



**Republika e Kosovës**  
**Republika Kosovo-Republic of Kosovo**  
*Kuvendi - Skupština - Assembly*

---

**Law No.03/L –178**

**ON CLASSIFICATION OF INFORMATION AND SECURITY  
CLEARANCES**

**Assembly of Republic of Kosovo,**

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

Adopts

**LAW ON CLASSIFICATION OF INFORMATION AND SECURITY  
CLEARANCES**

**CHAPTER I  
GENERAL PROVISIONS**

**Article 1  
Purpose**

The purpose of this law is to establish a uniform system for classifying and safeguarding information related to Kosovo's security interests and for security clearances of all persons who have access thereto.

**Article 2  
Scope of Application**

1. This law shall apply to all public authorities that exercise executive competences, legislative and judicial ones and towards the Presidency of Kosovo.

2. This law shall also apply to natural and legal persons who in any form may have access to classified information.

### **Article 3 Definitions**

1. Terms used in this law have the following meaning:

1.1. **Access** - the ability or opportunity to gain knowledge of classified information.

1.2. **Business Organization** - the meaning as defined in the Law on Business Organizations No. 02/L-123.

1.3. **Classification** - the act or process by which information is determined to be classified information.

1.4. **Classification Authority** - any person referred to in Article 7 of this Law having original or delegated authority to classify information.

1.5. **Classified information** - any information and material, the unauthorized disclosure of which would cause varying degrees of prejudice to security interests of the Republic of Kosovo.

1.6. **Classified contract** - any contract entered into by a public authority that contains information which are classified pursuant to this Law.

1.7. **Declassification** - the authorized change in the status of information from classified information to unclassified information.

1.8. **Document** - any physical or electronic mean on which the information is recorded.

1.9. **Downgrading** - a decision that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

1.10. **Foreign government information:**

1.10.1. information provided to the Republic of Kosovo by a foreign government or an international governmental organization;

1.10.2. information produced by the Republic of Kosovo pursuant to or as a result of a joint arrangement with a foreign government or international governmental organization with the expectation or requiring that such information, arrangement or both are to be held in confidence.

1.11. **Information** - knowledge that can be communicated in any form.

1.12. **Material** - includes documents as well as any machinery, equipment or weapons either manufactured or in the process of manufacture.

1.13. **Processing** - any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.14. **Public authority** - includes all institutions and entities referred to in Article 2.1 of this Law.

1.15. **Security interests** - refers to defense, intelligence and law enforcement activities, security or foreign relations of the Republic of Kosovo, including its territorial integrity, integrity of its institutions, the constitutional order and economic stability and development.

1.16. **Spouse** - any relationship established by lawful marriage and shall include for the purposes of this Law any extramarital relationship between two natural persons.

1.17. **Agency** - the Kosovo Intelligence Agency.

1.18. **Head of a public authority** - for the purposes of this Law the highest civil servant of a public authority at the level of a Permanent Secretary, Chief Executive Officer or any other equivalent position.

1.19. **Necessity for knowledge** – the decision taken from an authorized holder of classified information that the next receiver needs to have access to specific classified information to work or help in a legal function and authorized by government, official duty or public function.

1.20. **Authorized holders of classified information** – a person possessing the classified information, has a valid security permit and fulfils other conditions that allow access to classified information, unless otherwise determined by the law.

## **CHAPTER II CLASSIFICATION OF INFORMATION**

### **Article 4 Classification Criteria**

1. Information shall be classified only if necessary and if
  - 1.1. the classification is conducted by a competent Classification Authority as determined in this Law;
  - 1.2. the information is owned by, produced by or for, or is under the control of the Republic of Kosovo;
  - 1.3. the information falls within one or more of the following categories:
    - 1.3.1. public security;
    - 1.3.2. defense, military plans, weapons systems, or operations;
    - 1.3.3. foreign relations and foreign government information, including confidential sources;
    - 1.3.4. intelligence and law enforcement activities, including intelligence methods and sources;
    - 1.3.5. systems, installations, infrastructures, projects, plans or protection services relating to security interests of the Republic of Kosovo;
    - 1.3.6. scientific, technological, economic, financial activities related to security interests of the Republic of Kosovo; and
  - 1.4. the Classification Authority decides for the level of classification of information depending on the level of damage that would come from its unauthorized publication in security interests of the Republic of Kosovo.

### **Article 5 Prohibition of Classification**

1. Classified information shall be prohibited to:
  - 1.1 conceal violations of law, abuse of authority, inefficiency or administrative error;
  - 1.2 prevent embarrassment to a person, public authority or organization;

1.3 restrain competition; or

1.4 prevent or delay the release of information, which is not clearly related to security issues.

