activity in the classified information communication systems;

1.11. suffers from chronic mental illness.

2. The behaviour and circumstances of a spouse, cohabitant or close family member may also be considered relevant when assessing the safety.

Article 22
Security Interview

1. APCI may conduct interviews with persons who have applied to be equipped with a PSC and security clearance procedures have been undertaken in this regard.

2. APCI may conduct interviews with third impartial parties, who know the past and the activities of the person who has been subject to Security clearance.

Article 23
Validity of PSC

1. The TOP SECRET PSC shall be valid for a five (5) year period from the date of its issuance.

2. The SECRET PSC shall be valid for a seven (7) year period from the date of its issuance.

3. The CONFIDENTIAL PSC shall be valid for a ten (10) year period from the date of its issuance.

Article 24
Extending the PSC validity period in emergency circumstances

1. Under emergency circumstances, the APCI has the right to extend an individual's PSC validity period only one time, for up to sixty (60) calendar days during its validity cycle under the following conditions:

1.1. the individual, which requires the extension of the validity period, must have a valid PSC, issued in full procedure. The extensions of the validity period for a PSC issued under circumstances of urgency extraordinary emergency are exempted.

1.2. there is an official request clarifying the circumstances of extraordinary emergency and proves that circumstances do not allow applying under normal procedures for re-equipped with a new PSC, when:
1.3. an individual is exercising a short-term official duty, for which it was impossible to

follow the procedures according to foreseen time limits;

1.4. an individual needs to participate in an unpredicted international activity, which has rendered impossible to follow the procedures according to foreseen time limits;

1.5. an individual, who was equipped with a PSC, is in the circumstance that requires extending the time limits for participating in military missions abroad and it is impossible to apply according to normal procedures for re-obtaining a new PSC;

1.6. the extension of the PSC validity period under the aforementioned conditions is allowed for the PSC of “Confidential”, “Secret” and “Top Secret” levels.

2. All individuals to whom the PSC has been extended under extraordinary circumstances and conditions are obliged to state, in the writing, that they have understood all their obligations to protect the classified information.

Article 25
Repetition of Security Clearance

1. The persons to whom a PSC has been issued are subject to new security clearances during the following regular intervals:

1.1. every ten (10) years for persons with PSC of security that allows them access to classified information at “CONFIDENTIAL” level;

1.2. every seven (7) years for persons with PSC of security that allows them access to classified information at “SECRET” level;

1.3. Every five (5) years for persons with PSC of security that allows them access to classified information at “TOP SECRET” level.

2. The Vetting Authority or the head of the public institution, where the verified person is employed, may require that person to undergo a new Security clearance procedure even before the PSC validity expires, if there are indications that events have taken place or there are circumstances that raise doubts whether the verified person still constitutes an acceptable security risk.

Article 26
Refusal, Revocation, and temporary Suspension of PSC

1. APCI shall take a decision on refusal, revocation or suspension of PSC in cases where they have received information inferring that the equipment or possession of PSC by a specific person constitutes an unacceptable security risk in referral to the general and fundamental criteria of security assessment.

2. The notification of the decision taken by APCI to refuse, revoke or suspend the PSC is communicated in writing to the head of the concerned public institution which has initiated the request for performing the Security clearance procedure.

3. The procedures for verifying the security of personnel shall be determined by a sublegal act proposed by APCI and approved by the Government.

Article 27
The Right to Appeal

1. The person, to whom the Personnel Security Clearance was refused, has the right to lodge a complaint before the APCI within fifteen (15) days from the date of receipt of the notice.

2. Complaint shall be reviewed by the Complaints Commission.

Article 28
Complaints Commission

1. The Complaints Commission consists of five (5) members with one (1) representative of the following institutions:

1.1. Ministry of Defense;

1.2. Kosovo Police;

1.3. Kosovo Prosecutorial Council;

1.4. Kosovo Judicial Council;

1.5. Kosovo Intelligence Agency.

2. Upon the proposal by the heads of relevant institutions, the Government shall establish the Complaints Commission by virtue of a decision.

3. The mandate of the members of the commission is three (3) years, with the possibility of extension.

4. Members of the compliant commission should be professionals, with high integrity and to possess the highest level of PSC with information to be reviewed during the compliant procedure.

