# Classified Information Act

**Classified Information Act (official consolidated text) (ZTP-UPB2)**

CHAPTER 1

GENERAL PROVISIONS

Article 1

This Act lays down the basic principle of a common system for the determination and safeguarding of and access to classified information in the sphere of activity of Government agencies of the Republic of Slovenia relating to public security, defence, foreign affairs or the intelligence and security activities of the country and for the declassification of such information.

This Act shall be binding on Government agencies, local community agencies, holders of public authorisations and other agencies, and commercial companies and organisations which, in carrying out their statutory responsibilities, obtain or have at their disposal information referred to in the preceding paragraph (hereinafter referred to as agencies), as well as on individuals in such agencies.

This Act shall also be binding on suppliers, contractors and service providers (hereinafter referred to as organisations) to whom the classified information referred to in the first paragraph of this Article is imparted for the purpose of implementing procurement contracts for agencies.

Responsibility for the protection of classified information and the preservation of its confidentiality shall apply to all those to whom such information has been entrusted or who have become acquainted with the contents thereof.

Article 2

The meaning of individual terms used in this Act shall be as follows:

1. Classified information: a fact or means from the sphere of activity of an agency relating to public security, defence, foreign affairs or the intelligence and security activities of the country which, for reasons defined in this Act, must be protected against unauthorised persons and which has been defined and marked as confidential in accordance with this Act;
2. Classified information of a foreign country: information which a foreign country or its agency, or an international organisation or its agency have conveyed to the Republic of Slovenia on the understanding that it will be kept secret, and information resulting from cooperation between the Republic of Slovenia or its agencies with a foreign country or an international organisation and its agencies which is to be kept secret by mutual agreement;
3. Document: any written, drawn, printed, copied, filmed, photographed, magnetic, optical or other record of classified information;
4. Medium: any medium containing classified information;
5. Classification: an act or procedure by which a piece of information is assessed as secret and assigned a level and duration of secrecy in accordance with this Act;
6. Declassification: the statutory change of classified information into information accessible in accordance with regulations governing the business of the agency;
7. Access: acquainting of a person with classified information or the possibility for a person to obtain classified information on the basis of permission to access;
8. Vetting procedure of a person: the investigation carried out by a competent authority before the issuing of permission to access classified information with the aim of gathering information about potential security restrictions;
9. Security restrictions: such findings from a background investigation as cast doubt upon the dependability and loyalty of a potential candidate for permission to access classified

information;
10. A threat to the vital interests of the country: a threat to the constitutional order, independence, territorial integrity and defence capability of the country;
11. Treatment of classified information: determination, marking, access to, application, recording, copying, transmission and destruction of carriers of classified information, storage, archiving and other measures and procedures providing their security.

Article 3

The following persons may, in connection with the discharge of their functions, have access to classified information without permission to access (hereinafter referred to as permission):

1. the President of the Republic;
2. the Prime Minister;
3. deputy;
4. State adviser;
5. mayor and municipal adviser;
6. minister and head of Government services directly answerable to the Prime Minister;
7. ombudsman and deputy ombudsman;
8. governor, deputy governor and vice governor of the Central Bank;
9. member of the Court of auditors;
10. judges;
11. the Public Prosecutor;
12. the State Attorney General and
13. commissioner for access to public information.

The persons referred to in the preceding paragraph shall be granted permission after entering the service and signing a statement to the effect that they are acquainted with this Act and other regulations governing the protection of classified information, and that they undertake to handle classified information in accordance with these regulations.

Article 4

The Commission of the National Assembly of the Republic of Slovenia for Supervision of the Work of the Security and Intelligence Services shall, in the discharge of its function, have access to classified information without the need for permission.

Article 5

Under the provisions of this Act, a piece of information may be defined as classified if it is so important that its disclosure to unauthorised persons could or might obviously prejudice the security of the country or its political or economic interests, and is related to:

1. public security;
2. defence;
3. foreign affairs;
4. the intelligence and security activities of Government agencies of the Republic of Slovenia;
5. systems, appliances, projects and plans of importance to the public security, defence, foreign affairs and intelligence and security activities of Government
6. agencies of the Republic of Slovenia;

7. scientific, research, technological, economic and financial affairs of importance to the public security, defence, foreign affairs and intelligence and security activities of Government
8. agencies of the Republic of Slovenia;

Article 6
A piece of information that has been defined as classified in order to cover up a criminal offence, the exceeding or abuse of authority, or some other unlawful act or behaviour shall not be considered to be classified.
Article 7
Access to classified information shall be restricted and permitted in a manner and under conditions specified by this Act and the regulations based thereon, and in the manner and under conditions specified by other systematic procedural laws or international treaties concluded by the Republic of Slovenia.
Article 8
Officials and employees of agencies shall be bound to safeguard classified information no matter how such information has come to their knowledge.
The obligation for the persons referred to in the preceding paragraph to safeguard classified information shall not terminate with the termination of their function or employment at the agency.
Article 9
Protection and access to classified information of a foreign country or international organisation shall be carried out in accordance with this Act or the regulations based thereon, or in accordance with international treaties concluded between a foreign country or international organisation and the Republic of Slovenia.
CHAPTER II
CLASSIFICATION OF INFORMATION
Article 10
A piece of information shall be designated as classified by an authorised person, under conditions and in a manner specified by this Act. Authorised persons shall include:
1. the director of an agency;
2. elected or appointed officials of the agency authorised to classify and disclose information in accordance with the law or the regulation based thereon, or in accordance with a written authorisation from the director and
3. employees of the agency to whom the director of the agency has issued written authorisation to classify information.
The authorised persons referred to in points 2 and 3 of the preceding paragraph may not transfer their authorisation to third persons.
The TOP SECRET level may only be assigned by the President of the Republic, the President of the National Assembly, the chairman of the Commission referred to in Article 4 of this Act, the chairmen of commissions of inquiry set up by the National Assembly, the Prime Minister, ministers and directors of agencies attached to the ministries, certain military commanders, certain heads of diplomatic and consular representations of the Republic of Slovenia and heads of Government services directly answerable to the prime minister or their deputies.
The minister responsible for defence shall designate the military commanders referred to in the preceding paragraph. The minister responsible for external affairs shall designate the heads of diplomatic and consular representations of the Republic of Slovenia referred to in the preceding paragraph.
The manner and procedure of classification of information in commercial companies,

institutes and organisations which, in the discharge of their statutory duties, receive or have at their disposal information referred to in the first paragraph of Article 1 of this Act, shall be prescribed by the minister responsible for defence, in agreement with the minister responsible for the interior.

Any official, employee, or other person performing a function or working in an agency, shall be bound within the scope of their duties or competencies to assess the security importance of information and propose to authorised persons that such information be designated as classified if they deem it should be classified.

Article 11

An authorised person shall determine the level of classification of a piece of information at the origin of that piece of information, i.e. at the beginning of the performance of a task of the agency that results in classified information.

In determining the level of classification, the authorised person shall assess the possible adverse effects of the disclosure of information to an unauthorised person on the security of the country or on its political or economic interests. On the basis of that assessment the level of classification and the method of declassification shall be determined, after which the information shall receive the markings prescribed by this Act.

The assessment on the basis of which a piece of information is given the level of classification shall be in written form.

Where the elaboration of a written assessment prior to the performance of urgent tasks of an agency would make the performance difficult or impossible, the authorised person may determine the level of classification of a piece of information orally and mark it with the level of classification. A written assessment shall be elaborated as soon as possible, but within three days at the latest.

Article 12

An authorised person shall also designate as classified the information created by uniting or linking pieces of information which, taken separately, are not sensitive but which, joined together, represent information or a document that must be protected for reasons specified by this Act.

Where only a smaller part of a document or an individual document of a matter contains classified information, that part of document shall be detached from the remaining document and treated and protected in accordance with the level of classification markings.