## **Article 6 Classification Levels**

1. Information may be classified at one of the following levels:

1.1 “TOP SECRET” shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to security interests of the Republic of Kosovo;

1.2. “SECRET” shall be applied to information the unauthorized disclosure of which could seriously damage security interests of the Republic of Kosovo;

1.3. “CONFIDENTIAL” shall be applied to information the unauthorized disclosure of which could damage security interests of the Republic of Kosovo;

1.4. “RESTRICTED” shall be applied to information the unauthorized disclosure of which could be disadvantageous to the security interests of the Republic of Kosovo.

## **Article 7 Classification Authority**

1. Notwithstanding paragraphs 2 and 3 of this Article, classification authority shall be vested solely in the originator of the information.

2. “TOP SECRET” original classification authority may be exercised only by:

2.1. the President of Kosovo,

2.2. the President of the Assembly of Kosovo,

2.3. the Prime Minister,

2.4. the Chair of the Kosovo Security Council;

2.5. the Director of the Kosovo Intelligence Agency;

2.6. the Director General of the Kosovo Police;

2.7. the Commander of the Kosovo Security Force;

3. The persons listed in paragraph 2 of this Article may delegate their classification authority to their direct subordinate officials.

4. "SECRET", "CONFIDENTIAL" and "RESTRICTED" original classification authority may be exercised only by Permanent Secretaries, Chief Executive Officers or Executive Directors of public authorities and other equivalent senior positions, unless they delegate such classification authority to subordinate senior officials.

5. Officials authorized to classify information at a specified level shall also be authorized to classify information at a lower level.

6. Delegations of classification authority shall be limited to the minimum required to implement this Law. Authorities referred to paragraphs 2 and 4 of this Article, shall be responsible for ensuring that any delegation of classification authority to subordinate officials is withdrawn if there is no demonstrable and continuing need for the officials to exercise such classification authority. Classification authority delegated to officials pursuant to paragraphs 2 and 4 of this Article shall not be sub-delegated to any other person.

7. Each delegation of classification authority shall be in writing and shall identify the official clearly by name and position title as well as the classification authority.

8. The Agency shall establish, maintain and regularly update a register of officials with "TOP SECRET", "SECRET" and "CONFIDENTIAL" classification authority.

9. When an official, employee or contractor of a public authority, who does not have original or delegated classification authority, originates information, which in the opinion of that person requires classification, he/she shall protect such information in a manner consistent with this Law and immediately transmit the information to the official, which has appropriate classification authority and responsibility for the subject-matter. The person with classification authority and responsibility shall decide within eight (8) days whether to classify this information.

## **Article 8**

### **Classification Decision**

1. A Classification Authority shall decide whether to classify information and determine the classification level of the information as of the moment when the information is originated.

2. The decision whether to classify information and its level of classification shall be based on an evaluation of the possible harmful effects of unauthorized disclosure of such information to the security interests of the Republic of Kosovo. The evaluation shall be in writing and shall be attached as an annex to the document, which contains the classified information.

3. A Classification Authority shall avoid over-classification of information and shall assign to information only such classification level that is necessary to safeguard the interests of the Republic of Kosovo.

### **Article 9**

#### **Classification of parts of a document and of separate documents**

1. Individual pages, paragraphs, Articles, annexes, appendices, attachments and enclosures of a given document, which require different classifications, shall be marked accordingly. The classification of the document as a whole shall be that of the most highly classified part.
2. The classification of a letter or a note covering enclosures shall be as high as the highest classification level of its enclosures. The Classification Authority shall indicate clearly at which level the letter or note should be classified if detached from its enclosures.
3. A Classification Authority may classify information contained in separate documents, which separately are not considered to require classification, but which when combined as a whole require protection from unauthorized disclosure.

### **Article 10**

#### **Marking**

1. All documents containing classified information shall on their face have the following marking:
  - 1.1. Classification level;
  - 1.2. Date of classification
  - 1.3. Name and position title of the Classification authority;
  - 1.4. Public authority of origin;
  - 1.5. Distribution list, if any; and
  - 1.6. Declassification information.
2. Markings shall be applied as follows:
  - 2.1 on "RESTRICTED" documents, by mechanical or electronic means;

2.2 on “CONFIDENTIAL” documents, by mechanical means and by hand or by printing on pre-stamped registered paper;

2.3 on “SECRET” and “TOP SECRET” documents, by mechanical means and by hand.