5. The person authorized by APCI shall present the case before the members of the Complaints Commission.

6. After reviewing the appeal, the Complaints Commission recommends the APCI Director to make a decision.

7. The work rules and procedures of the Complaints Commission and other issues related to the review of complaints are regulated by a sub-legal act proposed by APCI and approved by the Government.

Article 29
Deadlines and duration covering Security clearance

1. The overall deadline for carrying out the procedures for verifying and issuing the PSC by APCI is up to one hundred and twenty (120) calendar days.

2. This period may be longer when verifications are conditional on the performance of proceedings in cooperation with other countries' national security authorities.

3. The security vetting covers a period of not less than the last ten (10) years. In cases when such a period is deemed insufficient, the verification shall extend from the age of eighteen (18) to the current age.

4. If the Vetting Authority is unable to collect and compile all required information to conduct Security clearance within the time limits specified in paragraph 1 of this Article, the Vetting Authority may, by means of a decision, extend the time limit up to sixty (60) calendar days. The director of the respective institution shall be notified with the decision.

Article 30
Obligation of natural persons to protect classified information

1. Every person is obliged to protect classified information according to this law, regardless of how they have been granted access, received, or in any other form has managed to possess classified information.

2. When leaving a public institution, termination of employment relationship or any other contractual relationship, the official or the contracted person is prohibited from disclosing or removing classified information, in any way, from the control of the public institution.

Article 31
Inter-institutional cooperation

1. While performing the Security clearance procedure, the Vetting Authority cooperates with other public institutions of the Republic of Kosovo, as appropriate. Other public institutions are obliged to provide information upon request.

2. Cooperation between APCI and the Kosovo Intelligence Agency, the Ministry of Internal Affairs, the Ministry of Defence and other public security institutions will be of primary importance.

3. While conducting the security clearance procedure, the Vetting Authority shall cooperate with other States' counterpart institutions, as appropriate.

Article 32
Security Verification for the employees of the Kosovo Intelligence Agency

1. The Security clearance for Kosovo Intelligence Agency (hereafter: KIA) employees is performed by KIA in accordance with the respective law on Kosovo Intelligence Agency and by applying the criteria and standards established by this law regarding the security of personnel.

2. APCI provides KIA employees with PSC at KIA's request.

Article 33
Security File

1. The Security Certificate, the completed security questionnaire and all other relevant documents and materials related to Security clearance are kept by the Vetting Authority in the security file.

2. In addition to data specified under paragraph 1 of this article, the security file also contain information on subsequent changes regarding the information presented in the security questionnaire.

3. The head of the public institution and the verified person are obliged to immediately inform the Vetting Authority of any new development, events or circumstances that may result in the change of information provided in the security questionnaire or which in some other way may adversely affect the Security clearance of the concerned person.

4. The Head of the public institution has the obligation to inform APCI of any change that is related to officials who have PSC for transfer, promotion or dismissal.

5. The Vetting Authority classifies and maintains the security file in a way that gives the security file the level of classification and protection it deems necessary to safeguard the security interests of Kosovo.

Article 34
Data processing

1. The Vetting Authority may process the personal data of the verified person contained in the security file only for the purpose of exercising his/her functions and responsibilities as defined by this Law.

2. The Vetting Authority does not transfer personal data contained in the security file to other public institutions, unless there is a priority public interest, without prejudice to security interests of the Republic of Kosovo, and only for the needs of:

2.1. activities related to law enforcement;

2.2. activities related to disclosure;

2.3. Parliamentary investigations.

3. The public institution receiving such data may use and process them only if absolutely necessary and for the purposes specified under paragraph 2 of this Article and shall provide protection against unauthorized publication required for relevant classification level.

4. Law Enforcement agencies may use and process data specified in paragraph 2 of this Article for the purposes of criminal prosecution only as the last resort, when such data cannot be collected in other forms or if the criminal prosecution would be seriously hindered due to the lack of access to such data.

Article 35
Information on personal data

1. A person previously or currently subject to verification has the right to be informed by the Vetting Authority of all personal data collected and stored during the security clearance procedure. Information on such personal data is provided by the vetting authority on the basis of a written request submitted by the verified person.