Article 13

Classified information referred to in Article 5 of this Act shall, in view of possible adverse effects its disclosure to an unauthorised person might have on the security of the country or on its political or economic interests, be given one of the following levels of classification:

1. A TOP SECRET classification shall be applied to classified information the disclosure of which to unauthorised persons would put in jeopardy or do irreparable damage to the vital interests of the Republic of Slovenia;
2. A SECRET classification shall be applied to classified information the disclosure of which to unauthorised persons could seriously harm the security or interests of the Republic of Slovenia;
3. A CONFIDENTIAL classification shall be applied to classified information the disclosure of which to unauthorised persons could harm the security or interests of the Republic of Slovenia;

4. A RESTRICTED classification shall be applied to classified information the disclosure of which to unauthorised persons could harm the activity or performance of tasks of an agency.

In determining the levels of classification of information, agencies shall only apply the levels set out in the preceding paragraph.

Article 14

In classifying information an authorised person shall give the lowest level of classification that still ensures such a degree of protection as is necessary to safeguard the interests or ensure the security of the country.

A document composed of already classified pieces of information shall be given at least such a level and duration of classification as the piece of information with the highest level and longest duration of classification.

Article 15

An authorised person shall declassify classified information once the conditions which this Act provides for such a status have ceased to exist. The authorised person shall notify of the declassification all those who have received or have access to the classified information involved.

The reasons for declassification of information shall be given in writing.

Declassification of information may be requested by a person whose request for classified information has been turned down.

The request from the preceding paragraph shall be decided on by the director of the agency concerned.

Article 16

The level of classification may be changed by the authorised person of an agency where the level was determined.

The reasons for the change of classification of information shall be given in writing.

The authorised person shall change the level of classification once the conditions for the application of individual levels as provided by this Act have changed. The authorised person shall notify of the change all those who have received or have access to the classified information involved.

Article 17

Every classified information or every document containing classified information shall be marked with the level of classification and the information about the agency, unless otherwise obvious.

The markings from the preceding paragraph shall be used in a manner appropriate to the kind and characteristics of the medium.

A piece of information or a document shall be treated as classified even if it is marked only with the level of classification.

The Government of the Republic of Slovenia (hereinafter: the Government) shall prescribe in detail the methods and forms of marking the classification of information or documents.

Article 18

The classification of information shall terminate:

1. on a specified date;
2. with the advent of a specified event;
3. with the expiry of a specified time period;
4. with declassification.

Where, due to the nature or content of information, the termination as set out in the preceding paragraph cannot be applied, classification shall terminate with the expiry of the time period laid down in the law governing archival materials and archives.
An authorised person shall check TOP SECRET classified information once a year, whereas the remaining levels of classification only every three years and shall assess whether the need for the classification of information still exists.
An authorised person may change the prescribed method of declassification, provided that well-founded reasons for the change exist. In that case the authorised person shall immediately notify thereof all those who have received or have access to the classified information involved.
Article 19
If confirmation of the existence of classified information might adversely affect the interests or security of the country, the agency receiving a request for classified information shall not be obliged to either confirm or deny the existence of the requested information.
Article 20
The markings of the classified information of a foreign country or international organisation shall, as a rule, remain in the form in which they are used in that country or international organisation, or may also be marked as provided by this Act, on condition that the levels of classification are comparable and ensure an equal degree of protection.
The method of marking classified information of the Republic of Slovenia in a foreign country or international organisation, and the determination of such a degree of protection of that information as will compare with the provisions of this Act, should be specified in an international treaty on the exchange or provision of classified information between a foreign country or international organisation and the Republic of Slovenia.
Article 21
Entitled users of classified information that have legally received the information may propose to the authorised person that a particular classification that they deem unjustified or incorrect be changed.
The authorised person shall consider the proposal from the preceding paragraph and notify the proposer of the decision taken.
Article 21a
Where the director of an agency considers, in accordance with the law governing access to public information, that justification of the prevailing public interest for disclosure should be assessed in connection with the request for access to public information relating to a piece of information determined as classified, he shall submit a proposal to the Government.
The Government shall decide on the justification of access to the piece of information referred to in the previous paragraph on the basis of the provisional opinion of the Commission. The Commission shall consist of representatives of the ministry responsible for defence, the ministry responsible for the interior, the ministry responsible for external affaires, the Slovene Intelligence and Security Agency and the National Security Authority.
The representative of an agency that classified the information may not participate in the Commission. The Commission shall regulate the method of its work by its rules of procedure which shall be approved by the Government.
The Commission referred to in the preceding paragraph shall call upon the agency that classified the piece of information to submit an assessment of adverse effects on the basis of which the classification of the piece of information was made and also upon every recipient of the classified piece of information to give his opinion on the justification of the disclosure of the piece of information and the reasons for the preservation of its confidentiality respectively.
The Commission referred to in paragraph 2 of this Article shall within 30 days after the

submission of the request for access to public information prepare an opinion on the justification of the request and submit the opinion to the Government.
Should the Government decide that the public interest concerning the disclosure is stronger than the public interest for limited access to the piece of information due to its confidentiality, it shall order the agency that classified the piece of information to declassify the classified piece of information. The agency shall declassify information no later than 15 days after the day it received the decision of the Government referred to in this paragraph and shall acquaint the applicant with the information.
The Commission referred to in this Article may upon the proposal of the director of the agency deliver its opinion on the justification of the request for the declassification of information referred to in Article 15 of this Act or on the proposal for the declassification or the change of classification referred to in the preceding Article.
Where the request for access to public information is addressed to a national agency that is not directly answerable to the Government in its work, the director of the national agency shall decide upon the justification of access to the classified piece of information in accordance with the same procedure as laid down for the decision of the Government.

III. PERMISSION TO ACCESS CLASSIFIED INFORMATION

Article 22

Permission to access classified information of the CONFIDENTIAL, SECRET and TOP SECRET levels shall be issued by the ministry responsible for the interior, the ministry responsible for defence, the Slovene Intelligence and Security Agency, and the Police (hereinafter: competent authority).
For officials and employees of the ministry responsible for the interior, the ministry responsible for defence, the Slovene Intelligence and Security Agency or the Police, who need access to classified information in order to discharge their functions or tasks, permission shall be issued by the minister responsible for the interior or the minister responsible for defence or the director of the Slovene Intelligence and Security Agency or director-general of the Police, in accordance with the provisions of this Act and the regulations based thereon. Notification of the issuing of permission shall be forwarded to the National Security Authority.
For persons who require access to classified information in order to discharge their tasks or functions in another agency, permission shall be issued by the minister responsible for the interior or, if the performance of defence duties or military service is involved, by the minister responsible for defence, at the proposal of the director of that agency. Notification of the issuing of permission shall be forwarded to the National Security Authority. Security clearance for the issuing of permission in cases involving the performance of defence duties and military service shall be regulated by means of special regulations.
For persons who need permission for the treatment of classified information in organisations referred to in paragraph 3 of Article 1 of this Act, permission shall be issued by a body responsible for the issue of security permission (PSC) to organisations.

Article 22a

In view of the envisaged access of an individual to information of different classification levels, the competent authority shall carry out:

1. basic security clearance,
2. extended security clearance, and
3. extended security clearance with security inquiry.

Basic security clearance shall be used for checking the data on persons to be granted permission to access classified information of the CONFIDENTIAL level, extended security clearance for checking the data on persons to be granted permission to access classified information of the SECRET level, while extended security clearance with security inquiry shall be used for checking the data on persons to be granted permission to access classified information of the TOP SECRET level.

Article 22b

For the purpose of basic security clearance the competent authority shall check the individual's statements in the security clearance questionnaire. In this regard, information referred to in Article 25 of this Act may be collected and used from the data subject as well as from registers and other databases maintained by database administrators of personal and other data.

When a security restriction is suspected on the grounds of basic security clearance, the competent authority may additionally check the data relating to individual security restrictions by means of security inquiry.