3. Unless otherwise provided by treaty, to which the Republic of Kosovo is a party, or any other binding international instrument, the marking of a document of a foreign government or international organization containing classified information shall retain its original classification markings or may be assigned classification under Kosovo legislation classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

### **Article 11 Duration of Classification**

1. Information shall remain classified only as long as it requires protection. Unless the Classification Authority has established a specific date or event for declassification taking into account the duration of the sensitivity of the information the following timelines shall apply for automatic declassification:

1.1. information classified as “RESTRICTED” shall be declassified one (1) year from the date of the classification decision;

1.2 information classified as “CONFIDENTIAL” shall be declassified five (5) years from the date of the classification decision

1.3 information classified as “SECRET” shall be declassified fifteen (15) years from the date of the classification decision; and

1.4 information classified as “TOP SECRET” shall be declassified twenty five (25) years from the date of the classification decision.

2. In the event that the Classification Authority considers that information requires protection for a longer period of time than provided for under paragraph 1, it shall take a new classification decision in accordance with Article 8 of this law. Such decision shall not be taken earlier than six months before the date of declassification according to paragraph 1 of this Article.

### **Article 12 Declassification**

1. Information shall be declassified as soon as it no longer requires protection and does not meet the criteria for classification of information pursuant to this Law.



2. The Classification authority, which has originated classified information, shall conduct the declassification of such information.
3. The decision for declassification of information shall be in writing and shall provide reasons for the declassification. The decision shall be communicated immediately by the Classification authority to all public authorities and other addressees, to whom they have sent or copied the document.
4. The Classification Authority which has originated classified information shall conduct a review every five (5) years to verify if classified information continues to require protection in accordance with the classification criteria established by this Law. Should the Classification Authority come to the conclusion that the classified information does not meet classification requirements, it shall immediately issue a declassification decision.
5. Notwithstanding the requirement for a mandatory review pursuant to paragraph 4 of this Article, a Classification Authority referred to in paragraph 2 of this Article shall immediately declassify information if it becomes aware of facts that clearly indicate that the information does not require protection according to classification criteria established by this Law.
6. Classified foreign government information may be declassified by Kosovo authorities only if such information has been declassified by the foreign classification authority that has classified the information.

### **Article 13** **Downgrading and Upgrading of Classification Levels**

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 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 classification level.
3. Paragraphs 3 and 4 of Article 12 of this law shall apply mutatis mutandis to the downgrading of classification levels of classified information.
4. Classified foreign government information may be downgraded by Kosovo authorities only if and to the extent the foreign classification authority, which has the competence to downgrade said information, has downgraded the classification level of such information.
5. The Classification Authority, which has originated classified information, may upgrade the classification level of a classified information if such upgrading is necessary to protect security interests of the Republic of Kosovo and if it meets the requirements set

out in Article 6 of this Law for the respective classification level to which classification will be upgraded.

#### **Article 14 Challenge of Classification**

1. Authorized holders of classified information, who, in good faith, believe that its classification status is improper or not justified according to law, may propose to the Classification Authority that has originated the classified information to review the classification status and eventually declassify the information or downgrade the classification level.
2. The Classification Authority shall consider the proposal and shall inform such authorized holder in writing of the decision within (eight) 8 days from the day of the receipt of the proposal.
3. Persons, who have been denied access to classified information, may challenge the classification decision by filing a request for review with the Classification Authority that has originated the classified information. Such request for review shall be filed within 3 (three) days from the date of receipt of the decision for access to classified information. The provisions on administrative review of the Law on Administrative Procedures shall apply accordingly and does not have a suspension effect.

#### **Article 15 Derivative Classification**

1. Authorized holders of classified information who reproduce, extract, summarize, incorporate, paraphrase, restate or generate in new form classified information shall apply classification markings consistent with classification markings that apply to the source information.
2. Authorized holders of classified information who use derivative classification markings shall
  - 2.1. observe and respect original classification decisions; and
  - 2.2. carry forward to any newly created documents the pertinent classification markings.
3. For information derivatively classified based on multiple sources the derivative classifier shall carry forward
  - 3.1. the highest classification level of any of the multiple sources;

3.2. the date or event of declassification that corresponds to the longest period of classification among the sources; and

3.3. a listing of these sources on or attached to the official file or record copy.

### **Article 16**

#### **Preparation and Translation of Classified Information**

Documents containing information classified as “CONFIDENTIAL” or above shall be typed, translated, stored, copied or in any other form reproduced only by persons who have a valid security certificate for the classification level of the respective document.

### **Article 17**

#### **Distribution of Classified Information**

1. Documents containing information classified “CONFIDENTIAL” or above shall be distributed only to persons who have a valid security certificate and a need to know.

2. The initial distribution of classified information shall be specified by the authority originating the information.

3. Security standards to be applied for the purpose of distributing classified information shall be established by secondary legislation.

### **Article 18**

#### **Transfer of Classified Information**

1. Classified information shall not be removed from official premises and in no other way transferred to other public authorities unless the originating authority authorizes such transfer. The public authority receiving classified information shall not disclose such information without the approval of the originating authority.

