

# THE CROATIAN PARLIAMENT

2483

Pursuant to Article 88 of the Constitution of the Republic of Croatia, I hereby issue the

## DECISION

### ON PROMULGATING THE DATA SECRECY ACT

I hereby promulgate the Data Secrecy Act, passed by the Croatian Parliament at its session on 13 July 2007.

Class: 011-01/07-01/97

Reg. No.: 71-05-03/1-07-2

Zagreb, 18 July 2007

The President of the Republic of Croatia  
Stjepan Mesić, m.p.

#### DATA SECRECY ACT I BASIC PROVISIONS Article 1

(1) This Act establishes the notion of classified and unclassified information, degrees of secrecy, the procedure of classification and declassification, classified and unclassified information access, classified and unclassified information protection and oversight over the implementation of this Act.

(2) This Act applies to state authorities, local and regional self-government bodies, legal persons with public authority and legal and natural persons that, in accordance with this Act, gain access to or handle classified and unclassified information.

#### Article 2

Particular notions within the meaning of this Act shall have the following meaning:

- information are documents, or any written, copied, drawn, painted, printed, filmed, photographed, magnetic, optical, electronic or any other type of recording, insight, measure, procedure, object, verbal announcement or information that, considering its content, is significant for its owner in terms of trustworthiness and integrity,
- classified information are documents that were, within the stipulated procedure, classified as such by the competent authority and for which the degree of secrecy has been determined, and information that were thus classified and delivered to the Republic of Croatia by another country, international organization or institution that the Republic of Croatia cooperates with,
- unclassified information are documents without the determined degree of secrecy, that are used for official purposes, and information that were thus marked and delivered to the Republic of Croatia by another country, international organization or institution that the Republic of Croatia cooperates with,
- classification is the process of determining the degree of secrecy regarding the security threat degree and area of values protected by this Act,
- declassification is the process of determining the cease of reasons for which the information were classified with the appropriate degree of secrecy, after which it shall become unclassified with restricted use only for official purposes,
- originator is the competent authority within whose scope of work the classified or unclassified data were created,
- certificate is Personnel Security Clearance that enables classified data access

### Article 3

Information shall not be classified in order to conceal crime, exceeding or abuse of authority and other types of illegal proceedings within state authorities.

## II DEGREES OF SECRECY

### Article 4

Classified information degrees of secrecy are as follows:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED

### Article 5

Taking into consideration the degree of security threat to values protected with degrees of secrecy referred to in Article 4 of this Act, information from the scope of activity of state authorities in the field of defence, security intelligence system, foreign affairs, public security, criminal proceedings and science, technology, public finances and economy may be classified in case those information are of security interest for the Republic of Croatia.

### Article 6

Secrecy degree TOP SECRET shall be used to classify information whose unauthorised disclosure would result in exceptionally grave damage to national security and vital interests of the Republic of Croatia, and especially to the following values:

- basis of the structure of the Republic of Croatia as laid down by the Constitution
- independence, integrity and security of the Republic of Croatia
- international relations of the Republic of Croatia
- defence capability and security intelligence system
- public security
- basis of the economic and financial system of the Republic of Croatia
- scientific discoveries, inventions and technologies that are of great significance for the national security of the Republic of Croatia

### Article 7

Secrecy degree SECRET shall be used to classify information whose unauthorised disclosure would result in grave damage to values referred to in Article 6 of this Act.

### Article 8

Secrecy degree CONFIDENTIAL shall be used to classify information whose unauthorised disclosure would be damaging to the values referred to in Article 6 of this Act.

### Article 9

Secrecy degree RESTRICTED shall be used to classify information whose unauthorised disclosure would be damaging to the functioning of state authorities and enforcing tasks referred to in Article 5 of this Act.

## Article 10

State authorities that implement the classification process shall, by Ordinance, establish the criteria for determining degrees of secrecy in detail within their scope of work.

## III CLASSIFICATION AND DECLASSIFICATION PROCESS

### Article 11

Classification shall be done when classified information is originated or during periodical assessments referred to in Article 14 of this Act.

### Article 12

- (1) During the classification process the originator shall determine the lowest degree of secrecy that will secure the protection of interests that could be threatened by unauthorised disclosure of the said information.
- (2) In case the classified information contain certain parts or enclosures whose unauthorised disclosure does not threaten the values protected by this Act, such parts shall not be classified with the degree of secrecy.

### Article 13

- (1) classification with TOP SECRET and SECRET degrees of secrecy may be done by: the President of the Republic of Croatia, the President of the Parliament of the Republic of Croatia, the President of the Government of the Republic of Croatia, ministers, Chief State Attorney, Head of the General Staff of the Armed Forces of the Republic of Croatia and Heads of authorities of the security intelligence system of the Republic of Croatia and those that are authorised to do so by the said persons.
- (2) Persons referred to in paragraph 1 of this Article shall transfer their authority to other persons in written and solely within their respective scope of work.
- (3) classification with CONFIDENTIAL and RESTRICTED degrees of secrecy may be done, apart from the persons referred to in paragraphs 1 and 2 of this Article, by heads of other state authorities.
- (4) Persons referred to in paragraphs 1, 2 and 3 of this Article shall classify information for scientific institutions, bureaus and other legal persons when working on projects, discoveries, technologies and other jobs of security interest for the Republic of Croatia.