The security inquiry referred to in the preceding paragraph shall be carried out only in the case when, after the discussion of suspected security restriction, the persons subjected to clearance give their written consent to security inquiry and fill in the first part of the additional questionnaire. When the person subjected to clearance fails to give consent or to fill in the additional questionnaire, the competent authority may, already on the grounds of a suspected security restriction, refuse to issue permission to access classified information.

Article 22c

When performing extended security clearance, besides the measures referred to in the first paragraph of the preceding Article, the competent authority shall verify by the person subjected to clearance, other authorities competent for security clearance or in the existing databases the data from the special questionnaire that are of importance for access to classified information of the SECRET level.

When a security restriction is suspected on the grounds of extended security clearance, the competent authority may further check the data relating to individual security restrictions by means of security inquiry.

The security inquiry referred to in the preceding paragraph shall be carried out only in the case when, after the discussion of suspected security restriction, the persons subjected to clearance give their written consent to security inquiry and fill in the first part of the additional questionnaire. When the person subjected to clearance fails to give consent or to fill in the additional questionnaire, the competent authority may, already on the grounds of a suspected security restriction, refuse to issue the permission to access classified information.

Article 22d

For the purpose of security inquiry the competent authority shall carry out interviews with the persons specified in the first part of the additional questionnaire by the person subjected to clearance, and who may confirm the information given in the questionnaire.

When a security restriction is suspected on checking the information referred to in the preceding paragraph, the competent authority may also check data concerning circumstances relating to the security restrictions with other persons, bodies and organizations that may know anything about the person subjected to clearance.

Article 22e

When a security restriction referred to in the second paragraph of Article 22.c and 22.d of this Act is suspected on the grounds of the circumstances relating to the marital spouse or the cohabiting unmarried partner or any other adult person cohabiting with the person subjected to clearance, these persons may be interviewed about the presumed security restrictions and, after obtaining their written consent, subjected to basic security clearance.

For verification of information from the preceding paragraph, the first paragraph of Article 22b and the first paragraph of Article 25 of this Act shall apply *mutatis mutandis.*

Article 22f

The vetting procedure for the issue of permission shall be initiated on the basis of a written proposal of the director of an agency referred to in the second paragraph of this Article (hereinafter referred to as proposer).

The proposers of the vetting procedure for the issue of permission are:

1. the director of an agency referred to in the first paragraph of Article 1 of this Act for persons who will need the permission for the performance of tasks pertaining to the position at that agency and for persons employed in organisations referred to in the third paragraph of Article 1 of this Act.
2. the minister responsible for economy for persons employed in organisations that will need permission to access classified information in order to implement public or other procurement contracts within the framework of which they will need access to classified information of a foreign country or international organisation.
3. the director of the National Security Authority for cases not included in the preceding points of this Article.

Article 22g

The procedure for issuing a permission shall be initiated at the written proposal of the proposer for a person who needs to undergo security clearance (hereinafter referred to as person subjected to clearance) and shall include data on the level of classification of information, for the access to which a proposal for the issue of the permission was given.

The proposer shall annex to the proposal a written consent of the person subjected to clearance, a proof of the training passed in the field of classified information treatment, a written statement certifying that the person is ac q uainted with this Act and regulations based thereon and a sealed envelope with the uestionnaire filled in by the person subjected to clearance.

Article 22h

During the vetting procedure the proposer may propose a change of the level of classification for which the proposal was given, if the person subjected to clearance is transferred to a function or position that requires access to classified information of another level of classification than the proposed one.

When the change of the proposal refers to the issue of a permission for a higher level of classification, the proposer shall annex to the request for change a completed corresponding security questionnaire and a written consent of the person subjected to clearance declaring that he agrees with the changed scope of security clearance.

Article 22i

If prior to the issue of the permission the employment of a person subjected to clearance terminates in an agency or organisation or if the person is transferred to another position where permission for access to classified information is not needed, the proposer shall withdraw his proposal for the issue of the permission.

Article 22j

The proposer of the procedure shall cooperate with the competent authority during the entire procedure. If the proposer upon receiving a written notice from the competent authority does not supplement the application in accordance with the required documentation referred to in Article 22g of this Act, his silence shall be taken as a withdrawal of the proposal.

Article 23

The competent authority shall issue permission to access classified information of the CONFIDENTIAL level with a validity of ten years after having carried out the basic security clearance, permission to access classified information of the SECRET level with a validity of five years after extended security clearance, while permission to access classified information of the TOP SECRET level shall be granted after extended security clearance with security inquiry for a period of five years.

The permission to access classified information referred to in the preceding paragraph shall be delivered personally to the person subjected to clearance and to the director of the agency who proposed the security clearance.

When the competent authority shall conclude, on the basis of information checked in the vetting procedure, that a security restriction laid down in this Act exists, it shall refuse to issue the permission. The rejection notice need not contain an indication of the sources used for security clearance.

The competent authority shall decide on the request for the issue of permission no later than three months after the day it received a complete application. In exceptional cases this time period may be extended if the competent authority has not yet received the security clearance data from bodies of foreign countries and in case of longer absence of the person subjected to clearance or the witnesses.

A person who has permission and changes his personal name, shall within 15 days after the occurred change submit a proof thereof to the competent authority that issued the permission. The issue of a decision on the change of the personal name in the permission does not change its validity.

The Government shall specify the manner of verifying, the form and content of the forms to be used in the vetting procedure and in the process of issuing permission and a more detailed process of issuing permission.

Article 23a

Against the decision issued in the procedure of security clearance of persons no complaint shall be permitted; however, administrative challenge, which may be initiated by the proposer or the person subjected to clearance, shall be permitted.

Article 24

In carrying out security clearance, the competent authorities may cooperate with the security clearance agencies of foreign countries and international organisations, in accordance with international treaties concluded between foreign countries or international organisations and the Republic of Slovenia, and in accordance with regulations on personal data protection in the Republic of Slovenia.

Article 25

Security clearance shall apply to the information on a person who has passed training in the field of treatment and protection of classified information and who has been previously informed about the reasons to obtain permission for access to classified information of a certain level, the extent of security clearance and the content and procedure for obtaining this permission; further, the person should have given a written consent to security clearance, completed the corresponding security questionnaire and signed a statement to the effect that he has been acquainted with the legislation governing the treatment of classified information, and that he undertakes to handle classified information in accordance with the mentioned legislation.

A corresponding security clearance questionnaire for obtaining permission to access classified information of individual classification levels referred to in the preceding paragraph is as follows:

1. CONFIDENTIAL – a basic questionnaire for obtaining permission to access classified information,
2. SECRET – a basic and special questionnaire for obtaining permission to access classified information, and
3. TOP SECRET – a basic, special and the first part of additional questionnaire for obtaining permission to access classified information.

The basic questionnaire shall contain the following data:

1. name, including any previous names;
2. personal identification number (EMŠO);
3. date and place of birth;
4. nationality or nationalities, including any previous;
5. place of residence (permanent, temporary and actual);
6. stays abroad, when lasting three months or longer (place, period and reason for the stay abroad);
7. marital status and number of children;
8. occupation and job performed;
9. military service;
10. study and participation in seminars or other forms of training and education abroad, when lasting three months or longer (place and period);
11. employers (present and past) and their addresses;
12. unerased final convictions for criminal offences prosecuted ex officio, and data on offences dealt with by violation authorities or the court;
13. ongoing criminal proceedings;
14. alcohol, drug or other addiction;
15. disease or mental disturbance that might threaten safe treatment of classified information;
16. contacts with foreign intelligence and security services;
17. membership or participation in organizations or groups which threaten vital interests of the Republic of Slovenia or the Member States of political, defence or security alliances, of which the Republic of Slovenia is a member;
18. disciplinary measures pronounced ;
19. previous security clearances according to the present Act.