2. Classified information shall be transferred only to public authorities:

2.1. that meet information security standards as set out in this Law or subsidiary legal acts; and

2.2. whose personnel has an appropriate security clearance and a need to know.

3. The public authority transferring classified information shall keep record of all documents transferred and public authorities receiving such documents.

4. In the event of a transfer of classified information together with a transfer of functions the receiving public authority shall be considered to be the originating authority. This shall not apply in the event that classified information is transferred to another public authority for storage purposes only.

5. In the event that the originating authority has ceased to exist and no transfer pursuant to paragraph 4 of this Article, to a successor authority has been effected, the public authority in possession of such classified information shall be considered to be the originating authority.

6. Security standards applied for the purpose of transferring classified information shall be established by secondary legislation.

### **Article 19** **Physical Security and Information Security**

All public authorities shall ensure physical security and information security related to classified information in accordance with standards and procedures established by secondary legislation, which shall be in compliance with relevant standards established by the North Atlantic Treaty Organization and European Union security regulations.

### **Article 20** **Loss of Classified Information**

1. All authorized holders of classified information shall immediately report to their respective public authority any loss, suspected loss, any breaches or suspected breaches of security of classified information and any actual or suspected unauthorized access to classified information. The respective public authority shall immediately inform the Agency of such event and take all necessary measures to:

1.1. investigate the event;

1.2. identify the causes of the loss;

1.3. track any disclosure to persons not authorized to access such information;

1.4. remove any harmful effects and prevent further loss of classified information;

1.5. initiate disciplinary, criminal and other available legal procedures against persons who have caused the loss of classified information and who have received such information without authorization.

## **CHAPTER III PERSONNEL SECURITY**

### **Article 21 General Provisions**

1. Every person has the duty to protect classified information in accordance with this Law irrespective of how such person has gained access to or has received or in any other form established possession of classified information.
2. When leaving the public authority, termination of working relation or any other contractual arrangement, an official or contracted person of a public authority shall be prohibited to remove classified information from the public authority's control.

### **Article 22 General Rules on Access to Classified Information**

1. A person may have access to information classified as "CONFIDENTIAL", "SECRET" or "TOP SECRET" provided that person:
  - 1.1. has a valid security certificate;
  - 1.2. has a need-to-know for carrying out his/her official mission or duty; and
  - 1.3. has signed an approved nondisclosure statement.
2. Only the President of the Republic of Kosovo, the President of the Assembly of Kosovo and the Prime Minister are authorized to access classified information for the purpose of discharging their official duties without fulfilling the requirements set out in paragraph 1 of this Article provided they have a need to know.
3. All persons authorized to access classified information pursuant to paragraph 1 and 2 of this Article shall sign a statement of non-disclosure attesting that they:
  - 3.1. access and use classified information solely for the purpose of discharging their official duties;
  - 3.2. are familiar with the provisions of this Law and other relevant legislation concerning access to and safeguarding of classified information and the respective legal sanctions for non-compliance;
  - 3.3. will handle classified information in their possession strictly in accordance with the provisions of this Law and any other relevant legislation;

- 3.4. will not disclose to any unauthorized person classified information in their possession and any knowledge related thereto during and after their term of office.
4. Access to information classified as “RESTRICTED” shall be permitted without a security certificate to all officials and contracted persons who
- 4.1. have a need-to-know for carrying out his/her official mission or duty;
  - 4.2. have signed a non-disclosure statement set out in paragraph 3 of this Article.

### **Article 23**

#### **Request for Access to Classified Information**

1. The head of a public authority where classified information is generated, processed, stored, received or transmitted shall be responsible for ensuring that all persons having access to such classified information fulfill the conditions set out in Article 22 of this law permitting access to classified information.
2. The head of a public authority referred to in paragraph 1 of this Article shall ensure that all security measures are taken by the public authority as required by this Law and any secondary legislation issued there under to ensure security of classified information.
3. All requests for access to classified information in possession or in control of a public authority shall be submitted to the head of the public authority who shall make a decision permitting or denying access to classified information in accordance with this Law.
4. The head of a public authority, while retaining residual responsibility, may delegate the responsibility to decide on access to classified information and to administer classified information within the public authority pursuant to this Law to a senior official of the public authority who has the necessary security clearance and adequate professional qualifications and experience to exercise the delegated responsibility.

### **Article 24**

#### **Vetting Authority**

1. The Kosovo Intelligence Agency shall be the Vetting Authority responsible for conducting security clearance procedures as set out in this Law for all public authorities of the Republic of Kosovo and their contractors.
2. The Kosovo Intelligence Agency shall establish a special Vetting Department exclusively responsible for conducting security clearance procedures. The Vetting Department and all its employees and assigned personnel shall be strictly politically neutral, professional, unbiased in their judgment and act solely in accordance with the law and not be subject to instructions or guidelines from any person or institution.