2. The vetting authority shall reject the request if;

2.1. the publication of the information required would undermine public security or the security interests of the Republic of Kosovo; or

2.2. information should be kept confidential in order to protect the legitimate rights and interests of a third person or intelligence sources.

3. In case of a refusal of a request, the person requesting the information may file a complaint with the Information and Privacy Agency in accordance with the relevant law on personal data protection.

CHAPTER IV
INDUSTRIAL SECURITY

Article 36
Protection of classified information in the industrial field

1. Protection of Classified Information in the Industrial Area is done through the determination of measures and procedures for preventing unauthorized disclosure, loss or violation of Classified Information Security which is dealt with under the terms of a project/program /contract/classified subcontract.

2. Defining Standards when a natural or legal person has the ability to access classified information and possesses the capabilities required to administer this information before submitting an offer, negotiating or participating in a contract classified or work for a classified project, which includes access to classified information, is made in accordance with the requirements of the applicable legislation.

Article 37
The conditions for concluding a classified contract

1. Economic Operators interested in participating in procurement classified as ‘’SECRET’’ and ‘’CONFIDENTIAL’’, should be previously equipped with the required ISC level. The personnel representing the Economic Operator in classified procurement and other individuals who will have access to classified information must be appropriately certified in accordance with the requirements of the applicable legislation.

2. Economic Operators interested to participate in a classified procurement at the "RESTRICTED" level, are not equipped with ISC.

3. The personnel representing the Economic Operator in this procurement, and all persons who shall have access to classified information, are briefed of the security rules and procedures for the protection of classified information and individually accepting his or her responsibilities with regard to the protection of classified information and sign the statement for the storage of Classified Information prior to the commencement of classified procurement procedures.

Article 38
Obtaining an Industrial Security Clearance

1. The ISC shall be issued by APCI, based on requirements of the legislation into force.

2. For Economic Operators of other countries, the ISC shall be issued by the National Security Authorities or any Competent Security Authority of the country where the Economic Operator is registered. This certificate is considered valid for the purpose of participating in a classified procurement, only after written confirmation by the APCI, addressed to the Contracting Authority. Prior to confirming the ISC, APCI cooperates with Counterpart Authorities to carry out the relevant verifications.

3. Only after receiving the confirmation by APCI, the Contracting Authority shall grant the Economic Operator the right of access to classified information.

4. An economic operator providing security services may initiate procedures for provision with ISC before having a classified contract with public institutions, making a request to APCI with appropriate justifications for the needs of ISC.

5. Procedures for protection of classified information in the industrial field are defined by a sub-legal act in accordance with the relevant standards established by the North Atlantic Treaty Organization and the European Union proposed by APCI and approved by the Government.

Article 39
Basic criteria for assessment of industrial security

1. The verification procedures for issuance of ISC are carried out in accordance with the requirements of the applicable legislation and include aspects related to:

1.1. the Economic Operator's ownership structure, its financial viability, commercial reputation, technical capabilities and ability, as well as security aspects.

1.2. owners/shareholders and managerial staff who, due to their functions, will have access to classified information;

1.3. the person proposed in the position of security officer, his deputy and employee, who will have access to classified information.

2. APCI has the right to request information that it deems necessary from state institutions to verify the potential security risk of the Economic Operator and the categories of persons involved in classified procurements or pursuant to a classified contract.

Article 40
Conditions for concluding classified sub-contracts

1. The Contractor shall, prior to commencing the negotiations for concluding classified sub-contracts, at any case, first obtain the written approval of the Contracting Authority.

2. The Contracting Authority is not allowed to authorize a Contractor with whom it has concluded

a contract classified as ‘’TOP SECRET’’, to enter into contractual relations under the terms of a classified sub-contract.

3. All criteria for concluding/executing a classified contract are suitably applied with the subcontractor.

Article 41
Transportation and international visits

1. Transportation of classified material during implementation of the classified contract is carried out on land, sea, air and rail wayssubject to the safety rules as required by applicable legislation.

2. Classified Information security standards in the field of industrial security apply also during international visits.

CHAPTER IV
SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS

Article 42
Understanding the Security of Information Communication Systems

1. The security of classified information communication system is the set of standards for the protection of classified information, system services and resources in the means of communication that process, store or transmit classified information.

2. APCI is a national security accreditation authority of the electronic communication system that processes, stores, or transmits classified information.