The special questionnaire shall contain the following data:

1. participation in foreign armed forces or other armed formations;
2. financial obligations and guarantees undertaken respectively with the description of the type (such as loans, mortgages, maintenance), the scope of financial obligations, the reasons for the debt, the creditors and the statement of the total revenue earned last year, including the data on the real estate ownership. The person subjected to clearance shall also state data on the average personal income in the last three months prior to filling in the questionnaire;

3. VAT number;
4. particulars and circumstances in the life of the person subjected to clearance, which may be associated with exposure to blackmailing or other forms of pressure.

The additional questionnaire shall consist of two components. The first part shall contain the names and the addresses (permanent, temporary or actual) of three persons who may confirm the statements in the questionnaires, while the second part shall contain information on the persons referred to in the first paragraph of Article 22e of this Act (name, date and place of birth and address of permanent, temporary residence and actual address respectively), who may be subjected to security clearance in accordance with this Act.
The data referred to in the third, forth and fifth paragraph of this Article represent the substance of security clearance.
The data referred to in point 5, 8, 13 and 18 of the basic questionnaire and point 1, 2 and 4 of the special questionnaire shall be checked in the vetting procedure for issuing permission to access classified information of the CONFIDENTIAL and SECRET levels for the period of the last five years, whereas for issuing permission to access classified information of the TOP SECRET level for the last ten years, however, only after the person subjected to security clearance has completed 18 years of age and only data not yet deleted from records because of being time-barred.
The persons who may confirm statements in the questionnaires cannot be the same as the persons referred to in the first paragraph of Article 22e of this Act.

Article 25a

When the security clearance shall reveal a suspected alcohol, drug or any other addiction referred to in point 14 of the third paragraph of the preceding Article or a suspected disease or mental disturbance referred to in point 15 of the third paragraph of the preceding Article, the competent authority may check the suspicion by referring the person subjected to security clearance for a medical examination in a
health institution or to a private physician that has been authorised by the minister responsible for health to perform such examinations.
The checking referred to in the preceding paragraph shall be carried out on the basis of the decision on referral. If the person subjected to security clearance fails to attend the medical examination within the time period set by the health institution or private physician for unjustified reasons, the issue of the permission shall be refused.
The Slovene Intelligence and Security Agency and the Intelligence and Security Service of the Ministry of Defence shall not be bound to provide information referring to point 16 and 17 of the third paragraph of Article 25 of this Act if this might jeopardize the sources used for identifying or checking the information provided.
If the competent authority in carrying out security clearance collects personal and other data on the person subjected to security clearance from the already existing data collections, the authorities, organisations and other entities keeping data collections in accordance with the law are bound to provide the requested personal and other data free of charge on the basis of a written request or a request equal to a written request stating the adequate legal base for providing the data and the appropriate number or other designation of the request.

Article 25b

If a security restriction referred to in Article 27 of this Act is suspected with regard to a person having permission to access classified information, an intermediate vetting procedure shall be carried out.
The intermediate vetting procedure shall be carried out at the proposal of the director of an agency or organisation, in which the person is exercising a function or task and the provision of Article 22a of this Act shall be applied *mutatis mutandis.*

The National Security Authority may submit to the competent authority a proposal for intermediate vetting procedure if it suspects a security restriction referred to in Article 27 of this Act on the grounds of the monitoring referred to in the sixth indent of the third paragraph of Article 43b of this Act. He shall notify thereof the director of the agency or organisation, where the person for whom he proposes intermediate vetting procedure is employed.

Article 25c

Intermediate vetting procedure shall also apply to a person:

1. prior to the performance of tasks pertaining to the position requiring access to classified information, if more than 12 months have elapsed from the issue of permission for taking up the performance of tasks pertaining to that position;
2. prior to further performance of tasks pertaining to the position requiring access to classified information, if the person has not performed the tasks pertaining to the position at the agency referred to in the second paragraph of Article 1 of this Act for more than 12 months during the period of validity of the permission.
3. who obtained the permission for the purpose of implementing procurement contracts for organisations referred to in the third paragraph of Article 1 of this Act and if more than 12 months have elapsed from the completion of the procurement work within which the person had access to classified information to the need for further access to classified information.

The competent authority shall initiate an intermediate vetting procedure for the purpose of reconfirming the validity of the permission (hereinafter referred to as confirmation of the validity of permission) at the proposal of the director of an agency or organisation in which the person is executing the function or tasks or at the proposal of the National Security Authority if this results from international treaties or accepted international obligations by the Republic of Slovenia.

The procedure of confirming the validity of the permission is identical to the process of issuing permission to access classified information of a certain level of classification as laid down in this Act.

When the person does not agree with the initiation of intermediate vetting procedure referred to in the previous Article or does not agree with the introduction of a procedure confirming the validity of permission or does not fill in the appropriate security questionnaire, the permission shall be revoked.

The director of the agency or organisation shall render access to classified information for the person concerned impossible until the conclusion of the intermediate vetting procedure referred to in Article 25b of this Act and the conclusion of the procedure relating to the confirmation of the validity of permission. He shall notify thereof the National Security Authority.

Article 25d

During the validity period of the permission the permission holder is bound to inform the director of the agency or organisation on any change of data in the basic or special questionnaire.

The director of the agency or organisation or the person authorised for this purpose by the director in writing, is bound to carry out an interview with the person from the preceding paragraph regarding the changed data referred to in the preceding paragraph. If a security restriction referred to in Article 27 of this Act is suspected during the interview, the director

of the agency shall propose to the competent authority intermediate vetting procedure.

Article 26

When a person with a permission needs to access classified information even after the expiry of the permission's validity, the competent proposer referred to in Article 22f of this Act shall propose to the competent authority at least three months prior to the expiry of the validity of the permission to initiate a process for issuing a new permission.

When security restrictions for the issuing of permission are established by the competent authority during repeated or intermediate vetting procedure referred to in Article 25b or 25c of this Act, the competent authority shall revoke the previous permission if its validity has not yet expired during the procedure. The competent authority shall serve the decision on revocation on the person whose permission has been revoked and on the proposer of the procedure and notify thereof the National Security Authority and the current employer of the person subjected to security clearance.

Article 27

Security restrictions for which the issuing of permission to access classified information may be denied shall include:

- false statements of the person subjected to security clearance in the security clearance questionnaire or in the vetting procedure interview;
- an unerased final conviction of unconditional imprisonment in the duration of at least three months for offences prosecuted ex officio;
- a final disciplinary measure for a serious disciplinary infringement relating to the treatment and protection of classified information;
- alcohol, drug or other addiction that might have an impact on the refusal of issuing permission;
- membership or participation in organizations or groups which threaten vital interests of the Republic of Slovenia or the States being members of political, defence or security alliances, of which the Republic of Slovenia is also a member;

The competent authority may refuse the issuing of permission also in the following cases:

- final indictment for criminal offences prosecuted ex officio, with the exception of criminal offences where as the main sentence a fine or imprisonment up to three years is prescribed.
- non-final judgement of conviction for criminal offences prosecuted ex officio, with the exception of criminal offences where as the main sentence a fine or imprisonment up to three years is prescribed.
- unerased final convictions or several pronounced fines for offences laid down in this Act;
- other findings resulting from security clearance that raise reasonable doubts about the individual's trustworthiness, reliability and loyalty as to secure handling of classified information;
- other security restrictions defined by laws or international treaties.