3. Requests for conducting a security clearance shall be submitted by the respective head of public authority in writing to the head of the Vetting Department specifying the classification level for which security clearance is required.

### **Article 25 Security Certificate**

1. The Vetting Authority shall issue a security certificate to a person only if such person, after having conducted a security clearance procedure in accordance with this Law, has been determined to be an acceptable security risk.
2. The security certificate shall clearly indicate the level of classified information to which the cleared person may have access. A security certificate for a given classification level shall give the holder access to information with a lower classification level.
3. Every public authority shall respect the decision of the Vetting Authority and shall not allow a person who has been denied a security clearance access to classified information.

### **Article 26 Unacceptable Security Risk**

1. A person shall be an unacceptable security risk if there are clear indications that he/she
  - 1.1. is not loyal to the Republic of Kosovo and its constitutional order and values;
  - 1.2. has a preference or may be manipulated, induced or blackmailed to help a group, person, organization or foreign government in a manner detrimental to the security interests of the Republic of Kosovo; or
  - 1.3. displays conduct that indicates a personality of emotional or mental disorder, lack of judgment or discretion, dishonesty, self-control or lack of willingness to comply with rules in a manner that raises doubts about that person's reliability, trustworthiness and ability to protect classified information.
2. A person may be considered an unacceptable security risk if his/her spouse fulfills one or more of the criteria listed in sub-paragraph 1.1. up to 1.3. of this Article.

### **Article 27 General Rules on Security Clearance Procedures**

1. The purpose of a security clearance procedure is to reveal whether a person constitutes an unacceptable security risk as set out in Article 26 of this law.

2. Refusal to fully participate in the security clearance procedure shall automatically constitute an unacceptable security risk.
3. When conducting a security clearance procedure and deciding whether a person constitutes an unacceptable security risk, the Vetting Authority shall pay due regard to the whole person and shall evaluate information on the person's conduct in line with, but not limited to, the following factors:
  - 3.1. the nature, extent, and seriousness of the conduct;
  - 3.2. the circumstances surrounding the conduct;
  - 3.3. the frequency and recency of the conduct;
  - 3.4. the person's age and maturity at the time of the conduct;
  - 3.5. the extent to which participation is voluntary;
  - 3.6. the presence or absence of rehabilitation and other permanent behavioral changes;
  - 3.7. the motivation for the conduct;
  - 3.8. the potential for pressure, coercion, exploitation or duress; and
  - 3.9. the likelihood of continuation or recurrence.
4. Any doubt concerning a person being vetted shall be resolved in favor of Kosovo's security interests.
5. Any security clearance procedure shall be conducted with the consent of the respective person unless otherwise determined by law. The consent shall be given in writing but not in electronic form. Persons subject to security clearance procedures shall be eighteen (18) years of age or older.
6. A security clearance procedure of a spouse, as may be required by paragraph 3 of Article 32 of this law, shall be conducted only with the consent of the spouse. Paragraph 5 of this Article shall apply accordingly. Refusal of the spouse to participate in the security clearance procedure may result in denial of security clearance.
7. Failure to obtain a security certificate shall result in the transfer of the official person to another equivalent post for which no security clearance is required. If this is not possible, then the failure to obtain a security certificate shall result in the termination of the person's employment or service contract with the respective public authority if the possession of a valid security certificate is a necessary requirement for the respective employment or service.



**Article 28**  
**Rights of the person undergoing a security clearance**

1. In the event that the security clearance procedure gives reasons to believe that the person is an unacceptable security risk, that person shall be given the opportunity to be heard before a decision is made. Such person may be assisted by an authorized person during the hearing.
2. The hearing shall be conducted in a manner that protects legitimate privacy rights and interests of the person.
3. No hearing shall be held if the conduct of a hearing would be detrimental to legitimate security or political interests of the Republic of Kosovo.
4. A person who has been found to be an unacceptable security risk shall be issued a decision in writing denying the issuance of a security certificate. Such person may file an appeal against the decision within fifteen (15) days from the day he/she has been notified of the decision. The appeal shall be filed and processed in accordance with the Law on Administrative Procedures and does not have suspension effect.