Article 43
Guaranteeing information security

1. Guaranteeing Information Security is the practice of guaranteeing information security and risk management related to the use, processing and transmission of information or data in systems or other processing used for this purpose.

2. Guaranteeing information security is the protection of Communication and Information Systems in balance with the principles of Confidentiality, Integrity, Availability, Authentication and Non-Denial.

Article 44
Communication and Information Systems

1. Security management mechanisms and procedures are established to avoid, prevent, detect, resist, and recover from the impacts of incidents affecting classified information security objectives, including reporting security incidents. These measures include:

1.1. ensuring sufficient information to allow for investigation of intentional or accidental compromising of security objectives in accordance with the damage that may be caused;

1.2. reliable identification and authentication of persons, equipment and services authorized for access. The information controlling the access to the Communication and Information Systems shall be controlled and protected in compliance with the information classification level to which the system grants access;

1.3. controls access to classified information in accordance with the “need to know” principle;

1.4. management of integrity, origin and availability of classified information

1.5. controlling of Communication and Information System connections that handle Classified Information;

1.6. determining the Communication and Information System's security mechanisms reliability level;

1.7. assesses and verifies the proper functioning of the Information and Communication System's security protection mechanisms, throughout their lifespan;

1.8. investigation of users and communication and information systems activities;

1.9. ensuring the non-deniability that the sender of the information to be provided with the acknowledgement of the message from the receiver and the receiver to be provided with the sender's identity confirmation;

1.10. ensure that in case of a breach of security all legal and natural persons involved are informed that the information was violated.

CHAPTER VI
PHYSICAL SECURITY

Article 45
Physical Security

1. Physical security shall mean the set of physical, technical, electronic and procedural measures undertaken for the purpose of safeguarding areas, buildings, offices, rooms, spaces and equipment where the Classified Information is produced, recorded, used, transmitted, stored, archived and destroyed, including the risk management process for preventing unauthorized access to security areas.

2. State institutions are obliged to take measures for physical security of areas, buildings, offices, rooms, spaces and equipment where classified information is produced, recorded, used, transmitted, stored, archived and destroyed, in accordance with the standards and procedures established by sub-legal acts, which are in compliance with relevant standards determined by the North Atlantic Treaty Organization and the European Union.

3. The head of the institution shall approve the division of security areas by means of an Order, which shall be accompanied by the physical security plan and scheme of the building where classified information is stored and managed.

4. State institutions where classified information is processed, shall establish security structures/ security officers, depending on the volume of classified information.

5. In cooperation with state institutions, APCI shall periodically conduct electronic disinfection of buildings, offices, rooms, and premises where the Classified Information is produced, recorded, used, transmitted, stored, archived and destroyed.

6. The rules for the physical transport of classified information shall be defined by a sub-legal act.

Article 46
Classified Information Unit

1. Any public institution that produces and manages classified information must, within its own structure, appoint an officer or unit and provide the appropriate offices or premises where classified information is maintained and administered.

2. Public institutions shall maintain Registers for classified information according to the model established by the APCI.

3. The model for marking classified information shall be unique and determined by APCI and all public institutions shall be obliged to implement it.

4. The process of establishing, maintaining and managing the unit or concerned officer, offices or respective premises, including the maintenance of Registers for Classified Information, shall be determined by a sub-legal act approved by the Government, upon proposal of the APCI.

Article 47
Registers

Any head of a public institution that generates and manages classified information should establish minimum security standards for protection of classified information and appoint persons responsible for managing such information.

Article 48
Foreign information

1. State institutions shall safeguard classified information of foreign states or international organizations pursuant to standards that provide a degree of protection that is equivalent to that required by the state or international organization.

2. Any institution shall, prior to the signing of an agreement or technical protocol involving the exchange of Classified Information, consider the opinion of APCI.

3. The signing of a technical agreement or protocol involving the exchange of classified information shall be preceded by the signature of a general agreement on the provision of classified information between the national security authorities of the States Parties.

Article 49
NATO and EU classified information

1. The NATO and EU's classified information Registry System shall consist of the Central Registry Office in APCI, the Sub-register Office of NATO and EU classified information, and control points established in the Ministry and state institutions.