Article 28

The competent authority shall keep the entire documentation elaborated relating to security

clearance.
Agencies referred to in the forth paragraph of this Article shall return the written consent to security clearance and the completed security questionnaires kept in a special part of the personnel file of the person to the competent authority that issued permission to the person no later than within three months after the entry into force of this Act.
Personal data of individuals laid down in this Act may only be processed for purposes of security clearance, keeping of records in accordance with this Act and performing other competencies in accordance with this Act.
The agency or organisation in which the person concerned is employed shall keep the permission and statement referred to in the second paragraph of Article 31a of this Act in the personnel records of that person.
Article 28a
When the person concerned does not fulfil the conditions required for the position because her/his permission to access classified information has been denied or revoked, the provisions of the law governing the public servants system shall apply.
Article 29
Agencies and organisations which, within the framework of their duties, handle classified information of the CONFIDENTIAL, SECRET or TOP SECRET levels shall keep records of permissions containing data referred to in point 1 of Article 43e of this Act.
Data about security clearance shall be stored for five years after the expiry of validity of permission or the refusal of issuing or intermediate vetting procedure. After that period they shall be destroyed.
The person shall, in accordance with the law governing personal data protection, have the right to view, copy and extract data relating to his security clearance, with the exception of data that would endanger the sources of security clearance.
Article 30
In exceptional cases, the person may be allowed single access to information classified one level higher than indicated in the person's permission. Such access is allowed only on the basis of written substantiation by his director about the reasons for such access and is limited only to classified information which needs to be accessed for the fulfilment of a particular task. If need arises for more permanent access to information of a higher level of classification, the person must obtain a corresponding permission.
The person may start performing tasks pertaining to the position requiring permission to access classified information of a higher level than the one that the person already holds without the corresponding permission, however, under the condition that the procedure for issuing the corresponding permission has already been initiated and that the body responsible for security clearance, or another body, if so stipulated by an international treaty or obligations arising from the membership of the Republic of Slovenia in international organisations, approves of it. Temporary permission to access classified information under the specified conditions may be granted for no more than six months.
CHAPTER IV
ACCESS TO AND PROTECTION OF CLASSIFIED INFORMATION
Article 31
Only persons who have permission and must use such information in order to fulfil their function or perform their tasks may have access to classified information. They shall only have access to the level of classification indicated in the permission.
No person shall be permitted to obtain classified information before it is needed, or more information than is indispensable for the exercise of his or her function or the performance of his or her tasks.
Article 31a

Every person who fulfils his or her function or works at the agency shall have access to information classified at the RESTRICTED level.
The persons referred to in the preceding paragraph shall each time they take up a function or duty sign a statement to the effect that they are acquainted with this Act and other regulations governing the protection of classified information they will treat within the framework of executing their functions or duties, and that they undertake to handle classified information in accordance with these regulations. The directors of the agencies shall provide appropriate training in the field of treatment and protection of classified information for the persons concerned before they sign the statement.

Article 32

(deleted)

Article 33

A person who becomes acquainted with classified information in the course of performing his duties shall use such information for no purposes other than the exercise of his function or the performance of his tasks.
The director of the agency may, at the request of competent authorities, relieve a person of the obligation to keep secret information that has been defined as classified in this agency, however, solely for the purpose and to the extent specified in the request of the competent authority.
The director of the agency may, at the request of competent authorities, be relieved of the obligation to keep information secret by the agency that appointed him under the conditions of the preceding paragraph.

Article 34

Classified information may be transmitted to other agencies which must abide by this Act, or to persons in such agencies, only on the basis of written permission from the director of the agency that designated the information as classified, or where so provided by law.

Article 35

Classified information may only be transmitted to an organisation referred to in the third paragraph of Article 1 of this Act that is in possession of a security permission (FSC) in order to fulfil the conditions for safe treatment of classified information (hereinafter referred to as security permission (FSC)).
A security permission for procurement contracts (FSC) in the field of defence shall be issued by the ministry responsible for defence, for procurement contracts concerning the work of the Slovene Intelligence and Security Agency by the Slovene Intelligence and Security Agency, whereas in all other cases by the Police. Notification of the issuing of security permission (PSC) shall be forwarded to the National Security Authority.
The security permission (FSC) shall be issued for a period of five years or for a period laid down in the procurement contract, however, for not more than five years.

Article 35a

The procedure for issuing a security permission (FSC) referred to in the preceding Article of this Act shall be initiated on the basis of a written proposal of the:

- director of an agency referred to in the second paragraph of Article 1 of this Act for organisations implementing procurement contracts for the agency concerned;
- head of the ministry responsible for economy for organisations that need the security permission (FSC) for the purpose of taking part in public procurements or implementing procurement contracts of a foreign country or international organisation.

The proposer referred to in point 2 of the preceding paragraph may prior to submitting the proposal obtain an opinion of the ministry responsible for the field of work of the organisation concerned.
The proposer shall annex to the proposal for the initiation of a vetting procedure the following documents proving that the proposed organisation fulfils the criteria for the recognition of competencies for safe treatment of classified information, i.e.:

- that it is registered with the competent court or another authority - extract from a judicial or other relevant record;
- that the organisation is not subject to a criminal proceeding for a suspected criminal offence concerning bribery or that the organisation has not been finally convicted for such an offence – certificate of the ministry responsible for judicial affairs that the organisation has not been entered into conviction records;
- that no compulsory composition proceeding, bankruptcy proceeding or liquidation proceeding or another proceeding has been opened or initiated against the organisation the result or purpose of which is the termination of operations of the organisation - extract from judicial records or records considered equivalent.
- that the organisation settled taxes and contributions in accordance with the legislation of the State where the organisation has its registered office or that an organisation with its registered office abroad settled in the Republic of Slovenia the duties it was obliged to settle - a certificate issued by a tax authority or another competent authority of the state where the organisation has its registered office;
- that no penalty has been imposed on the organisation for an act relating to its business and that the consequences of the judgement have already been erased respectively – a certificate of the ministry responsible for judicial affairs that the organisation has not been entered into conviction records;
- a proof of the ownership structure of the organisation - extract from judicial or other relevant records;

The competent authority referred to in the second paragraph of the preceding Article may in the process of issuing a security permission (FSC) collect data from the organisation to which the data refer or from other bodies, organisations or persons being in any way acquainted with these data, for the purpose of verifying data referred to in the preceding paragraph and complying with the conditions referred to in the first paragraph of Article 35b of this Act.
Article 35b
The competent authority shall issue a security permission (FSC) to an organisation if:

- the organisation meets physical, organisational and technical requirements for the protection of classified information in accordance with this Act and the regulations based thereon;
- persons who, in the course of their duties in the organisation, have access to classified information shall undergo security clearance and have permission to access classified information;
- the organisation shall ensure that only persons who must be able to view such information in the course of their duties for the purpose of executing a procurement contract for an agency may have access to classified information;

- the competent authority appoints a person responsible for the supervision and guidance of security measures relating to the execution of procurement contracts, training of persons having access to classified information, reporting to the competent authority on the circumstances that influence the issue of a security permission (PSC) and the implementation of other prescribed measures for safe treatment of classified information.

A person who, in the course of her/his duties in the organisation, has access to classified information at the RESTRICTED level, shall in addition to the conditions referred to in the second paragraph of Article 31a of this Act meet the following conditions:

  - he is not subject to a final conviction for premeditated criminal offences prosecuted ex officio and was not convicted to a final sentence of unconditional imprisonment in the duration of more than 6 months;
  - he is not subject to a criminal proceeding for a criminal offence referred to in the preceding indent.