**Article 29**  
**Security Questionnaire**

1. All persons undergoing a security clearance shall fill out a security clearance questionnaire which shall contain at a minimum the following:
  - 1.1. name, surname, including previous names and surnames;
  - 1.2. date and place of birth;
  - 1.3. nationality, including previous or multiple nationalities;
  - 1.4. civil status;
  - 1.5. dwellings inside and outside of Kosovo;
  - 1.6. current profession;
  - 1.7. contact data of current and previous employers;
  - 1.8. number of children;
  - 1.9. name, surname, place and date of birth, nationality and place of residence of persons living in common household;

1.10. name, surname, place and date of birth, nationality and place of residence of parents, step-parents, foster parents or custodians;

1.11. education and employment history;

1.12. military service;

1.13. all ID and travel documents held and their numbers;

1.14. information on bankruptcy or liquidation procedures or enforcement measures taken during the last ten (10) years;

1.15. information on current financial situation, including debts and other financial obligations;

1.16. contacts to foreign intelligence services, domestic and foreign media and political parties;

1.17. contacts to organizations acting contrary to the constitutional order of the Republic of Kosovo;

1.18. criminal records, minor offences and ongoing criminal proceedings;

1.19. disciplinary measures taken;

1.20. alcohol and drug usage;

1.21. mental, and emotional disorders, and current health condition;

1.22. information on relatives in or other connections to foreign states;

1.23. previous security clearances;

1.24. two references.

2. The security questionnaire shall include a statement to be signed by the person undergoing the security clearance authorizing the Vetting Authority to access private data held by financial, medical and other institutions related to this person for the purpose of verifying the information provided in the security questionnaire. Article 27, paragraph 2 of this law shall be applied accordingly in the event that the person refuses to sign such statement.

**Article 30**  
**Simple Security Clearance Procedure**

1. A simple security clearance procedure shall be applied to persons who shall have access to information classified not higher than “CONFIDENTIAL”.
2. The Vetting Authority shall verify whether the information provided in the completed security questionnaire examination are complete and accurate. For this purpose, the Vetting Authority shall inspect civil status registers, criminal record registers and any other official national or international registers or databases.
3. A simple security clearance procedure shall be completed within three (3) months from the day the procedure has been initiated.

**Article 31**  
**Extended Security Clearance Procedure**

1. An extended security clearance procedure shall be applied to persons who shall have access to information classified not higher than “SECRET”.
2. For the purpose of conducting an extended security clearance procedure, the Vetting Authority shall take all actions authorized pursuant to paragraph 2 of Article 30 of this law and in addition to that it shall:
  - 2.1. order a medical examination if this is considered necessary to verify information concerning alcohol and drug usages, addictions or any mental or emotional disorders;
  - 2.2. request information from Kosovo’s security institutions if this is considered necessary to verify information related to contacts to foreign governments and intelligence services and related information;
  - 2.3. access bank account balances and request debt related information from banks and other financial institutions;
  - 2.4. conduct interviews with neighbors at the place of residence and with current and former employers.
3. An extended security clearance procedure shall be completed within six (6) months from the day the procedure has been initiated.

**Article 32**  
**Special Security Clearance Procedure**

1. A special security clearance procedure shall be applied to persons who shall have access to information classified as “TOP SECRET”.
2. For the purpose of conducting an extended security clearance procedure, the Vetting Authority shall take all actions authorized pursuant to paragraph 2 of Article 30 and paragraph 2 of Article 31 of this law and shall require the spouse to complete a security questionnaire. In addition to that it shall conduct interviews with the person undergoing a security clearance, the spouse and the persons listed as references.
3. A special security procedure shall be completed within nine (9) months from the day the procedure has been initiated.

**Article 33**  
**Extension of Timeline for Security Clearances**

In the event that the Vetting Authority is not able to collect and process all required information for conducting a security clearance within the timelines set out in Articles 30, 31 and 32 of this law, it may by decision in writing communicated to the person undergoing the security clearance extend the timeline for a non-renewable period of not more than three (3) months.

**Article 34**  
**Security Clearance Cooperation**

1. When conducting a security clearance procedure, the vetting authority may cooperate with agencies of foreign governments or international governmental organizations responsible for security clearance as may be set out in international treaties to which the Republic of Kosovo is a party or other relevant binding international instruments. The Vetting Authority shall thereby respect relevant legislation on data protection.
2. When conducting a security clearance procedure, the vetting authority may cooperate with other public authorities as may be needed. Other public authorities shall provide available assistance as may be required.

**Article 35**  
**Repeat of Security Clearance**

1. Persons who were issued a security certificate shall undergo a new security clearance at regular intervals as follows:

- 1.1. every ten (10) years for persons with a security certificate permitting access to information classified as “CONFIDENTIAL”; and
  - 1.2. every five (5) years for persons with a security certificate permitting access to information classified as “SECRET” or “TOP SECRET”.
2. The Vetting Authority or the head of the public authority where the vetted person is employed may request this person to undergo a new security clearance procedure even before the expiry of the validity of the security certificate if it has indications that events have occurred or circumstances have emerged that raise doubts as to whether the vetted person is still an acceptable security risk.