2. NATO and EU classified information shall be exchanged and managed only through this System.

3. NATO and EU classified information Register System shall be responsible for the registration, distribution and administration of classified information exchanged in the framework of cooperation with NATO and the EU.

4. State institutions shall be obliged to protect NATO and EU classified information according to standards that provide a level of protection equivalent to that required by NATO and the EU respectively.

5. The Central Registry Office of NATO and EU classified information in APCI shall be the structure responsible for managing the exchange, oversight and control of the security aspects of NATO and EU classified information within the Register System.

Article 50
Unclassified information of NATO, the EU, other states and international organizations

Unclassified information of NATO, the EU, other states and international organizations shall be the information that does not contain any of the classification levels but is used only for official reasons by state institutions and is not accessible to the public.

Article 51
Implementation of EU and NATO standards

1. APCI is a Security Authority in the Republic of Kosovo dealing with achievement of security standards for the protection of classified information in compliance with the requirements deriving from the security directives of NATO and EU.

2. APCI shall exchange classified information with all NATO and EU member states as well as with other States under the agreements signed and the relevant legislation in force.

3. Under the NATO and EU directives, APCI recognizes the security certificates of the personnel and industrial security certificates of the States with which it has signed security arrangements.

Article 52
Security breaches and disclosure of the classified information

1. A security breach occurs as a result of an act or omission by a person who acts in contravention of the security rules set forth in this Law and other sub-legal acts.

2. The disclosure of classified information occurs when, as a result of the breach of security, has caused a complete or partial disclosure of information to an unauthorized person.

3. Any breach or suspicion of a breach of security shall be reported immediately to the APCI Security Authority.

4. When known or when there is sufficient reason to assert that classified information is compromised or lost the security authority shall take measures in accordance with the law and sub-legal acts by:

4.1. inform the originating authority;

4.2. ensure that the case is being investigated by a neutral person regarding the matter;

4.3. determine the potential damage that is caused to the interests of the Republic of Kosovo or other states and organizations;

4.4. take appropriate measures to prevent a repetition;

4.5. notify the relevant authorities of the action taken.

5. Any person responsible for violation of the security rules set forth in this Law and sub-legal acts shall be liable to disciplinary penalties in accordance with the legislation in force.

6. Any person liable for compromise or loss of classified information shall be liable to disciplinary action or legal action in accordance with the relevant legislation into force.

Article 53
Loss of Classified Information

1. For any suspected loss, alleged breach of classified information security, and any alleged unauthorized access to Classified Information, all Authorized Classified Information Holders shall immediately report to their respective institution public, state prosecution and APCI.

2. APCI, upon its own initiative or at the request of the appropriate authority in cases of alleged violations with this Law, shall immediately take all necessary measures to:

2.1. notifying the state prosecutor in case the alleged violation is suspected of constituting a criminal offense;

2.2. inspecting the case;

2.3. identifying the cause of loss,

2.4. track down any opening by unauthorized persons to access such information;

2.5. removing any harmful effect and prevent further loss of classified information;

3. In case if the alleged violation is suspected of constituting a criminal offense, it shall notify the state prosecutor.

CHAPTER VII
PUNISHMENT PROVISIONS

Article 54
Criminal sanctions

1. Anyone who discloses or does not store classified information as a “CONFIDENTIAL” commits a criminal offense and is sentenced to imprisonment of one (1) to five (5) years.

2. Whoever discloses or retains classified information as “SECRET” commits a criminal offense and is sentenced to imprisonment of three (3) to ten (10) years.

3. Whoever discloses or retains classified information as “TOP SECRET” commits a criminal offense and is sentenced to imprisonment of five (5) to twelve (12) years.

Article 55
Inspection of Public Institutions and Economic Operators

1. APCI conducts inspections related to the implementation of security measures for the protection of classified information to public institutions and economic operators that have classified information.

2. The Inspection takes place out on a regular basis and with prior notice of the public institution.

3. The object of the inspection without prior notice shall be only that institution or economic operator for which there is reliable information that there is security breach regarding the administration of classified information.

4. Objects of inspection are the disciplines below:

4.1. Personnel security;

4.2. Industrial security;

4.3. Security of communication systems and information;

4.4. Physical security;

4.5. Administration of classified information.

5. APCI provides the physical security standards for the protection of classified information that administers and monitors their implementation according to the requirements set out in the legislation into force.