The conditions referred to in the preceding paragraph shall be verified by the agency responsible for the issue of a security permission (FSC) to an organisation in which the person will access to classified information.
The manner and procedure of verifying whether the conditions for the issue of a security permission (FSC) are being met shall be specified by the Government.
Article 35c
The competent authority may refuse to issue a security permission (FSC) to an organisation if the organisation does not meet the conditions for the recognition of competencies referred to in the third paragraph of Article 35a of this Act.
The competent authority shall not issue a security permission (FSC) if the organisation does not meet the conditions referred to in the first paragraph of the preceding Article.
Article 35d
If after the issue of a security permission (FSC) circumstances arise that indicate that an organisation does not meet several conditions for the recognition of capabilities referred to in the third paragraph of Article 35a or the conditions referred to in the first paragraph of Article 35b of this Act, the competent authority referred to in the second paragraph of Article 35 of this Act shall carry out an intermediate vetting procedure.
Intermediate vetting procedure shall be carried out at the proposal of the competent proposer referred to in Article 35a or 43b of this Act.
The National Security Authority may submit a proposal for intermediate vetting procedure if circumstances are established during the supervision referred to in the sixth indent of the third paragraph of Article 43b of this Act indicating that the
organisation no longer meets the conditions for the issue of a security permission (FSC).
The intermediate vetting procedure shall be identical to the vetting procedure for the issue of a security permission (FSC). If during the intermediate vetting procedure the competent authority establishes that the organisation no longer meets the conditions laid down in this Act for issuing a security permission (FSC), the security permission (FSC) shall be revoked.
Notification of the revocation of security permission (FSC) shall also be forwarded to the National Security Authority.
An administrative challenge to the refusal of issuing or revocation of the security permission (FSC) shall be permitted.

Article 36
Entitled users that have received classified information from an agency may not transmit that information to other users without the consent of the agency, except in cases defined by regulations.
Article 37
The authorised person of an agency and organisation shall establish a record and supervision of the distribution of classified information outside the agency. The record shall be kept up-to-date and show clearly when and to whom the classified information was transmitted.
Article 38
Each organisation and agency shall, in accordance with this Act and the regulations based thereon, establish a system of procedures and measures for the protection of classified information that meets the requirements of the specific levels of classification and renders the disclosure of classified information to unauthorised persons impossible.
The procedures and measures from the preceding paragraph shall include:

- general security measures;
- protection of persons with access to classified information;
- protection of premises;
- protection of documents and media containing classified information;
- protection of communications over which classified information is transmitted;
- method of marking levels of classification;
- protection of equipment for handling classified information;
- method of acquainting users with the measures and procedures of the protection of classified information;
- controlling and recording of access to classified information;
- controlling and recording of the dispatch and distribution of classified information.

The director of an agency and organisation shall once a year provide additional training of persons executing tasks relating to treatment and protection of information classified CONFIDENTIAL and information of a higher level.
The director of an agency and organisation shall issue an act providing the implementation of measures and procedures referred to in the second paragraph of this Article.
The act referred to in the preceding paragraph shall be prescribed for courts of general competence and for specialised courts by the President of the Supreme Court of the Republic of Slovenia, whereas for the State Prosecutor's office the State Prosecutor General of the Republic of Slovenia.
The programme and manner of training persons referred to in the third paragraph of this Article shall be prescribed in detail by the Government.
Article 39
Agencies shall keep classified information in a manner that ensures that access to such information is permitted only to those persons who have permission to access and need such information for the performance of their tasks or exercise of their functions.
Classified information may only be sent outside the premises of the agency provided that the security measures and procedures ensuring that the information will be received by the person with permission to access and right to use it are respected.
Security procedures and measures for the sending of classified information outside the

premises of the agency shall be prescribed in accordance with the level of classification of such information.
Agencies may not transmit or send classified information using unprotected means of communication.
Detailed physical, organisational and technical measures and procedures for the protection of classified information shall be prescribed by the Government.
Article 40
Officials, employees and other personnel in agencies, who establish that a loss or unauthorised disclosure of classified information has occurred, shall immediately notify the authorised person thereof.
A recipient of classified information from Articles 34 and 35 of this Act respectively, who establishes that classified information has been lost or transmitted or delivered to an unauthorised person, shall immediately notify the authorised person of the agency that sent or reported the classified information to him.
The authorised person shall immediately take all necessary steps to identify the circumstances that occasioned the loss of classified information or its disclosure to an unauthorised person, remove any harmful effects, and prevent further losses and unauthorised disclosures of such information.
CHAPTER V
SUPERVISION
Article 41
Internal control of the implementation of this Act and of the regulations based thereon shall be the responsibility of the directors of agencies and organisations.
In agencies and organisations that treat classified information of the CONFIDENTIAL level or information of a higher level, a special post within the job classification system shall be provided for internal supervision and other professional duties in connection with the determination and protection of classified information, or else an existing organisational unit of the agency or organisation shall be charged with the execution of such duties.
Article 42
All agencies shall, through internal supervision, ensure the regular monitoring and assessment of individual activities and of the activity of the agency as a whole in respect of the implementation of this Act and of the regulations and measures based thereon.
The Government shall prescribe in detail the method and content of internal supervision of the implementation of this Act and of the regulations based thereon.
Article 42a
Inspections of the implementation of the provisions of this Act and of the regulations based thereon and on international treaties concluded between a foreign country or international organisation and the Republic of Slovenia, unless otherwise provided in an international treaty, shall be carried out by the Inspectorate of the Republic of Slovenia for the Interior, with the exception of the field of defence, where the inspections shall be carried out by the Inspectorate of the Republic of Slovenia for Defence.
Article 42b
Unless otherwise specified in this Act, the provisions of the law regulating inspections and the law regulating the general administrative procedure shall apply to inspectors and the carrying out of supervisory inspections.
An inspector shall have permission to access classified information of the TOP SECRET level.
Article 42c
The inspector shall carry out inspections in agencies and organisations referred to in Article 1 of this Act by verifying the system of classification, marking, protection and access to

classified information.
In exercising his powers the inspector shall not request access to the content of a piece of classified information, with the exception of internal legal acts of the agency or organisation regulating the manner of implementing this Act.
In agencies and organisations the inspections shall be carried out in the presence of the director or a person authorized by the director.
Article 42d.
In addition to his general powers laid down in the law regulating inspections, the inspector shall have the following rights and duties:

- specify the deadline for the elimination of shortcomings or irregularities in the implementation of classified information regulations;
- request a competent person for comments in writing concerning the content of classified information;
- carry out procedures in accordance with the law regulating offences;
- file an information to the competent authority on offences prosecuted ex officio;
- propose the opening of a disciplinary procedure against the offender of regulations concerning classified information;
- prohibit access to and transmission of classified information in the event the security of classified information is jeopardized, because the measures for its protection have not been fulfilled in their entirety;
- order urgent measures for the protection of classified information and if required also the transmission of information to an area or an agency determined by the National Security Authority.

A complaint may be lodged against the decision of an inspector at the ministry responsible for the interior and the ministry responsible for defence respectively within fifteen days of its delivery. An appeal against the decision shall not suspend its enforcement.
The responsible ministry shall decide on the complaint within 30 days of its delivery.
The competent inspectorate shall report annually to the National Security Authority on the findings of inspections regarding classified information. When a competent inspecting authority carries out inspections following a request by the National Security Authority (seventh indent of third paragraph of Article 43b), it shall submit to the National Security Authority a copy of the minutes relating to the carried out inspection.
Article 42e
The Government shall prescribe in detail the method of carrying out inspections relating to classified information and the content of a special part of a proficiency examination for inspectors.
Article 43
The implementation of this Act and of the regulations based thereon and international treaties concluded by the Republic of Slovenia shall be monitored and coordinated by the National Security Authority, unless otherwise provided in an international treaty.
The tasks of the National Security Authority relating to the protection of classified information shall be performed by the Government Office of the Republic of Slovenia for the Protection of Classified Information.
Article 43a
The National Security Authority shall monitor and coordinate the situation relating to the treatment and protection of classified information, propose measures to improve the

protection of classified information, ensure the development and implementation of physical, organisational and technical standards of classified information protection in agencies and organisations, coordinate the activity of agencies responsible for security clearance, draw up proposals for regulations relating to classified information for the Government, give opinion as to the compliance with this Act of general acts of agencies and organisations in the field of treatment and protection of classified information and shall perform other tasks set forth by this Act and the regulations based thereon.

Article 43b

The National Security Authority shall attend to the implementation of international treaties and the accepted international obligations signed or accepted by the Republic of Slovenia with regard to the treatment and protection of classified information and cooperate in this field with the corresponding agencies of foreign countries and international organisations, unless otherwise specified by an international treaty.