### **Article 36 Revocation of Security Certificate**

1. The Vetting Authority shall revoke a security certificate before expiry of its validity if:
  - 1.1. a new security clearance procedure has resulted in a decision that the vetted person is no longer an acceptable security risk;
  - 1.2. the vetted person has resigned or has been transferred to a new duty or mission where he/she has no need to access classified information;
  - 1.3. the vetted person has been found guilty of a criminal or disciplinary offence that is so serious that the person has to be considered an unacceptable security risk.
2. In the event that a new security clearance procedure is initiated pursuant to paragraph 2 Article 35 of this law, the Vetting Authority may suspend the validity of the security certificate until completion of the security clearance procedure.
3. Revocation of a security certificate shall result in termination of the person’s employment or service contract with the respective public authority if the possession of a valid security certificate is a necessary requirement for the respective employment or service.

### **Article 37 Provisional Access to Classified Information**

1. In exceptional cases, when there is a compelling official need to access classified information, the head of a public authority may permit a person who has not an appropriate security clearance for the required classification level access to classified information after giving the vetting authority prior notification provided

- 1.1 the person has a valid security certificate though not for the classification level to which access is sought;
  - 1.2 the vetting authority does not object in writing within fifteen (15) days from the receipt of the notification.
2. Permission for provisional access to classified information shall be valid for a non-renewable period not exceeding six (6) months.
  3. No provisional access to information classified as “TOP SECRET” shall be permitted.
  4. The head of the public authority shall keep record of name, surname, title and rank of all persons who have been permitted provisional access to classified information, including the documents they have inspected or used and immediately inform the Vetting Authority thereof.

**Article 38**  
**Emergency Access to Classified Information**

1. In a state of emergency or during extraordinary operations the head of a public authority may grant in writing persons who have no security clearance access to classified information provided that there:
  - 1.1. is an absolute official need for that that person to access such information;
  - 1.2. are no reasonable doubts about the person’s loyalty, trustworthiness and reliability.
2. The head of the public authority shall keep record of name, surname, title and rank of all persons who have been permitted provisional access to classified information, including the documents they have inspected or used and immediately inform the Vetting Authority thereof.

**Article 39**  
**Meetings and Conferences**

The head of a public authority shall ensure that all officials or contracted persons attending a meeting or conference where classified information are produced or distributed have appropriate security clearance and have been duly authorized to attend such meeting or conference.

**Article 40**  
**Security Register**

1. Every head of a public authority shall establish and regularly update a security register, which shall contain information on name, surname, post and rank of the persons authorized to access classified information held by the respective public authority.
2. The Vetting Authority shall maintain a central register of name, surname, post and rank of all persons in Kosovo authorized to access information classified as “CONFIDENTIAL”, “SECRET” or “TOP SECRET”.

**CHAPTER IV**  
**FILES AND DATA PROTECTION**

**Article 41**  
**Security File**

1. The security certificate, the completed security questionnaire and all other documents and materials related to the security clearance shall be kept by the Vetting Authority in a security file.
2. In addition to data referred to in paragraph 1 of this Article, the security file shall also include information on any subsequent changes to the information provided in the security questionnaire.
3. The head of a public authority and the vetted person shall have the duty to immediately inform the Vetting Authority of any new developments, events or circumstances that may result in a change of information provided in the security questionnaire or that may otherwise affect the security clearance of the respective person.
4. The vetting authority shall classify and keep the security file in a manner that accords to the security file the level of classification and protection that the Vetting Authority considers necessary to safeguard Kosovo’s security interests.

**Article 42**  
**Deletion of security file**

The security file shall be deleted ten (10) years from the day when the vetted person has ceased to have a valid security certificate unless the vetted person consents to a longer period of time or if a longer period of time is in the interest of the Republic of Kosovo.

**Article 43**  
**Processing of Data**

1. The vetting authority may process personal data of the vetted person contained in the security file for the sole purpose of exercising its functions and responsibilities vested in it pursuant to this Law.
2. Personal data contained in the security file shall not be transferred by the Vetting Authority to other public authorities unless there is an overriding public interest without compromising the security interests of the Republic of Kosovo and for the sole purpose of:
  - 2.1 law enforcement activities;
  - 2.2 intelligence related activities;
  - 2.3 parliamentary inquiries.
3. The public authority receiving such data may use and process them only if absolutely necessary and solely for the purposes specified in paragraph 2 of this Article and it must accord them protection from unauthorized disclosure required for the respective classification level.
4. Law enforcement agencies may use and process data referred to in paragraph 2 of this Article for the purposes of criminal prosecution only as a last resort when such data cannot be collected otherwise or if criminal prosecution would be seriously hindered without having access to such data.