6. Upon completion of the inspection of the security measures, the APCI compiles a detailed report on the findings and proposes to take appropriate measures to increase the degree of security of classified information.

7. The report is addressed to the head of the relevant public institution.

8. In coordination with the head of the public institution, the plan for the implementation of the recommendations resulting from the inspection report is drafted.

9. APCI supervises the implementation of the recommendations to the public institution and if the same are not implemented within the foreseen deadlines, it notifies in writing the direct supervision of the relevant institution of the respective institution which was the inspection facilities.

CHAPTER VIII
AGENCY FOR PROTECTION OF CLASSIFIED INFORMATION

Article 56
The establishment and status of the APCI

1. APCI shall be established as a national security agency in the field of protection of classified information for all public institutions of the Republic of Kosovo and their contractors who in any form may have classified information under administration.

2. All employees and personnel engaged in APCI shall be politically impartial, professional, without prejudices in their judgments, and act only in accordance with the law and shall not take instructions from any person or institution.

3. APCI is a legal person and has its headquarters in Prishtina.

4. APCI has its own logo.

Article 57
Responsibilities of APCI in the field of Classified Information Protection

1. APCI is a central institution specializing in the field of classified information classified with the mandate to organize, direct and control measures for storing, classifying and administering classified information and verifying security for all institutions of the Republic of Kosovo as well as their contractors, who are responsible for:

1.1. policy drafting;

1.2. follow up of procedures;

1.3. surveillance of institutions and contractors in classified contracts;

1.4. security education;

1.5. security of personnel;

1.6. physical security;

1.7. information security;

1.8. industrial security;

1.9. providing communication and information systems;

1.10. negotiation development of the conclusion of security agreements with respective states;

1.11. supervise the implementation of treaties or international instruments on the protection of classified information and proposes to take appropriate measures.

2. APCI is the competent security authority for the Republic of Kosovo regarding the protection of classified information of foreign states and international organizations.

3. APCI cooperates with public institutions, economic operators concerned and counterpart authorities of states and international organizations for the performance of the tasks provided for by the legislation in force.

4. The APCI's strategic plan contains the general and specific objectives for achieving security standards for the protection of classified information, proposed to the Prime Minister for approval.

5. The organization and internal functioning of APCI is regulated by a sublegal act proposed by APCI and approved by the Prime Minister.

Article 58
Budget preparation and provision

1. The Director of APCI shall prepare and submit to the Prime Minister the draft annual budget for APCI.

2. APCI shall be an autonomous budget organization with its own budget code.

3. APCI shall be provided with an annual budget that is sufficient for performing duties and responsibilities aimed at protecting classified information in accordance with the legislation into force.

Article 59
Criteria for appointing the Director General

1. The criteria for appointing the General Director of APCI are as follows:

1.1. to be a citizen of the Republic of Kosovo;

1.2. to have a university degree;

1.3. to have at least eight (8) years of professional experience in security institutions, out of which at least (5) years of leadership experience;

1.4. has not been convicted of a criminal offense by a final decision;

1.5. has not been convicted for serious disciplinary violations, within the last five-year (5) period;

1.6. does not have a conflict of interest with the position or as foreseen in the Law on Prevention of Conflict of Interest in Exercise of Public Function.

Article 60
Appointment of the APCI Director

1. The Prime Minister nominates the Director of APCI.

2. In case of vacancy, the Prime Minister appoints the Director of APCI within twenty (20) working days.

3. The Director of APCI shall be dismissed through the same process by which he/she was appointed.

4. The Director of APCI, in accordance with this Law, the Regulation on Internal Organization and other applicable laws, shall be responsible for all aspects of the management of APCI.

5. In the execution of his/her responsibilities, the Director of APCI shall be assisted by the Deputy Director, the Heads of Organizational Units and appropriately qualified personnel, as needed, in accordance with the rules and procedures set forth in this Law and the Regulation on Internal Organization.

Article 61
Completion of the Director's mandate

1. The Director's mandate ends when:

1.1. has been convicted of a criminal offense;

1.2. reaches retirement age;

1.3. resigns;

1.4. due to the impossibility of exercising the duty for a period longer than six (6) months;

1.5. upon expiration of the mandate;

1.6. due to poorly documented performance.