The National Security Authority shall coordinate activities providing the security of national classified information abroad and foreign classified information in the territory of the Republic of Slovenia.

With regard to the implementation of international treaties and accepted international obligations the National Security Authority shall perform the following tasks:

- issue and revoke permissions to access foreign classified information to natural persons;
- issue and revoke security permission (PSC)s to access foreign classified information to organisations;
- issue and revoke security permission (PSC)s for the systems and devices for transmission, storage and processing of foreign classified information in accordance with the adopted international treaties;
- certify that an individual agency or organisation fulfils the prescribed conditions for handling classified information set out by foreign countries and international organisations;
- issue instructions for handling classified information of a foreign country or international organisation;
- monitor the implementation of physical, organisational and technical measures for the protection of classified information of a foreign country or international organisation and in accordance with the findings from the monitoring issue mandatory directives for corrective measures to be implemented immediately by the agencies in order to eliminate the identified shortcomings;
- require from the competent inspectorate to carry out inspections in a certain agency or organisation;
- exchange information with the national security authorities of foreign countries and with international organisations;

Before issuing the permission referred to in the first and second indent of the preceding paragraph it may in case of receiving a notification of a foreign security authority about a security restriction demand of the body responsible for security clearance to carry out intermediate vetting procedure of a person or organisation.

Article 43c

The National Security Authority shall issue a permission referred to in the fist indent of the

third paragraph of the preceding Article at the proposal of the proposers referred to in Article 22.f of this Act if the person is in possession of a valid permission referred to in Article 22 of this Act and exercises functions or tasks on a position for which permission to access foreign classified information has been required. The permission shall be issued for a period of validity during which the person needs access to foreign classified information, however, it shall not exceed the period of validity referred to in Article 22 of this Act.
If a person who has been issued permission to access foreign classified information no longer performs tasks for which permission to access foreign classified information is required, the director of an agency or organisation shall immediately notify the National Security Authority thereof.
The National Security Authority shall revoke the permission for access to foreign classified information after the conditions for its issue referred to in the first paragraph of this Article no longer apply.
Article 43d
The National Security Authority shall issue the permission referred to in the second indent of the third paragraph of Article 43.b of this Act at the proposal of the proposer referred to in Article 35.a of this Act if the organisation meets the following conditions:

- it is in possession of a valid security permission (PSC) referred to in Article 35 of this Act;
- the persons who will have access to classified information in the organisation are in possession of a valid permission referred to in the first indent of the third paragraph of Article 43.b of this Act.

Before issuing a security permission (PSC) for access to foreign classified information to an organisation, the National Security Authority may if this arises from an international treaty ask the organisation for additional documentation or perform an additional review of the fulfilment of conditions required for the protection of classified information.
The security permission (PSC) for access to foreign classified information shall be issued to the organisation for the period of validity of a security permission (PSC) referred to in Article 35 of this Act.
The responsible person of an organisation shall notify the National Security Authority on the change of conditions referred to in the first paragraph of this Article.
The National Security Authority shall revoke the permission for access to foreign classified information if the organisation no longer meets the conditions referred to in the first paragraph of this Article.
Article 43e
For the purpose of implementing powers and tasks pursuant to this Act, other laws and binding international treaties the National Security Authority shall keep and process the following records:
1. records of permissions issued on the basis of Article 22 of this Act containing the following data:

- name;
- date and place of birth;
- agency in which the person concerned is employed;

- agency that issued the permission;
- level of classification of information to be accessed by the person concerned;
- number and date of issue and date of validity of the permission to access classified information;
- date and reason of intermediate vetting procedure and the authority that revoked the permission;
- date and reason of refusal of issue of the permission and the authority that refused to issue the permission;
- data of issue of the decision referred to in Article 25.c of this Act and the authority that issued the decision;

2. the records of permissions to access classified information issued to natural persons referred to in the first indent of the third paragraph of Article 43.b of this Act containing the following data:

- name;
- date and place of birth;
- agency in which the person concerned is employed;
- level of classification of information to be accessed by the person concerned;
- number and date of issue and the date of validity of the permission;
- number and date of permission issued to access foreign classified information and the date of its validity;

3. records of security permission (PSC)s referred to in Article 35 of this Act containing the following data:

- name and address of the organisation;
- agency that issued the security permission (PSC);
- number and date of issue and date of validity of the security permission (PSC);
- date and reason of revocation of the security permission (PSC) and the authority that revoked the permission;
- date and reason of refusal of the issue of security permission (PSC) and the authority that refused to issue the permission;
- name, date and place of birth and the position of the person referred to in point 4 of the first paragraph of Article 35.b of this Act;
- number of permission and level of classification of information to be accessed by the person referred to in the preceding indent;

4. records of security permissions (PSC)s referred to in the second indent of the third paragraph of Article 43.b of this Act containing the following data:

- name and address of the organisation;
- agency that issued the security permission (FSC);

- date and reason of revocation of the security permission (FSC) of an organisation and authority that revoked the permission to access foreign information to the organisation;
- date and reason of refusing the issue of the security permission (FSC) to an organisation and authority that refused to issue the permission to access foreign information to the organisation;
- name, date and place of birth and the position of the person referred to in point 4 of the first paragraph of Article 35.b of this Act;
- number of permission and level of classification of information to be accessed by the person referred to in the preceding indent;

5. records of temporary access to classified information pursuant to the second paragraph of Article 30 of this Act, containing the following data:

- name;
- date and place of birth;
- agency in which the person concerned is employed;
- level of classification of information to be accessed by the person concerned;
- number and date of validity of permission;
- level of classification of information to be accessed temporarily by the person concerned;
- period (duration) of temporary access.

The records referred to in this Article shall be kept permanently.

CHAPTER VI

PENALTY PROVISIONS

Article 44

A legal person or a sole proprietor shall be fined between SIT 1,000,000 and 3,000,000:

- if he allows a person who has not signed a statement (second paragraph of Article 3, second paragraph of Article 31.a) to access classified information;
- if he transfers authority for the classification of information to a third person (third paragraph of Article 10);
- if in determining the level of classification, he does not assess the possible adverse effects of the disclosure of information to an unauthorised person on the security of the country or on its political or economic interests (Article 11);
- if he acts in contravention of Article 12 of this Act;
- if he acts in contravention of Article 14 of this Act;
- if he changes the level of classification of a document in contravention of Article 16 of this Act;
- if he does not give a classified document the prescribed markings (Article 17);
- if the declassification of information or document is not specified in accordance with Article 18 of this Act;
- if he changes the manner specified for declassification without any justified reason in contravention of Article 18 of this Act;

- if he does not notify the National Security Authority of the issue or revocation of a permission to access classified information (Article 22, second paragraph of Article 26).
- if he does not propose intermediate clearance of a person (second and third paragraph of Article 25.b, second paragraph of Article 25.c);
- if he does not render access to classified information temporarily impossible to a person for whom the intermediate clearance procedure has not been completed yet (fourth paragraph of Article 25c);
- if he does not keep the permission and statement In the personnel file (Article 28);
- if he does not keep a record of permissions to access classified information (Article 29);
- if he allows access to classified information in contravention of the first paragraph of Article 31 of this Act;
- if he relieves a person of the obligation to keep information secret in contravention of Article 33;
- if he allows the transmission of classified information to an organisation in contravention of Article 35 of this Act;
- if he does not notify the National Security Authority of the issue of a permission to an organisation (second paragraph of Article 35);
- if he does not propose intermediate clearance of an organisation (first and second paragraph of Article 35.d);
- if he allows persons to access classified information in contravention of point 3 of the first paragraph of Article 35.b of this Act;
- if he does not designate a person referred to in point 4 of the first paragraph of Article 35.b of this Act;
- if he acts in contravention of Article 36 of this Act;
- if he acts in contravention of Article 37 of this Act;
- if he does not issue an act referred to in Article 38 of this Act;
- if he does not provide training of persons in the field of classified information treatment in accordance with the first paragraph of Article 25, second paragraph of Article 31a and third paragraph of Article 38 of this Act;
- if he acts in contravention of the first, second and forth paragraph of Article 39 of this Act;
- if he acts in contravention of the second and third paragraph of Article 40 of this Act;
- if he does not organise internal control of classified information treatment (Article 41);
- if he acts in contravention of the second paragraph of Article 43c of this Act;
- if he acts in contravention of the forth paragraph of Article 43d of this Act;

A fine between SIT 200,000 and 500,000 shall be imposed also on a responsible person of a state authority, an authority of a self-governing community, a legal person or a sole proprietor committing a breach referred to in the preceding paragraph.