**Article 44**  
**Information on Personal Data**

1. A formerly or currently vetted person shall have 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 shall be granted by the vetting authority upon a written request filed by the vetted person.
2. The vetting authority shall decline the request if:
  - 2.1. disclosure of the requested information would be detrimental to public security or security interests of the Republic of Kosovo; or
  - 2.2. the information must be kept confidential in order to protect legitimate rights and interests of a third person or intelligence sources.



3. In the event that the request is declined, the person requesting the information may file a request for administrative review with the vetting authority in accordance with the Law on Administrative Procedures.

## **CHAPTER V INDUSTRIAL SECURITY**

### **Article 45**

#### **General provisions on access to classified information**

1. Owners, managers and employees of business organizations and their sub-contractors who are invited to bid, negotiate or perform a classified contract or otherwise might gain access to classified information shall have access to such classified information provided they have a valid security certificate issued by the Vetting Authority and they have a need to know.

2. Classified information shall be released to a business organization only with the consent of the public authority that has originated the information.

### **Article 46**

#### **Security of business premises**

1. Business organizations and their sub-contractors whose owners, managers or employees have lawfully access to classified information shall ensure that their business premises, where such information will be handled, fulfill security standards as established in this Law and subsidiary legal acts. The Vetting Authority shall inspect such premises and shall prohibit access to classified information if the business premises do not comply with security standards established in this Law and with pertinent sub-legal acts.

2. The Vetting Authority shall from time to time and without prior notice inspect premises of business organizations which have access to classified information.

### **Article 47**

#### **Termination of Negotiations or Contracts**

1. Failure of a business organization to ensure compliance with security standards shall immediately be a cause for termination of ongoing negotiations or existing contractual arrangements without obligation to compensate any losses or expected profits to the respective business organization.

2. Paragraph 1 of Article 46 of this law shall be without prejudice to claims of the public authority against the respective business organization for compensation of losses caused by the termination of negotiations or contractual arrangements.

3. Paragraphs 1. and 2. of this Article shall apply mutatis mutandis if an owner, manager or employee of the respective business organization who has or should have access to classified information fails to have a valid security certificate for the respective classification level.

#### **Article 48** **Security File and Data Protection**

The Vetting Authority shall be responsible for keeping a security file for every owner, manager and employee that has lawfully access to classified information. The provisions of Chapter IV shall otherwise apply mutatis mutandis to personal data of such owners, managers and employees.

### **CHAPTER VI** **ADMINISTRATION OF THE CLASSIFICATION AND SECURITY** **CLEARANCE SYSTEM**

#### **Article 49** **Responsibilities of the Kosovo Intelligence Agency in the field of Classification of** **Information and Security Clearances**

1. For the purpose of implementing this Law, the Agency shall have the following functions and responsibilities:

1.1. conduct security clearance procedures and perform other functions as set out in this Law;

1.2. monitor and coordinate developments in the field of safeguarding classified information;

1.3. propose measures, including draft policies and legislation, to improve protection of classified information;

1.4. prepares secondary legislation for the implementation of this Law for adoption by the Government

1.5 issue guidelines and instructions related to administrative and technical aspects of this law;

- 1.6. ensure the development and implementation of physical, organizational and technical standards for protection of classified information;
- 1.7. oversee the implementation of international treaties or instruments on the protection of classified information and propose measures related thereto
- 1.8. cooperate and coordinate with counterpart institutions in other states and international organizations in matters pertaining to protection of classified information;
- 1.9. provide regular training and capacity-building in the field of protection of classified information.

## **CHAPTER VII FINAL PROVISIONS**

### **Article 50 Criminal Sanctions**

1. A person who discloses without authorization information classified as “CONFIDENTIAL” in accordance with this Law and any authorized holder of such classified information who fails to protect the information as required by this Law shall commit a criminal offence and shall be punished by imprisonment of one (1) to five (5) years.
2. A person who discloses without authorization information classified as “SECRET” in accordance with this Law, and any authorized holder of such classified information who fails to protect the information as required by this Law shall commit a criminal offence and shall be punished by imprisonment of three (3) to ten (10) years.
3. A person who discloses without authorization information classified as “TOP SECRET” in accordance with this Law and any authorized holder of such classified information who fails to protect the information as required by this Law shall commit a criminal offence and shall be punished by imprisonment of five (5) to twelve (12) years.

### **Article 51 Secondary Legislation**

On proposal of the Kosovo Intelligence Agency, the Government shall approve secondary legislation for implementation of this Law within one (1) year of its entrance into force.

**Article 52**  
**Entry into Force**

This law enters into force fifteen (15) days after publication in the Official Gazette of the Republic of Kosovo.

**Law No.03/L –178**  
**1 July 2010**

**The President of the Assembly of Republic of Kosovo**

---

**Jakup Krasniqi**