DATA SECRECY ACT

(Consolidated Text[1])

I BASIC PROVISIONS

Article 1

(1) This Act establishes the notion of classified and unclassified data, degrees of secrecy, the procedure of data classification and declassification, access to classified and unclassified data, protection of classified and unclassified data and oversight of the implementation of this Act.
(2) This Act applies to state authorities, local and regional self-government bodies, legal entities with public authority and legal entities and individuals that, in accordance with this Act, access or handle classified and unclassified data.

Article 2

Particular terms in the context of this Act shall have the following meaning:
- **Data** are documents, or any written, reproduced, drawn, painted, printed, recorded, photographed, magnetic, optical, electronic or any other type of data recording, insight, measure, procedure, object, verbal communication or information that, considering its content, is significant for its owner in terms of confidentiality and integrity,
- **Classified data** are data that were, under a stipulated procedure, designated as such by the competent authority and for which a degree of secrecy has been determined, as well as data that were delivered to the Republic of Croatia with such a marking by another country, international organization or institution with which the Republic of Croatia cooperates,
- **Unclassified data** are data without a determined degree of secrecy, that are used for official purposes, as well as data that were delivered to the Republic of Croatia with such a marking by another country, international organization or institution with which the Republic of Croatia cooperates,
- **Data classification** is a procedure of determining one of the degrees of data secrecy with regard to the degree of security threat and the area of values protected by this Act,
- **Data declassification** is a procedure of determining the cessation of existence of the reasons for which particular data have been classified with an appropriate degree of secrecy, after which the data shall become unclassified with restricted use only for official purposes,
- **Data owner** is a competent authority within whose scope of work the classified or unclassified data were created,
- **Certificate** is a Personnel Security Clearance that enables access to classified data.

[1] **The consolidated text of the Data Secrecy Act includes the Data Secrecy Act (Official Gazette 79/07) and the Act on Amendments to the Data Secrecy Act (Official Gazette 86/12, which state the time of their coming into force.**

Article 3

Data shall not be classified in order to conceal crime, overstepping or abuse of authority and other forms of illegal conduct within state authorities.

II DEGREES OF SECRECY

Article 4

Degrees of secrecy of classified data are as follows:
- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED

Article 5

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

Article 6

Secrecy degree TOP SECRET shall be used to classify data whose unauthorised disclosure would cause irreparable damage to the national security and vital interests of the Republic of Croatia, especially to the following values:
- Foundations 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 the security and intelligence system,
- Public security,
- Foundations of the economic and financial system of the Republic of Croatia,
- Scientific discoveries, inventions and technologies of significance to the national security of the Republic of Croatia.

Article 7

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

Article 8

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

Article 10

State authorities that implement the data classification process shall issue an ordinance specifying the criteria for determining degrees of secrecy in detail within their scope of work.

III DATA CLASSIFICATION AND DECLASSIFICATION PROCESS

Article 11

Data classification shall be carried out when classified data is generated or during periodical assessments referred to in Article 14 of this Act.

Article 12

(1) During the data classification process, the data owner shall determine the lowest degree of secrecy that will ensure the protection of the interest that could be threatened by unauthorised disclosure of the said data.
(2) If the classified data contain certain parts or enclosures whose unauthorised disclosure does not threaten the values protected by this Act, such parts of the data shall not be marked with a degree of secrecy.

Article 13

(1) Data classification with TOP SECRET and SECRET degrees of secrecy may be done by: the President of the Republic of Croatia, the Speaker of the Croatian Parliament, the Prime Minister of the Republic of Croatia, ministers, State Attorney General, the Chief of the General Staff of the Armed Forces of the Republic of Croatia, heads of the bodies of the security and intelligence system of the Republic of Croatia and persons authorised by them for that purpose.
(2) Persons referred to in paragraph 1 of this Article shall transfer their authority to other persons in written form and solely within their respective scopes.
(3) Data classification with CONFIDENTIAL and RESTRICTED degrees of secrecy may also be done, in addition to the persons referred to in paragraphs 1 and 2 of this Article, by the heads of other state authorities.
(4) Persons referred to in paragraphs 1, 2 and 3 of this Article shall also classify data for scientific institutions, bureaus and other legal entities when working on projects, discoveries, technologies and other tasks of security interest for the Republic of Croatia.