### Article 14

- (1) During the time when the degree of secrecy is valid the originator shall continuously assess the degree of secrecy of the classified information and shall make periodical assessments based on which the degree of secrecy can be changed or declassification can be done.
- (2) Periodical assessment shall be done as follows:
  - for TOP SECRET degree of secrecy at least once every 5 years,
  - for SECRET degree of secrecy at least once every 4 years,
  - for CONFIDENTIAL degree of secrecy at least once every 3 years,
  - for RESTRICTED degree of secrecy at least once every 2 years.
- (3) The originator shall inform, in writing, all the authorities that the information were delivered to about the change of the degree of secrecy or declassification.

### Article 15

- (1) Periodical assessment shall be made in writing for each individual degree of secrecy.
- (2) The originator is authorised to make periodical assessment jointly for certain groups of information.
- (3) Periodical assessment shall be classified with the same degree of secrecy as the information it refers to and shall be attached with the original in the originator's archives.

## Article 16

- (1) When there is public interest, originator shall determine the proportionality between the right for access and protection of the values stipulated in Articles 6, 7, 8 and 9 of this Act and decide on maintaining the degree of secrecy, changing the degree of secrecy, declassification or exemption from the obligation to keep information secret.
- (2) Prior to making the decision referred to in paragraph 1 of this Article the originator shall ask for the opinion of the Office of the National Security Council.
- (3) The originator shall inform other competent authorities stipulated by law of the procedure referred to in paragraph 1 of this Article.

## Article 17

The way of identifying classified information degrees of secrecy shall be stipulated by the Regulation adopted by the Government of the Republic of Croatia.

## IV INFORMATION ACCESS

### Article 18

- (1) Access to classified information shall be granted to persons with a need-to-know and who have Personnel Security Clearance (hereinafter: Certificate).
- (2) State authorities, bodies of local and regional self-government, legal persons with public authority, legal and natural persons (hereinafter: Applicants) are authorized to submit requests for Certificate issuance for their employees with a need-to-know.
- (3) Request for Certificate issuance shall be submitted in writing to the Office of the National Security Council. The request shall contain the following: first name, last name, duty or the jobs within which the person will have classified data access and the degree of secrecy for which the Certificate is requested.
- (4) Certificate shall be issued for TOP SECRET, SECRET and CONFIDENTIAL degrees of secrecy for a period of five years. Certificate shall not be classified with the degree of secrecy but shall represent unclassified data.
- (5) Certificate shall be issued by the Office of the National Security Council based on the assessment on absence of security impediments for classified information access. Existence of security impediments shall be determined by security vetting done by competent security intelligence agency.
- (6) Security impediments within the meaning of this Act are the following: false data stated in the Questionnaire for security vetting, facts that are stipulated by special Act as impediments for work in the civil service, pronounced disciplinary sanctions and other facts that represent reasonable doubt in the trustworthiness or reliability of the person to handle classified data.

### Article 19

- (1) In case the authority referred to in Article 18, paragraph 5 of this Act, based on the report on results of security vetting, determines that there are security impediments it shall deny the Certificate issuance by Decision.
- (2) The person for whom Certificate issuance was denied by Decision shall not have the right of appeal, but shall have the right to initiate administrative dispute within 30 days since the receipt of the said Decision.
- (3) During the procedure at the Administrative Court of the Republic of Croatia the Court shall, while determining facts and presenting evidence that might damage the work of security intelligence agencies and national security, take measures and actions from its scope of duty that will prevent the damage from occurring.

## Article 20

(1) Classified information access without the Certificate shall be granted to the Member of Parliament, minister, State Secretary of the Central State Administrative Office, judge and Chief State Attorney within the scope of their work.

(2) Persons referred to in paragraph 1 of this Article shall, before accessing classified information, sign the Statement of the Office of the National Security Council which confirms that they were briefed on the provisions of this Act and other rules and regulations that determine the classified information protection and that they shall handle classified information in accordance with the said provisions.

## Article 21

The content and the view of the Certificate referred to in Article 18 of this Act and the Statement referred to in Article 20, paragraph 2 of this Act shall be stipulated by the Regulation adopted by the Government of the Republic of Croatia.

## Article 22

(1) Access to classified information of another country or international organization shall be granted to persons with a need-to-know and who have the Certificate stipulated by international treaty or security agreement.

(2) Certificate referred to in paragraph 1 of this Article shall be issued by the Office of the National Security Council based on the request of the competent authority.

(3) The request referred to in paragraph 2 of this Article may be submitted only for the persons who were previously granted appropriate Certificate based on the procedure referred to in Article 18 of this Act.