Article 62
Director of APCI

1. The Director of APCI shall respond directly to the Prime Minister.

2. The Director of APCI shall:

2.1. advice the Prime Minister on matters related to the protection of classified information.

2.2. report and notify the Prime Minister on the activities of APCI;

2.3. provide information to the Prime Minister regarding the classification of information and security vetting;

2.4. protect and assist in the protection of classified information from unauthorized disclosure;

2.5. establish and coordinate relations with foreign counterpart agencies;

2.6. ensure that APCI performs work impartially and apolitically in relation to all communities and political entities;

2.7. ensure that APCI does not take any action aimed at influencing political processes, public opinion and media in Kosovo;

2.8. prepares the annual work report and propose the undertaking of necessary measures to increase the degree of classified information security;

2.9. initiate and sign Memorandums of Understanding and Cooperation with other institutions and other bodies;

2.10. reports to the respective parliamentary committee at least once a year.

Article 63
Deputy Director of APCI

1. The Deputy Director is appointed by the Prime Minister, upon the proposal of the Director from the staff of APCI.

2. The criteria for appointment and termination of the Director's mandate are also applied to the Deputy Director.

3. The Deputy Director of APCI shall assist the Director of APCI and govern the activities of organizational units of APCI under the supervision of the APCI's director.

4. The Deputy Director of APCI shall be dismissed through the same process by which he/she was appointed.

5. The Deputy Director of APCI shall temporarily act and exercise the powers of the Director of APCI when the Director is absent or incapacitated. In the event of permanent incapacity, the Deputy Director of APCI shall act and exercise the powers of the Director of APCI until the replacement of the Director of APCI.

Article 64
Specific Requirements for APCI Employees

1. Individuals selected for employment with APCI shall meet the strict security standards which are determined in accordance with the applicable law.

2. APCI shall not hire the candidates who fail to meet the security requirement.

3. In addition to the general employment requirements applicable to other government employees, special conditions may apply to the employees of APCI with regard to expertise, health, work duties and security requirements which are consistent with Kosovo's security interests.

4. The Regulation on APCI's Internal Organization shall set out the requirements for each position in APCI and shall set out the specific requirements for employment in APCI.

5. In accordance with the internal rules, APCI may contract third parties for ancillary services, where appropriate.

Article 65
Qualifications for Employment at APCI

1. The candidates for APCI shall meet the following requirements:

1.1. be a citizen of Kosovo;

1.2. have appropriate educational and professional qualifications as set out in the Regulation on Internal Organization;

1.3. carry out the medical examination required for the position;

1.4. be able to meet the security requirements to be determined by this law and sub-legal acts.

2. Rules and procedures on general requirements and recruitment procedures, employment relationships, training, career advancement and appointments of positions are set out in the Regulation on Employment Relationship in APCI, approved by the Government.

Article 66
Status of APCI employees

APCI employees shall have special status under this law. For issues not regulated by this law or the sub-legal acts deriving from this law, the legislation regulating civil service matters shall be appropriately applied.

Article 67
Rights of APCI Employees

1. The employees of APCI shall be entitled to:

1.1. permanent employment until retirement, with the exception of persons who have fixed-term employment contracts as well as those who are dismissed on reasonable grounds, in accordance with the legislation in force;

1.2. the leave in accordance with the legislation in force and resume the same or similar work when the leave ends;

1.3. remuneration for duties and performance of duties as defined by this law;

1.4. to receive salary, supplements and other allowances;

1.5. career advancement and professional development through training and other means;

Article 68
Prohibited behaviours of the employee

1. APCI employees cannot be members of political entities or receive instructions from them or persons outside APCI, and should not publicly express their political beliefs and preferences.

2. The employees may not perform any other paid public or professional activities or duties, which are inconsistent with the work of APCI, or create conflicts of interest.

3. APCI employees cannot be employed elsewhere as long as they have employment relations with APCI.

4. APCI employees are not entitled to actions aimed to stop the working activity or other forms aimed to collectively stop the work activity.

5. APCI employees, without prior consent of the Director of APCI, can not make public statements or otherwise comment on the work of APCI, or provide information to unauthorized persons on the data, documents, contacts, intentions, knowledge or staff of APCI.