Article 14

(1) During the validity of a degree of secrecy, the data owner shall continuously assess the degree of secrecy of the classified data and shall make periodical assessments based on which the degree of secrecy can be changed or declassification can be done.

(2) Periodical assessments shall be done as follows:
- For the TOP SECRET degree of secrecy at least once in 5 years,
- For the SECRET degree of secrecy at least once in 4 years, - For the CONFIDENTIAL degree of secrecy at least once in 3 years,
- For the RESTRICTED degree of secrecy at least once in 2 years.

(3) Data owner shall inform, in writing, all the authorities to which the data has been delivered about a change of the degree of secrecy or data declassification.

Article 15

(1) Periodical assessment shall be made in written form for each individual degree of secrecy.

(2) Data owner may make a periodical assessment jointly for certain groups of data.

(3) Periodical assessment shall be classified with the same degree of secrecy as the data it refers to and shall be attached to the original in the data owner's archives.

Article 16

(1) When there is public interest, data owner shall determine the proportionality between the right of data 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, altering the degree of secrecy, declassification or exemption from the obligation to keep the data secret.

(2) Prior to making the decision referred to in paragraph 1 of this Article data owner shall request the opinion of the Office of the National Security Council.

(3) Data owner shall inform the other competent authorities stipulated by law of the procedure referred to in paragraph 1 of this Article.

Article 17

The manner of identifying classified data degrees of secrecy will be stipulated by a regulation adopted by the Government of the Republic of Croatia.

IV ACCESS TO DATA

Article 18

(1) Access to classified data shall be granted to persons who have a need-to-know and hold a Personnel Security Clearance (hereinafter: Certificate).

(2) State authorities, bodies of local and regional self-government, legal entities with public authority, legal entities and individuals (hereinafter: Applicants) are authorized to submit requests for Certificate issuance for employees who have 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 jobs within which the person will have access to classified data 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 a degree of secrecy; it shall represent unclassified data.
(5) Certificate shall be issued by the Office of the National Security Council based on the assessment on the absence of security impediments for access to classified data. Existence of security impediments shall be determined by security vetting carried out by the competent security and intelligence agency.
(6) Security impediments in the context of this Act are as follows: false data stated in the Questionnaire for security vetting, facts that are stipulated by a separate Act as impediments for work in the civil service, disciplinary sanctions and other facts that represent reasonable doubt as to the confidentiality or reliability of a person for handling classified data.

Article 19

(1) If the authority referred to in Article 18 paragraph 5 of this Act determines the existence of security impediments, based on the report on the results of security vetting, it shall deny the Certificate issuance by a decision.
(2) The person for whom Certificate issuance was denied by a decision may not appeal, but may initiate an administrative dispute within 30 days from the receipt of the decision.
(3) During the procedure at the Administrative Court, the Court shall, while determining facts and presenting evidence that may cause damage to the work of the security and intelligence agencies and to national security, take measures and actions from its scope that will prevent the damage.

Article 20

(1) Access to classified data without a Certificate shall be granted to the state officials stipulated by the State Administration System Act, Members of Parliament, Ombudsman, judges, State Attorney General, Deputies to State Attorney General, Director of the Office for the Prevention of Corruption and Organised Crime, and deputies to the Director of the Office for the Prevention of Corruption and Organised Crime in the scope of their work.[2]
(2) Persons referred to in paragraph 1 of this Article shall, before accessing classified data, sign a statement to the Office of the National Security Council confirming that they have been briefed on the provisions of this Act and other regulations governing classified data protection and that they shall handle classified data in accordance with those provisions.

Article 21

The contents and the template of the Certificate referred to in Article 18 of this Act, as well as the Statement referred to in Article 20 paragraph 2 of this Act, shall be stipulated by a regulation adopted by the Government of the Republic of Croatia.

Article 22

(1) Access to classified data of another state and international organization shall be granted to persons who have a need-to-know and hold a Certificate stipulated by an international treaty or security agreement.

---

[2] Paragraph 1 was changed with the provision of Article 1 of the Act on Amendments to the Data Secrecy Act (Official Gazette 86/12) that came into force on 4 August 2012.