## Article 23

(1) Access to unclassified information shall be granted to persons with a need-to-know.

(2) Access to unclassified information shall be granted to interested authorised persons with right to access information based on the submitted request for gaining right to access information in accordance with the law.

## Article 24

The President of the Republic of Croatia, the President of the Parliament of the Republic of Croatia and the President of the Government of the Republic of Croatia shall be exempt to the procedure stipulated for Certificate issuance.

## V INFORMATION PROTECTION

### Article 25

The mode and implementation of classified and unclassified information protection shall be stipulated by the Act that regulates the information security area.

### Article 26

State officials and employees, local and regional self-government bodies, legal persons with public authority as well as legal and natural persons who gain access or handle classified and unclassified information shall keep the classified information secret during the time and after the cease of their duty or work until the information is classified or until by the decision of the originator they are free from the duty of keeping the secrecy thereof.

## Article 27

(1) In case classified information are destroyed, stolen or made available to unauthorised persons, the originator shall take all necessary measures to prevent the occurrence of possible damaging consequences, shall start the procedure to determine the responsibility and shall at the same time inform the Office of the National Security Council thereof.

(2) In case classified information are destroyed, stolen or made available to unauthorised persons within the body that is not the originator, the responsible person from the said body shall immediately inform the originator thereof and the originator shall then initiate the procedure referred to in paragraph 1 of this Article.

## Article 28

(1) The Office of the National Security Council shall, when issuing the Certificate or signing the Statement referred to in Article 20, paragraph 2 of this Act, brief the persons on the standards of handling classified information and on other legal and other consequences of unauthorised handling of the said information.

(2) The procedure referred to in paragraph 1 of this Article shall be implemented at least once a year during the Certificate validity period.

## VI OVERSIGHT OVER THE IMPLEMENTATION OF THE ACT

### Article 29

State authorities, bodies of local and regional self-government and legal persons with public authority shall keep records on insights into and handling of classified information.

### Article 30

(1) The Office of the National Security Council shall conduct oversight over classification and declassification procedures, the way of gaining access to classified and unclassified information, the implementation of the measures for the protection of classified information access and the performance of duties from the international agreements and treaties on classified information protection.

(2) In conducting the oversight the Head of the Office of the National Security Council has the authority to:

- determine the facts
- give instructions in order to eliminate the determined defects and irregularities that the bodies that were subject to oversight must eliminate within the designated period of time
- initiate the procedure in order to determine the data owner's responsibility
- take other measures and actions that he or she is authorised to according to special provisions

(3) Office of the National Security Council shall establish registries of Certificates issued, Decisions on Certificates denied, signed Statements referred to in Article 20, paragraph 2 of this Act and conducted briefings on standards referred to in Article 28 of this Act.

## VII TRANSITIONAL AND FINAL PROVISIONS

### Article 31

(1) Regulation of the Government of the Republic of Croatia referred to in Articles 17 and 21 of this Act shall be adopted within 30 days since the date when this Act enters into force.

(2) The Ordinance referred to in Article 10 of this Act shall be adopted by Heads of competent bodies within 60 days after the date when this Act enters into force.

(3) Heads of competent bodies shall determine the list of duties and jobs within their scope of work, for which the Certificate is necessary, within 90 days.

## Article 32

Degrees of secrecy determined by international treaties that the Republic of Croatia confirmed before the date that this Act enters into force, degrees of secrecy gained by international exchange before the date that this Act enters into force, as well as the degrees of secrecy that were determined before the date that this Act enters into force shall be translated as follows:

- STATE SECRET into TOP SECRET
- OFFICIAL SECRET-TOP SECRET and MILITARY SECRET-TOP SECRET into SECRET
- OFFICIAL SECRET-SECRET and MILITARY SECRET-SECRET into CONFIDENTIAL
- OFFICIAL SECRET-CONFIDENTIAL and MILITARY SECRET-CONFIDENTIAL into RESTRICTED

## Article 33

(1) Certificates that were issued by the Office of the National Security Council before the date that this Act enters into force shall be valid until the expiry date stated on the Certificate.

(2) Internal permissions to access classified data that were issued on the basis of the Act on Data Secrecy Protection (Official Gazette, No.108/96) shall be valid until the issuance of the Certificate according to the provisions of this Act.

(3) Sub-Acts adopted on the basis of the Act on Data Secrecy Protection (Official Gazette, No. 108/96) shall be implemented until the date that the appropriate Sub-Acts based on this Act enter into force.

## Article 34

On the date of entry into force of this Act the provisions of the Act on Data Secrecy Protection (Official Gazette, No. 108/96), except the provisions referred to in titles 8 and 9 of the said Act, shall cease to have effect.

## Article 35

This Act shall enter into force 8 days following its publication in the Official Gazette.

Class: 804-04/07-01/01  
Zagreb, 13 July 2007

THE CROATIAN PARLIAMENT

The President of the Croatian Parliament

Vladimir Šeks, m.p.