6. If an employee is running in the elections for the Assembly of the Republic of Kosovo or for local government bodies, the same shall seek release from duty and may no longer be readmitted to APCI.

Article 69
Employee's Personal Legal Obligations

1. Each employee of APCI shall perform the duties assigned in accordance with this Law and relevant legislation into force and shall be personally responsible for the lawful implementation of APCI duties as defined by this Law and which are within the duties given to certain employees.

2. If an employee believes he/she has received an unlawful order, he/she shall inform the issuer of the order about his/her concern.

3. In case the instructor reiterates the order, the employee shall request a written confirmation of such order. If the employee still hesitates to execute the order, he or she shall convey the order to the principal supervisor of the issuer of the order and report the case to the Director.

4. The employee shall protect and shall not disclose, unless authorized, classified information that he or she has become aware on or off duty. This is an obligation that continues even after termination of employment relationship with APCI.

5. The employee shall not use the information obtained while on duty for purposes other than those set forth by law.

6. The employee shall protect and shall not disclose personal data and data related to the professional activity of people, which is protected by law and for which he/she has become aware while on duty.

Article 70
Salaries and Remuneration for the APCI Employees

1. Salaries and additional remuneration for the APCI staff shall be determined by the Government, in compliance with the work specifics and the special status of APCI.

2. In addition to the basic salary, the APCI employees may be entitled to other forms of allowances, such as wages and benefits, based on factors that include work-related difficulties, overtime or special skills.

Article 71
Termination of Employment

1. Employment of APCI employees may be terminated as follows:

1.1. voluntary resignation from the APCI;

1.2. termination of contract;

1.3. retirement age;

1.4. permanent disability to perform official duties due to health conditions, provided that the employee cannot be transferred to another appropriate position within APCI;

1.5. loss of Kosovo citizenship;

1.6. final conviction for a criminal offense;

1.7. dismissal from APCI due to disciplinary proceedings.

Article 72
Identity Cards

APCI employees shall be provided with identity cards. The type, form and content of the identity card of the APCI employee shall be determined by a decision issued by the Director of APCI.

Article 73
Regulation on Internal Organization

The internal organization of APCI shall be defined by the Regulation on Internal Organization, which is approved by the Prime Minister.

CHAPTER IX
TRANSITIONAL AND FINAL PROVISIONS

Article 74
Transitional Provisions

1. After the appointment, the Director of APCI in cooperation with the Director of KIA starts the procedures of transferring the verification department with the respective files to APCI.

2. Current employees of the Security Vetting Department within the KIA have the right to choose, through a voluntary declaration, continuation of work in APCI or remain within the KIA structures.

3. Employees of the former Security Vetting Department within the KIA who will continue to work in APCI shall be entitled to the work experience gained in KIA.
4. The APCI Director and the KIA Director may, through cooperation agreements, provide with the KIA's assets and staff until the functionality of APCI.

5. All security licenses issued by the Security Vetting Department within the KIA continue to remain in force until their expiration date.

6. Procedures for security verification initiated prior to the entry into force of this law shall be completed within a time period of three (3) months in accordance with the provisions of Law No. 03 / L-178 on Classification of Information and Security Clearances.

7. The Government provides an appropriate facility with security standards in the function of achieving the mandate of APCI for the protection of classified information of the Republic of Kosovo.

8. In any provision of the laws, sub-legal acts, the term KIA used in the sense of the vetting authority, with the entry into force of this law, shall be replaced by APCI.

Article 75
Sub-legal acts

1. The Government shall adopt sub-legal acts for the implementation of this law within six (6) months from its entry into force.

2. Sub-legal acts that are currently into force shall apply, provided that they are not in contradiction with this Law and until the issuance of sub-legal acts determined by this Law.

Article 76
Repeal

Upon entry into force of this Law, there shall be repealed the Law No. 03/L-178 on Classification of Information and Security Clearances.

Article 77
Entry into force

This Law shall enter into force fifteen (15) days after its publication in the Official Gazette of the Republic of Kosovo.

Law No. 08/L-175
9 February 2023

Promulgated by Decree No. DL-25/2023 dated 02.03.2023 President of the Republic of Kosovo Vjosa Osmani-Sadriu