Article 44a

A legal person or a sole proprietor shall be fined between SIT 500,000 and 1,000,000:

- if he acts in contravention of the first and second paragraph of Article 15 of this Act;
- if he, in determining the level of classification, exceeds the competencies within the authority for the classification of information;

- if he does not act in accordance with the third paragraph of Article 18 of this Act;
- if he refrains from an obligation referred to in the second paragraph of Article 25d of this Act;
- if he does not propose at least three months prior to the expiry of the permission's validity the initiation of a process for issuing a new permission to a person who will need this permission even after the expiry of the permission's validity (first paragraph of Article 26);
- if he acts in contravention of the second paragraph of Article 28 of this Act;
- if he allows a person access to classified information in contravention of Article 30 of this Act;
- if he allows a person access to classified information of a higher level than indicated in the permission or allows the person to obtain classified information before it is needed and to a larger scope than needed for the exercise of tasks and performance of functions (second paragraph of Article 31).

A fine between SIT 100,000 and 300,000 shall be imposed also on a responsible person of a state authority, an authority of a self-governing community, a legal person or a sole proprietor committing a breach referred to in the preceding paragraph.
Article 45

An individual shall be fined between SIT 100,000 and 200,000:

- if he acts in contravention of Article 8 of this Act;
- if he assigns a classification level to a piece of information or a document without being authorised to do so (Article 10);
- if he refrains from an obligation referred to in the first paragraph of Article 25.d of this Act;
- if he accesses classified information in contravention of the first paragraph of Article 31 of this Act;
- if he uses classified information for purposes other than the exercise of certain working tasks or performance of functions (Article 33);
- if he transmits classified information in contravention of Article 34 of this Act;
- if he transmits classified information to an organisation that is not in possession of a security permission (PSC) (first paragraph of Article 35);
- if he allows a person to access classified information in contravention of point 3 of the first paragraph of Article 35.b of this Act;
- if he does not carry out procedures and measures relating to the treatment of classified information as prescribed in this Act and the regulations based thereon;
- if he does not notify an authorised person of the loss or unauthorised disclosure of classified information or provision of classified information to an unauthorised person (Article 40).

Classified Information Act - ZTP (Uradni list RS, no. 87/01) contains the following transitional and final provisions:
CHAPTER VII
TRANSITIONAL AND FINAL PROVISIONS
Article 46
The Government of the Republic of Slovenia shall, no later than six months after the entry

into force of this Act, issue the regulations referred to in the fourth paragraph of Article 17, the seventh paragraph of Article 23, the fourth paragraph of Article 35, the fifth paragraph of Article 39 and the second paragraph of Article 42 of this Act.
The minister responsible for defence, in agreement with the minister responsible for the interior, shall issue the regulation referred to in the sixth paragraph of Article 10 of this Act no later than six months after the entry into force of this Act.
The Government of the Republic of Slovenia shall found the Office referred to in Article 43 of this Act no later than six months after the entry into force of this Act.
Article 47
- in compliance with the amendments to the Classified Information Act (ZTP-A)

No later than one year after the entry into force of this Act, agencies shall pass regulations and prepare organisationally for the entry into force thereof, or shall bring the existing acts and the organisation of their activities in line with the provisions of this Act.
Agencies shall ensure that all employees and officials who in the course of their duties or functions must have access to classified information are issued permission to access such information no later than three years after the entry into force of this Act. The employees and officials who will not be granted the permission will not be allowed to access classified information.
Article 48
- in compliance with the amendments to the Classified Information Act (ZTP-A)

Classified information for which the level of classification was determined according to the previous regulations and are kept in the collection of unresolved cases shall be reclassified in accordance with this Act by no later than 31 December 2004.
Irrespective of the deadline set in the preceding paragraph the level of classification need not be changed for the classified information in electronic or other (not hardcopy) form or for those kept in the current or permanent collections of documentary material. This classified information shall be reclassified when reapplied or forwarded to other users.
During the transitional period, classified information referred to in the first paragraph of this Article shall be treated as follows:

- information designated as DRŽAVNA TAJNOST or DRŽAVNA SKRIVNOST (STATE SECRET) shall be treated as STROGO TAJNO (TOP SECRET);
- information designated as URADNA TAJNOST, URADNA SKRIVNOST or VOJASKA SKRIVNOST - STROGO ZAUPNO (OFFICIAL SECRET or MILITARY SECRET - HIGHLY CONFIDENTIAL) shall be treated as TAJNO (SECRET)
- information designated as URADNA TAJNOST, URADNA SKRIVNOST or VOJASKA SKRIVNOST - ZAUPNO (OFFICIAL SECRET or MILITARY SECRET -CONFIDENTIAL) shall be treated as ZAUPNO (CONFIDENTIAL), and
- information designated as URADNA TAJNOST, URADNA SKRIVNOST or VOJASKA SKRIVNOST - INTERNO (OFFICIAL SECRET or MILITARY SECRET -INTERNAL) shall be treated as INTERNO (RESTRICTED).

Article 49
This Act shall enter into force on the fifteenth day following its publication in the Uradni list Republike Slovenije.
The Act Amending the Classified Information Act ZTP-A (Uradni list RS, no. 101/03) shall contain the following transitional and final provisions:

TRANSITIONAL AND FINAL PROVISIONS

Article 16

Until the establishment of the National Security Authority, its duties shall be performed by the Office of the Republic of Slovenia for the Protection of Classified Information.

Article 17

The permissions to access classified information or certificates to access classified information of foreign countries and international organisations issued before entry into force of this Act shall remain valid.

Article 18

This Act shall enter into force on the day following its publication in the Uradni list Republike Slovenije.

The Act Amending the Classified Information Act ZTP-B (Uradni list RS, no. 28/06) shall contain the following transitional and final provisions:

TRANSITIONAL AND FINAL PROVISIONS

Article 41

The Government of the Republic of Slovenia shall no later than three months after the entry into force of this Act harmonise the regulations referred to in the sixth paragraph of Article 23 and the forth paragraph of Article 35.b and shall issue a regulation referred to in Article 38 of this Act.

The Government of the Republic of Slovenia shall no later than six months after the entry into force of this Act issue a regulation referred to in Article 42.e of this Act.

Agencies and organisations shall issue a regulation referred to in the forth paragraph of Article 38 of this Act no later than one year after the entry into force of this Act.

Article 42

The Government of the Republic of Slovenia shall designate the commission referred to in Article 21a of this Act within one month after the entry into force of this Act.

Article 43

Permissions to access classified information, certificates to access classified information to natural persons and security certificates to legal persons issued in accordance with the Classified Information Act (Uradni list RS, no. 135/03 - consolidated text) shall remain valid.

Security certificates to organisations issued pursuant to the Decree defining the necessary conditions for the transmission of classified information to another organisation (Uradni list RS, 106/02) shall remain valid until the completion of the procurement contract for which it was issued.

Article 44

The provisions of Article 19, 29 und 30 of this Act begin to apply three months after the entry into force of this Act.

Article 45

This Act shall enter into force on the fifteenth day following its publication in the Uradni list Republike Slovenije.

(Published on 16 May 2006)