(2) The 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 have previously been issued an appropriate Certificate under the procedure referred to in Article 18 of this Act.

Article 23

(1) Access to unclassified data shall be granted to persons who have a need-to-know for official purposes.
(2) Access to unclassified data shall also be granted to interested persons authorised to access information based on the submitted request for access to information in accordance with law.

Article 24

The President of the Republic of Croatia, the Speaker of the Croatian Parliament and the Prime Minster of the Republic of Croatia shall be exempt from the procedure stipulated for Certificate issuance.

V DATA PROTECTION

Article 25

The manner and implementation of classified and unclassified data protection shall be stipulated by the act governing the area of information security.

Article 26

Officials and employees of state authorities, bodies of local and regional self-government, legal entities with public authority, legal entities and individuals, who have had access to or have handled classified and unclassified data, shall keep the classified data secret during and after their duty or employment, for as long as the data is classified or until they are released from the obligation to keep the secrecy thereof by the decision of the data owner.

Article 27

(1) In case classified data are destroyed, stolen or made available to unauthorised persons, the data owner 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 data are destroyed, stolen or made available to unauthorised persons within the body that is not the data owner, the responsible person from the said body shall immediately inform the data owner thereof and the data owner 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 a Certificate or signing the Statement referred to in Article 20 paragraph 2 of this Act, brief the persons on the standards of handling classified data and on other legal and other consequences of unauthorised handling of the data.
(2) The procedure referred to in paragraph 1 of this Article shall be implemented at least once a year during the Certificate's validity.

VI OVERSIGHT OF THE IMPLEMENTATION OF THE ACT

Article 29

State bodies, bodies of local and regional self-government and legal entities with public authority shall keep records on access and handling of classified data.

Article 30

(1) The Office of the National Security Council shall conduct oversight of the data classification and declassification procedures, the manner of gaining access to classified and unclassified data, the implementation of the measures for the protection of access to classified data and the fulfilment of obligations arising from international agreements and treaties on classified data protection.
(2) In conducting the oversight, the Head of the Office of the National Security Council shall be authorised to: - Establish the facts,
- Give instructions in order to eliminate the detected shortcomings and irregularities that the bodies undergoing oversight must eliminate within a designated period of time,
- Initiate a procedure to establish the data owner's responsibility,
- Take other measures and actions that he or she is authorised to under special regulations.

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

VII TRANSITIONAL AND FINAL PROVISIONS

Article 31

(1) The 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 from the day of entering into force of this Act.
(2) The Ordinance referred to in Article 10 of this Act shall be adopted by the Heads of the competent bodies within 60 days from the day of entering into force of this Act.
(3) The Heads of the competent bodies shall, within 90 days, establish a list of duties and jobs within their scope for which a Certificate is required.

Article 32

Degrees of secrecy established by international treaties that the Republic of Croatia confirmed before the date of entering into force of this Act, degrees of secrecy of the data obtained by international exchange before entering into force of this Act, and degrees of data secrecy that were established before the entry into force of this Act shall be translated as follows:

- STATE SECRET to TOP SECRET
- OFFICIAL SECRET-TOP SECRET and MILITARY SECRET-TOP SECRET to SECRET
- OFFICIAL SECRET-SECRET and MILITARY SECRET-SECRET to CONFIDENTIAL - OFFICIAL SECRET-CONFIDENTIAL and MILITARY SECRET-CONFIDENTIAL to RESTRICTED.

Article 33

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

(2) Internal authorisations for access to classified data that were issued pursuant to the Act on Data Secrecy Protection (Official Gazette 108/96) shall be valid until the issuance of a Certificate in accordance with the provisions of this Act.

(3) Subordinate legislation adopted pursuant to the Act on Data Secrecy Protection (Official Gazette 108/96) shall be applied until the entry into force of the appropriate subordinate legislation pursuant to this Act.

Article 34

Upon the entry into force of this Act, the provisions of the Act on Data Secrecy Protection (Official Gazette 108/96) shall no longer be in effect, except for the provisions referred to in titles 8 and 9 of the said Act.

Article 35

This Act shall enter into force on the eighth day from the day of its publication in the Official Gazette.

(Act on the Amendments to the Data Secrecy Act, Official Gazette 86/12, in force as of the 4th of August 2012)